



BELGRADE
METROPOLITAN
UNIVERSITY



www.bisec.metropolitan.ac.rs

PROCEEDINGS

The Eighth International Conference on Business Information Security



Belgrade Metropolitan University

Belgrade, 15th October 2016.

www.metropolitan.ac.rs

Publisher:

Belgrade Metropolitan University
Tadeuša Koščuška 63, Belgrade, Serbia
<http://www.metropolitan.ac.rs>

For Publisher:

Prof. dr Dragan Domazet

Editor:

Doc. dr Igor Franc

Tanja Ćirić

Chair of Programme Committee:

Doc. dr Igor Franc

Chair of Organizing Committee:

Tanja Ćirić

Printing:

Kruševac: Sigraf

Design:

Mladen Radić
Katarina Gobeljić
Petar Cvetković

Circulation

100

CONTENT

ZLATOGOR MINCEV, GEORGI DUKOV	13
“Emerging Hybrid Threats Modelling & Exploration in the New Mixed Cyber-Physical Reality”	
LYUDMILA ZHAROVA, VITO LEGGIO, ALEKSANDAR MIHAJLOVIĆ, SHAWN CAMPBELL, RADOMIR A. MIHAJLOVIĆ	18
“Road Vehicle Embedded IoT Security”	
IGOR VUJAČIĆ, IVANA OGNJANOVIĆ, RAMO ŠENDELJ	27
“SM@RT Home Personal Security and Digital Forensic Issues”	
NEMANJA MAČEK, IGOR FRANC, MITKO BOGDANOSKI, ALEKSANDAR MIRKOVIĆ	33
“Multimodal Biometric Authentication in IoT: Single Camera Case Study”	
ISAK MRKAIĆ	38
“Android Forensic Using Some Open Source Tools”	
IGOR FRANC, NEMANJA MAČEK, MITKO BOGDANOSKI, ALEKSANDAR MIRKOVIĆ, DRAGAN ĐOKIĆ	44
“Detecting Malicious Anomalies in IoT: Ensemble Learners and Incomplete Datasets”	
MIROSLAV D. STEVANOVIĆ, DRAGAN Ž. ĐURĐEVIĆ	50
“Internet of Things Challenges for Organized Societies”	
DUŠAN BOGIĆEVIĆ, IVAN TOT, RAMO ŠENDELJ	55
“IoT Security Optimization”	
ANDREJA SAMČOVIĆ	59
“Security Issues in Internet of Things Environment”	
KOMLEN LALOVIĆ, JASMINA NIKOLIĆ, TOT IVAN, ŽANA LALOVIĆ	66
“Software Algorithm of Device for Biometric Identification of Maternity – Parenthood”	

JOVANA ĐUROVIĆ, BOBAN MIHAILOV, IVAN TOT, IVANA OGNJANOVIĆ	72
“CryptoSMS Android Application”	
VIKTOR KANIŽAI	77
“Preventive Model of Data Leak Protection in Critical Infrastructure from Internal Risk Factors”	
NEMANJA MAČEK, PERICA ŠTRBAC, DUŠAN ČOKO, IGOR FRANC, MITKO BOGDANOSKI	82
“Android Forensic and Anti-Forensic Techniques – A Survey”	
DRAGAN ĐOKIĆ, MIHAILO JOVANOVIĆ, SNEŽANA POPOVIĆ, RAMO ŠENDELJ, NEMANJA MAČEK	88
“Raising Awareness of the Need for Safety of Information in Big Business Systems”	
IGOR OGNJANOVIĆ, RAMO ŠENDELJ, IVANA OGNJANOVIĆ	94
“Impact Analysis of Cyber Attacks on Cloud Systems”	
VELIBOR ŠABAN, IVANA OGNJANOVIĆ, RAMO ŠENDELJ	99
“Comparative Analysis of Some Cryptographic Systems”	
NENAD BIGA, MILOŠ JOVANOVIĆ, MARIJA PERKOVIĆ, DRAGAN MITIĆ	105
“Modern Business Environment: Information Technology as a Shield against Cyber Security Threats”	

Organizer



Co-Organizer



Partners



Република Србија
МИНИСТАРСТВО ПРОСВЕТЕ,
НАУКЕ И ТЕХНОЛОШКОГ РАЗВОЈА



Members of the Programme Committee:

Prof. Dr. Zlatogor Minchev, associate professor, *Bulgarian Academy of Sciences, Republic of Bulgaria*

Prof. Dr. Mitko Bogdanoski, associate professor, *Military Academy "General Mihailo Apostolski" Skopje, Republic of Macedonia*

Ramo Šendelj, PhD associate professor, *University Donja Gorica, Montenegro*

Prof. Dr. Marko Beko, associate professor, *Universidade Lusófona, Lisbon, Portugal*

Dr. Urska Cvek, associate professor, *Louisiana State University Shreveport, One University Place, Shreveport, LA*

Dr. Marjan Trutschl, associate professor, *Louisiana State University Shreveport, One University Place, Shreveport, LA*

Prof. Dr. Kavitha Chandra, *University of Massachusetts Lowell, Lowell, USA*

Dr. Miroslava Raspopović, associate professor, *Dean of Faculty of Information Technology, Belgrade Metropolitan University, Serbia*

Dr. Igor Franc, *Belgrade Metropolitan University, Serbia*

Prof. Dr. Ljubomir Lazić, associate professor, *Belgrade Metropolitan University, Serbia*

Dr. Dragan Đurđević, *Academy of National Security, Serbia*

Dr. Aca Aleksić, *Executive Director of Information Technology Services Dunav RE, Serbia*

Prof. Dr. Slobodan Jovanović, *Belgrade Metropolitan University, Serbia*

Dr. Ivana Ognjanović, assistant professor, *University Donja Gorica, Montenegro*

Dr. Nemanja Maček, SECIT security consulting, *Advanced Security Systems PhD assistant, The School of Electrical and Computer Engineering of Applied Studies Belgrade*

Language

The official language of the Bisec 2016 Conference is English. English will be used for all printed materials, presentations and discussion.

EMERGING HYBRID THREATS MODELLING & EXPLORATION IN THE NEW MIXED CYBER-PHYSICAL REALITY

ZLATOGOR MINCHEV

Institute of ICT, Joint Training Simulation & Analysis Center, Bulgarian Academy of Sciences, zlatogor@bas.bg

GEORGI DUKOV

Institute of ICT, Joint Training Simulation & Analysis Center, Bulgarian Academy of Sciences, gdukov@bas.bg

Abstract: The security environment nowadays is producing quite a lot of uncertainties and threats as a result of emerging cyber-physical hybrid clashes phenomena. Adequate exploration of this has to be taken into consideration jointly with future technological progress, combining both social & technological assets. A successful approach for handling the problem is demonstrated in the paper, implementing expert beliefs into an aggregated dynamic system model, together with further exploration, based on system analysis, validation & verification. The obtained results are showing promising holistic solution, giving opportunities for better understanding and countering future hybrid threats in the new mixed cyber-physical reality.

Keywords: Hybrid Threats, System Modelling, Validation & Verification, Cyber-Physical Reality

1. INTRODUCTION

The 21st century digital revolution is nowadays producing numerous opportunities and threats, resulting from human-machine multimodal interaction in the new cyber-physical mixed reality. This practically generates a different environment of living, working, communicating and finally - 'digitizing' the lifestyle as a whole [1].

The development of web technologies, from the other hand, has successfully shifted the human factor behaviour from a passive user of Web 1.0 to an active player in Web 3.0. This active behaviour, jointly with Artificial Intelligence (AI) advancing and Internet of Things (IoT) concept integration boom, could bring, in the near future, a different social evolution dynamics. An assignment of more active role to autonomous Web 4.0 technologies with multiple output soft- and hardware effectors, instead of people only, have to be expected [2].

Meeting these progressive results in a suitable manner is quite a challenging task because it moves notions like: 'privacy', 'reliability', 'culture' and 'ethics' on a new cyber-physical level of understanding.

Concerning the human factor transformation in the upcoming digital reality, it will inevitably emerge novel, hybrid threats, posted in the present and future social resilience context [3], [4].

The paper initially outlines digital threats hybrid evolution perspectives in the new cyber-physical world, forming the modern mixed environment. A further practical approach for threats proactive exploration, using system analysis with results validation & verification, is also given for achieving a comprehensive outlook to the problem.

2. EMERGING THREATS EVOLUTION

The new security landscape, though difficult to be uniquely described, requires proper futuristic understanding. Adequately facing the new threats hybrid evolution from human - technologies clash is a rather challenging task.

A graphical generalization in this context for year 2020, originating from an extended recent survey [5] among more than 400 representatives from academia, universities, defence community and industry is given in Figure 1.



Figure 1: Expected digital society priorities, outlooks, challenges and attack vectors up to year 2020

Several major conclusions could be drawn from the presented results for both human and technologies evolution perspectives: (i) *Environment and Quality of Life* – 52%, *Business & Production* – 25%, *Education & Research* – 15% are expected to be top priorities in the

next five years of the new digital era; (ii) *Technological* – 35%, *Economic* – 30% and *Social* – 20% outlooks will be considered as the e-clash assets, generating cyber challenges towards: (iii) *Privacy & Tech Addiction* – 35%, *Information Overload* – 30% and *Virtual, Augmented & Real World Mixing* – 20%, expected from several attack vectors: (iv) *Privacy and Social Engineering* – 40%, *Malware & Targeted Attacks* – 25%, *Data Breaching & Espionage* – 20%.

3. A SYSTEM ANALYSIS PERSPECTIVE

More detailed understanding of the outlined hybrid threats cyber-physical nature outlooks from Figure 1, is possible to be obtained with further system analysis implementation.

In the present study interviews and expert opinions data were used. The gathering process was based on: 14 nations during ‘Cyber Forum DESSERT B2S – S2B’, May, 2016 and 21 industrial companies, provided by Association of Communication & Information Specialists in the framework of ‘HEMUS 2016’ military exhibition and ‘Defend IT’, TeleGroup Workshop dedicated to IT Security, June, 2016.

Input data was generalized in I-SCIP-SA v.2.0 software environment. The application is specifically designed for multiple problems system exploration, based on complex discrete systems, machine Entity-Relationship (E-R) representation, organized over a weighted graph [6].

The resulting classification of model entities is visualized in 3D Sensitivity Diagram (SD) in accordance with relations weights (defined as single or multiple array values and measured in percentages from the interval [0, 1]): Influence – x (feed-forward), Dependence – y (feed-backward) and their relation – Sensitivity – z .

Four main sectors are defined in the 3D SD, following x and y values: buffering – green, active – red, passive – blue, critical – yellow. The model z values determine additional sub-classification of: active ($z \geq 0$) and passive ($z < 0$) entities in every SD sector.

A graphical interpretation of future hybrid threats exploration model (a) and resulting analysis classification (b) in I-SCIP-SA, v.2.0 environment is depicted in Figure 2.

The system model is encompassing eight generalized entities, separated in two main parts: social (‘Political Governance’, ‘Social Dynamics’, ‘Non-State Actors’, ‘Economic Changes’) and technological (‘Mixed Reality’, ‘Advanced AI’, ‘Hypermedia’, ‘Critical Digital Infrastructure’ – CDI).

The entities from Figure 2a are next classified, following the input expert data initial assumptions as follows: critical: ‘Political Governance’ – 2, ‘Economic Changes’ – 8, ‘Social Dynamics’ – 7; passive: ‘CDI’ – 6, ‘Hypermedia’ – 4; active: ‘Non-State Actors’ – 1; buffering: ‘Mixed Reality’ – 3, ‘Advanced AI’ – 5.

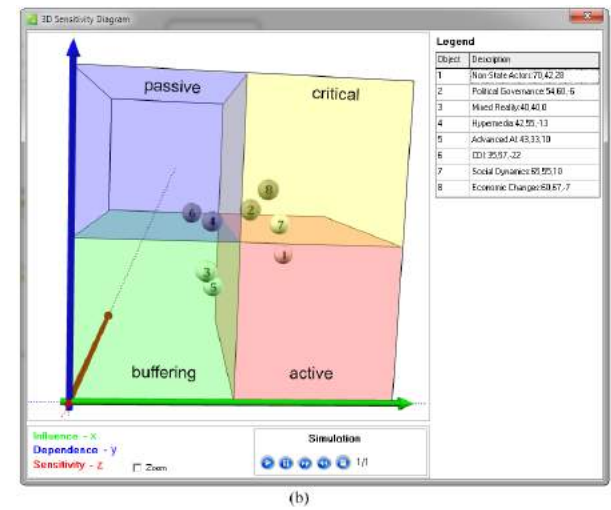
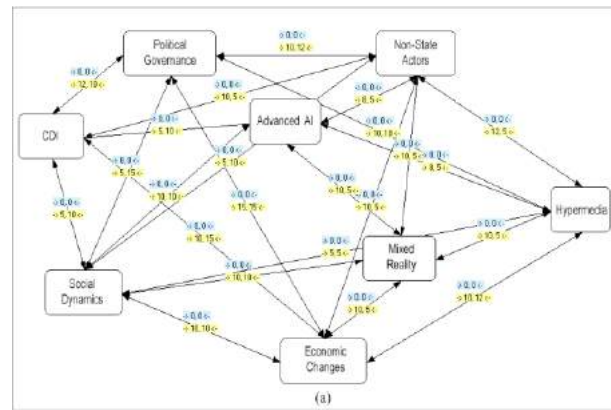


Figure 2: System model for future hybrid threats exploration (a) and resulting analysis 3D classification (b) in I-SCIP-SA, v.2.0 environment

Generally the obtained initial classification is giving priority to social factors importance versus the technological ones. However, it should be clearly noted that these model entities classifications are just introductory and static ones. So, for achieving comprehensiveness they have to be studied further and in the dynamic context, giving the presented system model a real forecasting value.

4. MACHINE VALIDATION

Concerning the validation necessities of the system analysis results both time series dynamics implementation [7] and stochastic modelling [8] are applicable.

The idea for system analysis studying, based on discrete approximation is generally providing a suitable approach for multiple scenarios evolution [4]. In this sense several good examples from the digital space, encompassing environment of living and sensors integration could be given [9], [10].

One of the major problems in this sense that have to be noted is connected to different speeds of dynamics that the real world entities (system variables) are generically interacting. This in fact is of significant importance in complex social systems proper modelling and thus for the new cyber-physical mixed reality exploration. A useful solution in this sense was proposed by Vester, using time delays [11].

Another more complex problem is the system stability that is difficult to be directly assessed and forecast without algebraic model representation. Furthermore, the problem with system reliable control in non-stationary (chaotic) mode stays open.

As far as real system models are usually both non-linear and non-stationary ones, a stochastic approach based on probability trends distribution expert assumption and further risk assessment, about system entities connectivity is presented.

The idea behind is using Beta distributions that are a priori defined over model entities interconnectivities. This approach provides enough flexibility to easily implement prognosis of different shapes, similar to other popular social dynamics descriptions [12], modifying just *alpha* and *beta* parameters [13] of the curves families.

A follow-up a posteriori probability assessment of entities interrelations' risk is calculated implementing the stochastic approach with suitable parametric models [8].

An illustration example of practical machine validation in Matlab R2011b environment for 'Hypermedia' interrelations probabilistic risk assessment from the model of Figure 2a is given in Figure 3.

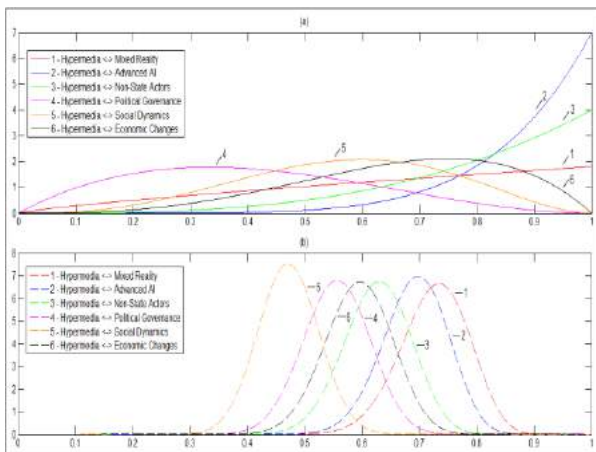


Figure 3: Probabilistic validation for 'Hypermedia' *a priori* (a) and *a posteriori* (b) trends in future hybrid threats study model (see Figure 2a)

What should be drawn as a conclusion of the proposed validation approach, based on stochastic simulation over the possible trends progress, are some difficulties for holistic system evolutionary assessment.

Concerning the expert based E-R model input this problem could be further translated into a multidimensional exploration space.

Following the system holistic nature principal assumption, this provides an opportunity for generalized measuring of the proposed E-R model system nature, using trends forecasting approach, similar to [7] but normally with some limitations that could be bypassed, following the proposed probabilities distributions implementation [8].

Finally, a practical mixed reality observation is added as a verification mechanism, providing an active role for the human factor future uncertain influence coping.

5. RESULTS VERIFICATION

The presented idea is attempting to extend the overall described concept for hybrid threats adequate coping in the new digital reality. The results verification is mainly giving a possibility for better prognosis exploration in a semi-real environment. The assumed practical implementation in this paper is using a mixed cyber-physical reality (real, virtual & augmented ones combination) for interactive simulation with human-in-the-loop extension.

Different fictitious exercise scenarios are tested within this idea, using expected and unexpected event-driven exercise scripts and measuring, at the same time, trainees' group selected psycho-physiological responses [14]. This practically provides an opportunity for future environments reliable exploration with the active role of the human factor.

In general the concept is based on broader security problems exploration solid approach via Computer Assisted eXercises [15], [16] including the cyber space [5], [17].

Here it should be noted that more simplified approaches like: table-top exercises or other multirole high-level games are also applicable in support of the presented solution. They however lack the technological part and could be used only as preparatory ones.

The main idea, encompassed in the present CAX based approach, was taken alive during the international Cyber Research Exercise – CYREX 2016, organized by Joint Training Simulation & Analysis Center at Plovdiv University 'Paisii Hilendarski' [18].

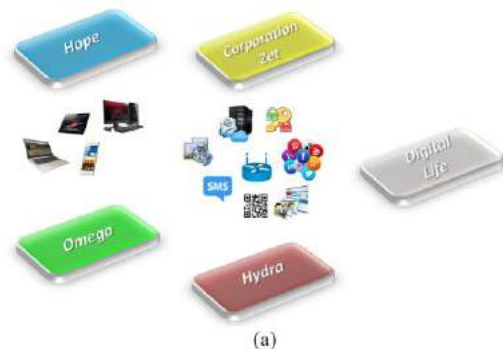


Figure 4: Organizational architecture (a) and selected moments (b) of international exercise CYREX 2016

The trainees were organized in Facebook closed group environment, connected with a mixed reality cyber-physical polygon (encompassing: tablets, phablets, smartphones, i-pods, ultrabooks, laptops and desktop machines) interconnected via LAN (both cable and wireless) from a private router (used also for easy event log recording).

Additional ad-hoc configured e-mail server accounts, SMS notifications and avatar Zoobe based messaging were implemented, together with Skype, Viber & Dropbox services.

DDoS selected participants IP attacks, encryption of messages, malware sources, augmented QR codes realities extensions with hidden information were also used for complex social engineering simulation motivated with hacktivism and industrial espionage ideas.

The participants (30 students, 20 years +/- 2, including 8 observers from academia, industry and abroad from both Republic of Macedonia & IFIP scientific community) were practically organized for approximately three hours in five teams (see Fig. 4) as follows: 1 – ‘Motivators’ – ‘White’ (a non-governmental organization ‘Digital Life’, trying to regulate the new digital society), 2 – ‘Hacktivists’ – ‘Green’ (non-formal hackers group ‘Omega’, fighting for justice in the digital space), 3 – ‘Insiders’ – ‘Blue’ (a start-up company ‘Hope’ established by ‘Omega’ for corporate espionage), 4 – ‘Investigators’ – ‘Red’ (a multinational cybercrime investigation and control organization ‘Hydra’) and 5 – ‘Corporates’ – ‘Yellow’ (a multinational ‘Corporation Zet’ suspected in terrorism funding and criminal connections).

The response times and impressions of all five teams were gathered individually (using router logs and self-reporting digital questionnaires) during and after the exercise.

Several important facts and hypothesis were found and proved from CYREX 2016 successful conduction, regarding the future hybrid threats successful exploration:

- A practical discovery of hypermedia important place in modern cyber-physical reality;
- The progressing share of Critical Digital Infrastructure was also confirmed, facing multiple smart devices and web services for advanced communication in the near future;
- Dual social dynamics and non-state actors’ significant roles, concerning criminal activities, terrorism & hacktivism, for the new challenges of the Advanced Persistent Threats (like: social engineering & espionage, see e.g. [19]) proper meeting.

5. DISCUSSION

The fast technological progress in the digital era is generating new, unstudied hybrid threats from both technological and human perspectives. This creates unforeseen possibilities for influencing human behaviour and emotions via the digital component that have to be expected in the next years.

The presented methodological approach clearly refers to the indisputable necessity for comprehensive coping of the problem in the new and fast evolving cyber-physical mixed reality.

Furthermore the described ideas could be extended from both validation & verification perspectives, implementing micro sensors data (from participants and environment) and more detailed cyberattacks models, including distributed computational powers and big data on-line analysis.

This will provide an opportunity for using the digital environment both as a source and consumer of data, giving a possibility of better understanding the technological evolution in the new digital century.

6. ACKNOWLEDGEMENTS

The authors give special appreciations for the expert & experimental support to: Association of Communication & Information Specialists – Bulgaria, Plovdiv University ‘Paisii Hilendarski’, Cyber Forum 2016 DESSERT B2S – S2B and CYREX 2016 sponsors and collaborators.

REFERENCES

- [1] L. Floridi, “The Fourth Revolution (How the Infosphere is Reshaping Human Reality)”, 1st ed., Oxford University Press, 2014.
- [2] N. Choudhury, “World Wide Web and Its Journey from Web 1.0 to Web 4.0”, *Int. Journal of Computer Science and Information Technologies*, vol. 5 (6), pp. 8096–8100, Nov-Dec. 2014.
- [3] K. Schwab, “The Fourth Industrial Revolution: What It Means, How to Respond”, *World Economic Forum*, Jan. 2016, Available at: <https://goo.gl/e1Kc3F>
- [4] Z. Minchev, “Human Factor Role for Cyber Threats Resilience”, in *Handbook of Research on Civil Society and National Security in the Era of Cyber Warfare*, 1st ed., M. Hadji-Janev & M. Bogdanoski, Eds. IGI Global, 2015, pp. 377–402.
- [5] Z. Minchev, “Cyber Threats Identification in the Evolving Digital Reality”, in *Proc. of Ninth National Conference “Education and Research in the Information Society”*, Plovdiv, Bulgaria, May 26-27, 2016, pp. 011–022.
- [6] Z. Minchev, “Methodological Approach for Modelling, Simulation & Assessment of Complex Discrete Systems”, in *Proc. of National Informatics Conference Dedicated to the 80th Anniversary of Prof. Barnev*, IMI-BAS, Sofia, Bulgaria, 2016, pp. 102–110.
- [7] Z. Minchev, & V. Shalamanov, “Scenario Generation and Assessment Framework Solution in Support of the Comprehensive Approach”, in *Proc. of SAS-081 Symposium on Analytical Support to Defence Transformation*, RTO-MP-SAS-081, Sofia, NATO RTO ST Organization, 2010, pp. 22–1 – 22–16.
- [8] Z. Minchev, G. Dukov, et al, “Cyber Intelligence Decision Support in the Era of Big Data”, in *ESGI 113 Problems & Final Reports Book*, 1st ed., Sofia: FASTUMPRINT, 2015, pp. 85–92.

- [9] Z. Minchev, & L. Boyanov, “Smart Homes Cyberthreats Identification Based on Interactive Training”. in Proc. of ICAICTSEE – 2013, 2014, pp. 72–82.
- [10] Z. Minchev, & L. Boyanov, “Augmented Reality and Cyber Challenges Exploration”, Nauchni Izvestia, issue 9 (195), 2016, pp. 28–30.
- [11] F. Vester, “The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity”, München: MCB–Verlag, 2007.
- [12] C. Sergio, S. Bertuglia, & F. Vaio, “Nonlinearity, Chaos & Complexity (The Dynamics of Natural and Social Systems)”, Oxford University Press, 2005.
- [13] A. Gupta, & S. Nadarajah, “Handbook of Beta Distribution and Its Applications”, 1st ed., New York: CRC Press, 2004.
- [14] Z. Minchev, “Multiple Human Biometrics Fusion in Support of Cyberthreats Identification”, Int. Journal Cyberetics & Information Technologies, vol. 15 (7), pp. 67–76, Dec. 2015.
- [15] V. Shalamanov, T. Tagarev, Z. Minchev, et al, “Security Research and Change Management in the Security Sector”, 1st ed., G. C. Marshall Association – Bulgaria, Sofia: Demetra Publishing House, 2008. (in Bulgarian)
- [16] E. Cayirci, D. Marincic, “Computer Assisted Exercises and Training: A Reference Guide”, 1st ed., Wiley-Blackwell, 2009.
- [17] L. Kick, “Cyber Exercise Playbook”, The MITRE Corporation, 2014, <https://goo.gl/SOKkw6>
- [18] CYREX 2016 Facebook News Post, February 26, 2016, <https://goo.gl/Pa8ArN>
- [19] T. Wrightson, “Advanced Persistent Threat Hacking”, 1st ed., McGraw-Hill Education, 2015.

ROAD VEHICLE EMBEDDED IOT SECURITY

LYUDMILA ZHAROVA

New York Institute of Technology, New York, NY, USA, lzharova@nyit.edu

VITO LEGGIO

Faculty of Organizational Sciences, UB, Belgrade, Serbia, leggio505315d@fon.bg.ac.rs

ALEKSANDAR MIHAJLOVIĆ

School of Electrical Engineering, UB, Belgrade, Serbia, aleksandar.mihajlovic@etf.rs

SHAWN CAMPBELL

IT Systems, New York, USA, shawnm.campbell@gmail.com

RADOMIR A. MIHAJLOVIĆ

New York Institute of Technology, New York, USA, rmihajlo@nyit.edu

Abstract: Users of motorized vehicles are continuously demanding new improvements that would further increase the efficiency, safety, and user friendliness, i.e., simplicity and pleasure of operating such vehicles. Computing and communication technologies have been major contributors driving and justifying these trends. Faced with the phenomena of the massive proliferation of computing micro systems as embedded components on board of modern motorized vehicles, we are forced to acknowledge the issue of security and reliability of such micro systems' operation. We present here a brief historical overview of the automobile embedded computing development, we analyze the complexity of automobile computing, its I/O exposure to benign as well as malicious user interaction, the standardization of automobile computing networks and problems related to opening these networks to the Internet, i.e., the problems of internetworking these networks. In addition we present a unique model of the malicious attack surface that motorized vehicles may present on various levels of abstraction hierarchy.

Keywords: Internet of Things (IoT), Security, In-Vehicle Networking (IVN), Privacy, V2V, Stuxnet.

1. INTRODUCTION

After several shocking road accidents, such as the tragic car crash in Paris (August 30, 1997) that claimed the lives of British Princess Diana and her friend Dodi Fayed [1] and the accident in California (June 18, 2013) where investigative journalist Michael Hastings died [2], the authors of this paper and several of their coworkers have decided to devote more attention to the problems of road vehicle electronic security and the dangers of so called "Car Hacking." This topic has attracted several groups of researchers and cyber security specialists [3-6], as well as all of the car manufacturers worldwide. The importance of the topic is self evident.

To be specific and to avoid dealing with all possible vehicles, (flying, floating and terrestrial vehicles), in our discussions we focus on the modern road vehicles, which are interchangeably referred to as land vehicles, motorized road vehicles, automobiles, autos or cars. Although inspired by unusual car accidents, we group cars, trucks and recreational vehicles (RVs) under one umbrella class of vehicles that we call road vehicles.

It is well known that modern automobiles contain a significant number of electronic devices whose sole purpose is diverse measurement signal collection, control

signal generation and signal transmission. Digital electronic devices found on board of road vehicles capable of performing various computation and communication activities are known as Electronic Control Units or ECUs [3]. To simplify our discussion, we assume that data input or sensor devices may also be included in the class of ECUs. Common modern automobile contains almost one hundred ECU devices, each dedicated to some electrical signal processing activity associated with a physical vehicle part that we may refer to as a vehicle Thing (vT). Each ECU presents an associated vT as a digital device. The ECU transforms the analog and possibly the non-electronic vT into a digital device that can compute and may be networked with other ECUs. For example, there is an ECU that "monitors" hand break or "opened door state" sensor. Some more sophisticated ECUs may be in charge of detecting ignition key presence and that the passenger is not in the car, producing a joint status signal that "instructs" another ECU in charge of preventing the car door lock from operating. A car that would prevent a user from locking doors and exiting the car with the keys in the ignition, would appear as an intelligent or smart car.

Figure 1 illustrates an example of the ECU attached to some vTs embedded in the physical road vehicle system labeled as the "Monitored & Controlled Plant." Evidently,

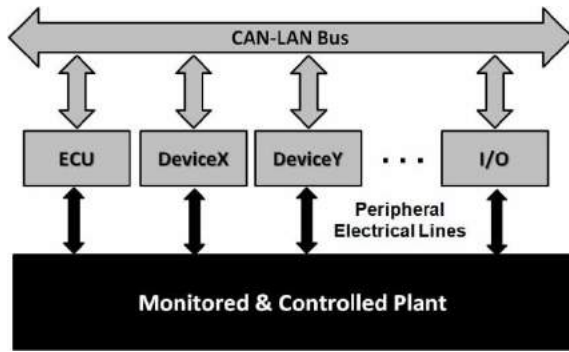


Figure 1: CAN-LAN bus topology minimizes wiring complexity of fully connected LAN and simplifies individual device and ECU activity synchronization.

once purely mechanical road vehicles have grown into mostly electrical and electronic devices. It may even be appropriate to look at the modern road vehicles as a network of computer hosts on wheels with network nodes loaded with millions of lines of code.

Our approach to IoT systems (illustrated in Figure 1) with clear division of “Things” related plant and “Internet” related network technology represents original way of extending security of complex systems such as nuclear power plants or electric grids to IoT systems found on board of road vehicles or vehicles of any kind.

ECU networks may be designed as single trunk or bridged local area networks that are commonly referred to in the literature as In-Vehicle Networks or IVNs. IVNs are as inevitable elements of today’s automobile as Local Area Networks (LANs) may be unavoidable in modern business offices. From the high-end to the lower classes of automobiles, IVNs are being expanded and rapidly developed aiming at the increased vehicle intelligence that may eventually lead to fully autonomous or driverless road vehicles. Smart or intelligent vehicles with complex computing architectures and underlined software present a wide spectrum of possible security holes, i.e., attack vectors that can be exploited in malicious attacks.

There are various architectures and implementations of the IVN in use today. We are still far from a unified standardized architecture accepted by all motorized vehicle manufacturers. Each of these networks operate under different specifications and provide different data transmission speeds (i.e., offers different transmission line bandwidths). As a result of this diversification, the application of IVNs may vary based on the data transmission speed requirements of the various vehicle components that they support. The most common networks that we may find in today’s vehicles are:

- Controller Area Network (CAN)
- Local Interconnect Network (LIN)
- FlexRay
- Media Oriented Systems Transport (MOST)

CAN IVNs are used for basic device to device control, status and data message transmission, i.e., to facilitate

medium speed link implementations, LIN IVNs are used for low-cost body electronics and lowest data-rate functions, FlexRay networks are convenient for safety critical tasks such as steering wheel and brake control message exchange, and MOST networks are high speed networks used for automobile infotainment systems.

Each of the mentioned approaches to IVN implementation may have certain desirable features, but among all of them CAN dominates and may be found in almost every modern road vehicle. Due to the limited scope of this paper we shall briefly present only details of CAN and will leave discussion about the other types of IVNs for our future presentation.

2. CAN IVN PROTOCOL

Controller area network is a serial bus based local area network with L1 strict physical layer specifications [7] and strict L2 data link (DL) protocol specification [8][9] where L1 and L2 are the bottom two layers of the seven ISO-OSI model [10]. The CAN bus with signaling speeds of up to 1Mbps is used to establish links between ECUs or links between vehicle’s onboard computer with the sensors that monitor various vT’s. Figure 2 illustrates CAN bus node basic structure.

The CAN protocol was developed in the mid 1980’s at Bosch for in-vehicle sensor networking. CAN has represented an important development step aimed at the reduction of the overall complexity and cost of the automobile electronic system. Prior to the CAN, if a new feature had to be added to an automobile, it meant adding additional wiring to the overall mash of wires to connect up the new feature device in a point to point fully connected network topology. By using a serial bus, the need for point to point full connectivity cabling became unnecessary. Each device had to be simply attached to the CAN bus as a node utilizing standardized bus interface (See Figures 1 and 2).

The CAN bus lines are made of two parallel twisted pair lines that are used in biased differential mode to backup each other and ensure data transmission in the event of one line failure [9]. Two wire-lines transmit opposite versions of the biased binary data pulse signal with one line called CANH high and the other CANL low line. The lines act as two lines of the differential signal transmission historically used for analog telephone voice signal transmission. When the CAN bus is in idle mode, both lines present bias voltage of 2.5V which makes line-to-line difference of 0V. Any noise signal of the same level present on both lines produces 0V differential value which makes CAN bus Electro-Magnetic Interference (EMI) noise immune. When high data bit is being transmitted, the CANH goes to +3.75V and the CANL goes low to +1.25V, producing line to line signal level difference of 2.5V. For low data bit values signal levels are opposite [7].

Differential nature of the CAN bus signaling, low signaling rates of under 1Mbps, and relatively short line length of less than 40m [8], makes the bus fairly robust.

In the electrically noisy environment under the hood of the road vehicles, this feature of the CAN bus makes it difficult to jam, i.e., perform an attack in the physical L1 layer.

Each node on the bus is connected to both lines and can use the bus rate in a half duplex mode, i.e., may send or receive data but not send and receive simultaneously. The nature of the CAN bus line set and signal format is important to an attacker that plans physical layer jamming attack.

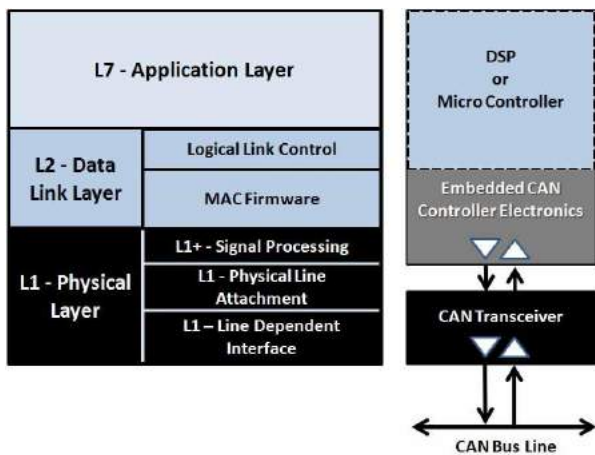


Figure 2: Simplified ISO-OSI relevant CAN bus node layered model.

In the seven layer ISO-OSI [10] or four layer Internet architecture model [11][12], the lower end of the L2 Data Link (DL) layer is defined as Media Access Control (MAC) protocol. CAN MAC layer is specified to operate like Ethernet Carrier Sense Multiple Access/Collision Detection (CSMA/CD) protocol. When the bus is idle (Carrier is not sensed), any node may start to transmit its data frame by sending start of frame (SOF) bit. If several nodes start transmitting their frames at the same time (Collision is detected) an arbitration process is started to control which node may transmit while the other nodes have to back off and delay their transmission (Perform multiple access). The bus arbitration process used in CAN protocol is CSMA/CD with Arbitration on Message Priority (AMP). The CAN bus MAC protocol is known as CSMA/CD+AMP.

Each message data frame on the CAN bus has a unique ID that determines the identity of the sending node and the priority of the message. Priority based arbitration is used when two IVN nodes attempt to use the bus media at the same time. The message with the lower priority numerical value as higher priority message wins and the lower priority message is retransmitted on the next bus cycle. Priority based protocol of arbitration guarantees that critical ECU will get their messages in its real time. One of the attack exploits may target the priority arbitration protocol and delay the delivery of critical messages.

CAN IVN broadcast nature has all messages that appear on the bus delivered to all IVN nodes. Individual nodes

are filtering all non-relevant messages and are accepting only relevant data which are passed up the stack for processing in the application layer (See Figure 2). Apparently, CAN bus as a CAN-LAN core resource and central point of failure is possible to attack and overload via physically planted malicious bus node device or ECU. Such a node device is easy to build [13][14]. In a L1/L2 Denial of Service (DoS) attack, remotely controlled malicious node may jam the bus with a flood of high priority rogue messages and prevent other vital operational messages from being transmitted. Defensive mechanisms that can be used to prevent physical addition of malicious CAN nodes are open for further research and development (R&D) work.

The CAN protocol is completely implemented on board of the CAN controller. The protocol for data link control is standardized by the ISO 11898-1 [15] document while the Medium Access Unit (MAU) i.e., electrical line interface level of the CAN node is specified by the ISO 11898-2/3 documents [16][17].

3. CONNECTING VEHICLE TO THE OUTSIDE WORLD

Modern automobiles are delivered with a number of data collecting sensors that may be classified into two major groups:

- Vital engine monitoring sensors, and
- Vehicle monitoring sensors of direct user interest.

The second class of sensors would cover: Global Positioning System (GPS) vehicle location sensor, temperature, speed, braking system sensors such as the slippery road detection sub system, etc.

Most of the sensors and the format of data that these sensors report are designed in a proprietary manner, to which we refer to as Original Equipment Manufacturer (OEM) design. Some of the data formats and data delivery technologies are already standardized or are in the process of standardization. An example of a standardized service and data format is the GPS data delivery and presentation vehicle user service.

On the higher levels, data are presented via:

- User interface (UI) programs and devices,
- Application communication protocols, or
- API class or function library.

For instance delivered music, video, Web browsing, road maps and traffic congestion reports data are presented via high level user services which has to be differentiated from the application program service such as Web or DNS service. Numerous user services have found their way into the vehicle by means of the IVN via Internet and IVN access points. The presence of such services and the need to have wireless Internet access point devices as IVN nodes has introduced additional level of systems

complexity that has to be defended from malicious attacks.

4. VEHICLE TO VEHICLE LINK SECURITY

A vehicle-to-vehicle (V2V) communication protocol and vehicle subsystems used for cooperative collision anticipation and warning as well as V2V ad-hoc networking are being introduced during the last decade [18][19][20]. V2V ad-hoc networking as well as vehicle-to-roadside (V2R) communications require establishment of wireless links and appropriate IVN access point node. Although promising to dramatically reduce road accidents via active safety mechanisms and promising to enable several new user level services, the opening of the IVN to wireless access over yet another link introduces a whole new attack vector and potential exploits.

The IEEE 802.11p is an extension of the IEEE 802.11 standard and was introduced to add wireless (WiFi) access in the band of 5.9GHz to IVN and specify links of short data frames needed for Intelligent Transportation Systems (ITS) sort of applications. Using the IEEE 802.11p IVN compliant access point, vehicles are able to establish temporary links with nearby vehicles or roadside V2V supporting systems. Due to the short time to live (TTL) nature of V2V and V2R links and dynamically changing link end points, no authentication protocol is proposed by this standard. A V2V link is established between two vehicles as soon as they are in range of each other. A warning may be issued to a vehicle user if a vehicle that may not be visible suddenly take some threatening action.

This feature, while presenting great possibilities as it relates to safety, will also present challenges from a security standpoint. If we allow communication without authentication we may not be able to trust the data that is being delivered. Some of the possible solutions that could minimize problems caused by the missing authentication protocol could be as follows:

- 1) Use application layer firewall that could filter data that are received via 802.11p standard link.
- 2) Restrict physical actions caused by the data received via V2V link. For instance, actions could be audiovisual vehicle user warning and not command message sent to some important ECU and vT causing vehicle maneuver action on the user's behalf
- 3) Restrict V2V message delivery only to a specific IVN segment that does not cover any critical ECU set.

These solutions could be applied to other V2V protocols that may be different from the 802.11p, (e.g., custom Bluetooth, Wi-Fi or cellular link).

With the distance limitation to roughly 10m, Bluetooth protocol may be inconvenient for use in the attack exploits on the road. It is very hard to maintain short distance between the attacker and target vehicle in motion. However, an attack could be pre launched at a target vehicle while being stationary by delivering

malicious data payload that may be executed at some later point in time.

WiFi links provide greater opportunity to execute an attack than Bluetooth links.

Cellular telephony links have been proven to be vulnerable to attacks and should be voided in all V2V network based applications.

The concept of vehicle to vehicle (V2V) communications with vehicles being linked directly with neighboring vehicles or indirectly via road side units assumes individual IVN exposure with all IVN ECUs attached to the potential malicious data traffic. Lotfi Ben Othmane et al.[20] has developed an estimations of the likelihoods of several security sorts of attacks aimed at V2V networked vehicles. Most of the analyzed vehicle attack exploits were found to be very unlikely. The survey showed that attacks on connected vehicles must be rapid, before being discovered or before the attack context would change, and be designed and executed by very sophisticated attackers with profound knowledge about the target.

5. V2V PRIVACY ISSUES

Vehicle to Vehicle (V2V) applications employ basic safety message (BSM) exchange between vehicles providing each other with additional safety data not delivered by the on board sensor networks. In order to minimize response time, by default design, BSM data is not encrypted. In order to provide data protection, BSM data packets are secured with a digital certificate which guarantees message authenticity, [21,22,23].

Since every digital certificate contains the owner's identification data [24] illegal or unplanned access of the vehicle digital certificate may lead to the illegal private data exposure, i.e., invasion of privacy. The main privacy concerns can be summarized as:

- Vehicle owner tracking – A study performed in 2009 by PARC indicates that more than 5 percent of US citizens can be identified by the pair of data identifying their place of work and their residence address. Tracking unique vehicle digital certificate enables reliable determination of both of these data items. Apparently V2V technology enables tracking vehicle geographical location [25] which onetime may be desirable and another time may not be.
- In traffic vehicle behavior tracking and automatic traffic violation citation distribution. Digital certificate could reinforce existing network of intersection monitoring CCTV camera networks and enable automated issuance of traffic violation citations. Such a facility would greatly increase local government revenue and as a deterrent improve traffic safety while outraging community of drivers.

It is reasonable to expect that the vehicle owners community aware of being continuously tracked, would massively protest and possibly endanger the acceptance of

the useful and secure V2V technology based on the digital certificate. To avoid such a situation unique, global and permanent vehicle identification has to be abandoned and possibly replaced with the locally unique vehicle identification with the limited time to live (TTL) identification data record (also known as Personally Identifiable Information or PII).

Some of the privacy protection methods may involve the following:

- Preventing PII message wireless transmission Data such as vehicle owner’s name, id number, vehicle license plate, vehicle identification number (VIN) or similar should not be a part of any wireless link data frame.
- Unique digital certificate should identify logical user, Logical user entity relevant to the user’s pass-code and not the user, i.e., user’s private identity data should be used in the digital certificates. Anonymous certificates where CA is not provided with the complete user’s data
- Rotating digital certificate that dynamically is changing, e.g., user uses N certificates each week, rotating them so one certificate can’t be used to track a person or vehicle, protecting against the home/work pairings found in the PARC study.

Necessary steps must be taken to preserve privacy of the vehicle owner while maintaining secure wireless V2V communication.

6. STRUCTURED APPROACH TO VEHICLE SECURITY

Some of the IVN networked ECUs are in charge of communications with the outside world as well as the internal ECUs. ECUs that are exposed to outside network access pose the biggest security risk to the vehicle and car users. Such ECUs permit internal IVN access that must be well controlled. The spectrum of exploits available to potential IVN intruder is determined by the additional layer of access control options in charge of individual ECU access.

We propose a multilayered model of vehicle security maintenance based on the extension of the network perimeter concept.

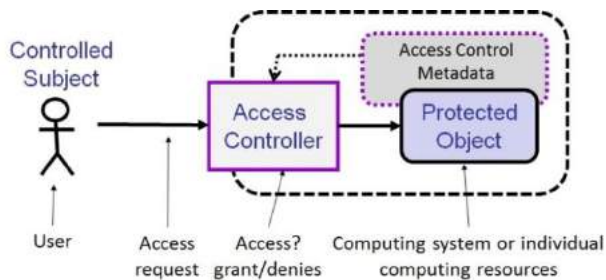


Figure 3: Elementary access control model.

Our multilayer security control model is based on the multiple levels of access control mechanisms that start with the outmost control point represented by the physical

car entry mechanism that may be direct key contact or wireless contactless based. We refer to this outmost access control as control AC₀. Figures 3 and 4 illustrate the layout of access control points where the point AC₁ represents the vehicle ignition key. There are numerous personalized mechanisms that may be employed to implement AC₀. From the ignition point on, at the lowerlayers of the access control hierarchy we find electronic devices communicating according to certain protocol specification.

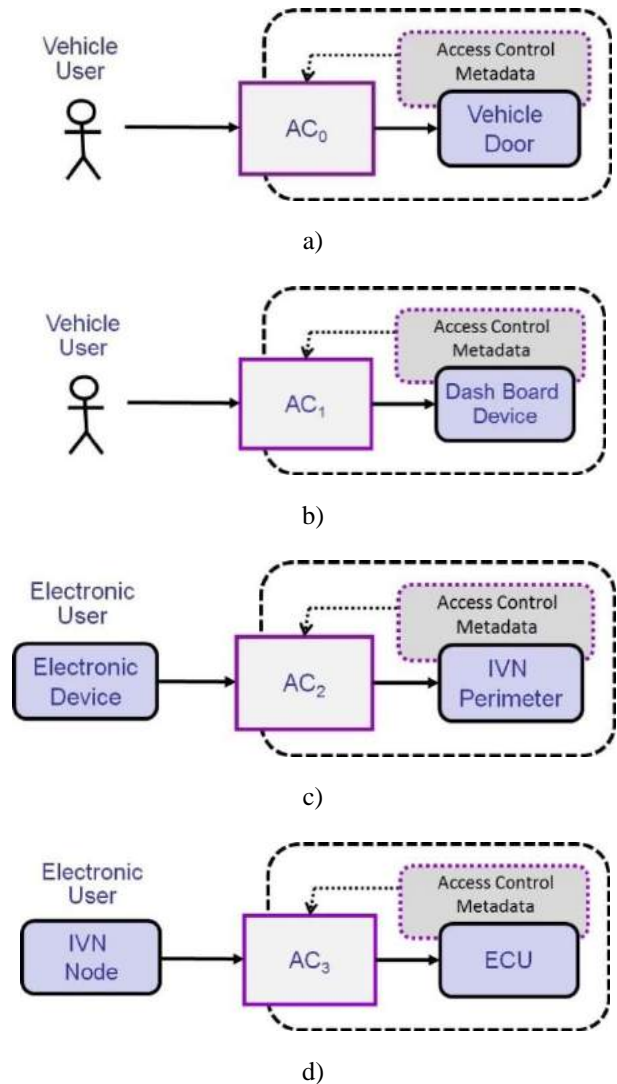


Figure 4: Multi level access control providing defense in depth layered protection of IVN ECUs.

7. REMOTE ATTACK PATTERN

By the classification of attacks (See [24]) on some protected resource, successful attack may result in:

- The denial of resource service (DoS) to legitimate resource users, or
- Illegal resource access and use.

The DoS attack may be:

- Hard DoS, with total destruction of the resource, or

- Soft DoS, resulting in reduced quality of resource service (QoS).

Both sorts of DoS attacks on the vehicle in motion may be catastrophic for the vehicle user and other vehicles that may be consequentially involved. In one of the attack patterns secondary target vehicle acting as a zombie or proxy attacker vehicle, may be subjected to electronic hard DoS while performing physical hard DoS on the primary target vehicle. This sort of the two stage attack is possible with very sophisticated vehicles with optional V2V primary to secondary target communications.

We distinguish two general sorts of the vehicle attacks:

- Physical, and
- Electronic or cyber attack.

A simple example of a hard DoS physical attack is the case of a planted car bomb or the use of an improvised explosive device (IED) placed alongside the road. IED hard DoS attack presents the greatest threat to US troops deployed overseas. An example of the soft physical DoS attack would be contamination of the gasoline or other vehicle liquids and sabotage on various vehicle physical parts, i.e., vTs. Common vT attacks involve vandalizing a vehicle, e.g., bycutting pneumatic hose or severing internal wire lines. In case of soft DoS attack, vehicle remains operational with suboptimal performance characteristics that may lead to total denial of vehicle service. Partial model of the vTs found in a common vehicle is shown in Figure 5. Our detailed model of the road vehicle is beyond the scope of this presentation and is not given here.

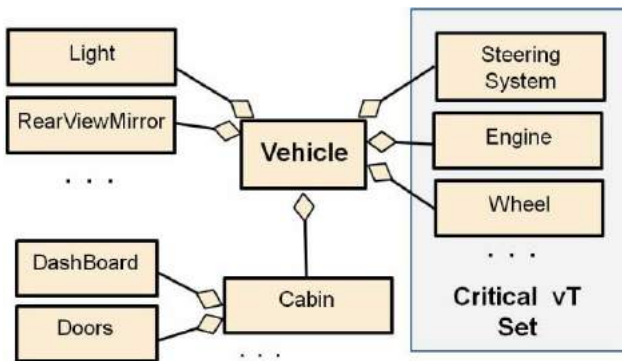


Figure 5: Partial UML class diagram of a vT set found in the common road vehicle.

Figure 5 shows distinguished set of critical vTs. Hard DoS on critical vTs may be tragic for the vehicle user. When an attacker desires to physically harm vehicle user, attack pattern has to involve critical vT set elements as favored targets.

As a rule, malicious cyber-attacks of remote modern automobile goes through following stages:

- Attacker establishes attack stepping stone device or IVN access point (AP).

- Using the IVN AP attacker gains access to the IVN of a vehicle.
- Attacker injects exploit message set into the IVN traffic stream.
- Injected message data controls targeted ECU and the vT behind it.

Primary subject of our work are problems of vehicle cyber attack of both, DoS and illegal access kinds via wireless link, i.e., remote cyber attacks.

We classify attacks on any protected system (System employing access controls) as:

- Front door, and
- Backdoor attacks.

Implementation of the protection of modern road vehicles is primarily focused on the access control at various user interface points in the vehicle cabin, (See Figure 6). The set of these user interface points forms physical front door of the system. Vehicle manufacturers offer variety of physical implementations of the physical front door access controls and penetration testers and hackers diligently work discovering new front door attack exploits.

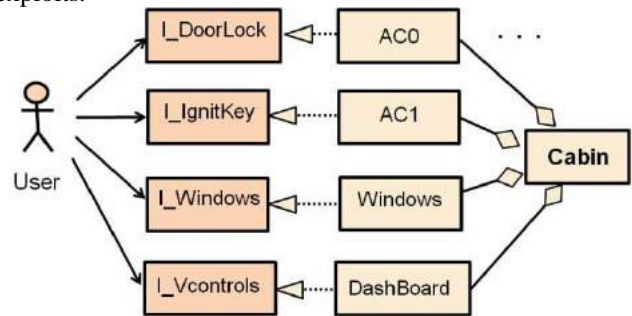


Figure 6: Partial UML class diagram of the vehicle cabin elements and implemented user interfaces.

Installing an IVN AP device in the initial phase of the DoS attack, may involve preliminary front door or backdoor attack. Physical backdoor vehicle attacker avoids standard user interface points and may be performed in repair shops, parking garages, in the streets, etc. Planting IVN AP (later to be used in the wireless cyber-attack), is equivalent to the initial steps taken with the 2010 first digital weapon use, known as the Stuxnet. We treat the Stuxnet and DoS road vehicle cyber-attack as two isomorphic attacks. In our models, a set of road vehicle things or a set of nuclear power plant things are equally treated as monitored and controlled plant (See Figure 1).

At the lowest level (physical level), electronic or cyber attack involves illegal use of ECU registers associated with some of the critical vTs. IVN ECUs appear precisely as I/O controllers attached to the computing host systems I/O bus. As specified in [24] all programmable I/O controllers, and consequently ECUs contain three sorts of registers:

- Read only status registers,
- Write only command or instruction registers, and
- Read/Write data registers.

Assuming control of the targeted IVN ECU implies use of all three sorts of registers with particular focus on the ECU command registers. Denying access to that type of ECU registers to the unauthorized command message is ideal IVN protection mechanism. Unfortunately most of the modern IVN and ECN solutions do not implement ECN instruction register access control which is in its simplest possible form implemented in the modern Central Processing Units (CPUs). Namely, the execution of the privileged CPU instruction must be accompanied by the appropriate privilege level flags or privilege ring code maintained in the Program Status Word (PSW) CPU register set [26]. Following this line of design reasoning, we propose that as the last perimeter of defense in depth IVN architecture, we have access control of each ECU command. In his thesis [27], Rogers describe methods of possible circumventing privilege level control of certain CPU instructions. The work of Rogers proves that the incomplete protection is not possible in the simple binary session between the actor and the protected resource. The last two authors have explicitly defined the fundamental condition for secure session implementation [24] which clearly states in an axiomatic form that binary session cannot be made secure without a third session node. In other words the only ternary session may recursively guarantees security of the production binary session. To be specific, secure binary production session employs two security related meta-sessions involving production session nodes and third secure domain management node. In our future paper we propose a solution of secure access control of command messages at the IVN ECU instruction registers.

8. DEFENDING ROAD VEHICLE IOT

A network on board of road vehicles connects a set of vTs via ECUs acting as interface. The combined set of the vT and the associated ECU form computing thing that can be networked, a thing that constitutes anode on the vehicle based Internet of Things (IoT). Vehicle based IoT is one specific example of the IoT that significantly differs from the commonly found IoT. Fundamental difference in question is that:

- Vehicle IoT devices have solid power source,
- The lines interconnecting IoTs are not wireless but wire line based,
- Justified by the absence of the fragile power sources and availability of funds to invest improving high price ticket item such as a road vehicle, computing power (CPU and memory) capacity does not have to be minimized.
- IoT wire lines are robust and reliable
- Data transmission rates do not have to be minimized

Taking all of the above mentioned features, we may conclude that implementing security extensions of the vehicle IoT on any level of complexity should not be

limited by the commonly found constraints in typical IoT networks such as wireless sensor networks.

Practically every American carmaker now offers IVNs capable of communicating with the external world via wireless links using a cellular service, Wi-Fi links (e.g., General Motors' OnStar, Toyota's Safety Connect or Ford's SYNC). All of the carmakers are actively engaged in the research and development of secure wireless vehicle IVN access solutions. Their engineers test their vehicles against wireless attacks. However, we must stress that the pace of mechanical vehicle engineering and computing technology evolution are significantly disproportionate. From the new vehicle design studio to the dealership sales floor, new model development and manufacturing may take on average up to four years [28]. At the same time new designs of sophisticated computerized cell telephones development with massive amount of new software features may be launched in less than a year. With such a vehicle mechanics to IVN computation development asymmetry, a car may be way behind the new digital developments that may include new, let us say zero day, malicious software tools and hacker's exploits. Apparently, motorized vehicles must be open to timely, i.e., frequent software patching, where frequent software patching opens new avenues of creative "car-hacking".

In order to engage as large as possible number of talented hardware and software specialists, we take a strong position that all road vehicle attacks must be urgently reported and widely advertised, i.e., must be open. Further research and development on the topic of secure timely vehicle network hardening is more than necessary.

ECUs are located in various places throughout the car. ECUs controls almost every aspect of the modern automobile, they take input from sensors and provide output to actuators. ECUs are executing proprietary code on proprietary hardware micro architectures and as such are very hard to infect. Even though most of the ECUs are running firmware code that is hard to erase and replace by some viral code, a dedicated attacker will devote time to backward engineer sample devices preload infected firmware and physically replace the ECU on the IVN with the malicious version. Physically guarding road vehicle from the unauthorized physical access is essential in the overall security measure set. Malicious ECU, shown in Figure 3 c) and d) may be used to perform illegal accessto other ECUs on the IVN or to execute DoS sort of an attack on any element of the IVN including the IVN bus.

9. CONCLUDING REMARKS

Several cases of strange accidents that have resulted in the deaths of prominent public and media figures have inspired a series of conspiracy theories claiming that modern high end vehicles such as Mercedes-Benz automobiles (e.g., 280-S [1] or C250 coupe [2]) may be maliciously attacked using cyberspace technologies. One of the most shocking Mercedes-Benz vehicle accidents has caused Russian President Putin's driver death [29]. In this tragic accident, Mercedes-Benz vehicle made a

similar maneuver to the one described in [1], crashed into a highway fence, crossed the fence and collided heads on with President Putin's official BMW vehicle moving in the opposite direction. Conspiracy theorists could classify the last accident as the first case of hacking cars to be used as a guided weapon. Unusual sequence of deadly car accidents involving the most sophisticated vehicles such as those manufactured by the Mercedes-Benz, definitely justify extraordinary attention to the road vehicle security and avoidance of possibly exploiting V2V communication between the physically attacking and attacked vehicles.

Since most of the original manufacturer's ECU software defects are timely patched we focus not on the defense against zero day attacks based on legitimate software bugs, but on the spear attacks based on the planted illegal IVN AP. Upon systems analysis of the vehicle elements, our explicit proposal how to defend against cyber attacks even after successful IVN AP installation (Initial step in the Stuxnet [30] or vehicle DoS cyber attacks), is to implement register level access control (See Figure 4 d). Since the standardization of the internal ECU implementations is still in its relative infancy, any modification of the existing ECU design or introduction of the new line of controllers is feasible and financially justifiable. Following the strategic recommendations of defense in depth, in addition to the register level security measures we could work on solutions which would prevent illegal IVN AP installation, i.e., detection of IVN nodes that are not originally built in the factory.

The scope of this text is practically limited. Under the given constraints, our presentation is focused on the most important elements of the topics of protecting road vehicles from cyber attacks. We leave additional details describing our work on structured approach to the security of the IoT networks embedded on board of motor vehicles for our future presentations.

REFERENCE

- [1] "Princess Diana cover-up," The UK & Ireland Database, 2016.
- [2] Mike Hogan, "Was Michael Hastings' Car Hacked? Richard Clarke Says It's Possible," The Huffington Post, Jun 26, 2013
- [3] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., Savage, S., "Experimental security analysis of a modern automobile," In Proceedings of the 2010 IEEE Symposium on Security and Privacy, pp. 447-462.
- [4] Pierre Kleberger, Tomas Olovsson, ErlandJonsson, "Security Aspects of the In-Vehicle Network in the Connected Car," 2011 IEEE Intelligent Vehicles Symposium (IV) Baden-Baden, Germany, June 5-9, 2011.
- [5] Stephen Checkoway, Damon McCoy, Brian Kantor, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno,, "Comprehensive experimental analyses of automotive attack surfaces," SEC'11 Proceedings of the 20th USENIX conference on Security, 2011, pp.6-6.
- [6] Mark Anderson, "Black Hat 2014: Hacking the Smart Car," Mark Anderson, IEEE Spectrum, Aug 6, 2014.
- [7] Steve Corrigan, "Controller Area Network Physical Layer Requirements," Texas Instruments Application Report, SLLA270–January 2008.
- [8] M. Di Natale, "Understanding and using the Controller Area Network," October 30, 2008.
- [9] Blackmore, J., & Monroe, S., "Overview of 3.3V CAN (controller area network) transceivers," Application Report, Texas Instruments. 2013.
- [10] William Stallings, "Handbook of Computer Communications Standards: Open Systems Interconnection Model v. 1," The Macmillan database/data communications series, Macmillan, March 1988.
- [11] Kevin R. Fall and W. Richard Stevens, "TCP/IP Illustrated, Volume 1: The Protocols," 2nd Ed., Addison-Wesley Professional Computing Series, Nov. 25, 2011.
- [12] Douglas E. Comer, "Internetworking with TCP/IP Volume One," 6th Ed., Pearson, May 5, 2013.
- [13] "CAN FD v1.0 LogiCORE IP Product Guide," Vivado Design Suite, PG223 November 18, 2015.
- [14] Pat Richards, "A CAN Physical Layer Description," Microchip Technology Inc., AN228 note, 2002.
- [15] "Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signaling," ISO 11898-1:2015.
- [16] "Road vehicles -- Controller area network (CAN) -- Part 2: High-speed medium access unit," ISO 11898-2:2003.
- [17] "Road vehicles -- Controller area network (CAN) -- Part 3: Low-speed, fault-tolerant, medium-dependent interface," ISO 11898-3:2006.
- [18] Hong Bong Kim, M. Emmelmann, B. Rathke, A. Wolisz, "A Radio over Fiber Network Architecture for Road Vehicle Communication Systems," Proc. IEEE Vehicular Technology Conf., VTC Spring 2005.
- [19] Xue Yang, et al., "A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning," The Fifth IEEE International Conference on Networking, Architecture, and Storage (NAS 2010).
- [20] Lotfi Ben Othmane, Ruchith Fernando, RohitRanchal, Bharat Bhargava, Eric Bodden, "Likelihoods of Threats to Connected Vehicles," International Journal of Next-Generation Computing, Vol. X, No. X, 07 2014.
- [21] Dorothy J. Glancy, "Privacy in Autonomous Vehicles," Santa Clara Law Review, Vol. 52, No. 4 Article 3, December 14, 2012.
- [22] Gene Carter, "Privacy in V2V communications: Is somebody watching you?," Security Innovation, May 18th, 2015.
- [23] Gene Carter, "V2X technology makes cars safer," Embedded Computing Design, April 10th, 2015.

- [24] Mihajlovic R, Mihajlovic A., "Operating Systems Security; The First Cut," Soft Electronics, New York, May 2015, ISBN-978-194327525-0, pp.256-285.
- [25] Matthew Jensen, "How To Track Your Vehicle on The Cheap, Using Your Smartphone?" Study Lifestyle, August 9, 2016.
- [26] Schroeder, M., Saltzer, J., "A Hardware Architecture for Implementing Protection Rings." Communications of the ACM, Vol. 15, No. 3, 1972.
- [27] David T. Rogers, "A Framework for Dynamic Subversion," Thesis, Monterey, California. Naval Postgraduate School, June 2003.
- [28] Laura Ionita, "Connectivity shifts the power in the automotive industry," Tuck School of Business at Dartmouth, Galsmer/McNamee, Center for Digital Strategies, T'15, March 28, 2015.
- [29] Lizzie Stromme, "Putin's official car involved in horror crash – killing leader's 'favourite' driver," Express, Sep 6, 2016.
- [30] Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," Wired Magazine, 11.03.14.

SM@RT HOME PERSONAL SECURITY AND DIGITAL FORENSIC ISSUES

IGOR VUJAČIĆ

University Donja Gorica, Humanistic studies, Montenegro, vujacic@gmail.com

IVANA OGNJANOVIĆ

University Donja Gorica, Humanistic studies, Montenegro, ivana.ognjanovic.edu@gmail.com

RAMO ŠENDELJ

University Donja Gorica, Humanistic studies, Montenegro, ramo.sendelj@gmail.com

Abstract: *These days we are facing with expansion of off the shelf IoT solutions for SM@RT HOME. Recently, concept of SM@RT HOME has evolved from simple, separated, products for home automation into complex IoT systems for home monitoring, automation and security. Unfortunately, this rapid expansion was not followed by proper set of standards, especially in field of security and protection of system per se.*

This paper will take into consideration, and addressed some problems and open issues of personal security, and digital forensic challenges in that respect. It will show a possible solution through implementation of risk management cycle strengthened by digital forensic enablers like logging systems.

Finally paper will conclude that only proper level of awareness, accompanied by comprehensive advanced security intelligence concept can provide high level of personal security in SM@RT HOME environment.

Keywords: *Information Security, IoT, SMART Home, digital forensics, personal security, open standards, industry standards*

1. INTRODUCTION

Home was and still is much more than just an object for housing people, or place for living. Commonly, people will describe it as a nest, personal and family fortress, as a place where they can express themselves, but at the same time place where they are safe, secure and comfortable. They like to make it better, easier for day to day activities, modern, safe, secure, and comfortable, in order to improve life quality.

For the sake of improving life quality at home, SM@RT HOME concept emerged as a combination of new Internet of Things (IoT), and traditional devices and services [1].

The very first step on the SM@RT HOME road map was paved, in cyber realm time scale, long time ago. First, simple, home automation technology, called X10, was developed in 1975. Since then, end user demands grows from simple automation and controlling tasks inside house to comprehensive house security, monitoring, control and automation inside house and remotely. Those demands, over the years, dictated developing of different technologies and product lines for every single demanded functionalities, and lastly to converged them into complex SM@RT HOME system.

Paradoxically, even though lot of products was developed for home safety and security, those products does not implement proper level of security per se.

In developing of other SM@RT HOME product lines, security is low ranked if it is considered at all.

Those product are key carriers of our private information, and they have to have built-in support at least for identification, authentication and authorization (IAA), security audit, communication protection, and data encryption.

Unfortunately, legislative branch did not address this field properly yet, too. For instance, in EU there is no censuses about SM@RT HOME systems, predominantly caused by different cultures, economies and understanding of so called information societies. That is main reason why there are no dedicated EU policies covers IoT and SM@RT HOME [2].

Combination of those factors led us into the field of open opportunities for exploits SM@RT HOME system vulnerabilities in order to steal personal information, or to overtake monitoring and control over the home, and its inhabitants.

This paper will argue that only holistic approach to SM@RT HOME implementation will reach the aim to make our homes smarter, and our lives more comfortable. It will show the necessity for both, proper level of awareness, and implementation of active advanced security measures to mitigate cyber threats.

The paper is organized as follows: Section 2 gives the overview of SM@RT HOME concept evolution and expansion, Section 3 presenting security issues and

emerging threats landscape, and Section 4 proposing solutions to mitigate existing and upcoming threats. Section 5 concludes the paper summarizing recommendations and key findings.

2. EVOLUTION AND EXPANSION

The first well known and well spread technology for home automation is X10. It was developed in United States by Pico Electronic in 1975. Until now it becomes well accepted for home automation with more than million units.

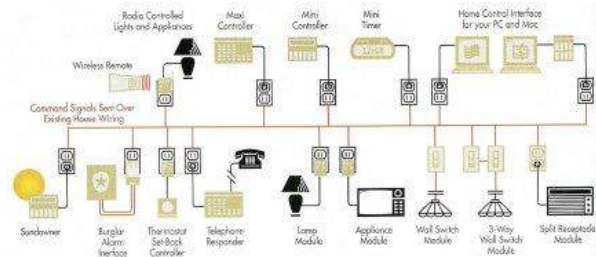


Image 1: X10 schematic [3]

Recently, concept of SM@RT HOME has evolved from simple, separated, products for home automation into complex systems for home monitoring, automation and security. Today, we have a plenty of home automation and more advanced SM@RT HOME IoT products on the market. Some of them are regular industrial products, some of them are hobby and DIY kits. There are plenty of hobby platforms on the market [1, Chapter 1.3] [4]. The most popular DIY platforms for building SM@RT HOME are ARDUINO [5] and Raspberry Pi [6]. The most popular open source project are OpenHUB [7] and Home Assistant [8]. For internal communication between devices different protocols were developed over time, like C-BUS, EnOcean, Insteon, KNX, Thread, Universal Power Bus, X10, xPL, Zigbee and Z-Wave. Some of them utilised power lines, some twisted pairs, Ethernet, RF spectrum or infra-red. Computing power of those devices vary from no computing functionalities to powerful devices.



Image 2: Modern SM@RT HOME system [9]

We can say today's SM@RT HOME is a melting pot of traditional real-time processing part of system: sensors,

actuators, controllers, etc. and packet oriented part of system: most of IoT units and appliances, cameras, entertainment equipment, etc. of local Home Area Network and Wide Area Network, of local data, and cloud services and big data, and so on, like illustrated in images 2 and 3.

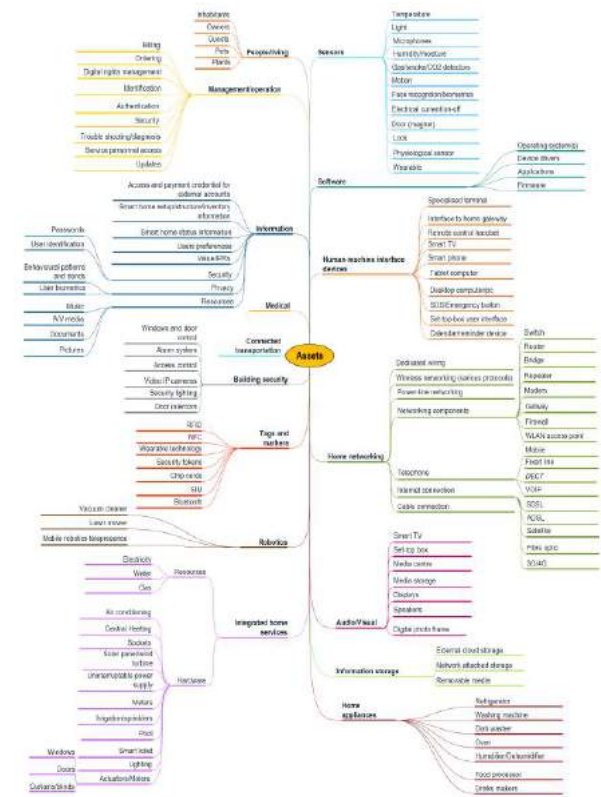


Image 3: Overview of Smart Home and Converged Media Assets [10]

From both images, 2 and 3, we can conclude that beside traditional automation equipment, IoT devices plays a big role in today's SM@RT HOMES. Proliferation of devices like wearables, smart thermostat, and similar devices bring IoT into our Home Area Network (HAN). Those devices for their communication and management function utilise same communication infrastructure like traditional IT equipment.

In order to understand it better, we can split SM@RT HOME pot into ingredients and categorized them:

- by functionalities into [10]:
 - *Home automation and robotics:* lightening, HVAC, smart home appliances (smart refrigerator, dishwasher, washing machine), home robots (various assets starting from vacuum cleaner, autonomous grass trimmers and so on)
 - *Home monitoring and security:* video surveillance, gas leakage and flooding detections, fire detection and autonomous firefighting systems, burglar and access control system
 - *Health support systems,* as autonomous or as a part of larger health care system: different monitoring devices, and devices that monitor,

- control, and drive or correct human body functions
- All other connected in home devices like: smart wearables, smart phones, tablets, computers, DVRs, receivers, set-top-boxes, streaming devices, game consoles, computers, and so on.
- by type of connectivity:
 - Wired,
 - Wireless long range,
 - Wireless mid-range,
 - Wireless short range.
- by interaction:
 - man 2 machine capable
 - machine 2 machine capable
 - hybrids
- by presence in Home Area Network
 - Permanently presented
 - Roaming between Home Area Network and external networks.
- by hardware (in [1], 2.1.2 Classes of IoT devices) on:
 - Constrained devices [11]:
 - class 0: simple sensors,
 - class 1: smart bulbs, smart locks, etc.
 - class 2: smart appliances and high-end smart sensors
 - High-capacity devices such as smart hubs/gateways and smart TV-s etc.

3. SECURITY ISSUES AND EMERGING THREATS

When we are talking about security issues in general, network security is one of key issues targeting almost each application and system [12], aimed on preventing and monitoring unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources [13].

Many authors differently define key goals of network security [13] [14], while the following six goals are commonly used related to the topic of SM@RT HOME [15]: *Confidentiality, Integrity, Availability, Authenticity, Authorization, Non repudiation*; with definitions listed in Table 1.

Table 1. Network Security goals

Network security goal	Definition/ description
<i>Confidentiality</i>	The assurance that “data will be disclosed only to authorized individuals or systems” [14]
<i>Integrity</i>	The assurance that data will stay as is (unchanged) over time on storage, in memory or in transition over networks. Any modification or destruction should be recognised and logged.

<i>Availability</i>	The assurance that network resources will be ready (available) for processing any authorised requests and blocking unauthorised requests (attacks).
<i>Authenticity</i>	The assurance that communication actors really are who they claim they are, and the packets send from each one really belong to him, and is really emitted from him.
<i>Authorization</i>	The assurance that requested access rights by actors are matching with his assigned rights.
<i>Non repudiation</i>	The assurance that no one can deny what has been found as evidence.

Even the goals are clear, there is no unique approach to be applied for different systems and applications [16], and that is a reason why specific approaches and models shall be developed and applied. However, variety of factors should be considered [17]: architecture complexity, network topology, physical security, communication security, and lot more.

SM@RT HOME complexity is obvious. It is a mix and match of different type of technologies, devices, appliances, interfaces and protocols. Even though this complexity is problem per se, some additional problems are identified:

- Lack of open or industry standards to cover all aspects of SM@RT home. Despite the fact that lot of standards are developed, some guidelines and dedicated standards still missing, especially those who will cover security issues properly [10, page 49].
- Vendors ether does not take a care about security, or make their own proprietary standards [1, Chapter 3.2]
- There are lot of cloud solutions for monitoring and control of our homes.
- Policy makers still does not have a consensus about SM@RT HOME, so there is a lack of laws and policies [2] [1 Chapter 8.5].
- Very limited knowledge and security awareness of end-users [10, Conclusions].

All those together are wide opened doors for personal security and digital forensic issues.

When we have bad planned, implemented or/and configure system, then we are exposed to both known and zero-day attacks. Significant problem, in ill configured system, is that we have no knowledge about security breaches. Once, when we finally became aware of it, then there are no logs and evidence that can be used for digital forensic to help us to figure out what was happened, what we have to face with, and what is

damage scale. Within more complex systems this is even harder.

From a privacy aspect there are a lot of static (our first, last name, social security or identification number, data about credit card, day of birth, information about relatives, and everything else what was submitted somewhere or stored inside devices) and dynamic data(logs from devices or on-line collected data that represent our behaviour), stored inside our Home Area Network, or in connected cloud service that could be misused to make our digital profile (digital ID card), or to generate perfect ransomware virus, to perform fraud, etc.

Form a security aspect we are faced with additional serious problem, that SM@RT HOME can be used against us. Just imagine, possible, scenario when some hacker overtake control of our Home Area Network. Then he can monitor and read data from many different devices. By misusing our home monitoring and security system he can see what we are doing, when we are at home, how many of us, where we are inside home. So, he can track our habits and behaviours. Furthermore, he can take an action to lock up people inside, to change temperature, shut down ventilation system, close blinds, water, cut off power, and so on. As an extreme example, hacker can overtake control over our health care, and medical life support appliances and perform possible kinetic effect that will have direct implications to our life.

In the literature, many researchers and organizations [1], [10], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [23] identified or/and addressed different kinds of potential threats and attacks for both, IoTs and SM@RT HOMEs. All agreed that identified issues having growing trends in recent time, and same forecast for upcoming period. Table 2 gives comprehensive view on security threats [10], possible attacks and scenarios [14] in relation to security goals previously defined in Table 1.

Table 2. SM@RT HOME security threats, possible attacks and scenarios

Security threats	Security Goals Compromised	Possible attacks / scenarios
Malware	All	Malware could be preloaded on device, or injected internally or externally.
Botnets (abusing IoT components as botnet nodes and/or C2 servers)	Confidentiality Availability Authenticity Authorization Non repudiation	Abused devices can attack other elements of SM@RT home, or could be abused for external attack.

Identity theft	Confidentiality Integrity Authenticity Authorization Non repudiation	Social engineering
Web based attacks	Confidentiality Integrity Availability	Spoofing DoS Information Disclosure Elevation of privileges ...
Physical theft/damage/ loss	Confidentiality Integrity Availability	Physical stealing, accidental damage, remote control action
Phishing	Confidentiality Authenticity Authorization Non repudiation	By misusing using smart devices
Insider threat	All	By physical presence or by utilising some air interface
Information leakage	Confidentiality Authenticity Authorization Non repudiation	Apps and applets, ad-ware software
Web application attacks	Confidentiality Availability Authenticity Authorization	By utilizing unblocked ports 80/443 to pass through firewall

4. PROPOSED SOLUTION

Lot of researches related to IoT security had be done so far, but not so many exclusively to SM@RT HOME security.

Bitdefender [18], Symantec [19], University of Michigan [20], and ENISA [1] [10] [21], for instance, took SM@RT HOME concept into consideration seriously, and published their research findings in research papers and periodic. In most cases, researches are focused on a few related issues, rarely to system overall.

It is really hard to address all those security threats and challenges. Only holistic approach to all aspects of SM@RT HOME, from design phase to the end of life cycle, can reach the aim to make our homes smarter, and our lives more comfortable, with simultaneously reduced risk of security breaches.

To reach that aim some prerequisites have to be fulfil:

- All stakeholders has to be actively involved in process.
- Policy makers and regulatory bodies has to change legal framework, and to adopt minimum requirements for standards, policies, guidelines etc.
- Industry has to be much more engaged in security (in making and introducing open standards), not only in upgrading functionalities and advertising of their products.
- Implementation and configuration has to be well explained as for dummies.
- End users has to be much more educated to be aware of security threats and their impact to their privacy, data, health and so on.

ISO/IEC 27001 [22] is good start in term of for risk management cycle. It covers planning an information security management system, risk assessment, and risk treatment. Additionally, well balanced combination of awareness, enforced with digital forensic enablers, like loggers, NextGen Firewalls [23], and trusted relation system can bring SM@RT HOME security to much higher level.

Unfortunately, most of SM@RT Home, and generally IoT industry argue there is no reason for implementation of advanced security in inexpensive products, like stated in [1]. They claim, that will raise up production costs and market price, and made products less affordable and less interesting. Furthermore, they still negate that IoT solutions including SM@RT HOME, are not targeted by hackers.

Some end-users argue there is no necessity for security measures implementation in Home Area Network, they ask for simplicity over security. They are refusing to learn how to configure system; they just like to have simple plug-and-play-and-forgot equipment. Those people does not take a care about privacy and security, either because they have lack of awareness, or they does not accepting at all that they can be a target of cyber-attack.

5. CONCLUSION

Even SM@RT HOME solutions are suddenly everywhere, security has been identified as important issue which is paying more attention by all, researchers, developers and native users. In this paper, we discussed SM@RT HOME solutions and identified key security issues, we also proposed key prerequisites to be fulfilled in developing new approaches and security models.

In addition to that, we conducted a review of recent literature on already identified security threats and possible attacks directly violating key security goals and principles. However, balance between simplicity and security should be maintained. SM@RT HOME solutions have to be planned, implemented and configure with that in mind. Only with this holistic approach SM@RT HOME will reach the ultimate aim to make our homes smarter, and our lives more comfortable with keeping security on desire level.

Acknowledgements. Research presented in this paper is conducted within the TEMPUS project ‘Enhancement of Cyber Educational System in Montenegro (ECESM)’, project no. 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES.

REFERENCES

- [1] ENISA, “SECURITY AND RESILIENCE OF SMART HOME ENVIRONMENTS, GOOD PRACTICES AND RECOMMENDATIONS”, DECEMBER 2015, ISBN: 978-92-9204-141-0 | DOI:10.2824/360120
- [2] THE EUROPEAN COMMISSION, “CONCLUSIONS OF THE INTERNET OF THINGS PUBLIC CONSULTATION “, PUBLISHED ON [HTTPS://EC.EUROPA.EU/DIGITAL-SINGLE-MARKET/NEWS/CONCLUSIONS-INTERNET-THINGS-PUBLIC-CONSULTATION](https://ec.europa.eu/digital-single-market/news/conclusions-internet-things-public-consultation) , AS ON AUGUST 31TH 2016
- [3] PACIFIC CUSTOM CABLE INC. “X10 HOME AUTOMATION TUTORIAL” [HTTP://WWW.PACIFICCABLE.COM/X10_TUTORIAL_5.HTML](http://www.pacificcable.com/X10_TUTORIAL_5.HTML)
- [4] JASON BAKER (RED HAT), “5 OPEN SOURCE HOME AUTOMATION TOOLS”, ARTICLE, [HTTPS://OPENSOURCE.COM/LIFE/16/3/5-OPEN-SOURCE-HOME-AUTOMATION-TOOLS](https://opensource.com/life/16/3/5-open-source-home-automation-tools)
- [5] ARDUIONO PROJECT HUB, “SMART HOME MINI ARDUINO – IN 30 MINUTES”, PUBLISHED ON [HTTPS://CREATE.ARDUINO.CC/PROJECTHUB/ANDREMENDES/SMART-HOME-MINI-ARDUINO-IN-30-MINUTES-POSTING-IN-UBIDOTS-224F0A](https://create.arduino.cc/projecthub/andremendes/smart-home-mini-arduino-in-30-minutes-posting-in-ubidots-224f0a)
- [6] “HOW TO BUILD A RASPBERRY PI SMART HOME”, TUTORIAL, PUBLISHED ON [HTTPS://WWW.PUBNUB.COM/BLOG/2015-08-04-TUTORIAL-BUILDING-RASPBERRY-PI-SMART-HOME-PART-1/](https://www.pubnub.com/blog/2015-08-04-tutorial-building-raspberry-pi-smart-home-part-1/)
- [7] OPENHAB FOUNDATION , OPENHAB PROJECT HOMEPAGE [HTTP://WWW.OPENHAB.ORG/](http://www.openhab.org/), GitHub
- [8] HOME ASSISTANT, OPEN SOURCE HOME AUTOMATION PLATFORM, HOMEPAGE, [HTTPS://HOME-ASSISTANT.IO/](https://home-assistant.io/), GitHub
- [9] SMART HOME ENERGY, LONDON, UK, “WHAT IS SMART HOME?”, [HTTP://SMARTHOMEENERGY.CO.UK/WHAT-SMART-HOME](http://smarthomeenergy.co.uk/what-smart-home)
- [10] ENISA, “THREAT LANDSCAPE AND GOOD PRACTICE GUIDE FOR SMART HOME AND CONVERGED MEDIA”, DECEMBER 2014
- [11] INTERNET ENGINEERING TASK FORCE (IETF), “REQUEST FOR COMMENTS: 7228 - TERMINOLOGY FOR CONSTRAINED-NODE NETWORKS”, MAY 2014, ISSN: 2070-1721
- [12] R. J. ROBLES1, T. KIM, „A REVIEW ON SECURITY IN SMART HOME DEVELOPMENT“, INTERNATIONAL

[13] ANGUS WONG, ALAN YEUNG, "NETWORK INFRASTRUCTURE SECURITY", EBOOK, ISBN 978-1-4419-0166-8

[14] V. ARAVINTHAN, V. NAMBOODIRI, S. SUNKU, W. JEWELL, "WIRELESS AMI APPLICATION AND SECURITY FOR CONTROLLED HOME AREA NETWORKS," POWER AND ENERGY SOCIETY GENERAL MEETING, 2011 IEEE, PP.1-8, 24-29 JULY 2011

[15] KOMNINOS, N., PHILLPOU, E. & PITSILLIDES, A. (2014), "SURVEY IN SMART GRID AND SMART HOME SECURITY: ISSUES, CHALLENGES AND COUNTERMEASURES.", COMMUNICATIONS SURVEYS & TUTORIALS, PP(99), DOI: 10.1109/COMST.2014.2320093

[16] R.ŠENDELJ, I.OGNJANOVIĆ, "SEMANTICALLY ENHANCED CYBER SECURITY OVER CLOUDS: METHODOLOGICAL APPROACH", INTERNATIONAL JOURNAL OF ADVANCES IN COMPUTER NETWORKS AND ITS SECURITY, 2014, VOL 4, NO.3, ISSN: 2250-3757

[17] TUHIN BORGHAIN, UDAY KUMAR, SUGATA SANYAL, "SURVEY OF SECURITY AND PRIVACY ISSUES OF INTERNET OF THINGS", RESEARCH PAPER,

[HTTPS://ARXIV.ORG/FTP/ARXIV/PAPERS/1501/1501.02211.PDF](https://arxiv.org/ftp/arxiv/papers/1501/1501.02211.pdf)

[18] BITDEFENDER, "THE INTERNET OF THINGS: RISKS IN THE CONNECTED HOME", RESEARCH PAPER, PUBLISHED FEBRUARY 2016

[19] MARIO BALLANO BARCENA AND CANDID WUEEST, "SECURITY RESPONSE; INSECURITY IN THE INTERNET OF THINGS", RESEARCH PAPER, SYMANTEC, MARCH 2015

[20] EARLENCE FERNANDES, JEAYEON JUNG AND ATUI PRAKASH "SECURITY ANALYSIS OF EMERGING SMART HOME APPLICATIONS", RESEARCH PAPER, IN PROCEEDINGS OF 37TH IEEE SYMPOSIUM ON SECURITY AND PRIVACY, MAY 2016

[21] ENISA, "ENISA THREAT LANDSCAPE 2015", JANUARY 2016

[22] ISO/IEC 27001:2013 "INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - INFORMATION SECURITY MANAGEMENT SYSTEMS - REQUIREMENTS"

[23] PATRICK SWEENEY, "NEXT-GENERATION FIREWALLS: SECURITY WITHOUT COMPROMISING PERFORMANCE", ARTICLE, TECHREPUBLIC, [HTTP://WWW.TECHREPUBLIC.COM/BLOG/IT-SECURITY/NEXT-GENERATION-FIREWALLS-SECURITY-WITHOUT-COMPROMISING-PERFORMANCE/](http://www.techrepublic.com/blog/it-security/next-generation-firewalls-security-without-compromising-performance/)

MULTIMODAL BIOMETRIC AUTHENTICATION IN IOT: SINGLE CAMERA CASE STUDY

NEMANJA MAČEK

School of Electrical and Computer Engineering of Applied Studies, Belgrade and SECIT Security Consulting,
nmacek@viser.edu.rs

IGOR FRANČ

Belgrade Metropolitan University, Faculty of Information Technologies and SECIT Security Consulting,
igor.franc@metropolitan.ac.rs

MITKO BOGDANOSKI

Military Academy General Mihailo Apostolski, Skopje, Macedonia, mitko.bogdanoski@ugd.edu.mk

ALEKSANDAR MIRKOVIĆ

eSigurnost Association, Belgrade and SECIT Security Consulting, amirkovic@secitsecurity.com

Abstract: This paper presents an approach to multimodal biometric authentication using face and iris biometric traits. Having in mind that variety of devices, such as laptops, smartphones and tablets have a high quality camera built in, it is possible to obtain images of iris and face simultaneously. By combining geometric and photometric techniques, such as fiducial point localization and Gabor filtering, features are extracted and biometric templates are generated. Generated templates are further used to identify and authenticate the user on any device which he is allowed to use, thus replacing the standard username – password authentication scheme with a single camera shot.

Keywords: Biometrics, Authentication, Iris, Face

1. INTRODUCTION

According to ITU-T Y.2060 recommendation, Internet of things (IoT) is defined as a global infrastructure for the information society, enabling advanced services by interconnecting physical and virtual things based on existing and evolving interoperable information and communication technologies, while the thing is defined as an object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks [1]. According to Gartner, Inc., 6.4 billion connected things will be in use in 2016, while approximately 20 billion devices on the IoT is expected in year 2020 [2].

Most of the criticism and controversies regarding IoT are related to privacy, autonomy, control and security of things. Variety of researchers have explored these areas, and many interesting results are reported in a literature. As an example, a report that states that the privacy of households using smart home devices could be compromised by analysing network traffic [3] is a bit spooky. Perera et al. have identified user consent, freedom of choice and anonymity as major privacy challenges in the IoT domain [4], which led to Privacy by Design principle being enforced in some applications, such as British Government smart metering program.

So where does the biometry fit in the IoT? It fits as a technology that can remove certain privacy and security issues off from some devices. Biometrics is defined as the science of establishing the identity of an individual based

on physical, chemical or behavioural attributes of the person [5]. Due to distinctive nature of biometric traits and non-repudiation it offers, biometrics is frequently used to enhance the overall security of the system it is implemented in [6]. Biometric authentication offers the ease and convenience users want and the verification enterprises and manufacturers require for IoT because it is able to verify the true identity of the user. There are various industries in which biometrics can be integrated, ranging from smart homes, to the automotive industry, banking, and healthcare. According to Gartner, Inc., 30% of organizations will use biometric authentication for mobile devices by year 2016, while biometric sensors, such as premise security entry consoles, will total at least 500 million IoT connections in year 2018 [7]. Acuity Market Intelligence forecasts that within three years, biometrics will become a standard feature on smartphones as well as other mobile devices [8].

2. PROPOSED AUTHENTICATION SCHEME

Two most common authentication methods are single-factor passwords or PINs and multi-factor authentication, such as a card combined with a PIN. Both having their drawbacks, such as losing cards or forgetting passwords made a clean path for biometrics to emerge as a new way of granting physical or logical access securely and conveniently. Biometrics can provide both single-factor and multi-factor authentication, and, having that said, one can differentiate two types of biometric systems: unimodal and multimodal. Unimodal systems employ single biometric sample, such as face or fingerprint. Multimodal

systems employ two or more modalities belonging to a same person, such as face and fingerprint. Many consider unimodal biometrics still not to be secure enough because of the limitations in biometric technology or using low cost sensors. Employing two or more modalities increases recognition accuracy, strengthens the proof [9], and reduces false rejection rates (FRR) and false acceptance rates (FAR). Multimodal biometric systems are based on information fusion that can be performed on several levels, typically at feature, match score or decision level.

Alternative approach to multimodal biometrics is presented in this paper: it is the replacement of typical username – password authentication method with two different biometric samples belonging to the same individual. For example, a user’s face can be captured by a camera and by using Principal Component Analysis his identity can be determined. This equals providing a username to a system. Once identified, a user provides a fingerprint to a sensor and a system verifies the generated template with one stored in the database belonging to that user. This equals verifying a password that user have provided to a system. If user is successfully identified and verified, access is granted. With high quality cameras available on many devices, two biometric samples can be captured simultaneously: face and iris. The system presented in this paper is based on aforementioned authentication scheme and employs face and iris samples captured by a high quality camera. The efficiency of proposed approach is experimentally evaluated using CASIA databases, collected by the Chinese Academy of Sciences' Institute of Automation [10].

3. IMPLEMENTATION: FACE AND IRIS

The proposed authentication scheme employs two images obtained by a single high quality camera. The image of the face is used to identify the user and the image of the iris is further used to verify the identity.

Face recognition is convenient, non-intrusive authentication method. There are various feature extraction methods reported in the literature and, roughly, they can be classified either as geometric or photometric approaches. Geometric approaches are based on developing the model based on geometric distances between fiducial points, while the photometric approaches are based on extracted statistical values [11]. Before the face features are extracted, input image is pre-processed. Pre-processing steps include image size normalization, background removal (region of interest selection), translation and rotational normalizations and illumination normalization. Normalization increases system robustness against posture, facial expression and illumination. Pre-processing is crucial as the robustness of a face recognition system greatly depends on it. The photometric normalization techniques used in this research are described in [12].

Gabor wavelets based feature extraction technique is reported to provide good results [13] and according to that is used in this research. Let (x, y) specify the position of a light impulse in the visual field, let θ denote the orientation of the filter and λ, σ, γ , and φ denote the parameters of the wavelet (wavelength, Gaussian radius, aspect ratio and

phase, respectively). A family of family of two-dimensional Gabor kernels [14] is used:

$$W(x, y) = \exp\left(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma'^2}\right) \cos\left(2\pi \frac{x'}{\lambda} + \varphi\right) \quad (1)$$

$$x' = x \cos(\theta) + y \sin(\theta) \quad (2)$$

$$y' = -x \sin(\theta) + y \cos(\theta) \quad (3)$$

The same values that have been reported in [15] are used in this research: orientation θ ranging from 0 to $7\pi/8$ with a step of $\pi/8$, wavelength $\lambda = \{4, 4\sqrt{2}, 8, 8\sqrt{2}, 16\}$, phase $\varphi = \{0, \pi/2\}$, Gaussian radius σ equal to wavelength and aspect ratio $\gamma = 1$.

A set of Gabor filters is used with 5 spatial frequencies and 8 distinct orientations, resulting in 40 different Gabor filters. Filter responses are obtained by convolving these filters with a simple face image, and these representations display desirable locality and orientation performance. When Gabor filters are applied to each pixel of the image, the filtered vector is high dimensional, which further leads to very large computational and storage costs. This problem can be solved without degrading overall robustness by obtaining Gabor features only at ten extracted fiducial points: three on each eye, two on the lips and two on the nose, as shown on Image 2. Fiducial points are extracted by analysis of the chrominance components in the YCbCr colour space: as an example, eyes present high values of Cb and small values of Cr component [16], while the geometric points of nose and mouth are extracted using Sobel filter [17].



Image 1: Fiducial points that Gabor features are obtained on

Each fiducial point will be represented by a Jet vector of n components, where n denotes the number of filters. Having that said, face is represented by a feature vector containing $10n$ real coefficients.

The face recognition process employs multi-layer perceptrons (MLPs). The system employs as many neural networks as much persons we want to identify (see Image

2). Inputs to the each network are Gabor coefficients and distances between fiducial points: the distance between the centres of the eyes, the distance between two eyes, width and height of nose, width of mouth and the distance between nose and mouth. Each network is trained by different samples of the same person obtained by rotation, translation and variation of the lighting and sufficient number of information about different persons. During the identification phase, only one network is allowed to identify the person – output neuron of only one network is allowed to have the positive value. If two or more networks provide positive outputs, the person is considered as not identified and the system repeats the recognition operation.

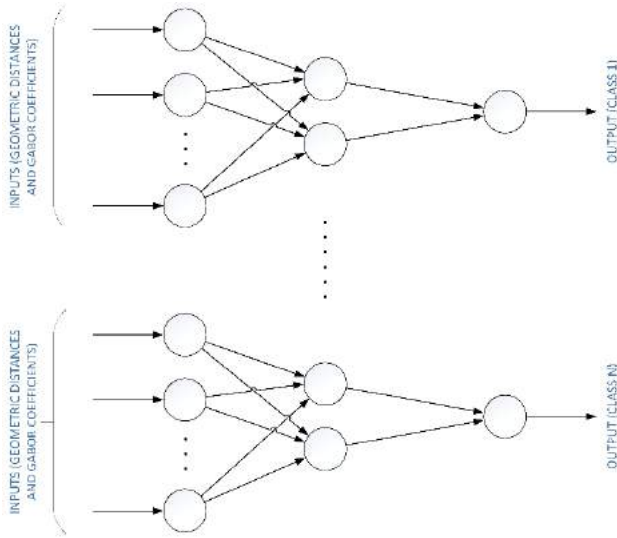


Image 2: Set of neural networks for face recognition

Once the user is identified via neural network face recognition, the system verifies the user by matching the generated iris template with the one stored in the database belonging to that user.

Iris is as first roughly localized from the obtained image in the YCbCr colour space [16] and further pre-processed. Once converted to grayscale, the outer radius of iris patterns and pupils are localized with Hough transform that involves a canny edge detector to generate an edge map. A poorly localized iris will result in unsuccessful segmentation and incorrectly generated biometric template – iris code. Hugh transform identifies positions of circles and ellipses [18]. It locates contours in an n -dimensional space by examining whether they lie on curves of a specified shape. Localization process is presented by Image 3.

Once an iris image is localized, regions of interests are defined and it is transformed into fixed-size rectangular image. The normalization process employs Daugman's rubber sheet model that remaps the iris image $I(x, y)$ from Cartesian (x, y) to polar coordinates (r, θ) [19]:

$$I(x(r, \theta), y(r, \theta)) \rightarrow I(r, \theta) \quad (4)$$

Parameter r is on the interval $[0, 1]$ and θ is the angle $[0, 2\pi]$. If iris and pupil boundary points along θ are denoted by (x_i, y_i) and (x_p, y_p) , respectively, the transformation is performed according to equations (2) and (3):

$$x(r, \theta) = (1-r)x_p(\theta) + x_i(\theta) \quad (5)$$

$$y(r, \theta) = (1-r)y_p(\theta) + y_i(\theta) \quad (6)$$

The rubber sheet model does not compensate rotational inconsistencies. However it produces a normalized representation with constant dimensions (see Image 4) set by angular and radial resolution by taking pupil dilation size inconsistencies into the account [20].

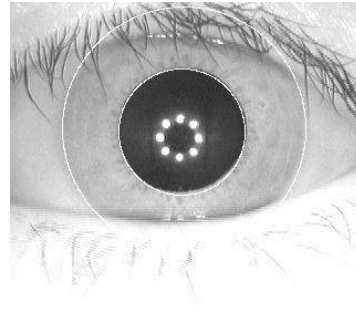


Image 3: Localized iris



Image 4: Normalized iris

There is a variety of iris feature extraction methods reported in the literature, such as Gabor filtering, log-Gabor filtering, zero-crossings of 1-D wavelets and Haar encoding (wavelet method). 1-D log-Gabor filtering is validated as suitable iris feature extraction method in various researches by other authors. A normalized image is broken into a number of 1-D signals that are convolved with 1-D Gabor wavelets. Let f_0 denote centre frequency, and σ the bandwidth of the filter. The frequency response of 1-D log-Gabor filter [21] is given by:

$$G(f) = \exp\left(-\left(\log \frac{f}{f_0}\right)^2 / 2\left(\log \frac{\sigma}{f_0}\right)^2\right) \quad (7)$$

Phase quantization is applied to four levels on filtering outputs (each filter produces two bits of data for each phasor) and the quantized phase data is used to encode an iris pattern into a bit-wise biometric template. The number of bits in the biometric template depends on angular and radial resolution and the number of used filters. Biometric template size used in this research is 9600 bits.

Iris biometric template is generated for each user in the enrolment phase, after training the neural network for face recognition. During the authentication, after successful used identification via face recognition, captured iris image is used to create iris code and measure Hamming distance with the one stored in the database belonging to that user. Let n denote the number of bits in the iris codes x and y of equal length and $n_d(x,y)$ denote number of positions at which the corresponding bits are different. Hamming distance is given by:

$$d(x, y) = \frac{n_d(x, y)}{n} \quad (7)$$

A match is considered to be perfect if $d=0$, while random strings are expected to provide a distance $d=0.5$. For iris codes, identical irises are expected to provide Hamming distance $d=0.08$, while verification is considered to be successful for values $d<0.32$.

4. EXPERIMENTAL EVALUATION

Performance of the proposed solution is experimentally evaluated using MATLAB R2016a (feature extraction and neural networks) and Python 2.7 (iris matching and scripting). As this research does not deal with image capturing hardware, CASIA-IrisV4 and CASIA-FaceV5 databases are used to evaluate the performance of the proposed authentication scheme. 50 randomly chosen subjects were used from CASIA-FaceV5 and each subject was accompanied with a randomly chosen subject from CASIA-IrisV4 Interval database.

The first step of the experiment is training the neural networks for face recognition. 50 MLP neural networks were trained with the 60% of the database subset used as a training set and remaining 40% as a testing set. Experimental results for different number of filters and accompanying orientations are given in the Table 1.

Table 1: Average face recognition rates

Wavelets	Orientations	Accuracy
5	$\theta = \{0\}$	98.2%
10	$\theta = \{0, \pi/8, 7\pi/8\}$	98.7%
15	$\theta = \{0, \pi/4, \pi/2\}$	99.1%
20	$\theta = \{0, \pi/4, \pi/2, 3\pi/4\}$	99.4%
25	$\theta = \{0, \pi/8, \pi/4, \pi/2, 3\pi/4\}$	99.6%

As Gabor wavelets represent feature points in special frequency at different orientations, it was expected that the MLP recognition rates will increase with the number of Gabor wavelets, which is proven with the results presented in Table 1. With 15 or more Gabor wavelets, recognition accuracy is over 99% and is considered to be satisfactory. One should note that if MLP is trained only with geometric distances as inputs, it provides significantly lower recognition accuracy. As an example, recognition accuracy ranging between 79.7% and 84.2% is reported in [22] if geometric distances only are used with neural networks.

The next step in the experiment is verification of the iris. For each successful face recognition attempt a set of 5 irises belonging to that person and a set of 5 irises belonging to a randomly selected imposter was provided to iris matcher. This allowed us to measure overall accuracy as well as FRR rates (the percentage of valid inputs which are incorrectly rejected). Experimental results are given in Table 2 and graphically presented on Images 5 and 6.

Table 2: Overall system accuracy and FRR

Wavelets	Accuracy	FRR
5	97.5%	2.4%
10	97.9%	~2%
15	98.3%	1.6%
20	98.7%	~1%
25	99.1%	0.8%

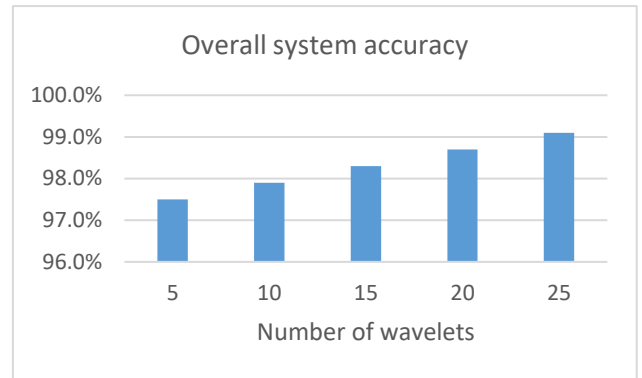


Image 5: Overall system accuracy

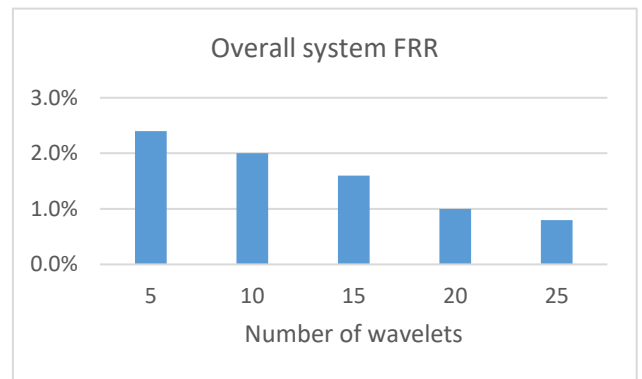


Image 6: Overall system false rejection rates

According to the experimental results we can conclude that the system which operates with face recognition that employs 25 wavelets and iris verification module based on 9600 bit iris code and $d<0.32$ Hamming distance provides 99.1% accuracy and less than 1% false rejection rate. To put it in the simple words, one in a hundred genuine authentication attempts is rejected. Regarding false acceptance rate, it is virtually set to zero as system employs face recognition system that is very hard for imposter to

trick as it employs both geometric and photometric features. Even if an imposter somehow manages to bypass face recognition (for example, an identical twin may somehow manage to do so), a single shot that captures the image will also capture the iris. And iris verification is very hard for an imposter to trick, as this biological trait is considered as one that distinguishes individuals with highest precision. For example, even a twin could not do so, as irises of identical twins differ as much as irises of unrelated persons due to a chaotic colour pattern in the eye and high degree of randomness iris possesses.

5. CONCLUSION

Various commercial products regarding biometrics and IoT exist on the market. For example, HYPR-2 enables one to secure any device with fingerprint, voice, face and eye recognition. Some solutions extend decentralized biometric authentication down to the firmware level, thus securely transforming smart things into biometric things. However, to the best of our knowledge, no commercial products employ multimodal biometrics in a way as it is described in this paper. The proposed solution is not computationally expensive, and does not require tons of storage space. Only one high quality camera is required on the device, and nowadays it can be found on most of smartphones and mobile devices (such as Samsung Galaxy S7 Edge) and users are further allowed to identify themselves and verify the identity using one shot. The only drawback of the proposed solution is the acceptability of iris biometrics and privacy concerns on stored templates. Further work will be focused on additional security countermeasures, such as implementing cancellable biometrics in this authentication scheme, which will preserve the privacy of stored biometric templates. Additionally, authors are about to explore different face recognition methods and see if any of them can improve overall accuracy and reduce processing and storage costs.

REFERENCES

[1] International Telecommunication Union, "Overview of the Internet of things," Recommendation ITU-T Y.2060, June 15, 2012.

[2] Gartner, Inc., "Gartner Says 6.4 Billion Connected Things Will Be in Use in 2016, Up 30 Percent From 2015", Nov. 10, 2015. Last time visited: August 18, 2016.

[3] J. Singh, T. Pasquier, J. Bacon, H. Ko, D. Eyers, David "Twenty Cloud Security Considerations for Supporting the Internet of Things" IEEE Internet of Things Journal. 3 (3): 1–1, 2015.

[4] C. Perera, R. Ranjan, L. Wang, Lizhe, S. Khan, A. Zomaya, "Privacy of Big Data in the Internet of Things Era", IEEE IT Special Issue Internet of Anything, 6., 2015.

[5] A. K. Jain, A. Ross, "Introduction to Biometrics", In "Handbook of Biometrics", A. Jain et al. (Eds), Springer, 2008.

[6] P. Balakumar, R. Venkatesan, "A Survey on Biometrics based Cryptographic Key Generation Schemes", International Journal of Computer Science and Information Technology & Security, Vol. 2, No. 1, pp. 80-85, 2012.

[7] Entertech, "Biometrics to Secure the Internet of Things", Dec. 9, 2015. Last time visited: August 20, 2016.

[8] Acuity Market Intelligence, "Biometric Smartphones Are Officially Mainstream", Published by PR Newswire, Feb 11, 2016. Last time visited: August 20, 2016.

[9] L. Hong, A. K. Jain, S. Pankanti, "Can multibiometrics improve performance?", In Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies, pp. 59-64, NJ, USA, 1999.

[10] Biometrics Ideal Test, <http://biometrics.idealtest.org>

[11] M. H Yang, D. Kriegman, N. Ahuja, "Detecting faces in images: A survey", IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 24, No. 1, pp. 34-58, 2002.

[12] R. Rouhi, M. Amiri, B. Irannejad, "A Review on Feature Extraction Techniques in Face Recognition", Signal & Image Processing: An International Journal (SIPIJ) Vol. 3, No. 6, pp 1-14, 2012.

[13] R. Chellappa, C. Wilson, S. Sorihey, "Human and machine recognition of faces: a survey", Proceedings of the IEEE, Vol. 83, pp. 705-740, May 1995.

[14] N. Petkov, P. Kruizinga, "Computational models of visual neurons specialised in the detection of periodic and aperiodic oriented visual stimuli: Bar and grating cells", Biological Cybernetics, pp 83-96, 1997.

[15] L. Wiskott, J. M. Fellous, N. Kruger, C. Malsburg, "Face Recognition by Elastic Bunch Graph Matching", Intelligent Biometric Techniques in Fingerprint and Face Recognition, Ch. 11, pp. 355- 396, 1999.

[16] R. L. Hsu, M. A. Mottaleb, A. K. Jain, "Face detection in color images", IEEE Trans on Pattern Analysis and Machine Intelligence, Vol. 24, No. 5, pp. 696-706, May 2002.

[17] H. Rowley, S. Baluja, T. Kanade, "Neural Network-based face detection", IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 20, No. 1, pp. 23-38, Jan. 1998.

[18] D. J. Kerbyson, T. J. Atherton, "Circle Detection using Hough Transform Filters", Fifth International Conference on Image Processing and its Applications, Edinburgh, UK, 04 – 06 July 1995, pp. 370-374.

[19] J. Daugman, "How iris recognition works", Circuits and Systems for Video Technology, IEEE Transactions on, 14(1) pp. 21-30, 2004.

[20] G. Amoli, N. Thapliyal, N. Sethi, "Iris Preprocessing", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 2, No. 6, pp. 301-304, 2012.

[21] D. J. Field, "Relations between the Statistics of Natural Images and the Response Properties of Cortical Cells", Journal of the Optical Society of America, Vol. 4, No. 12, 1987

[22] Y. B. Jemaa, S. Khanfir, "Automatic local Gabor features extraction for face recognition", International Journal of Computer Science and Information Security, Vol. 3, No. 1, pp. 116-122, 2009.

ANDROID FORENSIC USING SOME OPEN SOURCE TOOLS

ISAK MRKAIC

University of Donja Gorica, Humanistic Studies, isak.mrkaic@gmail.com

Abstract: In recent years Android operating system, being installed on huge numbers of smartphones, tablets and other devices, had a breakthrough on the market. Following that success, the need to recover and analyze data from Android OS, became important part of mobile forensics. Consequently, many commercial and open-source mobile forensic tools became available for forensics investigators. The subject of this paper is to present open source-free tools and to illustrate how to forensically recover data from Android based devices.

Keywords: Android OS, forensics, data acquisition, open source forensic tools.

1. INTRODUCTION

Advancement of mobile phones came along with the technological expansion of the 21st century. There has been a substantial increase of production, development and use of smartphone devices in recent years [1]. Consequently, Google's Android operating system is in the lead when compared to the competition: in 2015 Android operating system's market share has risen to 81.2%, while the competing systems like IOs, Windows and others took up 15,8%, 2,2% and 0.8% respectively [2]. Given that smartphones are used to exchange messages, emails, photos, etc. and that the considerable amount of data stored on them could be acquired and analyzed, forensics of mobile devices became a substantial segment of digital forensics in general.

Mobile phones are frequently used in criminal activities, so the law enforcement services consider them to be a significant source of evidence. The Boston Marathon bombing [3], uncovering of a child prostitution ring [4], attempt of bomb attack on Times Square in New York [5] and similar cases are just a few of numerous examples of mobile forensics and Android forensics used to investigate criminal activities.

The market offers some commercial programs that could be used to carry out a part of the forensic process related to the acquisition and analysis of the data from Android mobile devices. In spite of that, there is also a vast number of the open source tools that could be used to carry out certain forensic tasks. The hypothesis we set for this research is that the combination of various open source tools could be used to acquire a certain amount of data from Android devices, which, when analyzed, could be used as valid evidence in court of justice. Using these tools would cut down the expenses of buying the commercial software and enable forensic scientists to gain additional insights into Android forensics given that open source solutions require "step-by-step" approach.

In this paper we elaborate on one of the models of the forensic process and then we offer the framework of a possible realization for the part of the forensic process that is related to data acquisition and analysis. Having this framework in mind, concrete open source tools were used

to retrieve certain data from the tested mobile device. The retrieved data was then processed in the adequate programs.

Limitations of this research relate primarily to the fact that just one model of the phone with the Android operating system installed was tested. This limitation also reflects one of the greatest challenges mobile phone forensics faces: multitude of mobile phone models, operating systems and their versions on the market. Also we have only focused on some data we considered important (sms messages, call logs, emails...), so we haven't explored all of the potential of given open source tools.

We cannot safely claim that the given data could be used as valid evidence in court of justice given that this largely depends both on legislation of the country where a trial is conducted and the concrete forensic process.

Regardless of the limitations, some of the tools examined could be used in the actual forensic processes and they would be applicable to all the versions of Android and some other operating systems.

2. METHODOLOGY OF THE FORENSIC PROCESS

Forensic investigation on mobile devices comprises of the procedures which are defined by the phases that should be completed in order to round out the forensic process. It could be stated that there are no univesally accepted procedures, so they vary depending on the author's preference. Consequently, different methodologies of the forensic process have developed over the years.

In 2011 the group of scientists developed one of the all-encompassing models which also proved to function excellent in practice. This model, is known as **SRDIFM (Systematic digital forensic investigation model)** [6].

During the **preparation phase** the investigator gets familiar with the case and makes proper preparations. Following the preparation phase is **securing the scene**, then **survey** and **recognition** which imply making the initial plan as to how to collect and analyze the data. **Documentation of scene phase** comprises of making a

sketch map of investigated area and documenting all of the electronic devices on site, including the device itself with its equipment. Once this phase is completed, it is necessary to do **communication shielding**, i.e. to prevent the device from connecting to any mobile network, WiFi, etc. RF isolation, Faraday shielding, cellular jammers, which is followed by **collection** of all the available evidence. It is recommended to connect the device to the charger immediately. Once evidence is collected, it should be **preserved** and transported for further analysis. Collected evidence is **examined** in the way that analysis and filtering are performed. In addition to that, integrity of the data should be secured. During the **analysis** phase the results obtained in the previous phases are used to perform a thorough technical review of the evidence. This phase also sees use of the techniques more advanced than those used in the research phase. This level also implies the analysis of the hidden data, file recovery as well as file decryption. All the results obtained must be documented in order to complete the final report which sums up the entire process in the **presentation** phase. Finally, the results obtained are publicly shown [6] [7].

Reliability of the data depends directly on the methodology of the forensic process. Leaving any of the phases out during the investigation results in unreliable digital evidence which will not be valid in court of justice. As we have already stated before, there is no universal standard of the forensic process on mobile devices. It is up to a forensics scientist which model he will use and apply during the investigation. In this paper we will focus on the phases of research and analysis, i.e. we will explain ways of taking certain data from a confiscated device which is considered as evidence, as well as ways of processing the data in adequate programs thus making them usable for further presentation.

3. DATA ACQUISITION

Completing a forensic process requires preparation of the proper work environment. For that purpose one must own a personal computer of the adequate performances that is free from malicious programs and which has installed a software needed for the forensic work. Some of the programs needed are Android studio i Android Software Development Kit (SDK), mobile device drivers and tools for the work of the forensics scientist. It is recommended to use the original cables of the device on which we perform acquisition to connect it to the computer.

Depending on the possibilities, several methods of acquisition could be used. The first, and the simplest one is the manual acquisition in which the investigator searches the menu of the phone and examines the files that are accessible in user interface thus collecting data. Limitation of this method is that the investigator only accesses the data visible through user interface. The second method, called logical acquisition is performed by extracting data from the file systems which are visible on logical store of the mobile device. This method usually does not allow recovery of the data erased, or allows it to a limited extent. Physical acquisition is the most detailed and the most complete type of file extraction since it implies making a copy of the entire memory content [8].

Data obtained using these methods are often in form of unprocessed data and after the extraction is complete, several actions are performed in order to obtain information which is understandable and readable. Further investigation is done using the copy of the data which are obtained by acquisition, thus securing the integrity of the original data on the mobile device.

Copies of the taken data will be processed in an adequate forensic program. Data we aim to obtain are general phone data, contacts, call logs, sms messages, internet search history, social network applications (skype, viber, facebook) data, email messages, photos, video recordings, etc.

Files obtained by using these methods are then processed in programs that extract useful data for further analysis.

4. PRACTICAL ASPECT FRAMEWORK

The first step, as we have already stated, is to form a forensic work station and to install the required programs that are to be used during the data acquisition and processing. Following that is identification of the adequate cable to connect the device to the PC work station, then installation of the drivers for the mobile device which is the object of investigation. There is always a possibility that the Android version was changed or modified by the manufacturer, so it is highly recommended to download the drivers directly from their website. Once the adequate drivers and the cable are provided, the Android device is connected to the work station. While setting a connection up, the mobile device itself offers the options for the type of protocol it will use to communicate with the PC work unit. The latest models of Android use either Media Transfer Protocol (MTP) or Picture Transfer Protocol (PTP).

One of the challenges that could be faced during the extraction of data is how to unlock the phone protected by the PIN code or some other kind of protection. There is no such thing as the universal method of going around these protections. As is the case with majority of mobile phones, the protection related data is stored on **logical locations** and they can be **taken over** using the pull command, and then extracting the protection related data from the downloaded files [9].

Any further work requires Android Debugging Bridge (ADB) which is installed within Android Studio and Android SDK. If ADB is to work, we need to select the option USB Debugging on the mobile device thus enabling it to communicate with the PC. This option is usually found within Settings-Developer options in the phone menu.

Once the Android phone is successfully connected to the PC, ADB is started and the command adb.exe. devices or adb devices enables us to find out if the device is properly connected. The possible statuses we get after the given command is issued: offline – the device is not properly connected, i.e. there is a problem in communication, device- the device is properly connected and no device which means that device is not connected to the PC [10].

Once we set the connection up, the extraction of data from the Android device could be started. Adb shell

command enables us to access the Android shell further manipulation of the device. It is recommended to provide root access to the phone if possible. Further work requires the knowledge of the basic commands-functionalities that would be used. Some of the commands needed are:

adb pull – used for transfer of files from the mobile device to the forensic station – PC. It is important to note that the access to the majority of important files requires root privileges [11] [12].

dd – this command is used to make a bit-by-bit copy of the device, i.e. for the physical acquisition of data. Copied data is transferred to a separate SD card which is forensically clean. If we try to copy the files to the existing SD card in the phone we will make changes to the original data. Upon creating a file –data.img with the copy of the data in the card, we can transfer it to the PC by using the **pull** command or taking the card out and inserting it into work station. If we don't have a forensically clean SD card, the file could be directly transferred to the PC while its being created. This is done by using netcat and nandump programs [13].

Once the copy of data from a mobile phone is created, the data is processed using various programs. For this purpose the program Autopsy, which is considered to be one of the standard programs when it comes to data analysis, could be used. There are also other options such as SQLite browser, SQLite forensic explorer etc. There are also open source solutions which automatize the process and perform the complete acquisition and analysis. One of these programs is NowSecure Forensics Community Solution.

5. THE RESEARCH

For the purposes of this research we used the phone Alcatel One Touch 6012x with Android version 4.2.2 (Jelly Bean). The working station is a laptop Dell Inspiron 15, 4 GB RAM, 32-bit Operating System, Intel Pentium 3558U, with Windows 7, SP 1 installed on it.

A. Connecting To The Android Device

We connected the device with the original cable to the laptop and then turned on USB Debugging option. Given that this option was not available in the Settings menu, we turned it on by clicking several times on the option **Build number** in the **Settings-About** phone menu. That gave us access to the Developer menu and the option USB Debugging became available.

Once activating the option, we started the adb program to check whether the Alcatel had proper communication with the laptop. Since the device was connected, the command and the response were as follows:

```
C:\Program Files\Android\platform-tools>adb.exe devices
List of devices attached
* daemon not running. starting it now on port 5037 *
* daemon started successfully *
7LLFIRZPR4JZR8BI device
```

B. Unlocking The Phone

To unlock the phone we used the program Andriller [14] which, apart from the other options, offers this possibility

as well. It is a commercial program with the possibility of the free license for the 15 day period, upon expiration of which the program must be purchased. It is free for a six month period for the law enforcement officers. To unlock the phone, we processed the file gesture key with the above mentioned program. The gesture key we previously acquired from the phone through the pull command. After executing the command, we obtained the actual unlocking pattern (Image 1).

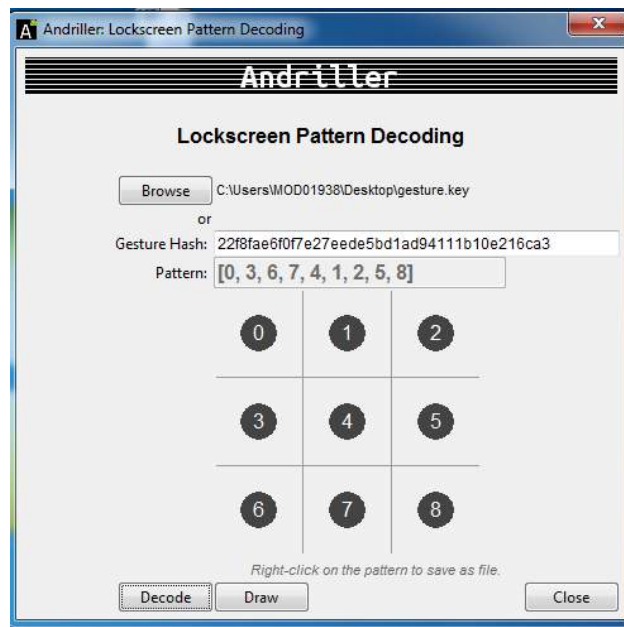


Image 1: Lockscreen pattern decoding

Open source solution would be to open the gesture file in hex editor, and then use SQLite Browser so as to compare the hash values of gesture.key with generated hash values of possible keys in order to get the unlocking pattern. The scripts could be generated in Python [9].

C. Rooting The Phone

Root access to the phone we gained after downloading the application KingRoot from google play and installing it directly on the phone. After installing it we connected to the device through ADB and then executed the command adb shell to enter the user account. Upon executing the command, we got the option to allow root access to adb application. Once we allowed it, we had the root access to the device and # appeared in shell (Image 2).

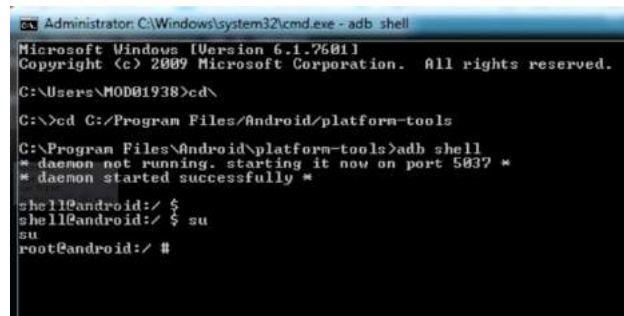


Image 2: Accessing shell as "root" user

D. Data Acquisition

The first method of acquisition was realized through using adb pull command which enabled us to copy the data from the folder to the destination folder on the C partition.

adb pull /data/data C:/forenzika/seminarski

The folder contained the data that could be interesting for further inspection:

- data from the SIM card which are stored on logical destination
/data/data/com.android.providers.telephony/databases/mmssms.db.

- data from the SIM card about contacts and call logs
/data/data/com.android.providers.contacts/databases/contacts2.db.

- data from the SIM card about email messages on gmail which were acquired from
/data/data/com.google.android.gm/databases/mailstore.isak.mrkaic@gmail.com.db.

The other method was realized through executing **dd** command. We inserted the empty SD card in the phone and the device recognized it. The command **#cat /proc/partition** was executed to learn about the existing partitions, which made us decide to acquire the contents of the flash memory **mmcblk0**

Next step was to execute the command

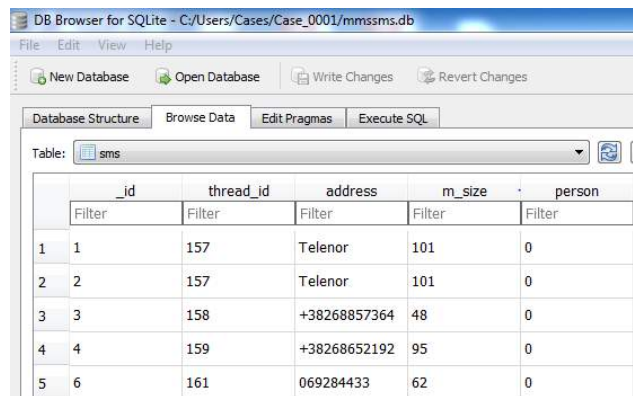
dd if=/dev/block/mmcblk0 of=/sdcard/data.img bs=512 conv=notrunc,noerror,sync

After the command was executed, the file **data.img** was created on SD card along with the folders android_secure, Android, googleota, KingMaster, LOST.DIR i e_config. We copied the files to the laptop simply by taking out the SD from the phone, inserting it into the SD card adapter and then inserting the adapter into laptop and copying the files to the D partition.

E. Data Analysis

The data acquired through logical acquisition, i.e. through executing the pull command, were processed by SQLite Browser [15] which enabled us to read **.db** files that seemed to be of interest to us

- **mmssms.db** file contained data about all of the sent and received SMS messages. More precisely, it included the phone numbers of both the sender and the receiver of the message, the date when it was sent, the message status (whether or not it was received), as well as the content of the message (Image 3).



The screenshot shows the SQLite Browser interface for a database named 'sms'. The table has the following structure:

	_id	thread_id	address	m_size	person
1	1	157	Telenor	101	0
2	2	157	Telenor	101	0
3	3	158	+38268857364	48	0
4	4	159	+38268652192	95	0
5	6	161	069284433	62	0

Image 3: SMS messages

- The file **contacts2.db** contained data about the call logs, namely the phone number of the caller and the receiver, call duration and the date when the call was made.

- The file **mailstore.isak.mrkaic@gmail.com.db** contained the data about gmail messages including the address of both the sender and receiver, time when the message was sent and the message content.

The data we got through physical acquisition of the flash memory acquired through dd command were analyzed using the program Autopsy [16]. This program is a free one and is intended for the analysis of majority of the files on Android (such as YAFFS, .ext, etc.).

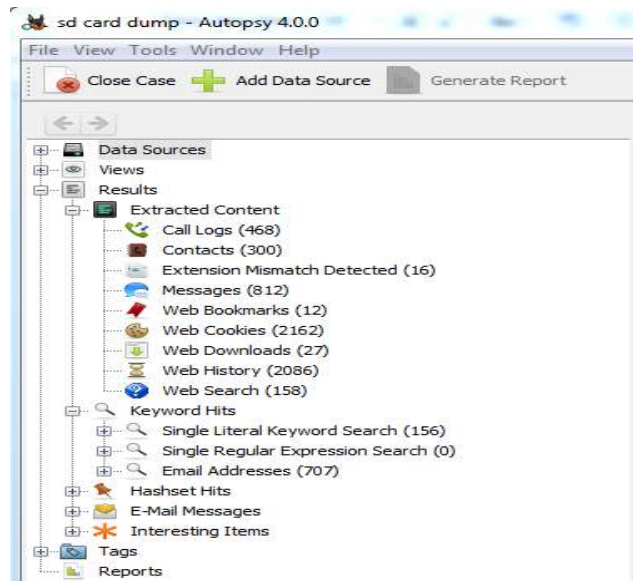


Image 4: Data acquired through Autopsy

As the result of the actions performed, we could access contacts, call logs, messages, etc., but also some of the files erased (Image 4).

F. Other Tested Open Source Tools

AF Logical OSE [17] is the program intended for data extraction through Content Provider. This program enables us to acquire some basic data such as SMS/MMS, contacts, logs, calendar, etc.. By using this program we managed to get the data about the SMS messages, call logs and contacts (Image 5).

ID	number	date	duration	type	new	name	number	numberlabel
1	12848	38269121073	1466668576450	130	2	0	jeca	2
2	12849	38269121073	1466671120943	9	2	0	jeca	2
3	12850	69689769	1466671689902	29	2	0	Spiki Nov	2
4	12851	68857384	1466672490342	330	1	0	BakocM	2
5	12852	69634819	1466673303941	7	1	0	Tata	2
6	12853	69634819	1466673346163	71	2	0	Tata	2
7	12854	38269121073	1466675348239	60	2	0	jeca	2
8	12855	69689769	1466678618602	0	3	0	Spiki Nov	2
9	12856	69121073	1466679641551	0	1	0	jeca	2
10	12857	69121073	1466679672060	0	2	0	jeca	2
11	12858	69689769	1466679708348	27	2	0	Spiki Nov	2
12	12859	69121073	1466679764009	0	2	0	jeca	2
13	12860	69121073	146667992031	0	1	0	jeca	2
14	12861	69121073	1466680070974	365	2	0	jeca	2
15	12862	69689769	1466682618064	43	2	0	Spiki Nov	2
16	12863	69634819	1466685729833	0	1	0	Tata	2
17	12864	69634819	1466685770569	20	2	0	Tata	2

Image 5: Call history

For logical acquisition and analysis of data we used program **Mobledit** [18], version 5.5.0.1148, which enables us to work in Lite regime if we don't want to buy the license. However, there are also some limitations, such as inability to export the files. Upon the installation and command execution we managed to set up a successful communication between the laptop and the Android device, so we could access the basic information about the SIM card, search the contacts, call logs, SMS i MMS messages and access the calendar.

NowSecure Forensics Community Solution [19] (up until a year ago it was called **ViaExtract**) is a tool which enables logical and physical acquisition of data. Its manufacturer is NowSecure. Free version enables logical extraction of data, while the purchased version enables both logical and physical extraction. The program is downloaded within the virtual surrounding and is installed on Santoku linux based on Ubuntu distribution. After being started, the program automatically recognized the mobile device This program also offers the option to root the phone by using certain exploits. After starting it, we proceeded to start Backup acquisition, Logical acquisition and File acquisition (Image 6).

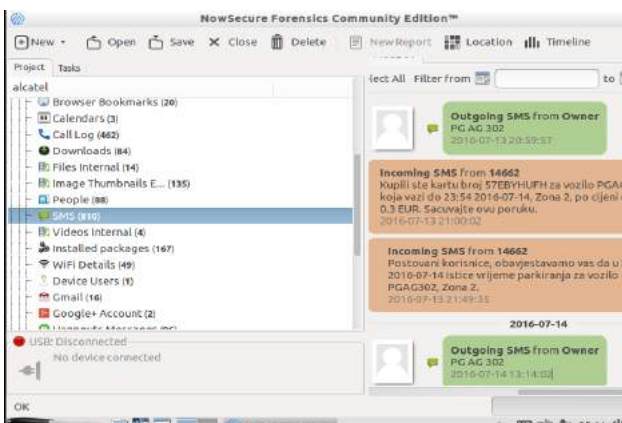


Image 6: SMS messages

NowSecure Forensics Community Solution is a great free tool which enables us to acquire a lot of data in short period of time.

6. RESULTS

On the phone that was used for testing we performed logical and physical acquisition of data, and then the analysis of the results obtained. The programs used as well as their basic characteristics are outlined in the table below.

Table 1: Comparative analysis of programs characteristics

Program	Acquisition	Analysis
NowSecure Forensics	Yes	Yes
Community Solution		
ADB (pull, dd)	Yes	No
Autopsy	No	Yes
SQLite browser	No	Yes

The most complete data from the device that was the object of our research were retrieved through the NowSecure program which performed the acquisition and the analysis automatically, yet it was not possible to extract the results from the program to the PC. Similar results were obtained by step-by-step acquisition by using dd functionality and then analyzing the file obtained using the programs Autopsy and SQLite browser, however it was possible to extract the data to the PC.

Table 2: Comparative overview of the results

Data retrieved	NowSecure (Backup, Logical and File acquisitions)	dd, SQLite browser and Autopsy
Audio	59	76
Images	270	506
Videos	4	4
Deleted data	-	66220
Viber Calls	513	513
Viber Participants	458	458
Viber Messages	9072	9072
Web History	20	2086
Contacts	36	300
Call Log	462	468
SMS	810	812

Gmail messages	16	16
----------------	----	----

The comparative overview of the data retrieved is given in the table above. The overview does not include all the data, just those we considered to be the most important. Based on the results, we can safely claim that a significant amount of data can be retrieved by using the open source tools.

7. CONCLUSION

This paper explores open source tools which enable data acquisition and analysis. Even though there is a multitude of these forensic tools, they are all limited in their functionalities and it is only by their combination that we can get satisfactory results.

Android forensics using open source tools is a challenging task and it largely depends on the tools available. Commercial programs like Encase i Oxygen Forensic™ Suite are user friendly and they offer a wide range of possibilities. Unlike them, open source programs must be used in combination to achieve comparable results. Limitations of the open source tools are reflected in the fact that they cannot offer ready solutions. Namely, after certain programs are used to perform acquisition and analysis, it is preferable to use a combination of different programs to compare and consolidate the data if the results obtained are to be valid. Also, majority of the open source tools are limited in their functionalities, so it happens that the analyzed data cannot be retrieved, or some functionalities only have trial versions. This in turn requires more time for extraction and analysis of data, then it is the case when commercial tools are being used. Having expansion of the Android platform in mind, it is expected that the number of available forensic tools will rise in near future and their functionalities would develop. In this paper we used the latest researches and the up-to-date literature, yet some links to the forensic software already became unavailable or outdated.

One of the examples is how the program NowSecure which we used for the purposes of our research is no longer available on the manufacturer's site. In the light of these facts, it is obvious forensicists, apart from having the knowledge of the field must also constantly follow trends and latest findings in the field

REFERENCES

- [1] <http://www.statista.com/statistics/263441/global-smartphone-shipments-forecast/>, Accessed August 01, 2016.
- [2] <http://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/>, Accessed August 01, 2016.
- [3] <http://forensicstore.com/the-boston-marathon-how-smartphones-are-changing-investigations>, Accessed August 01, 2016.
- [4] <http://forensicstore.com/taking-down-child-prostitution-rings/>, Accessed August 01, 2016.
- [5] <http://www.forensicon.com/forensics-blotter/cell-phone-email-forensics-investigation-cracks-nyc-times-square-car-bombing-case/>, Accessed August 01, 2016.
- [6] Soufiane Tahiri, Mastering mobile forensic, Packt Publishing 2016., page 5.
- [7] Ankit Agarwal, Megha Gupta, Saurabh Gupta & Prof. (Dr.) S.C. Gupta, "Systematic Digital Forensic Investigation Model", International Journal of Computer Science and Security (IJCSS), Volume 5, Issue 1, 2011, Available: <http://www.cscjournals.org/manuscript/Journals/IJCSS/Volume5/Issue1/IJCSS-438.pdf>
- [8] Rohit Tamma, Donnie Tindall, Learnig Android Forensic, Packt Publishing 2015., page 8.
- [9] Rohit Tamma, Donnie Tindall, Learnig Android Forensic, Packt Publishing 2015., pp 128-136.
- [10] Rohit Tamma, Donnie Tindall, Learnig Android Forensic, Packt Publishing 2015., page 50.
- [11] <https://developer.android.com/studio/command-line/adb.html>, Accessed August 06, 2016.
- [12] Andrew Hoog, Android Forensics: Investigation, Analysis and Mobile Security for Google Android 1st Edition, Syngress, 2011.,page 218.
- [13] Rohit Tamma, Donnie Tindall, Learnig Android Forensic, Packt Publishing 2015., pp 147-152.
- [14] <https://andriller.com/downloads>, Accessed 08. July 2016.
- [15] <http://sqlitebrowser.org/>, Accessed 08. July 2016.
- [16] <http://www.sleuthkit.org/autopsy/>, Accessed 08. July 2016.
- [17] <https://santoku-linux.com/howto/howto-use-aflogical-ose-logical-forensics-android/>, Accessed 12. July 2016.
- [18] <http://mobileeditlite.en.softonic.com/download>, Accessed 12. July 2016.
- [19] <https://www.nowsecure.com/forensics/community/>, Accessed 12. July 2016.

DETECTING MALICIOUS ANOMALIES IN IOT: ENSEMBLE LEARNERS AND INCOMPLETE DATASETS

IGOR FRANČ

Belgrade Metropolitan University, Faculty of Information Technologies and SECIT Security Consulting,
igor.franc@metropolitan.ac.rs

NEMANJA MAČEK

School of Electrical and Computer Engineering of Applied Studies, Belgrade and SECIT Security Consulting,
nmacek@viser.edu.rs

MITKO BOGDANOSKI

Military Academy General Mihailo Apostolski, Skopje, Macedonia, mitko.bogdanoski@ugd.edu.mk

ALEKSANDAR MIRKOVIĆ

eSigurnost Association, Belgrade and SECIT Security Consulting, amirkovic@secitsecurity.com

DRAGAN ĐOKIĆ

Belgrade Metropolitan University, Faculty of Information Technologies, dragan.djokic@metropolitan.ac.rs

Abstract: *Anomalies in IoT typically occur as a result of malicious activity. As an example, a point anomaly may occur once network intrusion is attempted, while collective anomaly may result from device being hacked. Due to the nature of the attacks, some anomalies are represented by incomplete captured instances or imbalanced captured datasets. For example, features may have some values missing from the row or may contain both categorical and numerical values. Once pre-processed, these datasets become suitable training sets for any machine learning classifier that detects anomalies. However, there are situations where pre-processing takes large amount of time in the operating phase or simply is not executable due to the nature of the data. For example, a feature that contains unknown number of categorical values, such as strings, cannot be converted into finite number of binary features before the training. In this scenarios, basic machine learning methods, such as Support Vector Machines or Decision Trees either fail to operate or provide poor classification performance. Unlike basic, ensemble learners manage these data instances efficiently and provide good anomaly detection rates. This paper analyses the performance of ensemble learners on incomplete IoT intrusion datasets, represented by point anomalies.*

Keywords: *Datasets, Anomaly, Ensemble, Boosting, GentleBoost*

1. INTRODUCTION

Anomalies are patterns in data that do not conform to a well-defined notion of normal behavior. As an example, anomalies in a simple two-dimensional dataset are points that are sufficiently far away from normal regions, i.e. regions that most points belong to. “Anomaly detection refers to the problem of finding patterns in data that does not conform to expected behavior” [1]. That being said, anomalies are detected by defining a region that represents normal behavior and declaring any pattern in the data that does not belong to this normal region as an anomaly. Although anomaly detection seems to be straightforward, several factors make this apparently simple task very challenging: defining a normal region that encompasses every possible normal behavior is difficult; normal behavior may evolve with time and current notion might not be representative in the future; the boundary between normal behavior and anomalies is often not precise and the lack of labeled instances for training may cause a problem. Consequently, the algorithm suitable for anomaly detection in all domains does not exist. The choice of technique suitable for the specific problem is based on the nature of

the input data, the amount of labeled instances in the training set and the type of anomaly.

The nature of the input data refers to the types of features that describe instances in the training set. Features can be binary, categorical (they can take one from the finite number of values) or continuous. Multivariate instances may contain features of same type or a mixture of different data types [2]. According to the amount of labelled instances in the training set, one of the following techniques is used: supervised detection (all instances are labelled), semi-supervised techniques (either the instances belonging to normal or anomalous behaviour are labelled) and unsupervised techniques, that requires no training data, as they are based on assumption that normal instances are far more frequent than anomalies in the test data. Anomalies can be classified as point, contextual and collective anomalies [1]: point anomalies are individual data instances that are anomalous, contextual anomalies are data instances that are anomalous in a specific context, and collective anomalies are collections of related data instances that are anomalous with respect to the entire data set.

In the Internet of Things, anomalies in the network traffic may indicate an ongoing malicious activity, such as network intrusion, eavesdropping, or a Thing in IoT being hacked or compromised in another way. While on the typical network various anomaly based intrusion detection systems use pre-processors to convert feature values into numerical values, IoT scenario may be a little bit different. Attacks in IoT differ due to vast variety of devices, which further causes some anomalies to be represented by incomplete feature vectors or imbalanced datasets. Features may have some values missing or may contain categorical and numerical values. Although pre-processors are typically used to resolve these issues, sometimes they cannot be implemented due to the nature of data: one cannot employ conversion from categorical to numerical features if number of categorical values is prior unknown. In these case basic machine learning methods fail to operate – Support Vector Machines operate with standardized numerical datasets, while Decision Trees cannot perform with sufficient precision as some nodes cannot be traversed down to the leaves due to lack of values. However, ensemble learners operate with sufficient precision and provide high anomaly detection accuracy. Having that said, within this paper, the efficiency of supervised ensemble machine learning methods on incomplete synthetic IoT intrusion datasets, represented by point anomalies and healthy traffic.

2. MACHINE LEARNING ALGORITHMS

Tom Mitchell’s widely quoted formal definition of machine learning [3] can be rephrased to the supervised anomaly detection context: “a learner learns to classify events (task T) into normal events and anomalies; performance measure P of this task is the classification accuracy, and the experience E is the training set of rules”. Supervised learning algorithms build a model from a training set (given in the form of feature vectors) with class label assigned to each instance. Once trained, supervised algorithms assign class labels to previously unseen examples of the same task [4]. Within the context of anomaly detection, typically a two-class problem is being solved and having that said, class labels given to the instances indicate normal or anomalous data.

In theory, every machine learning method has its own advantages and disadvantages, which can be perceived on the basis of how these methods operate. Decision trees recursively create a classification tree with decision nodes based on a subset of values of a corresponding feature and classifications on its leaves. Support vectors map learning examples from an input space to a new high dimensional (potentially infinite) feature space in which examples are linearly separable (see Image 1). Naive Bayes apply Bayes’ rule using assumption about mutual independence of features, and k-Nearest Neighbours assign class labels according to a classification of k closest training examples in feature space. However, there is no machine learning method that is the best for every problem (the Generalization Conservation Law [5] or the No Free Lunch Theorem [6]).

Machine learning methods used for classification can be divided into [7]: basic methods (artificial neural networks

[8], Support Vector Machines [9, 10], decision trees [11, 12], Naive Bayes [13, 14]), hybrid methods (for example, a hybrid of decision trees and Naive Bayes – a regular univariate decision tree, where leaves contain a naive Bayes classifier built from the examples that fall at that leaf [15]), incremental methods (Naive Bayes updatable), hybrid incremental methods (Hoeffding Tree [16]), basic ensembles (random forest [17]), hybrid ensembles (stacking) and hybrid incremental ensembles (Ada Hoeffding option tree).

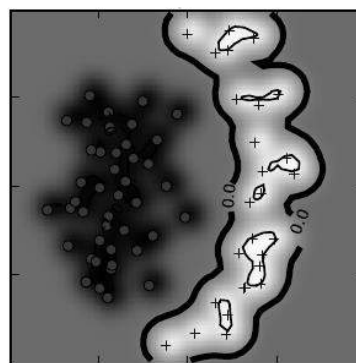


Image 1: SVM’s RBF kernel maps data from input space to high dimensional feature space

3. ENSEMBLES

Ensemble machine learning methods use multiple learning algorithms to obtain better predictive performance than could be obtained from any of the constituent learning algorithms alone [18, 19], as shown on Image 2.

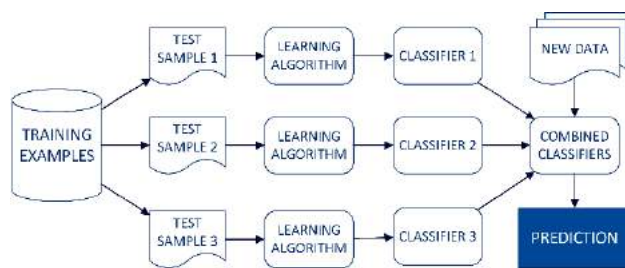


Image 2: Ensemble machine learning

Most common types of ensembles used in experiments reported in the literature are built by boosting, bagging and stacking. Boosting incrementally builds an ensemble: each new model instance is trained in order to emphasize the training instances that previous models have misclassified. Each model in the bagging ensemble votes with equal weight, and in order to promote model variance, bagging trains each model in the ensemble using a randomly drawn subset of the training set. For example, the random forest [17] combines random decision trees with bagging to achieve very high classification accuracy [20]. In some cases, boosting has been reported to provide better accuracy than bagging, but is less prone to over-fitting.

Stacking builds a hybrid ensemble by training a learning algorithm (combiner) to combine the predictions of several other learning algorithms. All of the other algorithms are trained using the available data and a combiner is further trained to make a final prediction using all the predictions of the other algorithms as additional inputs. In practice, a single-layer logistic regression model is often used as the combiner.

4. GENERATING IOT DATASET

The IoT dataset used in this research is built from traffic captured on the simulated network of Things, consisting mostly of mobile devices. All devices had their traffic rerouted through a single gateway where it has been captured using PCAP library on Linux operating system. Synthetic dataset consists of normal, healthy traffic recorded during one day period and variety of simulated attacks, ranging from vulnerability analysis to penetration attempts and successful exploitations, executed with variety of open source and commercial software products. Both healthy and malicious traffic have been recorded separately and cleansed from other protocol and service leftovers (partial noisy data removal), thus leaving clean normal and anomalous PCAP files, which reassembles a scenario for supervised anomaly detection. QoSilent Argus software was used to extract features values from PCAPs and create data instances which were labelled and shuffled into a separate training and test sets. Features used in this research do not include source and destination IP addresses. However, they include flags, connection states, protocols, port numbers and lots of statistical data. Once the feature extraction was done, a sneak peek into the generated CSV revealed the following facts that point up to incompleteness of the dataset.

1. Feature flags is categorical, but have fields with no values (blanks). Although somewhat convertible to numerical values, a change in the Argus software may result in need to change in the pre-processor.
2. Source and destination ports have decimal, hexadecimal and textual values. Examples of the values include: “51305”, “0xb6”, “netbios-dgm”, see Table 1 for more examples. As number of textual values is not documented in the software documentation, unknown number of textual values cannot be converted into finite number of numerical values during the training phase unless the model will be retrained on frequent basis.

Table 1: Example values of port features

Sport value	Sport type	Dport value	Dport type
33100	Decimal	https	String
0x0008	Hex	0x0100	Hex
35360	Decimal	domain	String
37159	Decimal	https	String
15039	Decimal	http	String

3. Source and destination TOS, TTL, TCP window advertisements and several other numerical features have blanks, which makes them virtually inconvertible into a numeric values, if a range of numerical values they make take is unknown or undocumented.

4. Source and destination diff service have both numerical and categorical values. Categorical values are not documented as well as the range of numerical values, thus making this field inconvertible to numerical values.

Although one might try to implement conversion to numerical values in the data pre-processor (for example, filling blanks with -1 or splitting features with mixed values into two or three features), aforementioned statements indicate that in this scenario it is not possible due to unknown or undocumented ranges. This leaves a learner to be trained and evaluated with incomplete datasets – sets from which aforementioned features are removed.

5. EXPERIMENTS

Performance of the basic and ensemble machine learning algorithms solution is experimentally evaluated using MATLAB R2016a with Statistical and Machine Learning Toolbox, version 10.2. Within this research the following machine learning algorithms available in aforementioned toolbox have been used to train and test IoT datasets: basic methods (decision tree and Support Vector Machines), bagging and boosting ensembles (Adaboost [21], RUSBoost [22], LogitBoost [23] and GentleBoost [24], all using C4.5 decision tree as a base learner). A training dataset consisting of one thousand lines with 41 features and a class label was imported into MATLAB. When imported into the Classification Learner, 11 features were discarded due to the feature values inconsistencies (inability of being pre-processed, as stated in Section 4 of this paper) and several additional categorical for SVMs. Five-fold cross validation was applied and the testing results for each classifier are listed below.

1. Complex tree.

- C4.5 decision tree using Gini’s diversity index as split criterion, with 100 splits and no surrogate decision splits.
- Overall accuracy of the classifier is 73.7%.

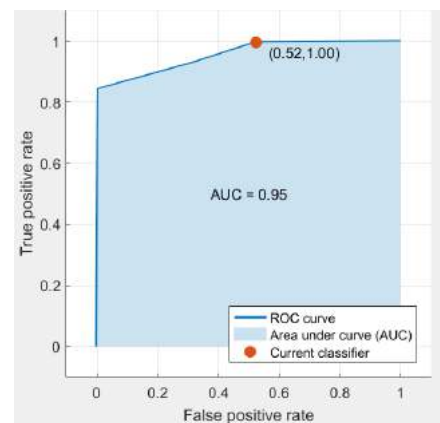


Image 3: Complex Tree ROC Curve

2. Fine Gaussian SVM.

- Standardized data, Gaussian kernel function, manual kernel scale mode 1.4.
- Overall accuracy of the classifier is 71.6%.

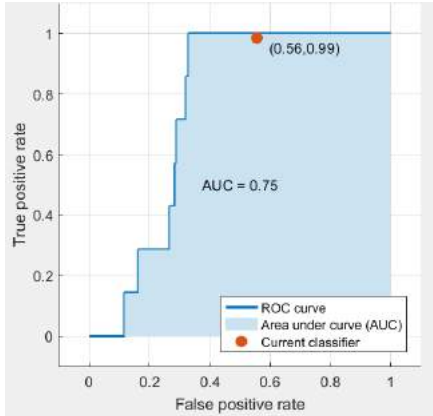


Image 4: Fine Gaussian SVM ROC Curve

3. Bagged trees.

- Decision tree as a learner, 20 splits, 30 learners, 0.1 learning rate, subspace dimension 1.
- Overall accuracy of the classifier is 89.0%.

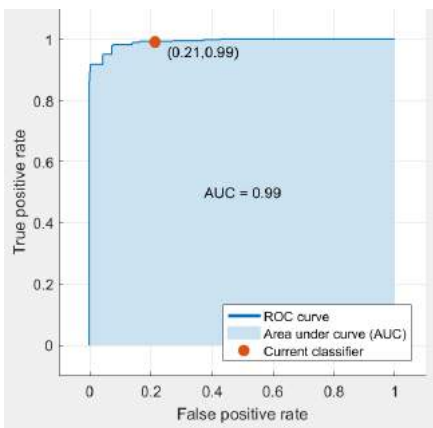


Image 5: Bagged Trees ROC Curve

Boosted trees are further examined with 20 splits, 30 learners, 0.1 learning rate and subspace dimension 1.

4. AdaBoost.

- Overall accuracy of the classifier is 94.8%.

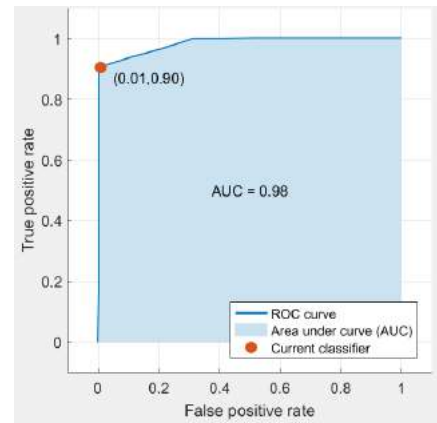


Image 6: AdaBoost ROC Curve

5. RUSBoost.

- Overall accuracy of the classifier is 73.7%.

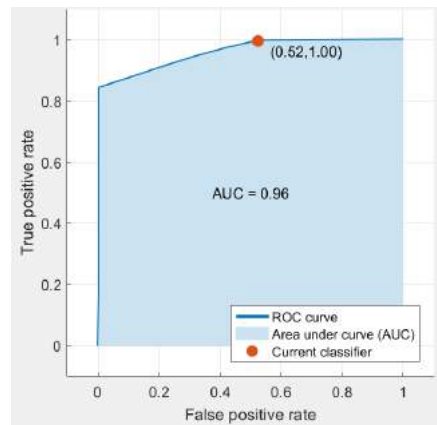


Image 7: RUSBoost ROC Curve

6. LogitBoost.

- Overall accuracy of the classifier is 91.9%.

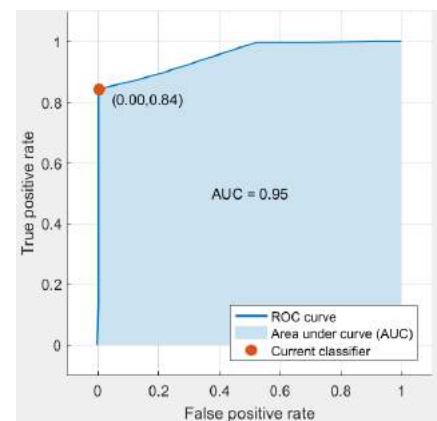


Image 8: RUSBoost ROC Curve

7. GentleBoost.

- Overall accuracy of the classifier is 98.6%.

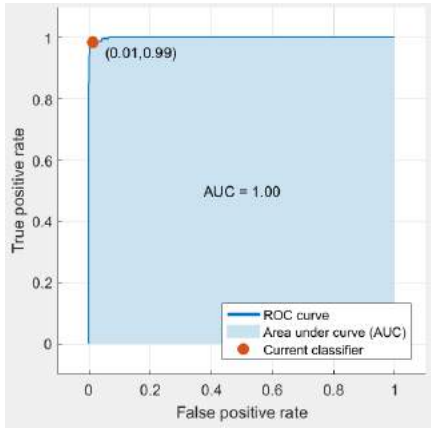


Image 9: GentleBoost ROC Curve

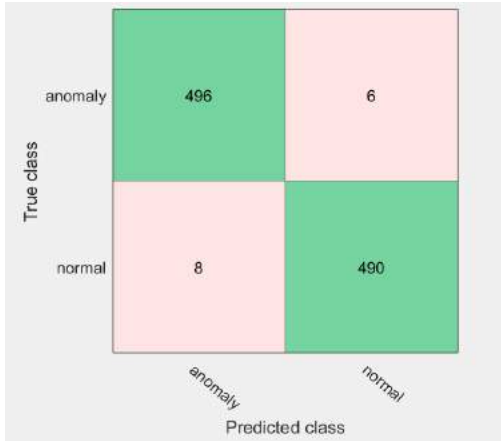


Image 10: GentleBoost confusion matrix

Results are further summarized in Table 2.

Table 2: Experimental evaluation summary

Classifier	Accuracy	AUC
Complex Tree	73.7%	0.95
Fine Gaussian SVM	71.6%	0.75
Bagged Trees	89.0%	0.99
AdaBoost	94.8%	0.98
RUSBoost	73.7%	0.96
LogitBoost	91.9%	0.95
GentleBoost	98.6%	~1

Although we have already stated and explained why basic machine learning methods are not expected to operate with high classification accuracy, and ensembles were expected

to, another question arises: why did the GentleBoost provide such level of accuracy on the dataset and have outperformed other ensembles?

Unlike the commonly used AdaBoost algorithm, the weak classifier in the GentleBoost algorithm is a soft-decision classifier with continuous output. This enables the strong classifier's score to be smoother and favourable for computing derivatives [25]. More formally, while other boosting algorithms minimize the overall test error as much as possible at each step, GentleBoost features a bounded step size. Let $w_{t,i}$ denote update weights, y_i desired outputs, $h_t(x)$ weak learners, x the samples and α_t the minimizer. Variable f_t is chosen to minimize:

$$\sum_i w_{t,i} (y_i - f_t(x_i))^2, \quad (1)$$

and no further coefficient is applied. GentleBoost will choose:

$$f_t(x) = \alpha_t h_t(x) \quad (2)$$

exactly equal to y , while steepest descent algorithms will try to set $\alpha_t = \infty$. According to empirical observations, this causes good performance of GentleBoost, even with incomplete datasets, as large values of α can lead to poor generalization performance [26, 27]. Second, the GentleBoost algorithm outperforms other boosting methods in that it is more robust to noisy data and more resistant to outliers.

6. CONCLUSION

The Internet of Things involves the increasing prevalence of objects and entities (Things) provided with unique identifiers and the ability to automatically transfer data over a network. Much of the increase in IoT communication comes from computing devices and embedded sensor systems used in industrial communication, home and building automation, vehicle to vehicle communication and wearable computing devices. IoT security is the area of endeavour concerned with safeguarding connected devices and networks in the IoT. As we have stated before, anomalies in the IoT traffic may occur as a result of malicious activities, such as attempt to hack or otherwise compromise a mobile device. These anomalies can be represented by a finite number of numerical or categorical features. In most scenarios pre-processors are able to convert all this data to numeric values and most of the machine learning algorithms are able to perform supervised anomaly detection after. However, due to a large number of different devices and variety of attacks, data may be incomplete and unsuitable to train basic learners such as decision trees or Support Vector Machines, or, even if trained, they will provide poor classification performance. Ensemble learners manage to build models and classify these data instances, which has been experimentally proven in this paper. Another issue that has arisen from the experimental evaluation presented in this paper is superiority of GentleBoost algorithm over other boosted ensembles on incomplete datasets resulting

from soft-decision classification with continuous output and robustness to noisy data.

REFERENCES

- [1] V. Chandola, A. Banerjee, V., "Anomaly detection: A survey", Technical Report, TR 07-017, Department of Computer Science and Engineering, University of Minnesota, August 15, 2007. ACM Computing Surveys (CSUR), 41(3), 15.
- [2] P. N. Tan, M. Steinbach, V Kumar, "Introduction to data mining". Addison-Wesley, 2006.
- [3] T. Mitchell, "Machine Learning", McGraw-Hill Science/Engineering/Math, 1997.
- [4] I. Hendrickx, "Local Classification and Global Estimation: Explorations of the k-nearest neighbor algorithm", PhD Thesis, Tilburg University, The Netherlands, 2005.
- [5] C. Schaffer, "A Conservation Law for Generalization Performance", in Proceedings of the Twelfth International Conference on Machine Learning, pp. 259-265, New Brunswick, NJ: Morgan Kaufmann, 1994.
- [6] D. H. Wolpert, "The lack of a prior distinctions between learning algorithms and the existence of a priori distinctions between learning algorithms", Neural Computation, 8, 1341-1390, 1391-1421, 1996.
- [7] V. Mišković, M. Milosavljević, S. Adamović, A. Jevremović, "Application of Hybrid Incremental Machine Learning Methods to Anomaly Based Intrusion Detection", Proceedings of 1st International Conference on Electrical, Electronic and Computing Engineering IcETRAN 2014, Vrnjačka Banja, Serbia, June 2-5, 2014, pp. VII.2.3.1-6.
- [8] S. Haykin, "Neural Networks: A Comprehensive Foundation, 2nd ed.", Prentice Hall, 1998.
- [9] V. Shawe-Taylor, N. Cristianini, "Kernel Methods for Pattern Analysis", Cambridge University Press, 2004.
- [10] V. Vapnik, "Statistical Learning Theory", John Wiley & Sons, 1998.
- [11] L. Breiman, J. H. Friedman, R. A. Olshen, C. J. Stone, "Classification and Regression Trees", Wadsworth, Belmont, 1984.
- [12] R. Quinlan "C4.5: Programs for machine learning", Morgan Kaufmann Publishers, Inc., 1993.
- [13] V. Cherkassky, F. M. Mulier, "Learning from Data: Concepts, Theory and Methods. 2nd ed.", John Wiley - IEEE Press, 2007.
- [14] I. H. Witten, E. Frank, M. A. Hall, "Data Mining: Practical machine Learning Tools and Techniques, 3rdEd", Elsevier Inc., 2011.
- [15] R. Kohavi "Scaling Up the Accuracy of Naive-Bayes Classifiers: A Decision-Tree Hybrid", in KDD (pp. 202-207), 1996.
- [16] P. Domingos, G. Hulten, "Mining high-speed data streams" In Proceedings of the sixth ACM SIGKDD international conference on Knowledge discovery and data mining, pp. 71-80, 2000, ACM.
- [17] L. Breiman, "Random Forests", Machine learning, 45(1), pp. 5-32, 2001.
- [18] R. Polikar, "Ensemble based systems in decision making", IEEE Circuits and Systems Magazine, 6 (3), pp. 21-45, 2006.
- [19] L. Rokach, "Ensemble-based classifiers", Artificial Intelligence Review, 33 (1-2): 1-39, 2010.
- [20] L. Breiman, "Bagging Predictors", Machine Learning, 24(2), pp.123-140, 1996.
- [21] B. Kégl, "The return of AdaBoost.MH: multi-class Hamming trees", arXiv: 1312.6086, Dec. 20. Last time visited: Aug 15, 2016.
- [22] C. Seiffert, T. M. Khoshgoftaar, J. Van Hulse, A. Napolitano, "RUSBoost: A hybrid approach to alleviating class imbalance", IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 40(1), pp.185-197, 2010.
- [23] S.B. Kotsiantis, "Logitboost of simple bayesian classifier", Informatica, 29(1), 2005.
- [24] J. Friedman, T. Hastie, R. Tibshirani, "Additive logistic regression: A statistical view of boosting", The Annals of Statistics, 38(2):337-374, 2000.
- [25] X. Liu, T. Yu, "Gradient feature selection for online boosting", in 2007 IEEE 11th International Conference on Computer Vision, pp. 1-8. IEEE, 2007.
- [26] R. E. Schapire, Y. Singer, "Improved boosting algorithms using confidence-rated predictions", Machine learning, 37(3), pp.297-336, 1999.
- [27] Y. Freund, R. Schapire, N. Abe, "A short introduction to boosting", Journal-Japanese Society For Artificial Intelligence 14(771-780), p.1612, 1999.

INTERNET OF THINGS CHALLENGES FOR ORGANIZED SOCIETIES

MIROSLAV D. STEVANOVIĆ

Security Information Agency, Belgrade, mstvnv297@gmail.com

DRAGAN Ž. DJURDJEVIĆ

Academy of national security, Belgrade, djurdjevic.dragan@gmail.com

Abstract: *The concept of the Internet of Things (IoT) implies consequent interconnectedness of humans, devices, equipment, and maybe even wildlife. In the process of spreading of IoT, societies become more complex, and thus exposed to new challenges for their stability. The problem, from the anthropocentric aspect, is how the concept of the IoT affects an organised society. We assume that the public administration has an institutionalised duty to prevent security breaches within its jurisdiction, and provide security of sensitive applications, including national infrastructure, security services, and the finance. In this article, we observe foreseeable challenges facing national administrations through the IoT order, and political balance. We find that information input and time consumption implied by the IoT will immanently affect decision making, that omnipresent infrastructure environment will broaden legal and national security issues of the State, and that interconnection introduces a concept of conflict in social life. The results indicate that to maintain social stability, States faced the necessity of preemptive action in the sense of creating educational, legal and technological preconditions for a new stage of technological change.*

Keywords: *IoT, Infrastructure Environment, Sustainability, Information Management, Human Rights*

1. INTRODUCTION

In the process of spreading of IoT, societies become exposed to new sensitive applications, including national infrastructure, security services, and the finance challenges for their stability.

In our previous articles concerning matters of national and public security challenges of spontaneous spreading of application and development of IoT, we have indicated a number of obstacles facing public authorities in regard to the interests of individuals. These obstacles are concerned with the problems of providing the functioning of networks, clouds, network security, or advances in a rational deployment of independently communicating sensors and appliances [1].

The approach which exposes only the responsibilities of public administration as a regulation of technological standards on the territory necessarily deprives a society of an organisational component.

The global network is not an artificial intelligence and, in the functional sense, it is just a tool through which mankind enhances its potentials. Structurally, it is unavoidable that widespread of "smart" sensors and applications will influence processes in various fields of human life. What is basically at stake is the stability of legal order, and political balance in changing societal arrangements, in which sensors have an independent influence on the decision-making process.

Questions arising from IoT concept exceed the comprehension of its functioning, and even potential misuse. They epistemologically root from dilemma is it possible to uncritically implement a complex system of interconnected and communicating sensors in a way that

would improve and not marginalise human rational efforts.

2. MATTER OF NATIONAL LEGAL ORDER

Internet of things includes the aspect of popular trust. Ethical framework of that trust creates a responsibility for public authorities of a country, as a consensually developed dominant organisational form in a political community, to publicise desired norms and to incorporate them in the framework of trust. Thus, the first obstacle is of epistemological nature, and concerns approaching the new revolutionary technology since the knowledge itself is simultaneously social and technological phenomenon.

Ethical trust in new possibilities of IoT necessitates the dedication of public authorities to present all perceivable frameworks [2]. There is little room for doubt that power of automatized computing will affect the everyday life. The fact that, due to that, society's environment can become better or worse, is the essence of the IoT. Independent objects become as they are functionally represented on the network: monitors, controllers etc. Having communication with objects, in new roles, necessitates a change in the philosophical paradigm of normative order, in terms that it has to include new mutual interrelations between prior subjects and objects. The consequences of the paradigm shift can already be conceptualised in many activities, automatized habitats, organised care of elders, children, life in cities etc. But, an organised society cannot effectively function if the normative intrusion is not in line with prior, more general norm, and that is subject to an ethical framework [3].

Conceptual implementation of IoT is still far from a full and necessary connection of all services and technologies. From that aspect, the question of new philosophical-

normative paradigm may seem premature, since today we are faced more with a variety of solutions and efforts aimed at ensuring The semantics of this orientation of IoT prioritises management of an as wide spectrum of services as possible [4] regardless of the normative requirements.

Normative ground for the functioning of IoT, apart from resolving the mentioned ethic dilemma, what is good and what is wrong in individual and collective behaviour, for the society, has to include an axiological aspect, namely a new aesthetic concept which will be imposed through the implementation of IoT [5].

The principle problem which organised societies encounter in all matters concerning the internet is that national law ends on national borders, and no individual state has exclusive jurisdiction over the internet, and especially not the IoT.

Public administrations perform many functions provided by the law. Some Cyber systems have the potential to optimise the use of processing and storing resources, like virtualization (abstracting applications from the hardware) or cloud technologies (based on virtualization), and enable sharing between various administrative entities [6]. Hosting of resources of public authorities on clouds outside institutional and democratic control poses a challenge for the protection of individual and collective values.

Apart from the institutional and democratic issue, organised communities are facing a challenge generated by the prompt availability of surrounding, which introduces IoT. Cloud computing is graded, flexible and omnipresent, with use almost everywhere, science, health care, economy and everyday life" [7]. Having in mind a projected sharp rise in quantity and volume of interconnected networks, the matter of norming safety and privacy cannot be left for ex post regulation. The prospect of connecting virtually everyone and everything inevitably has to affect basic communication norms of today, which are human-centric in a way which is impossible to anticipate. In the mentioned context, of service orientated network architecture, a challenge for nation states stems from the fact that artificial "intelligence" enables solving some specific problems, i.e. decision making, through physical and virtual entities fulfilling autonomous goals, which is an additional risk for public affairs, as well as privacy, in certain areas, like health.

3. MATTER OF POLITICAL BALANCE

Structures of power in contemporary societies (concerning the control of capital, statics and relations between social groups) today, in the post-modern age, are simultaneously highly exploitative, unjust or oppressive, and above all generate degradation of the human environment [8]. From only the aspect of public safety and security, the threat emerging from IoT pose ever more devices coming online with new ways to exploit them and possibilities of distributed attacks. But, in the interest of functional and effective society, there are more fundamental, practical questions facing every individuals and society: what are human beings giving away; where is

the data going; who will really own "our" devices in the new future; how the homes are automated, how we care for the elder, how do we monitor children, what concepts are used to organize life in cities etc. Answers to these questions are not currently a priority public concern, and producers don't have a commercial interest to explain the consequences.

From the aspect of these activities as societal arrangement, the IoT challenge extends beyond only the induction of normative elements, and can be generalized in the context of - for the benefit of whom, and for the good in accordance to what norm. Thus, this challenge is simultaneously political and ethical in nature.

The IoT will consist of perception technology embedded in physical entities, networks for exchanging the data they generate, computing power for interpreting them in real time (as a service), and finally, agents that react according to computing results. We can assume that capabilities of computing power distributed and embedded into everyday objects and the connectivity of the net will make everyday world more "intelligent". But, as devices and sensors will in many ways shift real-time connectivity to physical human body, it will have to effect social abilities in the real-world. The risk, namely, is that psychologies of confused identities and power play could cause chaos, or have some other limited negative repercussions [9].

Society will, considering the correlation in the tendency of high technologies towards investment centers, undoubtedly, generally be enabled by cheap technology [10]. Some will afford full automation, but will all, or at least most? Consequently, individuals and societies will, as a rule, be in a position to make simple commands, but not to influence complex actions together. So, the systemic functions that citizens rely on in everyday life will remain dependent on bureaucratic, but digital solutions. Integration of technologies will thus necessarily be an ongoing issue, from the aspect of purpose, and from the aspect of elitism.

There is no reason to assume, neither to doubt, that the humankind will eventually reach its potential to keep up with the "smart" machines, or even reach artificial intelligence. But, until that time there is a serious risk that IoT could lead to anonymous networks dominating the affairs and being factual caretakers. As the processes rely ever more on the digital world, even the interactions between humans may become ever more virtual.

All life has instinct value, independently of its usefulness to humans. Richness and diversity also have value in themselves, because they contribute to the well-being of life in society. If IoT should, as it seems, lead to a reduction of this richness and diversity, unless it is to satisfy vital needs in a responsible way, there is a question of a right for such alteration. Human lifestyles and population are key elements of human impact, and the diversity of life, including cultures, can flourish only if the human impact is reduced, regardless of advance of useful digital objectification in everyday life. This is why it seems inevitable that basic ideological, political, economic and technological structures must change. If we accept that there is an obligation to participate in

implementing the necessary changes that impose IoT, it must be assumed that it includes the duty to secure that they are peaceful and democratic in nature.

The impact of the IoT on society, and primarily the increased role of technology, could develop alienated automatism in many decision making processes. That is the direct purpose of many software and services that are produced and incorporated. This impact carries numerous social uncertainties, which are attributed, among others, to: generation of large quantities of generated data, which may or may not necessarily be valuable or needed, but are potential for use or misuse; privacy, data protection, and social issues opposed to the potential benefits in public safety, energy conservation, and lower costs, depend on public opinions and behavior; potentially large-scale, highly automated technological systems that can remove human intervention in order to increase reliability, but increase the potential for societal vulnerability, with uncertain inevitable higher quality in the provision of many services; and inequality in access to data of value to individuals and communities, parallel with other digital inequalities across societies [11].

But, if we consider technology to be a tool, interconnections and interoperability cannot be accepted as detrimental in decision making. That is why there is a need to consider the impact of the IoT on the wider society, and not just on organizations. Since IoT will change many social ways, crucial for its viability is organizational and institutional innovation.

4. MATTER OF INTERNATIONAL SYSTEM

Tomorrow's internet landscape could look very different: new smart systems, available on the go, new social media, cloud computing that is scalable, flexible, and everywhere, enormous data sets used in science, healthcare, economy, and everyday lives.

Networking of different technologies and domains, in building of architecture of interconnected humans and objects leads to new challenges in regard to manageability, security and privacy on the supranational level. Many fields of human activity require formal normative and political coordination of deployment and implementation of sensors at international level. Environment, chemistry, biology, radiology and the nuclear sector cannot be left to corporate technologies and services if IoT is to be trusted by populations.

Due to a large number of applications, providers and stakeholders, standards need to be adopted at international level, so that in practice IoT system would at least function as interoperable [12]. Interoperability is, as such, a specific potential risk generator for at least two reasons: firstly, due to the dissonance between management requirements and engineering concepts, on one side, as well as due to the discrepancy between the perception of decision makers and effectiveness and reliability of developed solutions. From that aspect, it seems that the current concept of security, as isolated criteria, needs adjusting, since it contains fundamental structural incompatibility with the idea of interoperability, which

tends towards global inclusiveness, thus also globalizing the challenges.

The question of national and international politics concerning management of cyber sphere is already being regionalized. Cyber defense is part of NATO strategy since 2002. Within this strategy, member and partner states are offered various mechanisms of potential crisis management and strengthening of national cyber defense capabilities. This way, countries are being guided into a unified frame of cyber defense of values on which the organization is founded [13].

At the universal level, the matter of normative regulation of national cyberspace has so far only been superficially treated. Cyberspace is, namely, often presented as "open", "decentralized" and "participatory". Such view is not substantiated in international law. In the context of international security, UN Charter and international law apply in cyberspace and sovereignty and international principles, in regards to ICT and ICT infrastructure within state's territory [14].

Cyberspace can be perceived as a global domain in the framework of information medium of interconnected communication networks, [15] or as an interconnected network of IT infrastructures (the internet, telecommunication networks, computer systems and built-in processors and controllers), [16] including virtual surrounding of information and interactions between people. That is the space with parallel flow of processes of territorialization of cyberspace and cyber activities, as well as de territorialization, in the sense of deriving regulatory mandates from territories under the jurisdiction of organized societies [17]. An example is Internet Corporation for Assigned Names and Numbers (ICANN), which is however incorporated within the legal system of the US, through an agreement with the Department of Commerce, but has sole responsibility for maintaining the Internet safe, stable and interoperable. As cyberspace, with IoT era, becomes integral in every aspect of modern societies, it develops into a domain and medium through which are various human activities conducted [18]. Due to their inherent responsibilities, states are faced with an obligation to provide that national networks which support stability, prosperity and security of their citizens, remain effective and meaningful. The nature of the new challenges requires that the problem of decision-making legitimacy be addressed at international level [19].

An illustration of possible discrimination at the global level is provided by a couple of examples. One of such is a global cell phone game on public space, called „Pokemon Go“. An important consequence of this game, from the aspect of functioning of the society in omnipresent digital world, is privileged position of its owners, who use public space for making profits, without respecting national laws, concerning commercial fair activities, leasing of public land (since it is not making virtual, but real profit), nor taxation. The fact that this game is spreading on the global network, like the „smart“ appliances that are being produced without respect to national standards, cannot relieve a state of its responsibilities, when equality and safety of its citizens are concerned. Also, who can foresee the consequences of

the future development of one of the benchmark tasks of computer vision - scene recognition, and the effects it could have on individuals and their automatic recognition on the network. A state is financed to protect long-term interests and values of its citizens, and one of the prior concerns is general upholding national laws and nondiscrimination.

5. CONCLUSION

Massive production and emission of digital data broaden possibilities for their use for the benefit of private and public life. But, there are no objective indications which would found the assumption that limitless use of digital sources of data can result in "programmed" societal functions. That is the principle argument in favor of intrusive state approach to IoT in national cyberspace.

Apart from uncertain organizational effects, challenges of the IoT concept for organized societies include some specific threats concerning critical national infrastructure systems, guarantees for privacy, and ethical degradation as a consequence of adjustment to techno centric requirements.

Spreading of the IoT cannot be limited in administrative fashion, and from the aspect of the functioning of organised society, the solution is not in the practising of state authority to limit or censor the contents of networks.

But, on the other hand, it seems self-evident that no producer, provider, service or technology can have priority over the concerns for securing of social norms and standards, whether in city life, health care, or other fields of common interest in a society.

IoT additionally complexes the problem since it leads to unpredictably wider and more autonomous spectrum of communication and decision limitations. Living in an organized political society raises legitimate expectations that the apparatus that is paid by the citizens will not only protect basic value system founded on an individual but above define and regulate standards in common interest to which the implementation of IoT will have to adjust.

Governing and regulating (norming) societal impacts of the IoT, includes an in advance anticipation of at least the following issues: data protection and institutional changes to adapt to the IoT concept; responsibility for failures and breaches; status of devices that will obtain information about their users; applicable standards for business, industry, and public decision-making; and functioning of local and national policies within regional and global practices and policies.

REFERENCES

[1] Djurdjevic, Stevanovic, "The Value Challenge of Interconnectedness in Cyberspace for National Security," in *Sinteza 2016 - International Scientific Conference on ICT and E-Business Related Research*, Belgrade, Singidunum University, Serbia, 2016, pp. 15-23; *The Problem of Protecting Security of Persons and Property in Light of Development of IoT*, Third ICT Security Conference, May 19-20, 2016, Belgrade.

[2] Freiman, Ori, "Towards the Epistemology of the Internet of Things: Techno-Epistemology and Ethical Considerations through the Prism of Trust", *International Review of Information Ethics*, 22:12/2014, p. 6; McCraw, Benjamin, *The Nature of Epistemic Trust*, *Social Epistemology*, 29:4/2015, pp. 413-430.

[3] Haarkötter, Hektor; Weil, Felix, "Editorial", *International Review of Information Ethics*, 22:12/2014, p. 1.

[4] Serrano, Martín et al., Executive Summary, in: "IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps", Serrano, Martín et al. (eds.), Brussels: European Research Cluster on the Internet of Things/European Commission, 2015, p. 6.

[5] Bibri, Simon Elias, "The Shaping of Ambient Intelligence and the Internet of Things: Historico-epistemic, Socio-cultural, Politico-institutional and Eco-environmental Dimensions", Amsterdam: Atlantis Press, 2015, p. 39.

[6] Beltrame, Francesco; Dagostino, Virginia, "Advances in Internet of Things as Related to the e-government Domain for Citizens and Enterprises", in: *Advances onto the Internet of Things: How Ontologies Make the Internet of Things Meaningful*, Gaglio, Salvatore; Lo Re, Giuseppe (ed.), Dordrecht: Springer Science & Business Media, 2013, pp. 221-222.

[7] Neelie Kroes, "Creating tomorrow's Internet", Speech at "Launch of Future Internet Labs", London, 3 September 2013, European Commission, p. 2.

[8] Talia, Domenico, "Towards Internet Intelligent Services Based on Cloud Computing and Multi-agents", in: *Advances onto the Internet of Things: How Ontologies Make the Internet of Things Meaningful*, Gaglio, Salvatore; Lo Re, Giuseppe (ed.), Dordrecht: Springer Science & Business Media, 2013, p. 276.

[9] Stevanovic, Djurdjevic, "The Capacity of Perception: The Need for an Educational System in Support of the National Security", *Creative Education for Employment Growth [The Fourth] International Conference Employment, Education and Entrepreneurship [EEE 2015]*, Belgrade, 2015, pp. 41-56.

[10] Ovidiu, Vermesan et al., "Building the Hyperconnected Society: Internet of Things Research and Innovation Value Chains", *Ecosystems and Market*, Vermesan, Ovidiu; Friess, Peter (eds.), Aalborg: River Publishers, 2015, p. 80.

[11] A report of a workshop on the Internet of Things, "The Societal Impact of the Internet of Things" organized by BCS – The Chartered Institute for IT, on Thursday 14 February 2013. <https://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf>, p. 4, 24.08.2016.

[12] Waher, Peter, "Learning Internet of Things", Birmingham/Mumbai: Packt Publishing, 2015, p. 214.

[13] Ziolkowski, Katherina, "NATO and Cyber Defence", in: *Research Handbook on International Law and Cyberspace*, Tsagourias, Nicholas; Buchan, Russell (eds.),

heltenham/Northampton: Edward Elgar Publishing, 2015, p. 427.

[14] UN General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN doc. A/68/98 (24 June 2013), paras 19-20.

[15] Kuehl, Daniel, "From Cyberspace to Syberpower: Defining the Problem", in: *Cyberpower and National Security*, Kramar, Franklin; Starr, Stuart; Wentz, Larry (eds.), National Defence University Press, 2009, p. 28.

[16] National Security Presidential Directive 54; also Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23).

[17] Brolmann, Catherine, "Deterritorializing International Law: Moving Away from the Divide between National and International Law", in: *New Perspectives on the Divide between National and International Law*, Nijman, Janne; Nollkaemper, Andre (eds.), Oxford: Oxford University Press, 2007, pp. 84-109.

[18] The White House, *Cyberspace Policy Review: "Assuring a Trusted and Resilient Information and Communications Infrastructure"*, 2009. <https://goo.gl/uUlxBx>, 03.02.2016.

[19] Weber, Rolf; Weber, Romana, "Internet of Things: Legal Perspectives", Heidelberg: Springer, 2010, p. 86.

IOT SECURITY OPTIMIZATION

DUŠAN BOGIĆEVIĆ

University of Nis, Faculty of Electronic Engineering, dusan.bogicevic@gmail.com

IVAN TOT

University of Defence, Military Academy, Serbia, ivan.tot@va.mod.gov.rs

RAMO ŠENDELJ

Univerzitet Donja Gorica, ramo.sendelj@udg.edu.me

Abstract: This paper deals with the safety of the Internet of Things (IoT) and research of IoT architecture. It is based on theoretical foundations of IoT. The points that could be potential places for an attack on the system are presented in this paper. Architecture that is proposed is based on the physical organization of devices and sensors, as well as on their communication with the servers and applications across different types of networks. Besides the physical part, the paper proposes a software architecture that would enhance the security of Internet devices.

Keywords: IoT, architecture, organization, sensors

1. INTRODUCTION

The term Internet of Things (IoT) came into existence some 15 years ago. It was conceived as a world of objects that exchange data. Data exchange is not between man and machine, but the communication between machines (M2M) is introduced. Kevin Ashton in his work from 2002, published under the title IoT said: "We need an internet for things, a standardized way for computers to understand the real world". [8]

After the appearance of social networks where people communicate with each other, we come into an era where "social devices network" is created - network that controls systems, collects data, analyzes and reacts depending on the data. "...The Internet of Things (IoT) promises to be the most disruptive technology since the advent of the World Wide Web. Projections indicate that up to 100 billion uniquely identifiable objects will be connected to the Internet by 2020, but human understanding of the underlying technologies has not kept pace. This creates a fundamental chal-lenge to researchers, with enormous technical, socioeconomic, political, and even spiritual, consequences. IoT is just one of the most significant emerging trends in technology but some people, such as Nikola Tesla had a vision of IoT almost 100 years ago, "when wireless is perfectly applied the whole earth will be converted into a huge brain ... " [7].

One of the leading companies in the field of IT Microsoft is developing support through its services for IoT called Microsoft Azure IoT Suite. Google has bought company Nest engaged in the production of "smart" thermostats. Also, Google owns Android, one of smartphones' operating systems. These two giants in the field of IT have devoted their resources and attention into studying IoT, from which we can conclude that this is something in our time (the present) and what awaits us in the future.

In 1965 Japanese researchers led by Yoshiro Hatano determined that the man should have a day walk with over 10,000 steps¹. Today we can analyze this statement by studying people and their movements. In addition to the movement we can analyze how much time people spend in their homes, in front of computers, what they like to buy, who they socialize with and much more. These data are now realistic, without observing the sampled population. The questions that arise are: Are all these data safe? and Why are these data are stored on the Internet?

It is good to analyze this data. For example, if our doctor looks at our physical activity, he can alert us to the possible harmful consequences. Alarm for our bad habits can be sent through software, and when we get to the doctor, he can have an accurate picture of our movement based on data and information obtained from the software. The image obtained in this way can contribute to better diagnosis and make our body back into a healthy state. The data collected this way about our movement can also be analyzed by an intruder, and to come to the conclusion that we spend two hours outside of home while doing some physical activity. In this way a burglar would have the information when he needs to organize a robbery.

These two examples intended to show the importance of information on the movements that are on the Internet in the case of medical treatment, and even more important objective, to protect information sent by devices (sensors). This paper is devoted to Internet of things.

2. PARTS OF IOT ARCHITECTURE

IoT architecture basically consists of three parts. These three parts are shown in image 1. [1]

¹<http://www.slideshare.net/mazlan1/internet-of-things-iot-we-are-at-the-tip-of-an-iceberg>

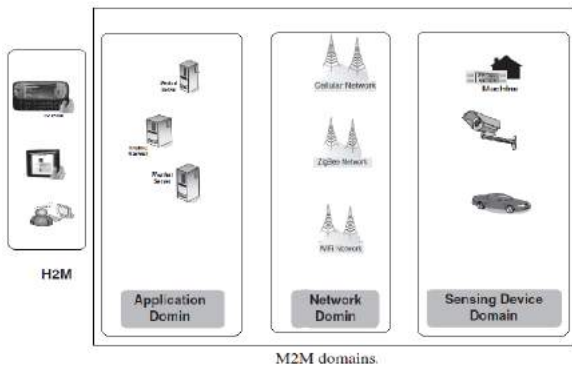


Image 1: IoT architecture

2.1 Application domain

Application domain (image 1) represents servers' architecture that participates in data processing, communication with other devices and communication with a human.

The purpose of these servers is similar to servers in banks, where data are collected, processed and stored. These servers with their services provide communication via Web, mobile and desktop applications with a human, and in addition to H2M communication provide M2M communication.

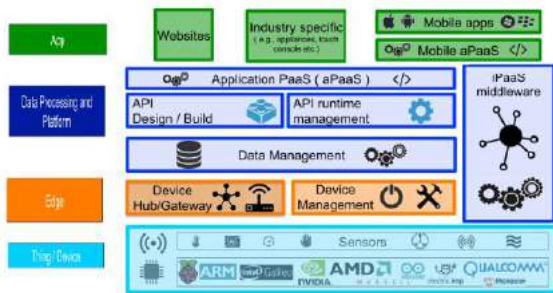


Image 2: IoT stack²

In the case of IoT stack, application domain is divided into:

- **application part** which serves as a user interface for device management. This part represents Web, mobile and desktop applications that communicate with servers in order to exchange information and send commands.
- **the part associated to the platform and data processing** which purpose is to make as much as possible realistic picture of actual objects, that is the real world. In this part, virtual objects we manage and which send us information live. If we IoT imagine as a human body, this would be his brain, a place where all the information from sensors are collected and the place which provides management.

2.2 Network domain

The network part of IoT uses existing technologies (Ethernet, WiFi, Bluetooth, ZigBee, GSM, etc.) for data exchange. The objective of this layer is to transfer information from device to server and vice versa. What is expected from this exchange is that it is safe and reliable. For IoT, the most significant is the wireless communication (radio communication) where it is necessary to take care of security. Most wireless networks have some cryptographic algorithms implemented. Wifi has implemented WEP and WAP methods of protection. 90% of data that are present on the Internet are personal data, and in 70% of cases non-encrypted traffic is used³.

If we look at IoT stack (image 2), the network part represents border section. Devices are equipped with implemented communication interfaces on one side, as well as servers on the other side through which the communication is accomplished and management of devices is ensured (image 1).

2.3 Device domain

Device (or sensor, actuator) domain is the beginning of IoT. It is the layer in which reality becomes virtual world. This is the place where data is received and converted into digital data used by servers (image 1). Types of devices used for collecting data can be in range from simple sensors such as sensors for heat, temperature, light, moisture etc. to location sensors, cameras and other complex sensors or devices (image 2). The number of connected devices exceeds the number of human population. In 2010 the number of devices was almost two times higher than the number of human population.⁴

This layer collects data from one or more sensors. Its aim is to process collected data mostly as analog values and forward it in digital format to the next layer. The collected data is processed on a specific hardware, which has its own software (firmware).[2]

Device domain, depending on the complexity and purpose of the device, can also have a management layer for devices. If we take a camera as an example, it sends us a picture as an information, but we may want to move it. The movement of the camera requires that we have a layer of software and hardware that will allow its management via the camera interface it provides.

3. BASIC ORGANISATION AND IOT SECURITY

IoT architecture is not based on one device, but on sets of devices that in a variety of ways collect information. In case of IoT, the most used term is environment, so we can see the prefix "smart" like smart homes, smart streets, smart parking, smart garbage cans, smart cities etc... Smart environments can be defined as sets (federation) of sensors and actuators that are designed for home, building, city, transport etc...[3][9]

²<http://www.slideshare.net/sumitcan/iot-architecture>

³<http://www.slideshare.net/jvermillard/the-5-elements-of-iot-security>

⁴<http://www.slideshare.net/mazlan1/internet-of-things-iot-we-are-at-the-tip-of-an-iceberg>

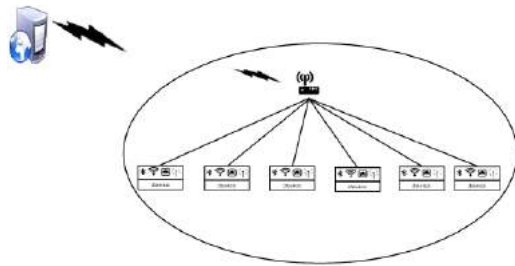


Image 3: Smart devices communication example

IoT is a complex system with a large number of sensors. The most perfect organization that works with the largest number of sensors is the human body. Every part of our body has its own task from touch receptors to nerve cells in the brain. Architecture which the IoT should aim is the architecture of the human body.

If we consider an IoT device with its sensor (sensors), we can forward its data to other devices and services. However, if we have an environment that consists of multiple devices that collect data and all of them send data to servers, then it is necessary to secure each communication. This approach increases hardware and software requirements for each device, whereby the price of each device increases.

4. POINTS OF POTENTIAL ATTACK

Each part of the IoT architecture may represent a potential point of attack. [4]

4.1 Security of device

Places that are the least sensitive to direct attacks are physical devices (sensors), because of their technology, which primarily consists of electrical circuits designed to convert received analog information from the environment into digital format. The devices themselves may offer to potential attacker only the information they possess. Attacks on this part of architecture, beside illegal reading the values from the sensors, may be realized by giving false values, whereby an attacker could test the system. By testing the system, one can get specific values that are important for its functioning. For example, if the humidity sensor sends a huge value, it is possible that the flood occurred, and the system will react by shutting off the water.

Security on the device layer should be realized through physical protection and devices' access control.

4.2 Network security

The next part of the IoT architecture that is sensitive to attacks are networks that are used in the exchange of information. The attacks in this part can also be realized by collecting information from one or more devices. Such

attacks where the traffic is only observed, are known as sniffing. Depending on the type of network used in communication (WiFi, Bluetooth, ZigBee...), depends the method of attack, given the specific character of the technologies used for the particular network. Another way of using the network layer for the attack is the phishing scheme using legitimate participants address.

Security in this part can be implemented by using cryptography algorithms which collecting information make difficult. As mentioned before, most wireless technologies already have some form of protection implemented, so those methods of protection should certainly be used, with possible improvement of existing algorithms. [5]

4.3 Application security

When considering the application layer, firstly one should pay attention to the application user. Logging on to the system should be the only place where the legitimate user may enter the system. However, it can also be the place of interest for potential attacks. This is the place where the greatest number of attacks is expected, so it represents a challenge for programmers. In addition to software protection, user education about the importance of the system and possible threats is essential.

5. ADVANCE ORGANIZATION

An approach that can relieve a server with a large number of connections and communication and management interfaces, is to introduce a central device, which would secure communication and provide management between the server and the sensors or the specific devices that need to be controlled. In this way, managed devices can be organized into the physical and logical parts. As said before, IoT is a large and complex system. To quote a Chinese strategist Sun Tzu: "Management of many is the same as management of few. It is the matter of organization."

This approach may relieve the individual peripheral devices in a way that they would possess only one communication interface (Image 4).

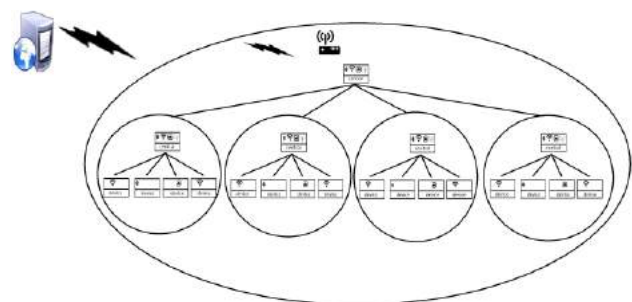


Image 4: Advance organization

In cases where there are multiple devices (sensors, actuators, etc.) that need to be controlled and are spatially apart, multiple control units can be used, which would represent logical or physical parts. These devices would

be central to local devices and would be connected to the main central device. The main central device would have the task of maintaining secure communication with the server, while allowing management of peripheral devices using multiple technologies such as wireless, Ethernet, GSM, BT etc. which provides a significant management functionality and security in case of loss of communication over a single medium. In this way if we want we can receive the data from a peripheral device through WiFi, BT or GSM even if it has only one interface, through which it is connected to a local (central) device. In addition to introducing the main central device, it would be desirable to allow a local central device to be able to take over the functionality of central device to provide redundancy in case of main central device failure.

One additional advantage is the reduction of the number of used addresses (IPv6 is not yet fully incorporated in Europe).

In case of a house with IoT devices (Image 5), which provide control of lights, air conditioning, heating etc., communication would start through the management application, which would address a server. Server would receive a command which needs to be executed and forward it over a network to a central device. Central device would translate the command into the command for a specific device and forward it for execution through local central device if it exists. For each command it is necessary to provide the confirmation that it is realized. Feedback should be returned from the local to the central device in the home, and then to the server, which would send it to the application to confirm the user that it has been successfully executed.

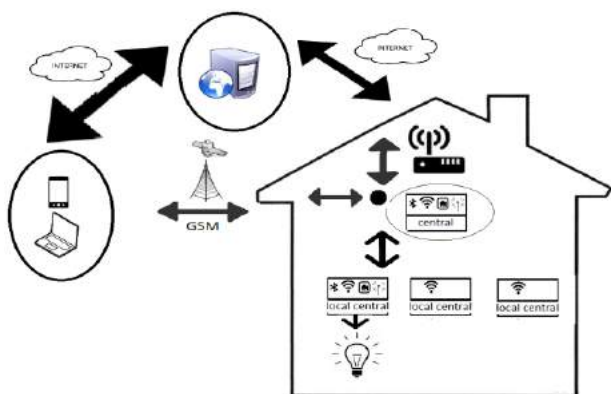


Image 5: Smart home example

Communication between central device and peripheral devices should be a compromise of price, quality and conditions that are present in the given case. By using a wired connection confidence would be achieved, while the security would be increased by using cryptography algorithms.

Regarding the security of the central device, it should have X.509 encryption standard implemented. Also, it very important to enable all devices that are capable of encrypting communication to be updatable since “you can’t secure what you can’t update”. A very common mistake is a firmware update via HTTP protocol which is

not secured and in that way could inflict some kind of damage in case there is a backdoor.[6]

6. CONCLUSION

The approach presented in this paper is aimed to propose a way to reduce the price of devices that we manage. In addition to price, their complexity decreases, and a central device is introduced. The possibility of protection increases while greater functionality for all devices is provided.

REFERENCES

Books:

- [1] D. Minoli, “Building the internet of things with IPv6 and MIPv6: The Evolving World of M2M Communications”, John Wiley & Sons Inc., Hoboken, New Jersey, 2013.
- [2] Gunther Gridling, Bettina Weiss, “Introduction to Microcontrollers Courses 182.064 & 182.074”, Vienna University of Technology, Institute of Computer Engineering, Embedded Computing Systems Group, 2007.
- [3] Dirk Slama, Frank Puhlmann, Jim Morrish & Rishi M. Bhatnagar „Enterprise IoT Strategies & Best Practices for Connected Products & Services”, O’Reilly Media, Sebastopol, United States of America, 2015.
- [4] H. Chaouchi, “The Internet of Things: Connecting Objects to the Web”, John Wiley & Sons Inc., Great Britain and the United States, 2010.
- [5] Fei Hu „Security and Privacy in Internet of Things (IoTs)”, CRC Press, New York, United States of America, 2016.
- [6] Peter Waher „Learning Internet of Things”, Packt Publishing, Birmingham, UK, 2015.
- [7] IEEE Computer. The Internet of Things: The Next Technological Revolution. Special Issue, February 2013.
- [8] Kai Sachs, Ilia Petrov and Pablo Guerrero (Eds.), „From Active Data Management to Event-Based Systems and More”, Springer-Verlag Berlin, Heidelberg, 2010, pp. 242-259.
- [9] Ovidiu Vermesan , Peter Friess,, Internet of Things - From Research and Innovation to Market Deployment”, River Publishers, Gistrup, Denmark, 2014,pp 7-141
- [10] Uckelmann, Dieter, Harrison, Mark, Michahelles „Architecting the Internet of Things”, Springer-Verlag Berlin, Heidelberg, 2011, pp. 229-252

SECURITY ISSUES IN INTERNET OF THINGS ENVIRONMENT

ANDREJA SAMČOVIĆ

University of Belgrade, Faculty of Transport and Traffic Engineering, andrej@sf.bg.ac.rs

Abstract: *Internet of Things (IoT) is a new concept which enables communication among devices connected to a network without human interaction. One of the greatest challenges in modern communications is the aspect of security. This paper presents security requirements for the physical and Media Access Control (MAC) layers in the IoT architecture, as well as relevant protocols and examples of applications. The corresponding IEEE 802.15.4 standard responsible for IoT communication includes the following security objectives, such as confidentiality, authenticity and integrity of data. Furthermore, security issues for network and application layer are also analysed.*

Keywords: *Information Security, IoT, Communication Protocols*

1. INTRODUCTION

As the number of physical objects connected to the Internet increases the idea of the Internet of Things (IoT) is realized, which improves the quality of life and plays an important role in other domains and environments such as traffic and transportation, health care, industrial automation, and emergencies such as natural disasters. IoT allows physical objects to "see, hear and think" and perform tasks by interacting with each other, sharing information and coordinating decisions. The transformation of these objects from traditional to smart is performed by the utilization of their fundamental technologies such as embedded devices, sensor networks, Internet protocols, applications, and so on. Smart objects along with their functions make domain of specific applications (vertical market), while the overall computing and application services form application domain with independent services (horizontal market) [1].

Expectations of IoT in the future are directed to significant consumer and business applications, better quality of life and to help the growth of the world economy. To keep up with this potential, service applications must grow in proportion to the market demand and customer needs. Devices must be designed to meet the users' requirements in terms of the availability of "anywhere, anytime". Also, new protocols are needed for compatibility between heterogeneous objects (vehicles, telephones, equipment, etc.).

Standardization architecture will serve as the backbone for IoT to create competitive environment for companies to create quality products. Furthermore, it is necessary to adapt the traditional Internet architecture to match the IoT challenges. Because of the large number of devices connected to the Internet, use of a large address space becomes necessary to meet the users' needs for smart objects. Security and privacy are another crucial requirements for IoT because of the heterogeneity of objects connected to the Internet and their ability to monitor and control physical objects. Also, monitoring and management are essential to ensure the delivery of

high quality services to customers at reasonable price. The global expansion of IoT environment requires from Internet service providers to provide quality of service for the combination of Machine-to-Machine (M2M), Person-to-Machine (P2M) and Person-to-Person (P2P) traffic flows.

This paper is outlined as follows. We first introduce the general security requirements in IoT environment. We summarize typical security treats over the corresponding IEEE (Institute of Electrical and Electronics Engineers) standards. Secure IoT communication at the network layer is introduced in the next session. Then, we deal with secure routing for IoT applications. Finally, secure IoT communication at the application layer is pointed out. Proposals for future work conclude the presentation.

2. SECURITY REQUIREMENTS

Professional societies responsible for standardization in the field of information and communication technology such as IEEE and IETF (Internet Engineering Task Force) create new communication and security protocols that will play a key role in facilitating future Internet of Things (IoT) applications. Technical solutions are achieved in accordance to the limits and characteristics of the devices and wireless communications and are designed to guarantee interoperability with existing standards on the Internet and communication with other entities in the context of future IoT applications. Available communication protocols designed by the IEEE and IETF make the protocol stack shown in Figure 1.

Communication low energy on the physical and Media Access Control (MAC) layer is supported by IEEE 802.15.4 standard, which sets the rules for communication in the lower layers of the protocol stack and sets the basic for upper-layer protocols.

The environment in which communication takes place with low energy consumption using IEEE 802.15.4 saves most of 102 bytes of data for higher layers of the protocol stack, much lower than MTU (Maximal Transmission Unit) of 1280 bytes, which is necessary for Internet Protocol version IPv6. Low power Wireless Personal

Area Networks (6LoWPAN) adaptation layer addresses this aspect by allowing the transmission of IPv6 packets over IEEE 802.15.4 and implements mechanisms for fragmentation and de-fragmentation package [2].

Routing over 6LoWPAN is supported by protocol RPL (Routing Protocol for Low power and Lossy Networks) [3]. Constrained Application Protocol (CoAP) supports communication at the application layer. This protocol is currently being designed by the IETF to enable interoperability [4].

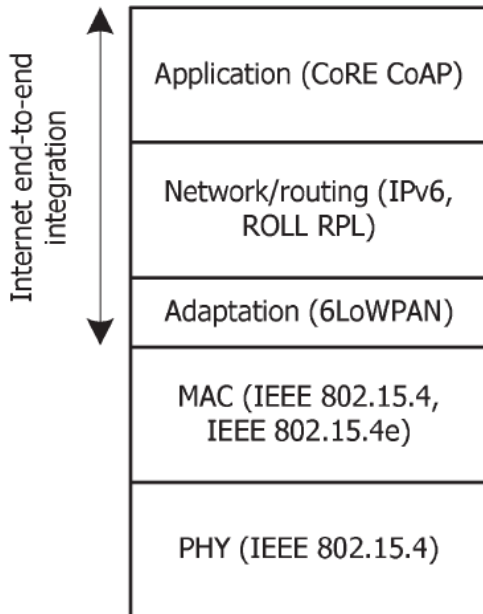


Figure 1: Internet of Things protocol stack

Security mechanisms are designed to protect communication with the above protocols. They must ensure communication in terms of confidentiality, integrity, authentication and non-repudiate flow of information.

Other security requirements should also be taken into account, for example Wireless Sensor Networks (WSN) environment may be exposed to attacks originating from the Internet, such as Denial of Service (DoS). In this context, the availability and flexibility are crucial requirements. The mechanisms for the implementation of protection against attacks on the fragmentation of the 6LoWPAN adaptation layer are also necessary. Other relevant security requirements include privacy, anonymity, responsibility and reliability, which are fundamental to the social acceptability of IoT applications.

IEEE standards facilitate platform rules for new technological developments. This is also the goal of IEEE 802.15.4 standard and as shown in Figure 1, a communication protocol stack for IoT uses this standard to support communications with low energy consumption to the physical and MAC layer. IEEE 802.15.4 supports communication speed of 250 kb/s on short range of about

10 m. The original standard from 2006, updated in 2011 with amendments including IEEE 802.15.4 [5], specifies additional physical layers. The version *e* of this standard enables additional modifications to the MAC layer to support time-synchronized multi-hop communications.

2.1. Communication at the physical layer

Due to its suitability for use in wireless communication with low power consumption, this standard sets the base for the design of standardized technologies such as 6LoWPAN or CoAP at higher layers. Although this technology has already been confirmed, industrial solutions are not designed to support Internet communication between sensor devices. ZigBee defines application profiles that have home automation and smart energy as the target zone, while the IEEE 802.15.4 is designed to support critical industrial applications.

IEEE 802.15.4 radio-frequency transceiver controls sensors, channel selection and signal power. The standard supports 16 channels in industrial, scientific and medical band which is 2.4 GHz. Reliability is achieved by using spread spectrum techniques with direct sequence (DSS), Ultra-Wideband (UWB) and Chirp Spread Spectrum (CSS) modulation techniques. DSS is presented in the original version of the IEEE 802.15.4 standard from 2006, while UWB and CSS are included in 2007. The main objective of these modulation techniques is to achieve reliability of transmitted information so that it occupies a wider frequency range with a lower spectral density of energy in order to achieve less interference between frequency bands, and improvement of the signal/noise ratio (SNR) at the receiver. In this standard, security is only available at the MAC layer.

2.2. Communication at the MAC layer

MAC layer controls, in addition to data services, operations such as access to a physical channel, network monitoring, checking the box, guaranteeing time slots, connectivity and security framework. Standard includes different sensor devices according to their ability and roles in the network. Full-function device (FFD) is able to coordinate the network devices, while reduced-function device RFD is able to communicate only with FFD or RFD devices. Using RFD or FFD, IEEE 802.15.4 can support network topologies such as peer to peer, star and cluster networks. IEEE 802.15.4 devices can be identified using a 16-bit (limited environment) or Extended Unique Identifier 64-bit identifier (IEEE EUI-64). 6LoWPAN adaptation layer provides mechanisms for mapping Internet standard IPv6 address in 16-bit and 64-bit identifiers.

In terms of formatting the transmitted data, the IEEE 802.15.4 standard defines four types of frames: frames with data, check boxes, beacon frames and MAC command frames. The issue of collisions during data transfer is solved by using Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) access method or alternatively a coordinator may establish super frame in which applications with pre-set requirements for the

scope can reserve and use one or more exclusive time slots. In this case, the beacon frames act as super frame boundaries and provide synchronization to other devices, and configuration information.

2.3. Communication with jumping between channels at the MAC layer

Single communication channel provided by the current version of the IEEE 802.15.4 standard can be unpredictable in terms of reliability, particularly in multi-hop scenarios and therefore is not well suited for applications with time constraints. To overcome this problem, the IEEE 802.15.4 supports multi-hop communication by introducing techniques in the form of Time-Synchronized Mesh Protocol (TSMP). TSMP protocol uses time-synchronized frequency hopping between the channels in order to cope with the effect of weakening multiple propagation paths, and external interference.

The mechanisms defined in IEEE 802.15.4 will be part of the next revision of the IEEE 802.15.4 standard and as such open the way towards the use of communication technologies in the context of time-critical applications. Devices in an Appendix to this standard are synchronized to slot the frame structure, whereas a group of slots is repeated over time. For every active slot, the schedule gives an indication to the neighboring device regarding communication and channel offset. Although the standard IEEE 802.15.4 provides a definition of how the MAC layer executes the schedule, it does not define how such an arrangement is made. Hopping between the channels also requires synchronization between the devices, which may be based on the certificate, or the context. In the first case, the receiver calculates the difference between the expected arrival of time frames and its real time and transmits this information to the sender in the relevant certificate, thus allowing the sender to synchronize its clock to the receiver clock. In the second case, the recipient only adjusts his clock with the same difference, thus synchronizing with the clock of the sender.

3. SECURITY OVER IEEE 802.15.4

The version of this standard from 2011 allows security services to the MAC layer, which despite being designed to provide a communication link layer, provides suitable security mechanisms designed to higher layers of the protocol stack.

Security modes: IEEE 802.15.4 standard supports various security modes to the MAC layer, which are described in Figure 2. The available security modes differ in guarantees for security and amount of data.

Security mode	Security provided
No Security	Data is not encrypted Data authenticity is not validated
AES-CBC-MAC-32	Data is not encrypted Data authenticity using a 32-bit MIC
AES-CBC-MAC-64	Data is not encrypted Data authenticity using a 64-bit MIC
AES-CBC-MAC-128	Data is not encrypted Data authenticity using a 128-bit MIC
AES-CTR	Data is encrypted Data authenticity is not validated
AES-CCM-32	Data is encrypted Data authenticity using a 32-bit MIC
AES-CCM-64	Data is encrypted Data authenticity using a 64-bit MIC
AES-CCM-128	Data is encrypted Data authenticity using a 128-bit MIC

Figure 2: Various security modes

- *Confidentiality:* security currently defined by IEEE 802.15.4 is optional, an application can be defined for the security of other layers of the protocol stack. For applications that require the confidentiality of communications at the link layer, transmitted data can be encrypted using Advanced Encryption Standard (AES) in counter mode, ie. using AES-CTR (AES-Counter) security mode, with 128-bit keys for support.
- *Authenticity and integrity of data:* applications that require authenticity and integrity of communication link layer can use the security mode AES with Cypher Block Chaining (CBC), producing code for message integrity (MIC) or message authentication (MAC) which is added to the transmitted data. Security techniques that support are AES-CBC-MAC-32, AES-CBC-MAC-64 and AES-CBC-MAC-128. That algorithms differ in size code integrity. This code is created on information from the 802.15.4 MAC header plus user content and in such security modes user content is transmitted unencrypted.
- *Confidentiality, authenticity and integrity of data:* CTR and CBC modes can be used for joint use of counter. They can be combined with CBC-MAC AES/CCM (Counter with CBC-MAC) mode for encryption, which is the standard used to support confidentiality, data authenticity and integrity of communications at layer connections. This mode is supported in some sensor platforms. Security modes are AES-CCM-32, AES-CCM-64 and AES-CCM-128, which differ in size of MIC code that accompanies each message. AES-CCM modes require the transfer of all fields relating to security.
- *Semantic security and protection against attacks on the feedback messages:* field counter frame and control key sub-headers can be set by the sender, and they support security in semantic terms and protect feedback messages in all IEEE 802.15.4 security modes. Counter frame sets a unique message ID and the field of control keys is controlled by the application, which can be incremented by the moment when it exceeds the maximum value of the

counter frame. Parts of the original package are sent in blocks with 16 bytes, where each block is identified by its own counter. They support semantic security and protect feedback messages, whereas each block is encrypted using a different initialization vector (IV).

- *Mechanisms of access control:* IEEE 802.15.4 standard also provides functional access control, allowing the sensor device to use the address of origin and destination of the frame, finds information and security mode that are necessary to ensure the message. Radio chips storage device access control lists (ACL) to a maximum of 255 entries, each of which contains information necessary for the security of communications for each device individually.
- *Security for a time synchronized communication:* IEEE 802.15.4 adopts protection of feedback messages and semantic security time synchronized network communications, as described. Appendix also defines the ability to use zero or 5-byte value of the field counter frame. In the second case, the value of this field is set to a global Absolute Slot Number (ASN) network. ASN stores the total number of time slots that have expired and is associated with the devices that are already on the network, thereby allowing new devices to be synchronized. In order to enable the use of ASN, the standard introduces modifications to fields of security control.

4. SECURE IOT COMMUNICATION AT NETWORK LAYER

The fundamental characteristic of the Internet architecture is that the packages enable transfer between networks using heterogeneous technologies, whereas the mechanisms required for the transport of IP packets over specific technology are defined in the relevant specifications. The IETF working group IPv6 over 6LoWPAN was formed in 2007 to specify transport of IPv6 packets over wireless networks such as low-power IEEE 802.15.4.

6LoWPAN is a key technology that supports Internet communications in IoT environment. Its adaptation is a good example how multi-layered mechanisms can enable standardized communication protocols for the IoT and IPv6 communication "from end to end" between IoT sensor and similar Internet entities. That way provides the required support for development of IPv6-based applications for the IoT. Characteristics of the IEEE 802.15.4 determine the use of optimized mechanisms to the adaptation layer.

4.1. LoWPAN format frame and header compression

As illustrated in Figure 1, the IEEE 802.15.4 supports communications at the physical and MAC layer, which allows the transfer of data communication protocols to higher layers of the protocol stack. In the absence of security at the link layer, contents for protocols on the

higher layers of the stack are limited to 102 bytes. 6LoWPAN adaptation layer optimized the use of limited space for user content by compressing packet headers and also defines mechanisms to support operations required for IPv6, in particular for the detection of neighbors and auto-configuration address. All 6LoWPAN encapsulated datagrams (IP packets) that are transferred via the IEEE 802.15.4 MAC frame. The field "type", which occupies the first two bits of the header, identifies each 6LoWPAN header and the standard currently defines four types of headers:

- 1) Headers without 6LoWPAN: indicate that given package is not intended for 6LoWPAN processing, thus enabling co-existence with devices that do not support 6LoWPAN;
- 2) Distributed headers: support IPv6 header compression, multicast and broadcast communication link layer;
- 3) Headers with mesh addressing: support forwarding of IEEE 802.15.4 frames at the link layer, as is required for the formation of a multi-hop network;
- 4) Headers with fragmentation: support fragmentation and de-fragmentation that are required for transmission of IPv6 datagrams over IEEE 802.15.4 networks.

The presence of each 6LoWPAN header is optional and the header must appear in a particular order, starting with the mesh addressing, then broadcast, fragmentation and distributed header. Support of 6LoWPAN communications is possible by using Bluetooth low energy, Digital Enhanced Cordless Telecommunications with Ultra Low Energy (DECT-ULE), ITU-T G.9959 and Near Field Communication (NFC).

4.2. Security over 6LoWPAN

- *Identification of security defects:* Request for Comments (RFC) document 4944 [6] is engaged in a discussion about the possibility of falsification or accidental duplication of (EUI-64) address, which can lead to the endangerment of global unique 6LoWPAN interface identifiers. The document also suggests that the detection of neighbors and the mesh routing mechanisms in the IEEE 802.15.4 environment are susceptible to security threats. AES link layer may provide the development of mechanisms for protection from such threats, especially for very limited devices. Discussion concerning security in RFC 6282 [7] focuses on the security problems posed by use of the mechanisms taken from RFC 4944 and security mechanisms using MIC codes are recommended.

- *Identification of security requirements and strategy:* RFC 4919 information consider addressing the different layers of the protocol stack, and the best approach depends on the required applications and limitations of a particular sensor device. Document also identifies the possibility of applying security at the network layer using IPsec protocol. Document RFC 6606 provides useful guidance in the design of specific approaches for routing and emphasizes the importance of addressing security and

utility of AES/CCM available at IEEE 802.15.4 sensor platform. The document also stresses the importance of designing security mechanisms that are able to adapt to changes in network topology and devices, before use of static security configuration. The essential are time synchronization, self-organization, provision of data and multi-hop routing of control packets. RFC 6775 deals with the optimization of enabling operation of discovering neighbors in 6LoWPAN environment.

5. SECURE ROUTING WITH RPL PROTOCOL

The working group of the IETF Routing over networks with low power losses was formed in order to solve the routing problem for IoT applications. Instant access routing in 6LoWPAN environment is materialized in the form of RPL protocol, whose internal operations and security mechanisms are discussed.

The adoption of appropriate strategies for routing the 6LoWPAN environments is a huge challenge due to different specifications for each application and limitations of used sensor devices. The consequence of this assumption is that RPL's routing must rinse the requirements of individual applications and the appropriate RFC document for each application (examples of RFC documents include RFC 5548 [8] for the city's low-power applications, RFC 5673 [9] for industrial applications, RFC 5826 [10] for applications of home automation and RFC 5867 [11] for applications of building automation).

RPL forms Destination Oriented Directed Acyclic Graph (DODAG) that has been identified for each source device and calculates the price of links. It is responsible for some features of nodes, information on the status of the node and the objective function. The topology is based on a ranking metric, which encodes the distance of each reference node, as defined by an objective function. RPL is designed to support three fundamental traffic topologies: Multipoint-to-Point, Point-to-Multipoint and Point-to-Point.

Current RPL specification recognizes the importance of protective mechanisms. It should provide routing of messages exchanged between the sensor device, so that RPL defines secure versions of various control message routing, as well as three security modes:

- *Unsecure* - in this mode, security is not applied to the control message routing, and this is the common mode used in RPL;
- *Preinstalled* - this security mode can be used by devices that use a preconfigured symmetric key to join the existing RPL instances, as a host or as a router. This key is used to support the confidentiality, integrity and authenticity of data to check control messages for routing;

- *Confirmed* - this security mode is suitable for users that operate as routers. The device can initially be connected to the network using preconfigured and preinstalled key security mode, and then a different cryptographic key is obtained with which it begins to function as a router.

6. SECURE IOT COMMUNICATION AT APPLICATION LAYER

Communication at the application layer is supported by Constrained Application Protocol (CoAP) [4], which is created by the working group CORE (Constrained RESTful Environments) IETF.

CoAP protocol implements a set of techniques to compress metadata without compromising interoperability and in accordance to the Representational State Transfer (REST) architecture network. CoAP is defined for communication over User Datagram Protocol (UDP) 6LoWPAN, while Transmission Datagram Protocol (TCP) is still in development.

Communication at the application layer enables IoT sensor applications interoperability with existing web applications without requiring special application-oriented-code or mechanisms for translating the address. CoAP restricts Hypertext Transfer Protocol (HTTP) syntax on a subset adapted limitations of 6LoWPAN sensor device and can be separated to allow communication between users, applications and such devices, in the context of IoT applications. CoAP protocol provides a request/response communication model between the end-points and applications to use key concepts of networks, in particular the use of Uniform Resource Identifier (URI) to identify resources available on a limited sensor devices. The protocol can support communication "from end to end" at the application layer between the limited sensor devices and other Internet entities, using only CoAP or alternatively translating HTTP to CoAP to reverse or direct gateway.

Messages within the CoAP protocol are exchanged asynchronously between two end-points, and are used to transfer CoAP requests and responses. Since these messages are transmitted over unreliable UDP protocol, CoAP allows simple mechanisms for reliability. By using these mechanisms, CoAP messages can be marked as the check for which the sender triggers a simple "stop and wait" re-transmission mechanism with exponential back-off strategy of withdrawal. The recipient must confirm the appropriate message or to reject it using the reset message. Appropriate check and reset messages are associated with a confirmation messages via message ID, along with the address of the corresponding end-points. CoAP messages can also be transferred from the lower reliability and in this case the recipient does not confirm that he has received the message.

In addition to a core set of information, most of the data in the CoAP are transmitted using this option. Options may be critical, secure and unsecure. Critical option is the obligate end-point, while elective end-points may be

ignored or not recognized. Secure and unsecure options specify how the option will be processed by the intermediate entity. Unsecure option must be accepted by the proxy server to be transmitted, while the secure option is forwarded even if the proxy is not able to process it.

CoAP header and the message format are shown in Figure 3. The message starts with a 4-byte fixed header, formed by a version field (2 bits), the T-field (message type, 2 bits), token length field (4 bits), field code (8 bits) and the message ID (16 bits). Token allows the entity to perform an operation connecting CoAP requests and responses, and the message ID supports detection of duplication and optional reliability.

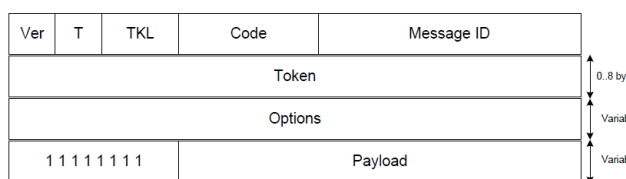


Figure 3: CoAP header and message format

6.1. CoAP security

CoAP defines connection with Datagram Transport-Layer Security (DTLS) to provide CoAP messages with certain minimum modifications in order to accommodate limited environments. DTLS supports confidentiality, authentication, integrity, non-repudiation and protection against attacks on the feedback messages and for communications at the application layer using the CoAP. The adoption of DTLS implies that security is supported at the transport layer. DTLS is essentially Transport-Layer Security (TLS) with improvements for unreliable nature of UDP communication.

The impact of DTLS on wireless sensor devices exists thanks to the support of initial protocol handling and security for each exchanged CoAP message. AES/CCM was adopted as a cryptographic algorithm to support the essential requirements for security in the current CoAP specification. The directed activity against attack response can also be achieved in the context of DTLS, using a different current value for each package provided by CoAP.

Security modes in CoAP are defined as annexes adopted by DTLS. CoAP currently defines four types of security modes that applications can use, and they differ in the way the negotiations take place around the key and authentication:

- *Disable security:* this mode in practice does not allow the use of secure CoAP transmitted messages;
- *Advance prior assigned keys:* this security mode can be used for sensor devices that are pre-programmed using symmetric cryptographic keys. They are required to support secure communication with other

devices or group of devices. This mode is suitable for applications that use devices that cannot support public keys. Applications can use one key by the target device or in the extreme case, one key group of destination devices.

- *Original public key:* This security mode is suitable for devices that require authentication based on public key, but cannot participate in the public key infrastructure. The device has an identity created from public key and leaves identity and public keys of nodes with whom it can communicate. This security mode is defined as mandatory for the implementation of the CoAP.
- *Certificates:* This security mode also supports authentication based on public key, or for applications that can take part in the chain of certification.

7. CONCLUSION

The aspect of IoT security is processed through the layers on the protocol stack. It can be concluded that the security solutions for IoT are based on solutions proven in traditional networks, with suiting limitations of connected devices and the complexity of IoT applications. The problem of authentication may also be pointed out as a challenge that will engage experts in the field of IoT in the future. Today's development has often the focus on the application and the expense of protection against abuse of the collected data.

REFERENCES

- [1] S. Krčo, B. Pokric, F. Carrez, "Designing IoT architecture(s): A European perspective", *Proc. IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, Korea, March 2014, pp. 79-84
- [2] N. Kushalnagar, G. Montenegro, C. Schumacher, "IPv6 over low-power wireless personal area networks (6LoWPANs): Overview, assumptions, problem statement, and goals", *IETF RFC 4919*, August 2007.
- [3] T. Winter, et al., "RPL: IPv6 routing protocol for low-power and lossy networks", *IETF RFC 6550*, March 2012.
- [4] Z. Shelby, K. Hartke, C. Bormann, "The constrained application protocol (CoAP) ", *IETF RFC 7252*, June 2014.
- [5] IEEE Std. 802.15.4a, "Specifications for Low-Rate Wireless Personal Area Networks (WPANs)", Sep. 2011.
- [6] G. Montenegro, et al., "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", *IETF RFC 4944*, Sep. 2007.
- [7] J. Hui, P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", *IETF RFC 6282*, Sep. 2011.
- [8] M. Dohler, et al., "Routing Requirements for Urban Low-Power and Lossy Networks", *IETF RFC 5548*, May 2009.

[9] K. Pister, et al., “Industrial Routing Requirements in Low-Power and Lossy Networks”, *IETF RFC 5673*, Oct. 2009.

[10] A. Brandt, J. Buron, G. Porcu, “Home Automation Routing Requirements in Low-Power and Lossy Networks”, *IETF RFC 5826*, April 2010.

[11] J. Martocci, et al., “Building Automation Routing Requirements in Low-Power and Lossy Networks”, *IETF RFC 5867*, June 2010.

SOFTWARE ALGORITHM OF DEVICE FOR BIOMETRIC IDENTIFICATION OF MATERNITY – PARENTHOOD

KOMLEN LALOVIĆ

Information technology school - Belgrade, Komlen.Lalovic@its.edu.rs

JASMINA NIKOLIĆ

Belgrade University, Jnikolic@fil.bg.ac.rs

TOT IVAN

Military Academy – Belgrade, Ivan.tot@va.mod.gov.rs

ŽANA LALOVIĆ

Golden Mind doo – ICT Company, New Belgrade, Office@GoldenMind.rs

Abstract: In this work it will be shown algorithm written in pseudo-code presented for each functionality that device posses, besides algorithm device will be shown throw many figures how the model is made, how cross-state look like and how it is constructed. In details will be presented what are possible advantages and benefits, what is qualitative jump in Health Care system, precicely in birth places as part of Health Care system worldwide. Possible wireless communication and storage types for fingerprint dana scanned from mother an baby together at moment of birth and generated unique ID reference, which will be encrypted and that dana will guarantee parenthood - maternity in 100% over every new born baby.

Keywords:

Algorithm, Baby, Biometry, Birth, Fingerprint, Mother, Patent, Pseudo-Code.

1. INTRODUCTION

There are various definitions of Algorithm1 in different science fields and disciplines. As for a computer science algorithm, it is a step by step set of commands, instructions and operations that are going to be performed. The purpose of algorithms is to provide calculation, the automatization of actions and data processing.

An algorithm is a set of steps as explained. One has to learn how to make algorithms using pseudo-code or real code and that is why people who develop algorithms need to have programming knowledge. [1]

If you want to optimize your algorithms, then you have to possess the knowledge of mathematics as well. In the end, you have to have some basic knowledge about all that, since it represents a combination of various knowledge. [2]

Good news is that learning about algorithms can be as simple as you want it to be, and as easy as you are able to acquire. [3]

If you want to optimize your algorithms, then you have to possess the knowledge of mathematics as well. In the end, you have to have some basic knowledge about all that, since it represents a combination of various knowledge.

In an attempt to solve a large human issue and remove bad shadow from possible past events in many countries, i.e. stealing or replacing the identity of new born babies, also preventing that kind of fear that all future mothers

¹ **Algorithm** – “Was al-Khwarizmi an applied algebraist?”, Oaks, Jeffrey A, University of Indianapolis. Retrieved 2008-05-30.

have, and make that bright moment of bringing new life to this world easier and more relaxed to gynecologists, midwives and nurses, this Patent device – Device for biometric identification of parenthood – maternity and this algorithm as the part of its software have been developed.

This work presents all the functions that the device possesses. The figures show how the model is made, how cross-state looks like, how it is constructed and implemented, what are possible advantages and benefits and what is a qualitative leap in Health Care system, precisely in maternities worldwide. The possible wireless communication and the storage types of fingerprint data are scanned from a mother and a baby at the moment of birth, simultaneously, and the unique ID reference is generated, which will be encrypted and will guarantee maternity of every new born baby with the probability of 100%.

The invention, generally, placed in filed applied Information technology, biometry system. Device makes a unique Identification (ID²) reference and that reference will be the Identifier for each “mother-baby relationship” for every newborn baby in maternities. [4]

According to the International classification of Patents, this patent is classified with a symbol **G06F21/00** which belongs to the biometry systems – devices for fingerprint scanners.

2. MATERIAL AND METHODS

Technical issue which needs to be set, examined and solved with this Algorithm of the Patent device consists of three partial task as follows:

- Writing one optimal algorithm for emulating and executing every function that device for biometric identification of maternity- parenthood possesses. In future, the realization will give recommendations for traversing that pseudo-code in accurate programming language, probably C programming language, since it has to be structural and low level, not OO and high level programming language as it is JAVA or C++ . It is very important that the algorithm realization is applicable for each existing platform including hardware and software,

² **ID – IDENTITY** (unique data for each fingerprint scanning process)

and C programming language is a proper choice for that. [3] [4]

Beside its common purpose and scanning two fingers of different persons at the same time it will provide a unique ID reference (similar Primary Key) which will be the base for every pair of a scanned mother-baby pair. [5]

3. EXPERIMENT

According to modern well known technical devices – fingerprint scanners which use different algorithms and methods in their process of work to determine the identity of individuals.

After having searched through the National base of Patents similar devices with this aim were not found, concretely dual biometric scanners, which contain their own lighting, battery supply and none of the Patents consider this idea and solution in this way, with dual biometric scanner.

Existing devices scan one or more fingers of **one** person only, we are emphasizing the fact that it is only one person, and there are no fingerprint scanners which scan fingers of two different persons at the same time using one device, especially not devices which make unique ID reference during scanning which will be connected with the record of fingerprint scanned and stored data.

In the issued Patent confirmation **II-2009/0253**, International classification **G 07 D7/12 (2008.04)** a device named “Hand mobile device for checking travel and personal documents, reading biometric data and face recognition of persons which carry those documents” is described, only one function of the device is scanning the fingerprint of one person at one moment. [6]

4. DISCUSSION

Also in the issued Patent confirmation 13848069.4 dated April 2, 2013, with remark WO2014059761 and classification G06F21/00, we can meet with classic scanner named “Fingerprint identification device”, where is completely described device which has a function of scanning and gives us data about the fingerprint of person (extractor software for *minutiae*³). [1]

³ **Minutiae** – fingerprint specific points visible on a finger image

However, this device does not have two fields for simultaneous scanning the fingers of two different persons, which at the same time generates unique unchangeable ID reference and is an additional guarantee of a person's identity and guarantee the of Parenthood of baby – precisely the maternity of a newborn baby.

Essence of innovation is dual biometric scanner has two fields for scanning fingerprints of a mother and the baby or two babies (one after another) if they are twins, or three or more, simultaneously, at the very moment of birth. Precisely one field is larger with the classic scan resolution of 500 dpi and the second field is physically smaller but with larger scan resolution – of minimum 1000 dpi so it can make scan of a baby fingerprint that is very small.

Science fact, or rather an axiom, in biometry as a branch of Advanced security systems, Discipline - Informatics and Computing, Science Field - Natural Sciences and Mathematics, is that fingerprint is formed during prenatal period for every fetus and stays constant in the shape of minutiae during whole life. [1]

According to many researches realized on fingerprints of fetus, ultra waves and biometry scanning the minutiae on each finger are formed by the end of 7th month of pregnancy. It is important to mention that babies who are born before regular time of birth, during 8th, and especially by the end of 7th month of pregnancy have fingerprint on each finger, both hands and foot's fingers already formed. [1]

This scientific fact is essential for this device, this research and the realization or the Project that will provide a qualitative leap in gynecology and midwifery and nursing in every maternity all over the world.

This is essential because minutiae – ridges and valleys are the only biometry that is formed prenatally and it can be used for the purpose of guaranteeing biometry identity. The whole idea for Patent Innovation is based on this scientific fact confirmed by both biometry system as Computer science and gynecology – midwifery as a branch of HealthCare protection system. [1]

Other biometrics such as Iris recognition is unstable, because until 4th year the pigmentation in children's eye is changing and becoming different. The shape and color both change which makes it impossible to be used for this purpose and for this goal.

The head, hand and body shape and size are rapidly changing since they normally grow up so it is obvious why they cannot be used. That is why this incredible scientific fact that fetus's fingerprint is formed prenatally, by the end of 7th month in a uterus of a pregnant mother and stays constant with the same construction of minutiae, is so great that is amazing.[1]

There are a large number of various fears during birth process, both of mother and of people in medical Care system in maternity. Reading and learning on study which was made in Australia and New Zealand from 2009 until 2011 and 17 workshops with over 700 midwives this device can prevent a part of one of those big fears – dealing with unknown (33 Fears). [7]

The data received during the process of fingerprint scanning of a mother and the baby, together with unique ID reference is encrypted and stored on the device's memory or on a server in encrypted form. The device shall never be left opened and available for public, and only authorized nurses, doctors and midwives shall have contact with it in maternities.

During every next process of scanning when the confirmation of parenthood, precisely maternity shall be confirmed for each pair – person with the baby, the authorized person-representative of a maternity and the mother shall enter PIN⁴ code that only they possess for their data. [8]

The change of stored data will be disabled and identity of a new born baby is guaranteed 100% and there is no possibility of making mistake during this process with the Patent device.

At any time it is possible to check parenthood and maternity of every baby in each maternity worldwide.

Information stored on the device or server with its backup copy are always in encrypted form and there is no possibility of corrupting or deleting this data. Just the possibility of archiving data is enabled after the confirmation of the mother that everything is fine and after this pair (mother-baby) leaves the maternity. That is the moment when proving the guarantee of maternity is no longer necessary. [9]

⁴ PIN – Personal Identification Number

It prevents any possible theft or replacing the baby's identity, which has unfortunately been probably happened at some places and parts of the World, especially in South-East Europe, in the Balkans, countries of former Yugoslavia. Now the device will guarantee, prove and serve as the evidence of maternity of newborn babies.

The inventor of the Patent has taken maternity symbolically because the maternal instinct is the strongest instinct in nature.

The application of the device is universal, on every Continent and Country, and there are no restrictions on the use. It requires basic IT equipment – PC, Server and this Patent device which is a dual biometric fingerprint scanner. The price of the device is not high and it can be installed in every maternity in the Health care system of each Country. [10] [11]

Benefits of the patent device:

- proof and evidence of parenthood for every newborn baby
- no possibility of replacing or stealing identities of newborn babies
- its own energy supply with batteries or an adapter connector with DC supply
- small size, low weight and portability - good price quality ratio, environment friendly - wide range of application and usage.

5. RESEARCH & DEVELOPMENT

For better understanding of functionality and usage of the device and its practical realization there is figure 3 that show the device in various views and cross-section of the Patent device. [12]

Figure 1 shows Algorithm1-Algorithm for determination of Identity of Parenthood – Maternity and new scan of minutiae. It starts after powering device On and choosing option 1 on device display. After starting device and choosing option 2, software initializes Algorithm2 – for checking identity of parenthood-maternity. [13]

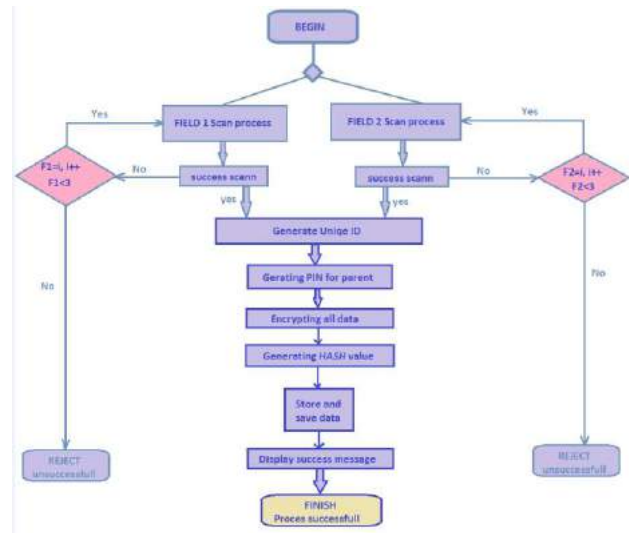


Figure 1: Data acquisition

Figure 2 shows all functionality, logic and behavior of this algorithm. Based on figure preview the conclusion can be derived about the possible usage of both cases and a sequence diagram of procedures and activities of software.

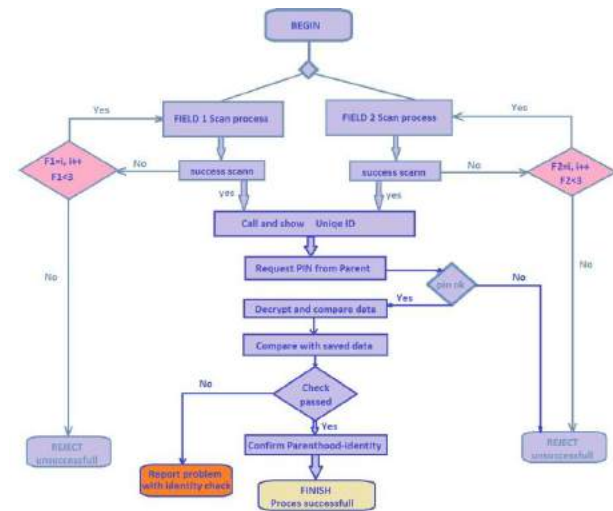


Figure 2: Data verification

Figure 3 shows the device for biometric identification of maternity in whole with digital display, switch and two fields for fingerprint scanning. [14]

The figure contains remarks as follows:

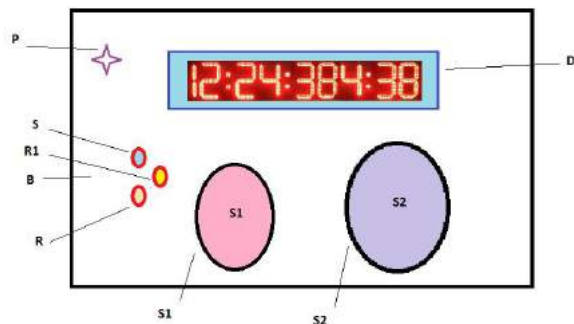


Figure 3: Device overview

6. FURTHER DEVELOPMENT

Software Algorithm of Device for biometric identification of maternity-parenthood is realized in pseudo-code in this work. It is also shown in details in figures 1 and 2 which show the essence of idea and programming. In future development it can be written in concrete programming language such as C.

Also, it can be a part of a much larger Health Care system regarding small children in pediatric institutions, where the device can provide basic data about possible allergies of each child and can improve that part of health care system globally.

7. CONCLUSION

Its essence it can share and spare on different ways in different areas of social and Health Care systems. It is modular, it can be updated and what is most important, it can be a base for some future development in the area of biometry systems. The device can be applied in dozen countries in a fight against the organized crime and help prevent thefts or replacements of newborn babies, especially in territories with low IT infrastructure and technological development.

Each biometry tries to minimize **FAR**⁵ and to maximize **FRR**⁶ in attempt to be much more accurate and secure. FAR and FRR are percentage of number of false in

⁵ **FAR** – False Accept Rate

⁶ **FRR** – False Reject Rate

acceptance or reject rate in Biometry. This device has accomplished that part since it combines two scanned data and its accuracy grows exponentially.

In modern countries it can provide a totally new quality of Health Care service, also help the staff in maternities, make process of birth much easier, relax in some way, for both future mothers the gynecologists, midwives, nurses, to put it short lines - for everybody. Baby has his own ID!

ACKNOWLEDGMENTS

Authors want to thank all people of good and open mind who helped this Patent – Innovation become very important and popular in the Republic of Serbia. A great thank you to all written media such as: Lepota i zdravlje, Lisa magazine, Ilustrovana politika, ALO magazine and Televisions with National frequency: RTS – Beogradska hronika, RTV Prva, RTV Pink and Regional TV Stations such as: TN N1, Kopernikus, YU EKO RTV Subotica. A special thank you to people who work at the Institute for Intellectual Property of the Republic of Serbia, MSc Saša Zdravković and nd the greatest thank to pregnant oman Jellena Lalović and baby Stefan.

REFERENCES

- [1] Handbook of biometrics, Anil K. Jain-*Michigan State University, USA*, Patric Flynn-*University of Notre Dame, USA*, Arun A. Ross-*West Virginia University, USA* (2008), Sringer, USA
- [2] Milosavljević, M., Grubor, G. (2007): *Osnovi bezbednosti i zaštite informacionih sistema*, Fakultet za poslovnu informatiku – University of Singidunum, Belgrade, Serbia
- [3] C PROGRAMMING TUTORIAL, Simply Easy Learning available on URL - http://www.tutorialspoint.com/cprogramming/cprogramming_tutorial.pdf
- [4] JAVA 7EE TUTORIAL, http://www.tutorialspoint.com/java/java_decision_making.htm
- [5] <http://www.epo.org/index.html>
- [6] <http://www.zis.gov.rs/pocetna.1.html>

[7] What do midwives fear? Authors: Hannah Grace Dahlen, Shea Caplice, Published Online: July 24, 2014 – Elsevier, *Women and Birth, Journal of Australian College of Midwives*

[8] <http://neurotechnology.com>

[9] Before We Are Born, 9th Edition, Authors: Keith Moore, T.V.N. Peraud, Mark Torchia, Elsevier UK, Saunders, ISBN: 9780323313377, 2014

[10] NIST publishes compression guidance for fingerprint, Journal Elsevier - biometric technology Today, Volume 2014 Issue 4, April 2014, Pages 12

[11] Algorithms (4th Edition) Hardcover, Authors: Robert Sedgewick, Kevin Wayne, – March/19/2011, ISBN-13: 978-0321573513 ISBN-10: 032157351X Edition: 4th

[12] Komlen Lalović, “New system of identification newborn babies and parenthood guarantee based on biometry”, University of Singidunum, July 2016.

[13] Komlen Lalović, Milan Milosavljević, Nemanja Maček, Ivan Tot, “Device for biometric identification of Maternity”, Serbian Journal of Electrical Engineering, Vol. 3, October 2015, DOI: 10.2298/SJEE1503293L.

[14] Nemanja Maček, Borislav Đorđević, Jelena Gavrilović, Komlen Lalović, “An Approach to Robust biometric Key Generation System Design”, *Acta Polytechnica Hungarica Vol.12, No.8, Year: 2015* DOI: 10.12700/APH.12.8.2015.8.3, Im. F. 0.65

***CryptoSMS* ANDROID APPLICATION**

JOVANA ĐUROVIĆ

University of Defence, Military Academy, Belgrade, jovanadjurovicloki@gmail.com

BOBAN MIHAILOV

Serbian Armed Forces, CKISIP, Belgrade, b.mihailov@ymail.com

IVAN TOT

University of Defence, Military Academy, Belgrade, totivan@gmail.com

IVANA OGNJANOVIĆ

Univerzitet Donja Gorica, ivana.ognjanovic@udg.edu.me

Abstract: *There are serious security risks that follow smartphones which includes Android cellular telephones. According to the claims of experts in the fields of mobile phones, it is known, for years already, that, from the aspect of security, the whole infrastructure of mobile phones is almost useless, and this is a fact that no one would refute. This is certainly exploited by, among others, those who wish to acquire certain data. Concerning the issue of which of the three following communication channels is the most secure: a call, an SMS message, or communication via the Internet, the latter prevails. The potential of Android mobile platform protection achieved by CryptoSMS application, which was created as a response to the task of preventing security lapses, more promptly to prevent certain people, who can record mobile communication, from spying on SMS messages, is shown in this paper.*

Keywords: *Android, SMS, security, cryptographic algorithms.*

1. INTRODUCTION

Today, it is unimaginable to work, provide services, information of high quality and exchange information without modern information technologies. Up until recently, paper has been used to communicate and great deal of time has been spent filling forms and reports. Information technology plays a key role in everyday life of today's society. It is used in every aspect of life.

In the last few years a huge increase of number of mobile phones in the population has been noticed. Because of that there is a need for cellular telephone application development so it would become more user friendly. *Android* operating system takes precedence in operating systems for mobile phones.

Android Inc which was sponsored by *Google*, and later in 2005. bought by it, created *Android* operating system. *Android* was presented for the first time in 2007. *Android* operating system is used for cellular telephones more than any other operating system. It is based on *Linux kernel* and it is usable for most mobile phones, tablet computers, *notebook* computers, *netbook* computers, *smartbook* computers, e-book readers, even for watches. *SQLite* database is used as data storage. *Android* supports connection technologies, such as *GSM/EDGE*, *CDMA*, *Bluetooth*, *Wi-Fi*, *LTE* and *NFC*. It also supports *SMS* and *MMS* and large number of languages. Additionally, it has modern *Web* browser, as well as different multimedia formats.

As well as every other mobile platform, *Android* mobile platform has some security flaws. Most of types of attacks on *Android OS* has already been seen in some form on different mobile operating systems. As the number of users grows so does the number of threats to *Android OS* and being the most used the number of threats is also the largest.

To develop its security, test application *CryptoSMS* that enables coded *SMS* exchange has been presented. This way secure flow of information has been provided.

2. SECURITY OF ANDROID OPERATING SYSTEM

Looking at scientific research program of mobile phones experts it has been known for years that the whole infrastructure of mobile phones is under great security risks and threats. This fact allows access to information to those who are not meant to see it [2] [6] [7].

If someone decides to encrypt or lock their data, they have to overcome certain logical obstacles at the start. For installation of encryption to be successful users at both ends need to install it. It is not enough for one user to encrypt their data. That way the data sent to the other user will be just a pile of unwanted data that can't be decoded. [1].

Other experts suggest that users should pay attention to certain characteristics of programs that are offered to them. *Android* applications should be made in accordance with the principle of open code. In other words, source code

should be visible to anyone who wants to see it. The best way for protection is to show how security is applied.

There are many free programs on the Internet with open source that make it difficult to listen in on or follow communications. To protect their smart phones, different programs are suggested for coding text and multimedia messages, for voice encryption in real time and for e-mail protection.

Users should ask themselves how much of their privacy are they ready to let go of. *G-mail* address is much more than regular e-mail address. At the same time user accepts that his mail goes through checking for marketing purposes.

Many programs, like *G-mail* and *Facebook*, look for user's approval to check their messages when they are sent via those programs. Applications for mobile phones with *Android OS* look for the same approval but it is made as a warning for users before they install a program. That is the moment when user can stop and think – why does the application look for access to user's phone book?

Vulnerabilities of *Android* devices are always assessed. Fact that *Android* devices are relatively new on the market and there are always new models and operating systems created makes it hard for experts to define all the vulnerabilities and risks [3].

Main concern of corporations is vulnerability of *Android*, because there is no proof of security and the risks are not fully known. That is the reason why corporations' smart phones are widely targeted, while their use is what hackers are mainly focused on [4].

3. IMPLEMENTATION OF THE CRYPTOSMS SECURITY SOFTWARE

SMS messages being sent from one mobile device to another are not protected, which means that there is a possibility that cyber criminals could intercept and access potentially sensitive data. The task is to develop an application which will guarantee a safe and secure data flow via *SMS*. The idea is to prevent illegal users from intercepting data traffic by implementing application layer security. In the event of data interception, hackers will not be able to utilize the actual data because it would be, as mentioned, previously protected.

Android mobile platform supports a multitude of cryptographic algorithms for use in data protection, both symmetrical and asymmetrical. Depending on users' needs, the most reliable algorithm will be used. Concerning symmetrical algorithms, because the same key is being used on both the sending and the receiving side, the problem is ensuring a secure key interchange. On the other hand, asymmetrical algorithms, which are usually by one order of magnitude slower than symmetrical algorithms, are suitable for solving this problem (secure key interchange), because they utilise a public key which is available to everybody. If we ignore the process of key/keys interchange, the question of choosing between these two types of cryptographic algorithms arises.

From the execution speed standpoint, symmetrical algorithms impose themselves as a logical choice (image 1). Considering the fact that the algorithm itself is executed on a mobile device, execution speed is an important factor in choosing the cryptographic algorithm to use.

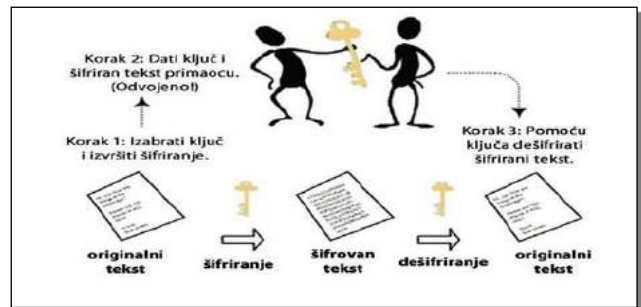


Image 1: Representation of encryption and decryption processes using a symmetrical algorithm

Thanks to extensive research, conducted in the course of previous years, a symmetrical cryptographic algorithm known as *AES* proved to be the most secure. *AES* algorithm implements encryption and decryption operations on a block of data in a variable number of cycles. The number of cycles depends on key length and equals 10/12/14 for the 128/192/256 bit key, respectively. Prior to encryption or decryption, key expansion is performed. Block encryption systems are utilized in one of the so-called block cypher modes of operation. In terms of cryptography, a mode of operation implies a method of usage of a base algorithm and usually involves a combination of some sort of a loopback and specific basic operations. Operations performed on the algorithm are usually fundamental in nature because the aspect of security is determined by the base algorithm itself and not the mode of operation. In the *CryptoSMS* software, *CBC* (*Cipher Block Chaining*) mode is implemented [5].

The application in question was developed for *Android 5.0.1* operating system, using *Android Studio*, because the earlier versions of the *Android* operating system do not possess the necessary features for some newer technologies and the fact that the popularity of the newer versions of *Android* operating system greatly surpasses that of the previous versions.

In order for the application to be able to utilize the features and services of the mobile device it must be provided with the necessary permissions. By analyzing possible application usage and resources needed for proper function, *SEND_SMS*, *READ_SMS* and *RECEIVE_SMS* services were determined as necessary. These permissions were implemented in *AndroidManifest.xml* file, and the users themselves permit the usage of those services in the installation process.

While designing the application, the necessary classes and methods were imported into the project so connection to the service could be established

For the means of display optimization, components which take up relatively little space on the display and enable dynamic display expansion depending on the data influx

were used. One of such components which was used extensively in the application is *ListView*. When using the aforementioned component, it is possible to set up the appearance of a single link, a *Listitem* and the data source, and the *ListView* control simulates the contacts list in the *CryptoSMS* application.

The database, implemented in the test application, enables the creation of a phonebook that is useful but not necessary for the application operation. Considering that the user, recipient and sender information needs to be saved because it is used in application operation, the process of basic data storage is enabled using a local database. Although *SQLite database* is relatively lightweight, in this instant it is an excellent option because such simple information does not require much space. In order for the *SQLite database* to be used, it is necessary to implement *Database Helper*. *Database Helper* is an auxiliary class used to manage the created database. It is an extension of *SQLite Open Helper* class which is used to establish a connection to the database if it exists, creates it if it doesn't, and upgrades it if necessary via *onCreate*, *onUpgrade* and *onOpen* methods.

SMS Manager which controls operations such as data, text and *PDU SMS* message transmissions is used to send *SMS* messages. By tapping the Send button in the *CryptoSMS* application, the text is encrypted and the recipient receives an encrypted message which can be decrypted only if they possess this application. Encryption, as well as decryption, is conducted using *AES* symmetrical cryptographic algorithm in *CBC* mode (image 2). Using the *Toast* component, which provides simple feedback about the operation performed, any errors that can arise are processed.

```
public static String encrypt(String key, String initVector, String value) {
    try {
        IvParameterSpec iv = new IvParameterSpec(initVector.getBytes("UTF-8"));
        SecretKeySpec skeySpec = new SecretKeySpec(key.getBytes("UTF-8"), "AES");

        Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5PADDING");
        cipher.init(Cipher.ENCRYPT_MODE, skeySpec, iv);

        byte[] encrypted = cipher.doFinal(value.getBytes());

        return Base64.encodeToString(encrypted,1);
    }
    catch (Exception ex) {
        ex.printStackTrace();
    }

    return null;
}
```

Image 2: Representation of *SMS* encryption via *AES* cryptographic algorithm

SmsBroadcastReceiver class, as an extension of *BroadcastReceiver* class, imports messages from the mobile device. When *SMS* is received by the mobile device, it is forwarded to *SmsBroadcastReceiver* which receives the *SMS* in the form it was sent. This class does not perform decryption as that is conducted by *SimpleCrypto* class. *SmsBroadcastReceiver* only receives the message and activates *SmsReader*. An example of *SMS* message extraction is given in image 3. *SmsReader* displays the *SMS* message after reception.

```
public void onReceive(Context context, Intent intent) {
    Bundle intentExtras = intent.getExtras();
    if (intentExtras != null) {
        Object[] sms = (Object[]) intentExtras.get(SMS_BUNDLE);
        String smsMessageStr = "";
        for (int i = 0; i < sms.length; ++i) {
            SmsMessage smsMessage = SmsMessage.createFromPdu((byte[]) sms[i]);
            String poruka = smsMessage.getMessageBody().toString();
            String brojPosiljaoca = smsMessage.getOriginatingAddress();
        }
    }
}
```

Image 3: *SMS* message extraction

When the user receives the *SMS* message, after accessing the inbox of the application, layoutactivity_sms.xml enables the display of sender information and of the message itself in decrypted form. *ListView* component which, depending on the message length, makes changes dynamically, is also used to display this activity. Image 4 represents the *SMS* message decryption process via *AES*.

```
public static String decrypt(String key, String initVector, String encrypted) {
    try {
        IvParameterSpec iv = new IvParameterSpec(initVector.getBytes("UTF-8"));
        SecretKeySpec skeySpec = new SecretKeySpec(key.getBytes("UTF-8"), "AES");

        Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5PADDING");
        cipher.init(Cipher.DECRYPT_MODE, skeySpec, iv);

        byte[] original = cipher.doFinal(Base64.decode(encrypted,1));

        return new String(original);
    } catch (Exception ex) {
        ex.printStackTrace();
    }

    return null;
}
```

Image 4: Representation of *SMS* decryption via *AES* cryptographic algorithm

4. USER INTERFACE

On application startup, a splash screen appears which serves as a feedback that the application has started, while in the background the environment is being initialized. After the splash screen, the *Main menu* page is displayed.

Main menu page prompts the user with three options:

- *Create an encrypted message,*
- *Phonebook* and
- *Received messages.*

Tapping on the *Phonebook* button, the contact list activity is displayed which enables the user to add a new contact by tapping the button *Add new*. If fields *Name* and *Phone number* are left blank, after the *Save* button is tapped, a notification informing the user that all fields need to be filled out is shown (image 5).

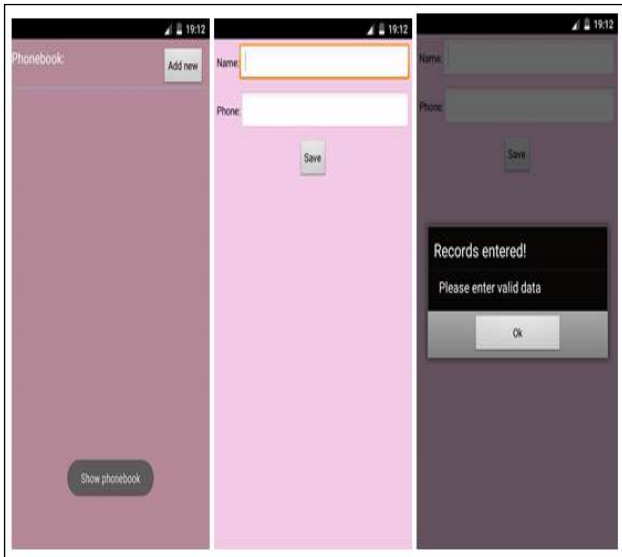


Image 5: Add new contact page

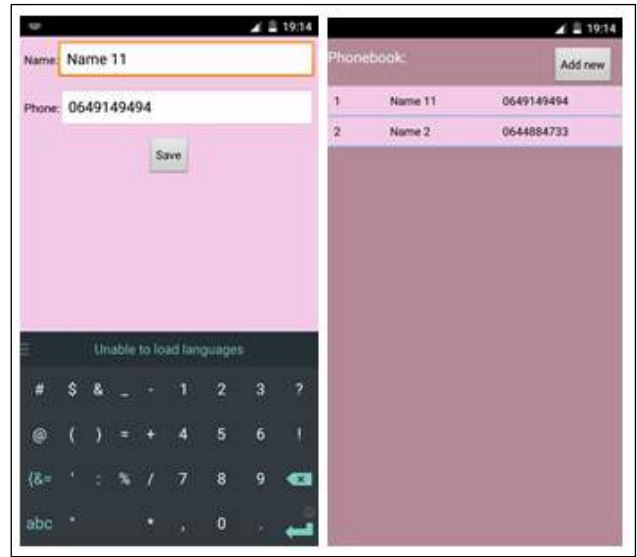


Image 7: Updating a contact

Deleting a contact from the phonebook is performed holding down the contact that is to be deleted (*ListItem* component) after which the user is prompted with the delete option (image 6).

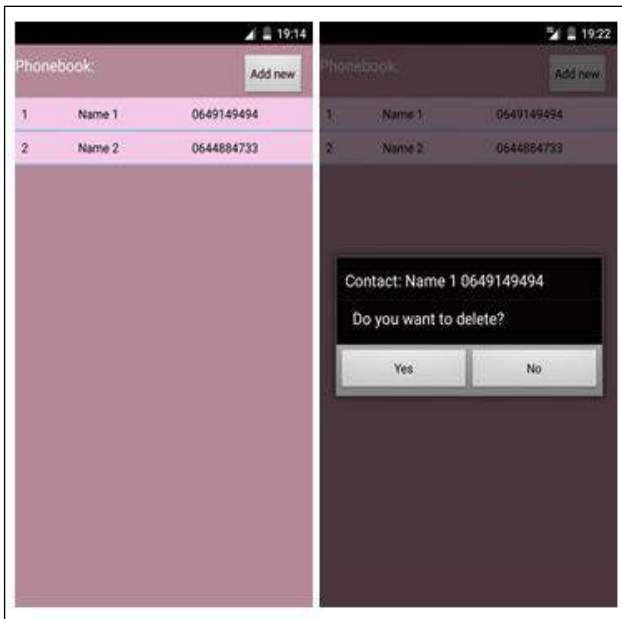


Image 6: Deleting a contact

Contact update (image 7) is done by tapping the contact in question. The updated contact is saved in the *SQLite* database and in further operation the contact will be stored in the phonebook.

The *Create an encrypted message* option is used for creating a message and selecting a contact to which the message is to be sent (image 8). Test application provides an option not to select a contact from the phonebook, but to enter the recipient number manually if that recipient was not previously added to the phonebook. By tapping the “+” button, a list of contacts stored in the phonebook will be displayed using a *Spinner*. After contact selection the message transmission is enabled because the message recipient is defined. After defining the recipient, the message intended for that recipient can be entered. After tapping the text input control, the keyboard is displayed which greatly increases input speed and reduces the probability of error.

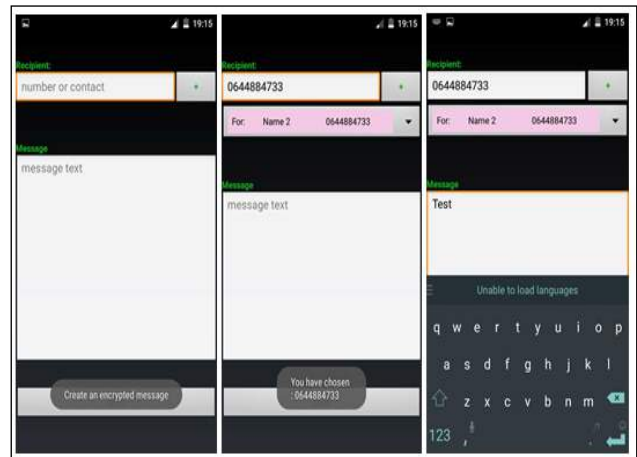


Image 8: Creating an encrypted message

SMS message is ready to be sent. Tapping the *Send* button multiple actions are performed:

- Encryption process is activated,
- Message is sent,
- Notifications about successful/unsuccessful operations during message transmission are displayed,
- If the *SMS* message is not delivered error processing is performed.

Assuming the message was sent successfully, the receiver would be able to open and read the message on their device. The message will be stored in the core messaging application on the device in encrypted form (image 9). This forces the illegal user who wishes to view received messages to decrypt the encrypted content. There is only one way of decrypting the content of such a message and that is via *CryptoSMS* application. Using the test application shown in this paper it is possible to view the actual content of the message.



Image 9: Representation of the received encrypted message

When a message is received, thanks to the built-in *Toast* control, the sender and content of the message will be displayed. Accessing the application itself and its *Received messages* option reveals the sender and the decrypted message content (image 10).

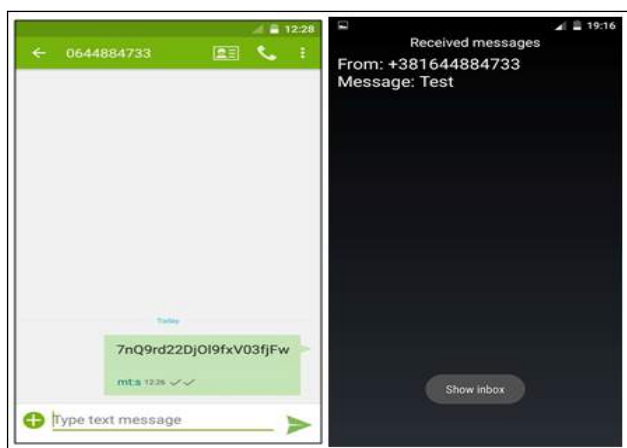


Image 10: Received and decrypted message in *CryptoSMS* application

As an end result, the security of *Android* mobile platform is improved. Testing consisted of using this application on real devices in communication between two or more users. If the aforementioned application requirements are met, the user can be certain that the content sent/received via *SMS* is not exposed to risk because the protection is implemented on the application layer. It is worth mentioning that absolute security does not exist, but it is

important to strive towards improving the existing solutions so every security risk can be resolved.

5. CONCLUSION

Security of the operating system is one of the biggest problems. With new discoveries come new problems that need to be solved. *Android* is a promising project. One of its main qualities is good organization that has a potential to use all the power and knowledge of the open source community.

While there is technology development, maintaining the security of every component will be the main mission. Innovations are what makes people want to improve themselves. Flaws are made knowingly, because that way people are going to want to improve and to look for new undiscovered facts. Security and protection of mobile phones are two of the main problems of today's society.

CryptoSMS application has already exceeded expectations. Next development of the application will be in the field of security and in its possibilities of applying it in reality. Expanding the functions or even making new ones is the main idea.

REFERENCES

Books:

- [1] Hoog A., "Android forensics", (Vol. 1st Ed). Waltham, MA, USA, Syngress, 2011., ISBN: 978-1-59749-651-3
- [2] Rogers D., "Mobile Security: A Guide for Users", Copper Horse Solutions Limited, 2013., ISBN 978-1-291-53309-5

Periodicals:

- [3] Hoog A., "Introduction to Android forensics", from DFI News, 2010.
- [4] Folloder A., "Digital Forensics and File Carving on the Android Platform", Department of Computer Science, University of Texas at Dallas, 2012.
- [5] Android Core Technologies, <http://source.android.com/devices/tech/>

Articles from Conference Proceedings (published):

- [6] A. Chatzikonstantinou, C. Ntantogian, G. Karopoulos, C. Xenakis, "Evaluation of Cryptography Usage in Android Applications", 9th EAI International Conference on Bio-inspired Information and Communications Technologies, At, New York USA, 2015.
- [7] A. Kandul, A. More, O. Davalbhakta, R. Artamwar, D. Kulkarni, "Steganography with Cryptography in Android", proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), pp 57-64, 2014.

PREVENTIVE MODEL OF DATA LEAK PROTECTION IN CRITICAL INFRASTRUCTURE FROM INTERNAL RISK FACTORS

VIKTOR KANIŽAI, PH.D.
OTP Bank, Serbia, viktor.kanizai@otpbanka.rs

Abstract: The use of information technologies in the critical infrastructure carries a high degree of risk, and therefore there should be paid special attention to the nature of the confidentiality, integrity and availability of the data that information systems of these institutions manage. Unauthorized outflow of information may cause financial and reputational damage, which in the current market may lead to permanent termination of business. It is necessary to establish an adequate model of preventive data leak protection in critical infrastructure from internal risk factors, for the protection to be comprehensive and effective. Risks cannot be completely eliminated, but can be reduced to acceptable levels. The author of this paper presented the three main pillars of the established model.

Keywords: data leak, data protection model, business information security, IT security, protection of critical infrastructure

1. INTRODUCTION

The basis of modern business represents the infrastructure of Information Technology (IT) - databases, communication flows, prompt data processing are necessary and also continuous access to services and products of the company. Taking into consideration the fact that the extraordinary events in the functioning of IT can lead to direct financial and reputational losses, the use of IT infrastructure in the critical infrastructure carries a high degree of risk.

It is necessary to pay special attention to the nature of the confidentiality, integrity, and availability of data which is managed by information systems of these institutions, as well as the dangers that threaten their functionality.

2. INTEGRATED MODEL OF DATA PROTECTION IN INFORMATION SYSTEMS OF CRITICAL INFRASTRUCTURE

The primary focus of protection should be the data, not a computer, computer network or computer system. The ultimate goal is to protect the data itself, regardless of where they are stored or where they are processed.

The most basic division of protection includes preventive and repressive protection. Repressive aims to establish the actual facts of the case of an extraordinary event that has already occurred or whose execution is threatening the security of data, and to propose measures so that such and similar events in the future would not be repeated. Preventive protection aims to prevent the occurrence of an incident and always has priority over repressive protection - it is always "better safe than sorry".

Data protection should cover all forms of data: voice, paper and electronic. It is necessary to pay attention to business talks with other parties, on the environment of the conversation, unauthorized persons not to hear the contents of the conversation and thus obtain access to the data of which the person is not authorized by his/her

working position. Also, it is necessary to apply the "clean desk policy", i.e. not to leave documents on the desk after working hours so that unauthorized persons couldn't get hold of the information contained in the printed material. The data in electronic form is the most difficult to guard, defining their protection requires a lot of expertise in the complex field of cybercrime. There is a noticeable increasing trend of high-tech espionage and warfare, as well as targeted attacks on "plain users" (i.e. ransomware virus - hides (encrypts) files on the user's computer and requires payment of a sum of money for the data to be returned).

Data protection should cover not only technology, but also human resources and business processes.

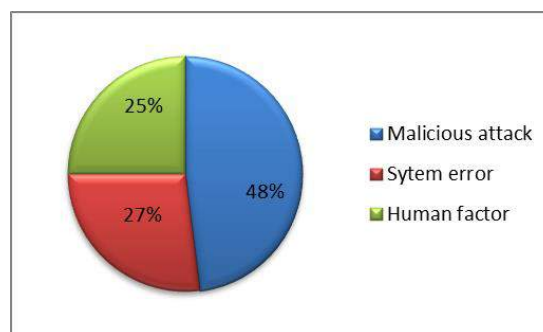


Image 1: Cause of security breach of data [1]

In addition to well-known headlines regarding unauthorized outflow of government information via WikiLeaks and Edward Snowden, we have also witnessed headlines about data leak events in companies (eg. JP Morgan [2], Citigroup [3]), at social networks (eg. Facebook [4]), on online services (eg. iCloud [5]), etc. It is necessary to pay special attention to the establishment of an adequate model to detect and prevent unauthorized outflow of information, especially in the critical infrastructure, because they handle sensitive and particularly sensitive data.

Unauthorized outflow of information can cause material and reputational damage to the critical infrastructure, which in the current market can lead to permanent closure of business.

To establish an adequate model of protection from unauthorized outflow of information it is necessary to answer the following questions:

- Where are we now?
- Where do we want to get?
- How do we want to reach the goal?

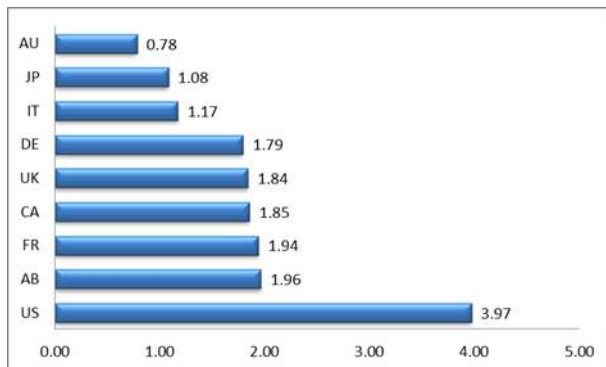


Image 2: Average operating loss due to breach of data security in nine countries in mill. US\$ [1]

3. PROTECTION FROM DATA LEAK THROUGH HUMAN RESOURCES

When it comes to unauthorized outflow of data, employees and external partners who have access to data pose the greatest threat.

Often data leak happens because of high-risk steps of employees who are not aware of the possible consequences of their actions.

Typical examples of behaviour of employees indicating the lack of diligence with regard to the safeguarding of sensitive data include loud talk about confidential information in public places, not logging off from workstations, leaving passwords in sight or unprotected, and access to unauthorized web pages. Especially big threat in this area comes from employees who are losing corporate devices such as laptop computers, mobile phones, and storage devices, or the devices have been stolen because of inadequate storage. Employees who are dissatisfied or who are trying to illegally obtain material gain for themselves or for another, represent a particular challenge in the fight against unauthorized outflow of information.

Legitimate network access and mobile devices enable disloyal employees to allow the outflow of corporate data. Some workers simply do not return company devices when they leave their job. This can be expensive and dangerous for the company, because it adds another path for data loss.

Even if only 5 percent of employees who leave the workplace takes the device with him, in the company of 1,000 employees this means 50 such workers. For larger

organizations risk and financial losses are far more significant [6].

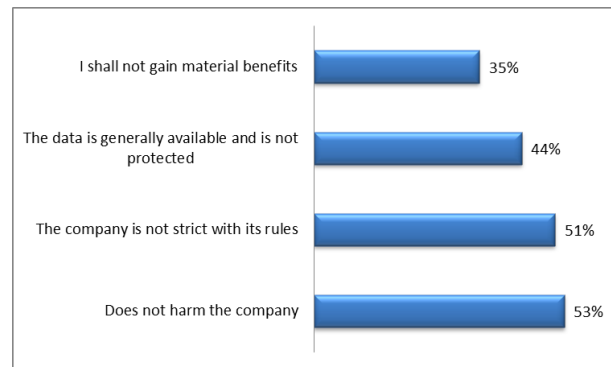


Image 3: The most common reasons due to which employees believe it is acceptable to take business data[7]

4. IT SECURITY TRAINING OF EMPLOYEES FOR DATA LEAK PREVENTION

Safety training of employees in critical infrastructure should primarily be aimed at raising awareness on the protection of data and IT during business. In order for training to be effective and successful it is necessary to previously examine the following aspects:

- The sensitivity (vulnerability) of IT that are of particular importance for the business,
- The effect of new technologies onto the protection of right to privacy, protection of trade secrets, personal data, etc.,
- The role of government and legislation in protecting data and IT,
- The application of standards in the field of IT security in corporate environment and in society in general.

In order for training to be successful people should be aware of the need for training.

Safety training on protection against unauthorized outflow of information should be aimed at raising awareness of employees about the need for security which is equal to business success. Through training it is needed to give clear answers to the following questions:

- What should be protected?
The answer to this question involves determining the objects of protection. Protection of an object can involve: data on employees, customer data, business data, databases, etc. This is essentially the first and crucial step in training and clarifying the problems of protection in the field of IT in the critical infrastructure. People need to be especially aware of what to protect and what the values that should be protected are.
- What and who should protect data and IT in the critical infrastructure?
The answer to this question involves the identification of risks, threats that more or less can compromise data and IT in critical infrastructure. These can include the following threats: force

majeure (earthquake, flood, fire, etc.), hardware and software shortcomings (hardware failure, software bugs, etc.), human-factor unintentional mistakes (negligence, carelessness, poor organization, incompetence, fatigue, etc.), human factor with intention (theft, sabotage, revenge, revealing business secrets, hacking, phishing, creating and distributing viruses, etc.), sources of threats from the environment (extended loss of electricity, air pollution, etc.). Through security training employees must be aware of the threats and risks to better protect data and IT in critical infrastructure.

- Why should data and IT be protected in critical infrastructure?
Possible consequences should be determined of the loss, or damage that critical infrastructure may have from exploiting one of the threats. Here we establish the damage, consequences or loss for the critical infrastructure that may arise due to the realization of threats to objects of protection. These consequences may include partial or complete physical damage (hardware, software, data, etc.), theft (hardware, software, data, reports, information, etc.) and modification (hardware, software, data, reports, information, etc.). Generally speaking, the consequences are breaching: integrity, availability and confidentiality.
- What to protect data and IT in the critical infrastructure with?
The answer to this question involves the choice of measures and resources that will be used to protect data and IT in critical infrastructure. Data protection and IT security in critical infrastructure can be seen as: normative regulation, measures of physical-technical security, logical security, security staff training and security control – monitoring.
- How will data and IT be protected in critical infrastructure?
This also includes a clear definition of IT security policy of the institution, IT security strategy, the development of internal normative acts, organizational structure. A clear answer to this question involves training employees on the use of modern methods and means for the protection of data and IT in critical infrastructure.

All should have the primary goal of raising awareness about the need for protection and IT security in critical infrastructure. The importance of training is enormous because employees become safer and thus more effective in their work.

The modern form of training involves the use of cyclic learning. Training should be based on the application of modern technology with involvement of highly specialized professionals in this field. Training should be active, to be based on encouraging and directing.

The training should include an analysis of experiences, both locally and globally. Training must be comprehensive, well-planned and organized in order to avoid certain types of commercial training, by offering short-term courses, one-day or half-day training often by

incompetent agencies and individuals. It is necessary to have direct cooperation between scientific and educational institutions with market operators, which should be well planned and organized in order to carry out quality training in the field of data protection.

The form of training in which users play active roles is the most effective way to meet the requirements for expert training, increase knowledge and awareness of data protection.

Training is the most effective preventive measure to protect data. If users have adequate awareness and knowledge in the field of data protection, then the actual execution of activities through IT is safer, regardless of the technical - technological solutions of protection. We should not forget, the first lines of defence are the users themselves.

5. TECHNOLOGICAL SOLUTIONS FOR PREVENTING UNAUTHORIZED OUTFLOW OF DATA

Technological solutions are used for policy enforcement, monitoring and warning on violations of security provisions, as well as to ensure data protection. They manage the risk of data loss, regardless of whether the event occurred intentionally or due to human error.

Technological solutions to prevent unauthorized outflow of information include:

- Tools for encryption,
- Antivirus protection,
- Firewall protection,
- Intrusion Prevention System,
- Tools to test on vulnerabilities,
- Web filters, and so on.

To detect events, DLP solutions commonly use the following principles:

- Described data: keywords, file types, data identifiers, etc.; attributes of the sender or recipient.
- Fingerprinted data: structured data, unstructured data.

The most important element of technological solutions is a dedicated solution for preventing unauthorized outflow of data (Data Loss Prevention - DLP solution). It is defined as a product which on the basis of centralized sets of rules identifies, monitors and protects data at rest (storage - file servers, databases, web servers, etc.), motion (network - e-mail, web, FTP, instant messaging etc.), and processing (workstations - computers, printers, data carriers, etc.), through a detailed analysis of the content.

When the DLP solution detects a suspicious event, it usually applies one of the following measures:

- Notifications: sending e-mails to the sender / manager / IT Security Department; pop-up windows; syslog alerts, etc.

- Blocking: blocking the SMTP, HTTP / S, FTP, IM, etc. traffic; blocking further use of peripheral devices, such as USB / CD / DVD, printer / fax, etc.
- Modification: modifies the data traffic itself in terms of encrypting sensitive data.
- Relocation or copying stored files.

There are many dedicated DLP technological solutions on the market, and the author of this paper wouldn't favour any one of them. Instead, Gartner's estimates on these solutions are shown below, on Image 4.



Image 4: Gartner's estimates on DLP solutions [8]

6. PROTECTION FROM UNAUTHORIZED OUTFLOW OF INFORMATION THROUGH BUSINESS PROCESSES IN CRITICAL INFRASTRUCTURE

For the DLP to be complete, it is necessary to protect business processes as well in the critical infrastructure. What is important to emphasize is that protection represents supporting process in terms of business operations, and as such should not distort the expected business processes which bring profit to the institution. Protection should not be a burden for the business of institutions which would break or permanently stop the business processes, but should protect them. Of course, sometimes the easiest way is to completely shut down some processes with the excuse that they carry a high degree of risk, but in this case it is not the goal, but to be in line with business requirements and find optimal solutions for the business processes to flow as expected, and at the same time they would also be secure.

For existing processes, it is necessary to conduct comprehensive and detailed risk analysis, identify possible points of unauthorized outflow of information. The most trivial examples are Internet access and the ability to use removable data carrier. The best and easiest way would be to prohibit access to the Internet completely and prevent the use of any removable media,

i.e. to close the information system of the institution in such way. But business needs impose and require constant access to the Internet and peripheral devices for storage and transfer of data. This is why in this case the protection means limiting, not abolition. And limitation means determination of who can access all content on the Internet and in what period of time, who can have the ability to use USB memory temporarily or permanently, and so on. On the other hand, there is the monitoring of those streams of data with the help of technical solutions to prevent unauthorized outflow of information, as described in the previous chapter of this paper.

In new business processes that are yet to be defined and introduced, it is necessary prior to their implementation to assess possible risks regarding the unauthorized outflow of information and mitigate identified risks by appropriate measures that will be part of the new business processes.

In this, and in all matters, the support from top management is essential. Without this support, all of the above will not function properly; it may be achieved that internal documents would cover the matter of DLP, but in practice it will not be implemented as intended. It is necessary for management, given the potential threats and losses, to invest into the protection of data from unauthorized outflow, and it shouldn't be seen as inevitable cost but as an investment into the security of business processes. On the other hand, it is also inevitable for the protection not be a disabling factor for business processes, but a factor that will make safe operation of institutions on the issue of unauthorized outflow of information.

7. CONCLUSION

The use of IT infrastructure in the critical infrastructure carries a high degree of risk, and therefore special attention should be paid to the nature of confidentiality, integrity and availability of the data that information systems of these institutions manage. Unauthorized outflow of information may cause financial and reputational damage, which in the current market can lead to permanent closure of operations.

The preventive model of data leak protection in critical infrastructure from internal risk factors, which is designed and presented in this paper, includes not only technology, but also human resources and business processes.

The greatest emphasis in this paper is on human resources, because employees in critical infrastructure constantly have access to the information that the institution stores and processes in accordance with and due to the nature of work performed, and are therefore they are the weakest link in the system of protection against unauthorized outflow of information. But from the other side, they also represent the first line of defence.

REFERENCES

- [1] Benchmark research sponsored by IBM, Independently conducted by Ponemon Institute

- LLC, “2016 Cost of Data Breach Study: Global Analysis”, June 2016.
- [2] “JP Morgan suffers data breach affecting 76 million customers”, <http://www.itgovernanceusa.com/blog/jp-morgan-suffers-data-breach-affecting-76-million-customers/>, last accessed on 10.07.2016.
- [3] “Citigroup Suffers Massive Data Breach In Japan”, http://www.huffingtonpost.com/2011/08/08/citigroup-suffers-another_n_920862.html, last accessed on 09.07.2016.
- [4] “Facebook Data-Leaking Bug Exposes 6 Million Users' Data”, <http://www.infosecurity-magazine.com/news/facebook-data-leaking-bug-exposes-6-million-users/>, last accessed on 09.07.2016.
- [5] “2014 celebrity photo hack”, http://en.wikipedia.org/wiki/2014_celebrity_photo_hack, last accessed on 10.07.2016.
- [6] Cisco Systems, Inc, “Data Leakage Worldwide: The High Cost of Insider Threats”, 2008.
- [7] Symantec Corporation, “What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk”, 2013.
- [8] Gartner, Inc., “Magic Quadrant for Enterprise Data Loss Prevention”, 28.01.2016.
- [9] An Osterman Research White Paper, “Best Practices for Dealing with Phishing and Next-Generation Malware”, April 2015.
- [10] Jeffrey Roman, “Morgan Stanley: Insider Stole Data – BankInfoSecurity, Employee Posted Some Client Information Online”, <http://www.bankinfosecurity.com/morgan-stanley-insider-stole-data-a-7750>, last accessed on 05.06.2016.
- [11] Vormetric, Inc., “The Insider Threat, How Privileged Users Put Critical Data at Risk”, 2013.

ANDROID FORENSIC AND ANTI-FORENSIC TECHNIQUES – A SURVEY

NEMANJA D. MAČEK

School of Electrical and Computer Engineering of Applied Studies, Belgrade and SECIT Security Consulting,
nmacek@viser.edu.rs

PERICA ŠTRBAC

School of Electrical and Computer Engineering of Applied Studies, Belgrade, pericas@viser.edu.rs

DUŠAN ČOKO

School of Electrical and Computer Engineering of Applied Studies, Belgrade, dusanc@viser.edu.rs

IGOR FRANČIĆ

Belgrade Metropolitan University, Faculty of Information Technologies and SECIT Security Consulting,
igor.fran@metropolitan.ac.rs

MITKO BOGDANOSKI

Military Academy General Mihailo Apostolski, Skoplje, Macedonia, mitko.bogdanoski@ugd.edu.mk

Abstract: *Technology concerning mobile devices has presented revolutionary growth during the last decade. Mobile phones do not serve only as a means of communication, but also as portable computers with advanced communication capabilities. Smartphones are able to store a rich set of personal information and at the same time provide powerful services, such as location-based services, Internet sharing via tethering, and intelligent voice, thus increasing the likelihood of a such devices being involved in a criminal activities. Mobile forensics is the science of recovering digital evidence from a mobile device under forensically sound conditions using accepted methods. During the last few years, a significant amount of research has been conducted, concerning various mobile device platforms forensics, data acquisition schemes, and information extraction methods. This paper provides a comprehensive overview of the field, by presenting a detailed assessment of methodologies regarding Android forensic and anti-forensic techniques.*

Keywords: *Android, Phone, Forensics, Anti-forensics*

1. INTRODUCTION

The Android mobile platform has quickly risen from its first phone in October 2008 to the most popular mobile operating system in the world by early 2011. According to Gartner, Inc., global sales of smartphones to end users totaled 349 million units in the first quarter of 2016, with Android Android regaining share over iOS and Windows to achieve 84 percent share [1]. The explosive growth of the platform has been a significant win for consumers with respect to competition and features. However, forensic analysts and security engineers have struggled as there is a lack of knowledge and supported tools for investigating these devices [2]. Criminals could use Android phones for a number of activities ranging from harassment through text messages and e-mail frauds to trafficking of child pornography and communications related to narcotics. The data stored on these phones could be extremely useful to analysts through the course of an investigation of these activities. Unless anti-forensics is somehow deployed, a large volume of probative information linked to an individual exists on every Android phone, including call history, contacts, messaging data, e-mails, browser history and chat logs. According to Lessard and Kessler, these phones have more probative information that can be linked to an individual per byte examined than most computers

[3]. However, this data is harder to acquire in a forensically proper fashion due to a wide range of phones available and a general lack of hardware and software standardization. As an example, even different models of the same manufacturee sometimes require different data cables and software to access the phone via computer.

Roughly, one may distinguish three types of scenarios where Android forensics may come in handy: an investigation that will adjudicated in a criminal or civil court of law, internal corporate investigations (intellectual property, data theft, inappropriate use of company resources or employment related investigations) and investigations that target family matters (divorce, child custody or estate disputes).

Having that said, one may ask a question: where does the anti-forensics fit in? Majority of users do not employ adequate security measures on their Android phones. So, let's observe the following scenario: a user that is not involved in anything related to crime does not employ a pattern to unlock the screen. The very same user does not have anti-theft software installed but somehow manages to lose his phone. A malicious person that has found the lost Android phone now has a temporary access to Gmail, Facebook, Twitter and all other accounts that the user was logged in to. Authors will allow readers to conclude the

story by themselves (suggestion: avoid happy endings). According to the aforementioned scenario, the data stored on a phone presents an obvious threat to the user's privacy. Data also provides a well-defined profile of the user that can further be used to reconstruct his actions at a specific time [4]. A user who wants to protect his privacy can employ anti-forensics techniques. According to Ryan Harris, "anti-forensics is considered to be any attempt to compromise the availability or usefulness of evidence to the forensics process. Compromising evidence availability includes any attempts to prevent evidence from existing, hiding existing evidence or otherwise manipulating evidence to ensure that it is no longer within reach of the investigator. Usefulness maybe compromised by obliterating the evidence itself or by destroying its integrity" [5].

This paper briefly analyses some of the Android forensic and anti-forensic techniques reported in the literature. The rest of the paper is organized as follows. Section 2 briefly describes Android operating system, certain security issues and discusses the features common to all devices that are fundamental to forensic investigation. A survey of forensic solutions reported in the literature and anti-forensic techniques is given in sections 3 and 4, respectively and section 5 concludes.

2. ANDROID OPERATING SYSTEM

Android, a mobile operating system developed by Google, is the best-seller for tablets since year 2013, and on smartphones it is dominant by any metric [6]. The middleware, libraries and APIs written in C and software running on an application framework which includes Java-compatible libraries reside on top of the Linux kernel (see Image 1).

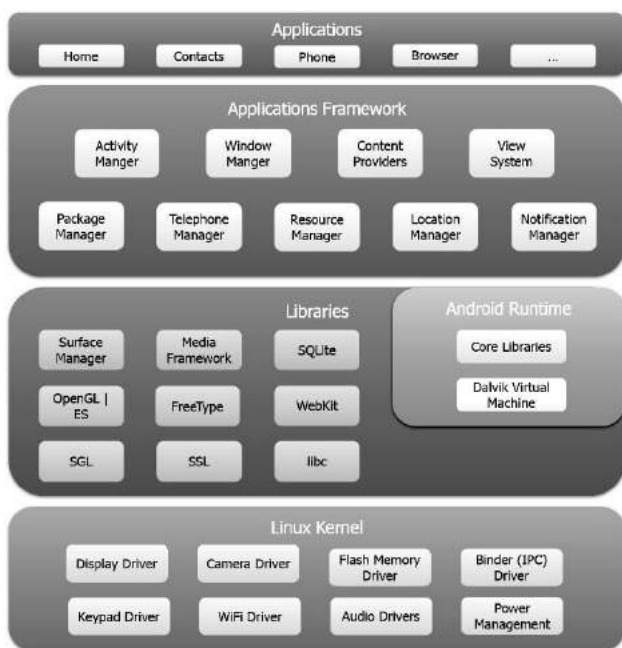


Image 1: Android software stack

Linux kernel is developed independently of other Android's source code and provides the support for some fundamental functions, such as device drivers, network infrastructure and power management [7, 8]. Libraries and Android runtime reside in the next level of the architecture. Libraries provide the infrastructure for applications to run properly, such as binaries and graphics support. Android's runtime consists of the Dalvik Virtual Machine (DVM) and the core libraries that provide the available functionality for the applications [7]. Its main purpose is the creation of a stable and secure environment in which applications are executed: each application runs in its own sandbox and therefore is not affected by other applications or system functions. A satisfying level of security is preserved by allowing certain resources to be used only if permitted by special privileges. The rest of the architecture consists of the applications framework and the applications layer that manage general application structure, such as containers, alerts and the applications themselves. As Android runtime libraries are written in Java, DVM translates Java to a language that the OS can perceive [9] – until version 5.0, Android used Dalvik as a process virtual machine with trace-based just-in-time compilation to run Dalvik executable code, which is usually translated from the Java bytecode. Following the trace-based just-in-time principle, in addition to interpreting the majority of application code, Dalvik performs the compilation and native execution of select frequently executed code segments each time an application is launched [10, 11].

Due to the small chip size, non-volatile nature and energy efficiency, NAND flash memory was selected to serve as Android storage [12]. Yet Another Flash File System 2 (YAFFS2) was the first filesystem implemented on devices running Android, but, due to certain limitations (such as large file coverage) [13], was replaced with Ext4 before the release of Android version 2.3 (Gingerbread). The Ext4 filesystem, apart from successfully coping with the weak points of YAFFS2, is enhanced with the journaling event function which provides recovery options and facilitates acquisition of unallocated files [13, 14]. As NAND flash memory was incompatible to the Linux kernel, a new technique was implemented to provide the ability to access the flash memory areas [8]. The Memory Technology Devices (MTD) system was one of the facilities serving as an intermediary between the kernel and the file system and is present in many Android devices. Handsets that do not support the MTD system usually utilize the plain Flash Transaction Layer (FTL) that enables communication between the two parts [14]. The flash storage on is split into several partitions: operating system resides on /system while /data is used to store user data and application installations. As root access is not gained to users /system and sensitive partitions are mounted read-only, unless device is rooted by exploiting security flaws.

Security and privacy issues of Android devices can be classified either as issues arising from surveillance by public institutions, such as NSA (see [15, 16] for more details), common security threats, such as malware that sends text messages from infected phones to premium-rate telephone numbers without the consent or even knowledge of the user [17] or technical security features, typically resulting from unnecessary permissions required to install

applications. As stated before, applications run in a sandbox, unless access permissions are explicitly granted by the user when the application is installed. This reduces the impact of vulnerabilities and bugs in applications, but the unnecessary required permissions that result from either developer confusion or lack of documentation work against effectiveness of sandboxing. Although since the version 6.0, users are allowed to block applications from having access to the contacts, calendar, phone, sensors, SMS, location, microphone and camera [18], full permission control is only possible if device is rooted.

So which features are common to any Android device and can they be used in the forensic investigation? According to Andrew Hoog [2], Android was engineered from the beginning to be online, whether using cellular or wireless networks. Being online is a prerequisite that allows the execution of another fundamental feature: downloading and installing applications from the Play Store. To a user, this feature presents the ability to extend the functionality of the device. To a forensic investigator, applications downloaded from the Store present a rich source of information. Finally, the ability for users to store their data on the devices is important as much to a forensic investigator as it is important to a user himself. Typically, stored data is the basis behind any forensic investigation.

3. ANDROID FORENSICS: A BRIEF SURVEY

Procedure for handling Android devices contains several steps, such as securing the device, isolating it from the network, circumventing the pass code and imaging mass storage devices. Depending on the way how data is accessed, android forensic techniques can be classified either as logical or physical. Logical technique extracts allocated data, typically by accessing the filesystem, with the exception of SQLite database (that might still contain deleted records in the database). Physical techniques, on the other hand, extract data from the physical storage medium directly and do not rely on the filesystem. There are advantages to this approach and the most significant is that with the physical forensic techniques it is possible to recover both the allocated and the unallocated (deleted or obsolete) data. One of the guiding principles of any forensic investigation is to avoid modification of the target device in any manner, and this principle works for Android devices also. The rest of this section will provide a review of the forensic techniques, solutions and methods reported in the recently published literature of interest.

Lai et al. [19] implemented a live-forensic acquisition procedure, based on commercial forensic suites through cloud computing, designed for Android devices. Although acquisition type was not specified, the procedure resembled to logical acquisition that can be applied to rooted devices as well. Since proper time-stamping is an essential for the validity and integrity of forensic evidence, actual date correction is another interesting feature in their approach.

Simao et al. [9] proposed a forensic acquisition framework for the Android in the form of flowchart, applicable to many scenarios, including damaged devices and fragmented memory page analysis. In order to validate the model, authors have conducted experiments on devices

with different conditions and figured out that the proposed scheme was applicable. Downside of their solution is lack of some crucial elements necessary for real-time investigation.

Research of Vidas et al. [8] deals with the forensic acquisition on devices protected by a screen lock. Since a brute-force attack on the device could lead to a further block, and possibly to inevitable data modification, another technique had to be implemented. To resolve the problem, authors have stated that booting with a recovery image could easily bypass any kind of active lock code. Recovery mode boot file residing in the Android root was significant for the acquisition process of the recovery image, as by booting into recovery mode, the boot process is circumvented with the boot target set to boot image currently loaded in the recovery partition. Boot image that authors have used consists of existing modified files and variety of transfer daemons and binaries. The authors have noticed that boot options differ between brands of mobile phones and have examined several different case studies. Downside of aforementioned research is the lack of statistic results of data retrieval.

Sylve et al. [20] referred to a lack of studies applicable to physical acquisition and highlighted the importance of this issue. The researchers presented “a methodology for acquiring complete memory captures from Android, code to analyse kernel data structures and scripts that allow analysis of a number of user and filesystem based activities”. Authors have also enumerated the existing methodologies on volatile memory analysis for Linux and Android operating systems and compared the capabilities of the corresponding tools. The results of their experiments provided a proof that Linux oriented forensic techniques were not compatible to the Android.

Andriotis et al. [21] implemented a forensic acquisition method that employs WiFi and Bluetooth. The most significant parts of their research was the fact that devices used were involved in actual crime scenes. Afterward, they presented a detailed step-by-step procedure to complete logical acquisition, which was common for all the devices participating in the experiment, which was considered a success as any critical evidence was recovered in every networking attribute.

Ext4 filesystem that became the successor of YAFFS was examined by Kim et al. [13]. Authors have used two rooted devices running Android and their research was limited to logical acquisition. Detailed description of the file system was provided and forensic acquisition for the journal log area was summarized.

Mylonas et al. [22] studied the involvement of context-measuring devices, such as accelerometers and GPS, in mobile forensics. Authors have stated that this kind of data can be of great importance and that a special approach is required because of the volatile nature of the data itself. Methodology on data acquisition from sensors was proposed, ranging from theory to practical procedures executed at the laboratory level. Data acquisition system they have developed took into consideration security mechanisms on the target devices as well as the procedures to bypass these mechanisms. As the system they have

developed consists of two parts (the workstation and the mobile agent), and as one of the possible use of the solution would be to acquire data from a phone belonging to a potential suspect, agent installation had to be forced and functionality to be obfuscated either via social engineering or fake error messages. According to their research, 12 out of 15 sensors need absolutely no permission to gain access to, leading to conclusion that security behind sensors is easy to bypass: agent is triggered each time the user accesses a sensor, acquires the data, encrypts it and sends it to a workstation if the device is connected to a network.

Live forensic methods as a means for surveillance of malware activity on Android is presented in work of Guido et al. [23]. The solution was developed as a mainstream Android application in order to avoid rooting. It comprised of five modules programmed in Python, each detecting changes in specific parts of the operating system: bootloader, recovery, filesystem, deleted files and APKs. Experiments consisted of three rounds of malware injections on target mobile devices, with many successful detections, but weak points, such as false positives and inability to detect some deleted entries have occurred also. Despite the defects, the solution proposed in the paper was one of the important contributions to the Android forensics. Similarly, Justin Grover [24] has developed DroidWatch application that performs continuous tracking of events and data flow on an Android device and sends the information to a Web Server. As rooting of the device was avoided due to authors policy, the range of acquired data was limited. The data process flow within the DroidWatch app is depicted in Image 2. Data collection and storage is a continuous process, with transfers scheduled by configurable variable. Upon a successful transfer to the enterprise server, events dated prior to the transfer are wiped from the local phone database. File transfer attempts that fail are logged in the database and do not result in the wiping of any events.

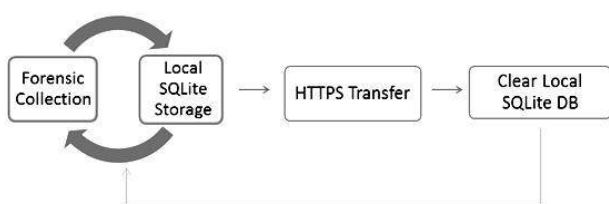


Image 2: DroidWatch data process flow diagram [24]

Son et al. [25] conducted an evaluation on the Recovery Mode method with seven rooted Samsung devices taking part as a sample. The results from the use of JTAG method served as a comparison vector to the Recovery Mode. A section was dedicated on the acceptable practices during the data acquisition phase in Recovery Mode. A flowchart related to the steps taken during the acquisition procedure was introduced, the importance of using the appropriate bootloader for each device was pointed to and issues with encrypted ones were mentioned. Actions that should have been taken into consideration during the restoration process have been highlighted, for example the prohibition of interaction with the menu elements in Recovery Mode

and the USB cable separation from the device before battery removal. Additionally, custom software was developed in order to conduct the data extraction tasks and check the integrity of the method. Finally, the hash values of the data partition that were extracted in both cases was calculated and proved to be equal, assuming that integrity was preserved.

Muller and Spreitzenbarth have investigated innovative techniques in an effort to assess how much valuable information can be extracted from encrypted Android phones [26]. A cold boot attack was performed by freezing to gain the device in order physical access to the device memory and acquire information such as encryption keys or personal data. The method, however, has an important limitation: the user partition gets wiped out when the device bootloader unlocks. Still, it is the first work to perform a successful and effective cold boot attack on Android phones and the implementation of cryptographic solutions does not appears as a problem that cannot be bypassed.

Konstantia Barmapsalou et al. provided a comprehensive review of forensic techniques applicable to other smartphone operating systems [14].

4. ANDROID ANTI-FORENSIC TECHNIQUES

As stated before, the purpose of anti-forensics is to compromise the availability or usefulness of forensic evidence. Distefano et al. distinguished several kinds of anti-forensics [27]: destroying evidence (making it unusable during the investigation), hiding evidence (subverting an analyst by decreasing the visibility of the evidence), eliminating sources (neutralization of the evidentiary sources) and counterfeiting evidence (creation of a fake version of the evidence which is properly made to carry wrong or deviated information in order to divert the forensic process).

Kessler [28] categorises anti-forensics into four groups: data hiding, artefact wiping, trail obfuscation, and attacks against forensics processes or tools, which refer to attacks that force the forensic analyst to perform non-standard procedures or call into question the data recovered. For computer anti-forensics, data hiding contains things like steganography, deleted files, and storing data in the cloud or in other storage space. On a non-rooted phone, information can be hidden by having an application store it somewhere secluded and restore it at a later time. This approach also allows quick mass-deletion [27]. Artefact wiping refers to overwriting data down to the level where it is impossible to restore it from, even with high-tech undeletion techniques. Two weaknesses with this class however may be noticed: they may miss some data, and they may leave traces of the wiping that have occurred (probably the wiping tool itself will remain). Since Android anti-forensics is mainly concerned with data legitimately stored and usable on the phone, and not with attacks or traces on other devices on the network, trail obfuscation is not considered to be very relevant anti-forensic technique. Trail obfuscation typically refers to network forensics. When an attacker does not need a reply, he can spoof the sender's address to make tracing the attack to its source harder. It is also possible to use spoofed sender

addresses for attack amplification, by tricking third parties into sending much more traffic to a victim than the attacker could on their own. Other tools in this category, such as onion routers, Web proxies and e-mail anonymisers, hide the real sender of traffic behind a server which serves many clients. Trail obfuscation also includes log file and timestamp alteration.

5. CONCLUSION

Variety of conducted research on Android, and in general, mobile forensics, as well as undergoing standardization attempts indicate that the area is under continuous development. The work presented in this paper provided a comprehensive review of the state-of-the-art research in the field of Android forensics, as well as a classification of important Android anti-forensic techniques. Any relevant current work, be it a research or review, can be used as a reference to anyone interested in better understanding the facts of this rapidly evolving and interesting research discipline.

REFERENCES

[1] Gartner Inc., “Gartner Says Worldwide Smartphone Sales Grew 3.9 Percent in First Quarter of 2016”, Egham, UK, May 19, 2016.

[2] A. Hoog, “Android forensics: investigation, analysis and mobile security for Google Android”, Elsevier, 2011.

[3] J. Lessard, G. Kessler, “Android Forensics: Simplifying Cell Phone Examinations”, *Small Scale Digital Device Forensics Journal*, 4(1), pp. 1-12, 2010.

[4] P. Albano, A. Castiglione, G. Cattaneo, A. De Santis, “A Novel Anti-Forensics Technique for the Android OS”, 2011 International Conference on Broadband and Wireless Computing, Communication and Applications, pp. 380-385, 2011, IEEE.

[5] R. Harris, “Arriving at an anti-forensics consensus: Examining how to define and control the anti-forensics problem”. *Digital Investigation* 35, pp. S44-S49, 2006.

[6] F. Manjoo, “A Murky Road Ahead for Android, Despite Market Dominance”, *the New York Times*, May 27, 2015, ISSN 0362-4331.

[7] I. I. Yates, “Practical investigations of digital forensics tools for mobile devices. In 2010 Information Security Curriculum Development Conference, October 2010, pp. 156-162, ACM.

[8] T. Vidas, C. Zhang, N. Christin, N., “Toward a general collection methodology for Android devices”, *Digital investigation* 8, pp. S14-S24, 2011.

[9] A. Simao A, F. Sicoli, L. Melo. F Deus, JR Sousa, “Acquisition and analysis of digital evidence in android smartphones”, *International Journal of Forensic Computer Science*, Vol. 6, No. 1, pp. 28–43, 2011.

[10] B. Cheng, B. Buzbee, “A JIT Compiler for Android's Dalvik VM” (PDF), android-app-developer.co.uk, Google, pp. 5–14, May 2010.

[11] H. Q. Raja, “Android Partitions Explained: boot, system, recovery, data, cache & misc”, *Addictivetips.com.*, May 19, 2011.

[12] C. Zimmermann, M. Spreitzenbarth, S. Schmitt, FC. Freiling, “Forensic analysis of yaffs2”, In *Sicherheit*, pp. 59–69, 2012.

[13] D. Kim, J. Park, K-g Lee, S. Lee S, “Forensic analysis of android phone using ext4 file system journal log”, in *Future Information Technology, Application, and Service*, Springer Netherlands, pp. 435-446, 2012.

[14] K. Barmapsalou, D. Damopoulos, G. Kambourakis, V. Katos, “A critical review of 7 years of Mobile Device Forensics”, *Digital Investigation*, 10(4), pp. 323-349, 2013.

[15] Staff, “Privacy Scandal: NSA Can Spy on Smart Phone Data”, September 7, 2013.

[16] James Ball, “Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data”, theguardian.com, January 27, 2014.

[17] E. Protalinski, “Android malware numbers explode to 25,000 in June 2012”. *ZDNet*, July 17, 2012.

[18] R. Amadeo, “Android 6.0 Marshmallow, thoroughly reviewed”, *Ars Technica*, May 10, 2015.

[19] Y. Lai, C. Yang, C. Lin, T. Ahn, “Design and implementation of mobile forensic tool for android smart phone through cloud computing”. In *International Conference on Hybrid Information Technology*, pp. 196-203. Springer Berlin Heidelberg, 2011.

[20] J. Sylve, A. Case, L. Marziale, GG. Richard, “Acquisition and analysis of volatile memory from android devices”. *Digital Investigation* 8, No. 3, pp. 175-184, 2012.

[21] P. Andriotis, G. Oikonomou, T. Tryfonas, “Forensic analysis of wireless networking evidence of android smartphones”, In *2012 IEEE International Workshop on Information Forensics and Security (WIFS)*, pp. 109-114. IEEE, 2012.

[22] A. Mylonas, V. Meletiadis, L. Mitrou, D. Gritzalis, “Smartphone sensor data as digital evidence”, *Computers & Security* 38, pp. 51-75, October 2013.

[23] M. Guid, J. Ondricek, J. Grover, D. Wilburn, T. Nguyen, A. Hunt, “Automated identification of installed malicious android applications”, *Digital Investigation* 10, pp. S96-S104, 2013.

[24] J. Grover, “Android forensics: automated data collection and reporting from a mobile device”, *Digital Investigation* 10, pp. S12-S20, 2013.

[25] N. Son, Y. Lee, D. Kim, J.I, James, S. Lee, K. Lee, “A study of user data integrity during acquisition of android devices”, *Digital Investigation* 10, pp. S3-S11, 2013.

[26] T. Muller, M., Spreitzenbarth, “Frost”, In: Jacobson M, Locasto M, Mohassel P, Safavi-Naini R, editors., *Applied cryptography and network security*, Lecture notes in computer science, vol. 7954. Berlin, Heidelberg: Springer, pp. 373–88, 2013.

[27] A. Distefano, G. Mea, F. Pace, “Android anti-forensics through a local paradigm”, *Digital Investigation* 7, pp. S83-S94, 2010.

[28] G. Kessler, “Anti-forensics and the digital investigator”, In *Proceedings of the 5th Australian digital forensics conference*, December 2007.

RAISING AWARENESS OF THE NEED FOR SAFETY OF INFORMATION IN BIG BUSINESS SYSTEMS

DRAGAN ĐOKIĆ

Belgrade Metropolitan University, Faculty of Information Technologies, dragan.djokic@metropolitan.ac.rs

MIHAILO JOVANOVIĆ

Executive director of IT, electronic communications and development Post of Serbia, mihailo.jovanovic@posta.rs

SNEŽANA POPOVIĆ

School of Computing, Belgrade, Serbia, spopovic@raf.edu.rs

RAMO ŠENDELJ

University of Donja Gorica, ramo.sendelj@udg.edu.me

NEMANJA D. MAČEK

School of Electrical and Computer Engineering of Applied Studies, Belgrade and SECIT Security Consulting,
nmacek@viser.edu.rs

Abstract: *In order to maintain constant communication with the family, friends or colleagues, we use a variety of devices whereby accessing the Internet mostly using unsecured hotspots. This makes us an ideal target for potential digital threats and abuse. Consequences at the individual level may well be serious, however, digital threats can have an even bigger, devastating impact on large business systems. Prevention and education in this area are, for the time being, the best weapon in the fight against digital attacks.*

The topic of this paper shows one of the possible solutions for intranet ongoing training of employees in the field of information security in large business systems, using the portal technology in conjunction with the Learning Management Systems.

Keywords: *threat, security, information, education, intranet, portal, adaptive, digital identity*

1. INTRODUCTION

An increasing number of professional public agree with the statement that civilization has considerably embarked on the information revolution. It is almost unthinkable to do any kind of work without at least a minimum use of IT resources.

Numerous specialized forums enable daily communication with various benevolent experts and persons who have certain knowledge and who are ready to give answers and advice to a large number of questions. All this leads to obtaining certain conditions for forming a huge base of global knowledge.

Today's reality is that a great amount of information and documents are generated in big corporate systems daily. These documents and information circulate and are shared on all hierarchical levels in the company with a permanent exponential trend of growth. These information and electronic documents are a great challenge for many hackers who wait for their opportunity in order to collect them and misuse them.

One of the possible solutions to the protection and security of information and electronic documents in big corporate systems is a permanent rise of the level of knowledge of

the employees in order to stop unauthorized access to the information. A platform that can provide permanent education of employees in big corporate systems is based on a web portal for intelligent management of electronic documents within which a segment is located with: specialized content, information on current threats, questionnaires - examinations and other activities aiming at raising the level of knowledge of employees in the said field.

This paper will present one of the possible conceptual solutions for adaptive and personalized system for raising the level of knowledge of the employees and their permanent education in the field of information security and data protection, based on the intranet portal.

2. DESCRIPTION OF BUSINESS PROBLEM

With the advancement of technology, management of large business systems are faced with the other side of the coin, and that is the fact that IT security threats grow day by day directly threatening the security of the company. Companies need to implement new technologies in order to ensure an adequate level of protection and one of the most effective ways is a permanent training of all levels of employees in the field of IT security and data protection. The application of this concept leads to a timely prevention

or reduction of the level of threats caused by advanced malicious programmes.

2.1. *Factors that affect the security of business information*

When large business systems are analyzed from the perspective of protection and security of business information and data, the following factors should be taken into account:

- Ramification - dislocation and the size of the business system;
- The organizational structure of the business system;
- The number and type of computers used in the company (servers and work stations);
- Communications infrastructure, access points and way of accessing the Internet;
- User account management policies;
- The total number of users of computer networks;
- The number of managers ranked on different hierarchical levels;
- Educational and professional profile of employees;
- Level of education of employees;
- The age structure of employees;
- Level of education and training of employees for using applications that are available to them and rules of conduct within the company's intranet, as well as on the Internet.

Bearing in mind that even the most perfect systems can be upset and threatened by the human factor, the awareness should be raised among employees that one of the most important ways to protect business information and electronic documents is a permanent training of each employee.

A large number of unstructured documents of various formats that circulate on a daily basis within the business system and are shared among a large number of employees makes it difficult to define the authorization concerning the document availability and access rights of employees. An additional complication is the fact that those documents are parts of complex and interwoven business processes. Classification and systematization of information and electronic documents, as well as their incorporation into clearly defined business process can significantly affect the security of business operations [1]. Some of the key reasons why the classification of data is one of the priorities in protecting the IT system are the following [2]:

- Unintentional misuse of the data amounts to 36% of the total number of incidents in 2013;
- Classification of documents is one of the priorities in 2014, reported 56% of respondents;
- Implementation of security policies for data management;

- Raising employee awareness about the value and importance of data.

In most cases the rights of access and information security fail to be taken into account to a sufficient extent; this is usually done haphazardly, defining certain rights from one case to another.

For this reason, it is very important to develop awareness and raise the level of education of employees so that they should be able to preserve their important business information and data in a possibly unorganized and unsafe environment. In this case the result and effectiveness of protection depends on their experience, creativity, interest and other subjective factors.

2.2 *User requirements*

When we analyse actual user behaviour, we come to a conclusion that their demands are becoming more numerous and more complex due to the progress and innovations in IT and the comfort provided to them in this way.

Customer requirements are moving towards:

- Access to a large variety of information of different formats and from any location (office, vehicle, restaurant, beach ...) and any device (desktop computer, laptop computer, PDA - Personal Data Assistant, tablet, smartphone, ...) that they own.
- Desire to share new photos with friends or colleagues on social networks, boast of visits to certain geographic locations, restaurants or resorts, which leads to a careless approach to the open WiFi hotspot networks thus jeopardising the security of user accounts.

It is no longer a question whether the IT sector can and should fulfill these requirements; rather, fulfillment of these demands is unconditionally taken for granted. The above mentioned features that allow for the user comfort and mobility, on the other hand, represent a serious potential safety hazard. The danger is reflected in the fact that unregistered corporate devices from any location on the Internet are required to provide access to information on the Intranet (BYOD - Bring Your Own Device) [3].

2.3 *Risks arising from hacker attacks*

Research shows that as many as 25% of organizations are faced with hacker attacks, viruses and similar problems 10 or more times during the year. More than 40% of large companies can give examples of confidential information being disclosed.

The presented data in Figure 1 show how much of a serious problem companies are faced with when it comes to this type of problem. As presented in Figure 1, 43% of companies never resume their business after they have suffered the disaster, while 29% go out of their business after 3 years. Only 28% of companies that have suffered the disaster continue to work. [4]

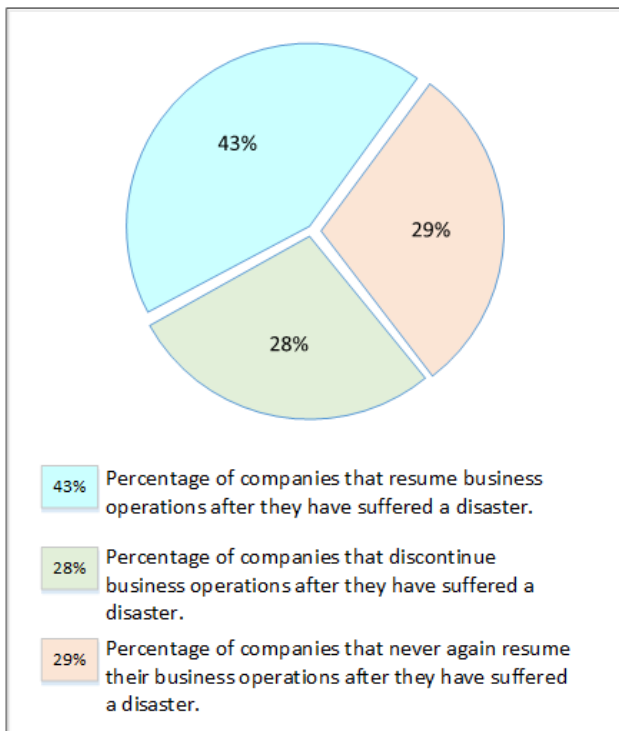


Figure 1: Problems with the continuation of business after the disaster suffered due to hacker attacks

3. CONCEPTUAL EXAMPLE OF A SYSTEM FOR RAISING THE LEVEL OF KNOWLEDGE IN THE FIELD OF INFORMATION SECURITY

A variety of hardware and software components interconnected with quick links with a plethora of attractive Internet services and contents available to customers represent a big challenge for any classic users of such infrastructure. That is why the responsibility of people in IT sector in charge of providing the necessary conditions for a user experience is heavy. When designing the system, it is very important that an appropriate technology platform should be selected.

3.1. Platform for education of employees in the field of Information Security

There are a number of solutions that can serve as a software platform for the development of the system. Three products, however, that are leaders in placing information, manipulating electronic documents and business process management can be singled out.

We have in mind:

- Alfresco system - Alfresco company is one of the leading manufacturers of Enterprise Content Management System (ECMS) [5]. It offers its solution as an open source Enterprise version, too. Out of box provides standard solutions such as document management, records management and Web content management.
- MS SharePoint is an ECMS collaborative platform developed with an aim to incorporate an increasing number of Web applications, services, and to, among other things, enable a functional management of web

sites and portals, of digital content and of business processes [6].

- MS InfoPath is an integral part of the Microsoft Office Suite that unifies and simplifies the process of gathering information by allowing users to independently create dynamic forms and fill in the forms in collaboration with the MS SharePoint.

In case of a system for raising the level of knowledge in the field of information security, the choice of platform has been made in favour of the Microsoft SharePoint and the InfoPath MS-a. There are a number of reasons for this decision, one of them being the fact that a large number of business systems use Microsoft Office as a software solution to work in an office environment. Therefore the compatibility of these two Microsoft's products gives advantage to Microsoft SharePoint.

3.2. Types of user roles

In case of the portal segment that refers to training employees and raising their level of knowledge in the field of information security, it is necessary to clearly define the necessary levels of access for different users of the portal.

The followig customer roles are defined on the portal:

- System administrators, whose role is to maintain the functionality of the platform of the portal;
- Content administrators, whose role is to: create news, create documents, define the test questions to assess knowledge, run and administer the purpose-specific forums and chat rooms.
- The role of employees is the central user role. All the employees are entitled to an adaptive and personalized access to the necessary contents and services in the field of data protection and information security, depending on the job requirements;
- Advanced users among whom are employees who, by the nature of their work, deal with the protection of data and information and the security of electronic documents at the enterprise level. Therefore their level of knowledge and training to carry out such work must be at a higher level. Advanced users are provided with additional information, services, and checklists and by higher level tests [7].

3.3. Criteria of adaptation

The term adaptation, in the context of this work, means the portal's ability to provide the necessary facilities for reaching the appropriate level of knowledge and permanent education in the field of information security and data protection with the possibility of evaluating the acquired knowledge by solving questionnaires and tests from this area [8], on the basis of automatic recognition of the user and his: attributes, desires, needs, interests, type of business, organizational unit affiliation, manner of behaviour when using a computer,

The functionalities that a specialized segment of the portal, among other things, is expected to provide are:

- Display of administrator functions at the level of sites and pages, depending on the level of user authorization;
- Display of current news related to a given issue;
- Identification of user's affiliation to an organizational unit of the company and, depending on that, a display of current content and tests;
- Definition of the part of the portal intended for marketing and publishing of various contents related to IT security and data protection intended for all users of the system;
- Forums with topics that cover the area of information security and data protection;
- Chat.

The process of accessing necessary services, contents and tests for education and knowledge verification in a specialized segment of the web portal, using the adaptive

and personalized user access, is realized through several phases (Figure 2):

- Phase 1 – Web portal user authentication is implemented in the way that a user logs in to the system by using a qualified electronic signature. Authentication is performed by the Active Directory (AD). Following a successful authentication at the AD group, affiliation is checked in the MS-SharePoint. In case of a new user, the process of creating a new user begins, which includes the opening of a user account in MS SharePoint and entering its attributes.
- Phase 2 – Adaptation is realized by applying complex criteria for adaptation, listed in the text above, on the basis of which the rights of users to view educational content and tests are defined [9].
- Phase 3 - personalized access to needed services, educational content and tests for verifying the knowledge in a specialized segment of the web portal, depending on the result obtained from the phase 2.

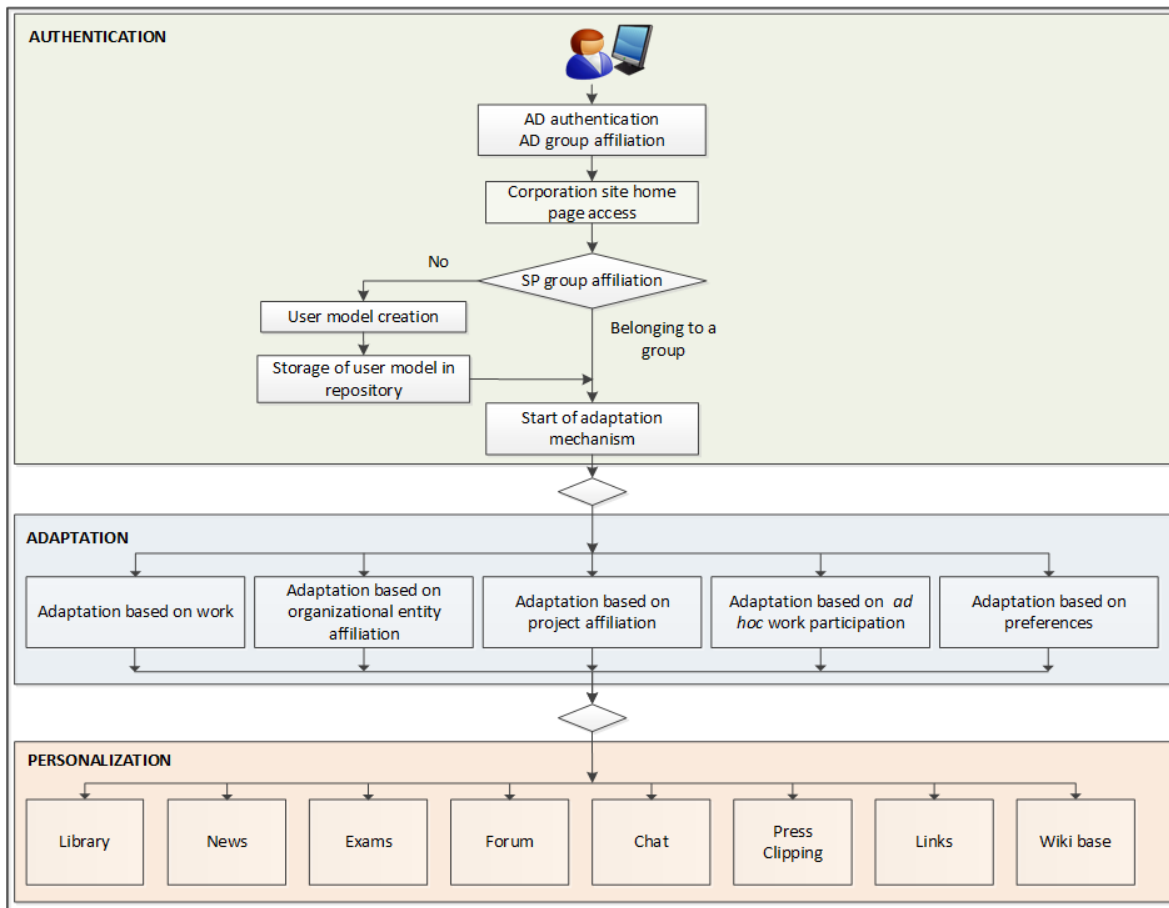


Figure 2: The process of adaptive and personalized access to services, contents and tests for Education

Upon the realization of the previous phases, the user may access the following functionalities and content in the field of information security and data protection of segments of Web portal, depending on his categorisation:

- Library;
- News of current events;
- Tests for knowledge assessment;

- Discussions - creation of discussion groups (forums);
- Chat rooms;
- Press Clipping;
- Links to specialized sites;
- Wiki base;

3.4. Testing system users' knowledge

Due to the specificity of individual jobs and the types of work individual employees are engaged in, the system can be used at most convenient times, that is, at times when employees are least engaged. For example, workers at the counters whose primary job is working with clients do not have the opportunity to train and expand their knowledge in specific areas at any time but are conditioned by the current workload imposed by the number of users who are waiting to do the business they came for.

One of the ways to check the level of knowledge of employees in the field of information security and data protection is the creation of a web questionnaire - tests by using Microsoft InfoPath forms.

Questionnaires can be realized in the form of questions:

- with check boxes where users can give multiple responses;
- with a possibility for users to give the answers to the questions by filling the text box provided for the answers;
- where users provide an answer by selecting options true or false, as shown in Figure 3.

Test of knowledge in the field of information security

In order to test the knowledge of IT security and data protection, it is necessary to answer the following questions.

Can the virus be hidden in the PDF document? true false

It suffices to check only the e-mail sender, it is not necessary to check a complete e-mail address? true false

Disclosing one's user name and password to the employees in the company's technical support unit is not allowed? true false

Figure 3: Example of the test for assessment of the knowledge of employees in the field of IT security and data protection

Distribution of tests for examination in the field of information security and data protection, depending on the need and urgency of the implementation of the action, could be realized in the following ways:

- By posting the questionnaire in a web form in the segment of the Web portal intended to raise the level of knowledge of employees in the said field. Employees then can access the test - questionnaire and solve it at the moment they find most convenient;
- By sending a questionnaire via e-mail, as an attachment. The option which is suitable in case some important information or test - questionnaire assignment has to be sent promptly and safely to each employee with the security of receiving confirmation of receipt of mail.
- By combination of the previous two. By posting the questionnaire in a web form in the segment of the Web portal and sending an e-mail with a hyperlink to the location to which the questionnaire is posted.

Upon the completion of testing, the process of control of the given answers as well as the the verification of the achieved points is activated. The results obtained are entered into the personal records of each employee, whereby providing conditions for monitoring the level of knowledge of each employee in a particular field. In addition, it is possible to conduct various types of statistics, for example, monitoring the response of employees regarding some topics and the percentage of correct answers given in relation to the respective topic.

5. CONCLUSION

Implementation of the system for permanent education of employees in the field of information security and data protection in large business systems using the segment of intranet web portal enables:

- actions to prevent the violation of the security of information and data;
- employee daily insight into news in this field;
- prompt, simple and efficient way to inform employees about current threats to which they are exposed thereby achieving a preventive effect on the protection quality;
- simple, easy and effective way of conducting periodic checks of employees' knowledge in this area using short control tests;
- placement of recommendations and warnings by system administrators with the aim of raising the level of protection of a computer system.

Measures taken to preserve information depend on a number of circumstances in each individual case as well as on the importance and value of the information itself, however, above all, the security of information itself depends on the human factor, which is a key element in this chain [10].

However, no matter what kind of computer threat we deal with, what is certain is that the permanent work on the education of all levels of users by using modern tools can to a large extent reduce or prevent a potential attack and consequently the damage.

REFERENCES

- [1] Boldon James: Data classification – Know your files, value your data, protect your business. Available online at <https://www.boldonjames.com/data-classification/>, [Last access date 25.08.2016].
- [2] Forrester: Understand The State Of Data Security And Privacy: 2013 To 2014.
- [3] CIO from IDG, Available online at <http://www.cio.com/article/2396336/byod/all-about-byod.html/>, [Last access date 25.08.2016].
- [4] KPMG - IT controls and risk management information systems. Available online at <http://www.infotech.org.rs/blog/wp-content/uploads/KPMG-IT-kontrola-i-upravljanje-rizicima-informacionih-sistema.pdf>, [Last access date 1.07.2016].

- [5] Alfresco community. Available online at <https://www.alfresco.com/> , [Last access date 15.08.2016].
- [6] Microsoft Corporation, Microsoft SharePoint. Available online at <https://products.office.com/en-us/sharepoint/collaboration/> , [Last access date 1.08.2016].
- [7] Symantec Corporation. Available online at <http://www.symantec.com/connect/blogs/tactical-cyber-security-checklist> , [Last access date 3.06.2016].
- [8] Esichaikul, V., Lamnoi, S. & Bechter, C., 2010. Student Modelling in Adaptive E-Learning Systems. Knowledge Management & E-Learning: An International Journal, 3 (3) pp. 342-355. Available online at <http://www.kmel-journal.org/ojs/index.php/online-publication/article/viewFile/124/102> , [Last access date 13.06.2016].
- [9] Dekson, D.E. & Suresh, E.S.M., 2010. Adaptive e-learning techniques in the development of teaching, electronic portfolio – a survey. International Journal of Engineering Science and Technology, 2 (9), pp. 4175-4181.
- [10] Symantec Corporation. ISTR – Internet Security Threat Report, Volume 21, April 2016.

IMPACT ANALYSIS OF CYBER ATTACKS ON CLOUD SYSTEMS

IGOR OGNJANOVIĆ

MG-Soft Montenegro; University Donja Gorica, Montenegro; igor.ognjanovic@gmail.com

RAMO ŠENDELJ, IVANA OGNJANOVIĆ

University Donja Gorica, Montenegro; {ramo.sendelj, ivana.ognjanovic}@udg.edu.me

Abstract: We are currently witnessing the maturing of Cloud Computing from a promising business concept to one of the fastest growing segments of the IT industry. Despite of all the hype surrounding the cloud, businesses are still reluctant to be deployed in the cloud, since security, data privacy and data protection continue to plague the market. As more and more information about both individuals as well as companies is placed within the cloud, unease keeps growing about just how safe an environment it is, making them potentially deliberate exploited by cyber attackers. This is a reason why exact analysis of causes and impacts of cyber attacks should be done over cloud systems in different domains of applications. In this paper, we show some models and features which could be used for assessing cyber attacks, their impacts, as well as some concepts of security intelligence that can defend these cyber threats.

Keywords: Cyber Attacks, Impact Analyses, Cloud Computing, Cloud Systems

1. INTRODUCTION

We are currently witnessing the maturing of Cloud Computing from a promising business concept to one of the fastest growing segments of the IT industry. Cloud computing is replacing computing as a personal commodity by computing from public utility, where e.g., health data is collected by iWatch and stored in a health log book in the cloud. According to the most commonly used definition from NIST [8], cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. The experts at global level expects the growth in cloud computing at a compound annual growth rate of 28.8%, with the market increasing from \$46.0 billion in 2009 to \$210.3 billion by 2015 [1].

Despite of all the hype surrounding the cloud, enterprise customers are still reluctant to deploy their business in the cloud. Security is one of the major issues which reduces the growth of Cloud Computing and complications with data privacy and data protection continue to plague the market. As more and more information about both individuals as well as companies is placed within the cloud, unease keeps growing about just how safe an environment it is.

That is, as more and more information on individuals and companies are placed in the cloud, concerns are beginning to grow about just how safe an environment it is. While worldwide IT spending is slightly down has slightly declined in recent years, spending on information security related products and services by small and large organizations alike large and small has been growing at a rate of increased by 17.6% per annum since 2004 [3]. According to the EMC Corporation and RSA Security, Cybercrime losses were around \$5.9 billion in 2013 [2].

Security departments are facing new challenges in protecting valuable business data against an ever-increasing wave of cybercrime attacks. Recently, several models are proposed, such as: [4] proposes four-tier framework for web-based development); a Trusted Third Party is proposed in [5] with defined specific tasks aimed on assuring specific security characteristics within a cloud environment; [6] gives a quantitative model of security measurements that enables cloud service providers and cloud subscribers to quantify the risks; [7] proposes innovative approach for increasing cyber security over cloud services by using Semantic Web technology, hierarchical ontology and intelligent reasoning techniques. However, there is no unique model/approach which addresses cyber attacks and their impacts in cloud environment [5, 7].

In this paper we go one step further and analyze how attack-countermeasure tree (ACT) [14] a combinatorial modelling technique for analyzing cyber attacks and countermeasures can be used for analyzing impacts of cyber attacks in cloud environment. The paper is organised as follows: Section II introduces security models on cloud systems, Section III provides overview of attack countermeasure trees, while Section IV provides key considerations about using ACTs with cloud security models. Section V concludes the paper with key findings and conclusions moving towards development of innovative impact analysis models of cyber attacks in cloud environments.

2. SECURITY MODEL FOR CLOUD SYSTEMS

The basic idea behind cloud computing is replacing computing as a personal commodity by computing as a public utility (from storing data to community via e-mail to collaborating on documents or crunching numbers on large data sets) [9]. According to the most commonly used definition, *clouds*, as the first-class citizens of cloud

computing environments, are sets of hardware, networks, storage, services and interfaces that combine to deliver aspects of computing as a service. *Cloud computing* is a disruptive technology that has the potential to provide distinct benefits to businesses of all sizes to improve digital productivity and simplify electronic business, through gaining discernible benefits, such as increased flexibility, online operating service availability, maintainability, affordability, and scalability [7].

Even though much effort is put on modelling and establishing innovative legal and technical procedures and standards for cyber security in all aspects of IT use and adoption, they cannot be directly applied in cloud computing environment as the. The cloud model is somewhat different: the cloud resource consumer and cloud resource provider are seldom rarely the same entity; the application software and databases are moved into the large data centres, where the management of the data and services are not trustworthy. Each participant has a different business strategy and thereby may stress some specific security aspects over others, and the implications of security breaches are confounded by the dynamics of communications and collaborations that occur throughout the network in the normal course of business. An increased understanding of Cloud Computing and the roles of various stakeholders in this realm is important. Furthermore, each participant operates autonomously and has legal and business control over its internal operations, data and other resources, and it is hardly to be expected that there exist homogeneity and compatibility between all parties. Traditional methods for collaboration between distributed systems include static and centralized approaches, trusted third party approaches and dynamic negotiation, which obviously expressed weaknesses associated with maintaining the security of the central security policy repository.

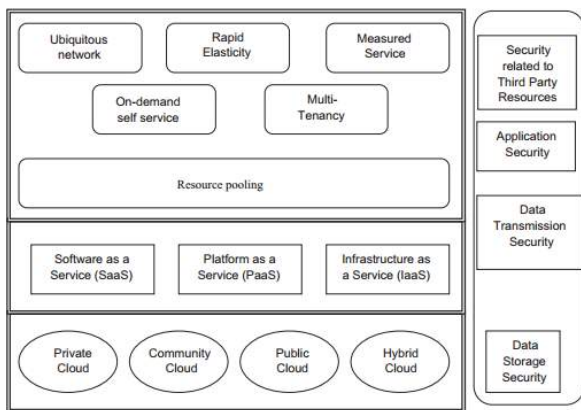


Figure 1. Complexity of security in cloud environment [26]

There are various security recommendations for Cloud Computing providers (e.g. international organizations like ENISA (European Union Agency for Network and Information Security) [10], etc.). It has also been shown, that security, privacy and usability is often contradictory what as been discussed in Al Abdulwahid et.al [11]. Consequently, security in cloud environments is currently one major area of interest with issues for both, scientific and ICT community, since threats and attacks are all

modern and sophisticated, whereas cloud solutions are still vulnerable and thus, cloud providers and users are facing serious challenges of their protection [6][7]. The complexity of security risks in a complete cloud environment is illustrated in Figure 1.

Recently, we proposed innovative semantically enabled model (CSM) [7] which showed solid potentials for addressing all cyber security issues in one integral framework with defined metrics (quantitative and qualitative), as shown on Figure 2. The model is developed by following hierarchical ontological structure which integrates all semantic diversity in characteristics, relationships and dependencies between cloud computing models and all involved parties [7]. The CSM model also enables integration of intelligent reasoning techniques and mechanisms [12] based on service transformation of clouds, as commonly used in the literature [13].

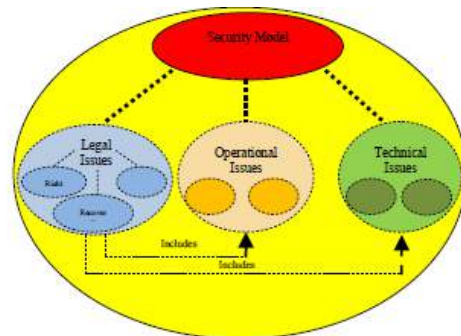


Figure 2. Cyber Security Model (CSM): Hierarchical structure [7]

3. IMPACT ANALYSIS OF CYBER ATTACKS: ATTACK COUNTERMEASURE TREES

The impact analysis is one of key issues in modelling system response to security threats, as focused on the interaction between the cyber and physical aspects of the system [18]. To this end, commonly used mathematical structure is a graph (defined as a collection of vertices and a collection of edges that connect node pairs), which is widely used for representation of pairwise relationships between a set of objects. Depending on the use of a graph, its edges may or may not have direction leading to directed or undirected classes of graphs, respectively.

Recently developed attack-countermeasure tree (ACT) [14] is an example of graph based structure for modelling and analyzing cyber attacks and countermeasures. Structure of tree is much simpler for processing and reasoning since it is simplified graph. In ACT, there are three distinct nodes, so-called *classes of events*: attack events (e.g. install keystroke logger), detection events (e.g. detect keystroke loggers) and mitigation events (e.g. remove keystroke logger). ACT can be consists of [14]: (i) a single attack event (Figure 3a), (ii) an attack event and a detection event (Figure 3b), (iii) an attack event and multiple detection events (Figure 3c), (iv) an attack event, a detection event and a mitigation event (Figure 3d) or (v) an attack event, n detection events and corresponding n mitigation events (Figure 3e).

Having structure of a tree, it is easy to automate the generation of attack scenarios [14] by using its minimal cut sets. Furthermore, each node is assigned with probabilistic of attack success at the goal; and straightforward mathematical equations are defined for each gate type and combination of attacks and detection events [14].

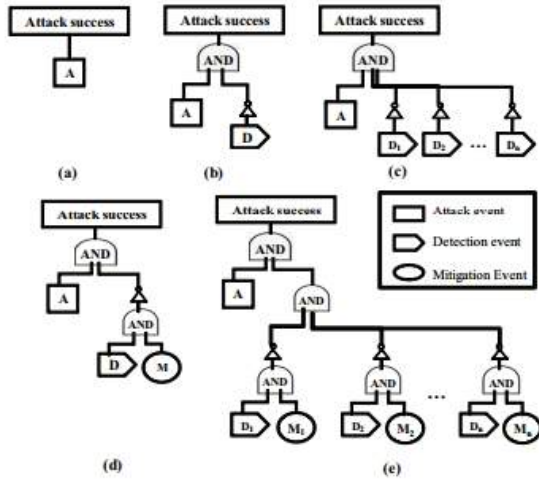


Figure 3. Attack Countermeasure Trees [14]

ACT is thus a structure which enables to perform probabilistic analysis (e.g. probability of attack at the goal node, attack and security investment cost, impact of an attack, system risk, return on attack (ROA) and return on investment (ROI)) in an integrated manner [14, 19].

4. ATTACK COUNTERMEASURE TREES FOR CLOUD BASED SYSTEMS

Having in mind that cloud computing can be defined as computing paradigm based on delivery of applications to users as services over the Internet [7, 15], each having specific requirements and available for participants; we will use service-oriented transformation of cloud based solutions [13, 7]. Furthermore, recent research shows [16, 12, 17] that semantically enhanced presentation of service-oriented architectures provides bases for intelligent reasoning over the model [16], automatic configuration and management [17], etc. That is a reason, why we decided to analyse how to use the advantages of using service orientation and ontological security model over clouds.

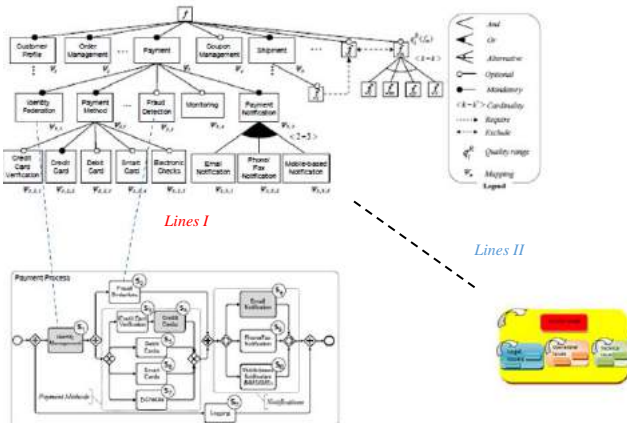


Figure 4. Service-oriented transformation of cloud models and corresponding security model

Both proposed models have structures of tree, ACT (see Figure 3) and service-oriented transformation of cloud based systems (e.g. service-oriented architectures, which is commonly presented by means of two models: business model templates and feature models). Due to limited space for the paper, we provide illustrative example (see Figure 4) which shows high-level representation of e-shop service oriented architecture. Key findings is one-to-one mapping between the two models (Figure 4-lines I), and its mapping to CSM model (Figure 4- lines II).

However, in order to develop comprehensive model for measuring impacts of cyber attacks on cloud systems, we propose integration of ACT with semantically enhanced CSM model, by following step-wised approach:

- (i) create ACT for each activity in service transformed cloud model;
- (ii) establish links to leaves in CSM model (having in mind all, legal, operational and technical issues);
- (iii) propagate values from leaves to the root by respecting relations at all models (and mappings – at Figure 4).

Even proposed solution presents methodological approach which needs more approval and theoretical analyses, they have strong roots in the following similar approach developed for the same models:

- Propagation of non-functional values over service-oriented model with mappings (Figure 4-line I) is formalised with simple mathematical functions: aggregation, multiplication, max, min. Figure 5 presents an excerpt from the fill version (available in [20]) and it is related to one non-functional property-cost;
- Aggregation of probabilities of attack success (as introduced in [14]- see Figure 6).

Mandatory-Optional-Excludability Pattern	Seq. Pattern	Cost (q _i)	
		QoS Properties	Cost (q _i)
<ul style="list-style-type: none"> 1 Sequence 2 Arbitrary Cycle 3 AND-AND 4 AND-DISC 5 AND-XOR 6 XOR-XOR 7 OR-XCOR 8 OR-OR 9 OR-DISC 	1	Sequence	$\left[\sum_{i=1}^n q_p(i) : \forall f_i \in j, \sum_{i=1}^n q_p(i) : \forall f_i \in j \vee j \right]$
	2	Arbitrary Cycle	$\left[\sum_{i=1}^n q_p(i) : f_i \in j \vee j, \sum_{i=1}^n q_p(i) : f_i \in j \vee j \right]$
	3	AND-AND	$\left[\sum_{i=1}^n q_p(i) : \forall f_i \in j, \sum_{i=1}^n q_p(i) : \forall f_i \in j \vee j \right]$
	4	AND-DISC	
	5	AND-XOR	$\left[\min \left(\sum_{i=1}^n q_p(i) : f_i \in j \vee j \right), \max \left(\sum_{i=1}^n q_p(i) : f_i \in j \vee j \right) \right]$
	6	XOR-XOR	
	7	OR-XCOR	$\left[\min \left(\sum_{i=1}^n q_p(i) : \forall F_{sub} = F_{sub}^i, \max \left(\sum_{i=1}^n q_p(i) : \forall F_{sub} = F_{sub}^i \right) \right) \right]$
	8	OR-OR	
	9	OR-DISC	

Figure 5. Aggregation rules for non-functional property: Cost [20]

Gate type	Prob. of attack success	attack cost	impact
AND	$\prod_{i=1}^n p(i)$	$\sum_{i=1}^n C_i$	$\sum_{i=1}^n I_i$
OR	$1 - \prod_{i=1}^n (1 - p(i))$	$\forall i \min C_i$	$\forall i \max I_i$
k-out-of-n*	$\sum_{i=k}^n \binom{n}{i} p^i (1 - p)^{n-i}$	$\sum_{i=1}^k C_i$	$\sum_{i=1}^k I_i$

Figure 6. Formulae for probability of attack success [14]

Having in mind dynamical nature of cyber space and cyber attacks, dynamical cyber system can be presented as a mathematical formalisation to describe time-

evolution of a state x (which can represent a vector of physical quantities) [18], and the following mappings:

- mapping f between models for presentation of service transformed cloud computing model (Fig. 4- lines I);
- mapping g between service oriented model and CSM model (Fig.4- lines II);
- mapping h between CSM and ACT model.

In continuous time, the impacts of cyber attacks can be presented as the deterministic evolution of the current states of the system, as follows:

$$\dot{x} = F(x, f, g, h, u) \quad (1)$$

where \dot{x} is the time-derivative of x and u an input vector [14].

4. DISCUSSION

Development of security models is well known issue for both, researchers and developers [7, 14, 13, 19]. In addition to existing technical challenges to overcome, the legal situation is continuously changing.

The EU General Data Protection Regulation (“GDPR”) has been adopted at the EU level on 14. April 2016 and is one big step towards a privacy-friendly Cloud. Most notable requirements are data breach notification, data security and risk assessment. The personal data breaches notification requires public electronic communications providers such as telcos and ISPs to report such breaches to the relevant national regulator, and this has led to a range of national guidance on when and how such reporting should be made. ENISA has also produced extensive guidelines on this matter [21].

There are many best practices, white papers, etc., which gives advice how to operate Cloud infrastructure in a secure and privacy protecting way [22]. To prove that all security controls are set have to be audited by third party and certified by e.g. STAR. Cloud audits are challenging by its dynamic infrastructure changes. Changing Cloud infrastructures are continuously audited using software agent technology [23], Ruebsamen et.al [24] discusses privacy issues during audits, and Ruebsamen et.al [25] uses the Cloud Trust Protocol to do auditing of Cloud provider chains.

5. CONCLUSION

In this paper we have introduced an approach to cyber attack impact analysis for cloud based solutions. The advantage of the proposed solution can be modelled within one framework allowing a single, but potentially powerful analysis approach which integrates different aspects, legal, economical and technical. Thus, effect relations for cyber-attacks are better managed for comprehensive impact modelling and analysis, also allowing intelligent reasoning and predicting. Future work will include completed solution of mathematical formalisms, formal verification of the model and simulation testing and analyses.

Acknowledgment. Research presented in this paper is conducted within the TEMPUS project ‘*Enhancement of*

Cyber Educational System in Montenegro (ECESM)’, project no. 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES.

REFERENCES

- [1] Australian Information Industry Association, ‘Modeling the Economic Impact of Cloud Computing’, 2012
- [2] EMC, ‘The current state of cybercrime 2014’, USA
- [3] C. Derrick Huang et al. ‘Economics of Information Security Investment in the Case of Simultaneous Attacks’, WEIS 2006
- [4] W. Tsai, Z. Jin, and X. Bai, “Internetware computing: issues and perspectives”, 1st Asia-pacific symposium on Internetware, China, 2009, pp.1-10
- [5] Z. Dimitrios, and L. Dimitrios, „Addressing cloud computing security issues“, Future Generation Computer Systems, 2012, Vol.28, pp.583-592
- [6] L. B. A. Rabai, M. Jouini, A. B. Aissa, and A. Mili, „A cyber security model in cloud computing environments“, J. of King Saud University- Computer and Information Sciences, 2013, vol. 25, pp.63-75
- [7] R.Šendelj, I.Ognjanović, "Semantically enhanced cyber security over clouds: Methodological approach", International Journal of Advances in Computer Networks and Its Security, 2014, Vol 4, No.3, ISSN: 2250-3757
- [8] P. M. Mell and T. Grance, ‘SP 800-145. The NIST Definition of Cloud Computing’, Jan. 2011
- [9] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, “A View of Cloud Computing”, Communications of ACM, 53 (4), 2010, pp.50-58
- [10] ENISA paper: Cloud Computing: Benefits, risks and recommendations for information security; <https://www.enisa.europa.eu/events/speak/cloud.jpg/view>
- [11] Al Abdulwahid A, Clarke NL, Furnell SM, Stengel I, Reich C; Security, Privacy and Usability - A Survey of Users' Perceptions and Attitudes; 12th Int. Conf. on Trust, Privacy and Security in Digital Business (TrustBus 2015), Valencia, Spain, pp153-168
- [12] M. Bošković, E. Bagheri, G.grossmann, D. Gašević, and M. Stumptner, „Towards Integration of Semantically Enabled Service Families in the Cloud“, CSWS 2011, Vol. 774, pp.58-69
- [13] T. Takahashi, Y. Kadobayashi, and H. Fujiwara, „Ontological Approach toward Cybersecurity in Cloud Computing“, SIN 2010, pp.7-11
- [14] A. Roy, D. Seong, K. S. Trivedi, „Cyber Security Analysis using Attack Countermeasure Trees“, CSIRW 2010, Oak Ridge, Tennessee, USA
- [15] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing." Communications of the ACM, 2010, 53(4), pp. 50-58

- [16] M. Asadi, B. Mohabbati, D. Gasevic, E. Bagheri, and M. Hatala, "Developing Semantically-Enabled Families of Method-Oriented Architectures", *IJISMD*, 2012, 3(4), pp. 1-26
- [17] I. Ognjanović, B. Mohabbati, D. Gašević, E. Bagheri, M. Bošković, "A Metaheuristic Approach for the Configuration of Business Process Families", *IEEE International Conference on Service Computing (SCC2012)*, Hawaii, USA, 2012
- [18] D. Kundur, et. al., "Towards modelling the impact of cyber attacks on a smart grid", *Int. J. Security and Networks*, Vol. 6 (1), 2011, pp.2-13
- [19] B. B. Madan, K. S. Trivedi, "Security Modeling and Quantification of Intrusion Tolerant Systems Using Attack-response Graph", *J. of High Speed Networks*, 13(4):297-308, 2004
- [20] B. Mohabbati, D. Gasevic, M. Hatala, M. Asadi, E. Bagheri, and M. Boskovic, "A Quality Aggregation Model for Service-Oriented Software Product Lines Based on Variability and Composition Patterns", *ICSOC 2011*, pp. 436-451
- [21] Andreas Rockelmann, Joshua Budd, Michael Vorisek, 'Data Breach Notification in the EU' (ENISA, 13 January 2011); Marnix Dekker and Christoffer Karsberg 'Technical guidance on the incident reporting in Article 13a' (ENISA, November 2013); Marnix Dekker, Christoffer Karsberg 'Technical guidance on the security measures in Article 13a' (ENISA, November 2013)
- [22] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations." SP 800-53. National Institute of Standards and Technology (NIST), April 2013
- [23] F. Doelitzscher, C. Fischer, D. Moskal, C. Reich, M. Knahl and N. Clarke, "Validating Cloud Infrastructure Changes by Cloud Audits," *2012 IEEE Eighth World Congress on Services*, Honolulu, HI, 2012, pp. 377-384. doi: 10.1109/SERVICES.2012.12
- [24] T. Rübsamen, C. Reich; Cloud Audits and Privacy Risks; On the Move to Meaningful Internet Systems: OTM 2013 Conferences, Lecture Notes in Computer Science Volume 8185, p: 403-413; 2013
- [25] T. Rübsamen, D. Hölscher, Ch. Reich; Towards Auditing of Cloud Provider Chains Using Cloud Trust Protocol; CLOSER 2016: Rom, Italy, 2016

COMPARATIVE ANALYSIS OF SOME CRYPTOGRAPHIC SYSTEMS

VELIBOR ŠABAN

School for secondary and vocational education „Sergije Stanić“ Podgorica, Montenegro, velibor.saban.mbs@gmail.com

IVANA OGNJANOVIĆ

University of Donja Gorica, Montenegro, ivana.ognjanovic@udg.edu.me

RAMO ŠENDELJ

University of Donja Gorica, Montenegro, ramo.sendelj@udg.edu.me

Abstract: *Cryptography is the study of techniques used for preserving data confidentiality. When the personal, financial, military or national security information is transferred from place to place, it becomes subject to eavesdropping tactics. Such problems can be avoided by information encryption thus making them inaccessible to unwanted (third) parties. Protocols are created by people trying to create a system that will prevent insertion of a third party in the communication or impersonation of a person in communication.*

In this paper the following cryptographic protocols, will be presented: Wide-Mouth Frog, Yahalom, Needham-Scroeder, Otway-Rees, Kerberos, Neuman-Stubblebine, Denning-Sacco and Woo-Lam. Firstly, we will present each protocol shortly with its most important properties, followed by their comparative analysis. We will also make analysis of the attacks they are resistant to, as well as the attacks that make them vulnerable and they are subject to. The main problem these protocols are working on is the safe exchange of secret keys between the two parties, and ensuring them that the communication is with the person they want, rather than with a stranger. Codes and protocols are important tools, but they are a poor substitute for the real, critical thinking about what is really protected and how different methods of defense may fall. Even if the intruder has access only to the ciphertext, such small cracks in some parts of the system could provide sufficient information, thus turning good cryptosystems into useless.

Examples in this research show us how by the application of logic can be caught slight difference between the protocols. For certain protocols we identify errors and suggest corrections. One of key mistakes could be found in the use of the Kerberos protocol with DES, which is however weak protocol, but it is still found in some products that have not implemented the newer and better AES protocol. Furthermore, the Kerberos could be weakened by using the lower protocols. Protocols that use synchronization of clocks, such as the Needham-Schroeder, which can be a source of the attack, must be supplemented with protocols to access the time servers. There is no easy way to make systems safer, there is no substitute for careful planning and continuous critical examination.

Keywords: *cryptography, protocols, error identification, protocols' improvements*

1. INTRODUCTION

Cryptography is the study of techniques used for preserving data confidentiality. Cryptographic protocols are used to establish secure communication over unreliable global networks and distribution systems. They rely on cryptographic protection methods in order to provide basic security services of confidentiality, integrity and undeniability. In the literature there are numerous protocols, but none of them is the perfect one.

Each has its advantages and disadvantages. When the personal, financial, military or the information of national security is transmitted through a computer network, it becomes vulnerable to listening tactics, which makes information become potentially vulnerable. Vulnerability of information is reflected in the illegal access, illegal modifications and integrity violation. Therefore, the aim of this work is to focus on the analysis and comparison of the existing cryptographic protocols while maintaining

message transfer through the network. The basic cryptographic approach is based on a combination of the authentication and key exchange, in order to solve a common computer problem: two entities -the sender (originator) and the recipient, who want to communicate through a computer network safely. The question is: how can these entities exchange secret keys and be sure to talk to each other, but not to the third party at the same time? A common cryptographic technique is to encrypt each individual conversation by using a special key. This key is called the session key, because it is used only for one specific session. Session keys are useful because they only exist during the session. However, an additional problem in a cryptographic protocol is a way of key distribution to the participants of a session. This study is focused on comparative analysis of algorithms that have different ways of solving the problem of key distribution and the results of the analysis are used to create the overall comparative picture about the properties of algorithms mentioned, which is still the basis for making guidelines on their practical usage and possible solutions.

2. CRYPTOGRAPHIC PROTOCOLS AND ATTACKS

2.1 Cryptographic protocols

There are two types of cryptographic protocols, symmetrical and asymmetrical. At *symmetrical protocols* the same key is used for encryption and decryption, and thus, the main problem with this protocol is the possibility of the password interception, which gives the intruder the ability not only to read the messages, but to send them out as well. Therefore, this encryption method is the most commonly used for data protection that isn't shared with other parties. On the other side, *asymmetrical protocols* use two types of keys, a public (which is used to encrypt the data and it is sent to all those we want to exchange encrypted data with) and a secret key (which is used for data decryption). Sending the public key, which is used only for encryption but not for decryption, is the main advantage of these protocols.

When we are talking about cryptography, the key issues are to provide the following: (1) integrity of encrypted data (to prevent unauthorized changing, deleting or information substitution); (2) information confidentiality (only authorized persons have the key); (3) authentication – introducing is the beginning of each communication followed by information exchange; and (4) Impossible to deny responsibility - Non-repudiation ensures that the

contract, particularly the one made over the Internet can not be overridden later by any of the parties involved.

Some considerable consequences can be caused by unauthorized access: the business could operate at a financial loss; a competitive business could become very profitable, decreased trust of service users or product consumers. The examples on this information include the following: data collection on wages, on employees, project files, accounting data, confidential contracts etc. The aim of the cryptographic system attack is getting the code that enables text encryption and decryption. There are many types of attacks, starting with the situation when the intruder has only a cipher text or a cipher text and a plaintext used to get the code. Whereas getting the code in this way is very difficult and it requires huge assets and knowledge as well, the intruders have found some easier ways to get it. These attacks are based on finding a way to be into the communication channel between the sender and the intended recipient, so-called man-in-the-middle attacks. Replay attack is carried out by an intruder who tries to use the old keys and establish communication in that way. In the systems where all the keys are kept at one place such as systems with KDC (Key Distribution Center) the risk of an attack is, at the same time, a possibility that the intruder could compromise or break down the KDC, which would compromise the entire system.

2.2 The types of attacks on cryptographic protocols

Probably the most common attacks on cryptographic protocols are freshness attacks. If the exchanged messages do not have appropriate timestamps, an intruder gets authorization by using a recorded copy of the message from a previous run of the protocol. To avoid this kind of attack the following should be taken into account during the designing of the protocol: (i) each cryptographic statement of the protocol should contain a random number generated by the receiver in the previous run of the protocol; (ii) the usage of synchronized clock and timestamps.

Replay attack refers to a possibility when the intruder uses the old password and frauds the participants of the communication by false representation (social engineering). In order to prevent this type of attack the following measures must be taken: a special session token for each session and time stamping. Parallel session- at this attack several sessions are run simultaneously. The intruder uses message from one session to run a parallel session.

Type attacks are based on the replacement of a part of the message with the other part of a different type, and a random number is used as the key. This attack can be avoided if these guidelines are followed: (i) When establishing contact between the sender and the receiver, in the systems with symmetric keys, at least one message must be sent containing the sender's identity; (ii) If the system with the public key is used, when establishing contact at least one message must be sent with the sender's identity as well; (iii) In the systems with the secret key, in establishing contact, both messages must contain the identity of the recipient

3. PROTOCOLS

3.1 Wide-Mouth Frog

The Wide-Mouth Frog protocol is a computer network authentication protocol published by Burrows, Abadi and Needham (1) in 1989. This is possibly the simplest symmetric key-management protocol that uses a trusted server. The trusted server has keys that it shares with the principals concerned (sender and receiver). These keys are used not for encrypting real messages between the principals concerned, but for the keys distribution. What makes this protocol special is the principal that generates and sets up a session key, not the center for the key distribution. The most important assumption in this protocol is that the sender is competent enough to generate good session keys, which is not easy to be done. To overcome this problem, a server must generate session keys. Timestamps are used so that the authentication center (server) and the receiver could know how much time has passed since the generation of the message itself. The message is ignored if it took more time than agreed on, (which makes difficult to a third party to find out the secret key or to insert in the communication between sender and receiver). This protocol has never been applied broader because it has several major flaws. The biggest flaw is that all principals and the server as well must have access to a single clock, and the same clock must be protected from the influence of a third party. Another problem is that the server knows all the keys so if it happens that the safety of the server is in danger, than all safe channels established through the server are in danger, too. The third problem is that the shared encryption key is fully determined by sender. Repeated attack at the Frog protocol, the adversary can keep the session keys for later reuse. This attack assumes that the server does not keep a record of keys used recently nor the timestamps as well.

3.2 Yahalom

This protocol uses authentication server and random numbers. In this protocol the server determines the session key, and it is symmetrical. It is designed to be applied in unsafe networks such as the Internet. It can be said that this protocol is a corrected version of the Frog protocol. Attack at Yahalom can be performed by an intruder masked as a sender who starts a parallel session, which is a parallel attack. In this way he is likely to mislead the receiver and to get the session key. In his work, Burrows, suggested a correction of this Protocol, by adding a random number of the receiver in the first message exchanged between the server and the receiver.[1] Even the corrected protocol is un resistant to attacks. For it is possible to be under a replay attack. This weakness comes from the recipient's inability to check whether the session key received a message from the sender or server. If the intruder presents himself as the sender, it is possible to use the old session key and start communicating with the receiver so that and the receiver can not see the identity switch. [2]

3.3 Needham- Schroeder

This protocol is available in two versions, the one with symmetrical and the other one with asymmetrical key, which is the public key. The version using the symmetric key was the basis for the development of the Kerberos protocol. It is used for the keys exchange in unsafe networks such as the Internet. The server for the key exchange and session key allocation is used here, too. This protocol could be attacked by a replay attack. The intruder can use an old session key and start communication with the receiver. The recipient is not aware that this is not a new key. This attack can be thwarted if the timestamps are used in the protocol as well. Type attack is also a possibility, when the intruder types his name instead of a random number.[3]This attack can be prevented if in the message, each field is checked whether it corresponds to the type it should.[4]Another type of attack that is possible on this protocol is freshness attack, the solution is to use timestamps. This solution is applied at the Kerberos protocol. Another type of attack is MIM (man -in -the middle) in which the sender and receiver think they communicate directly unaware that all communication is via the intruder. Correction of the protocol came out in 1995, and it consists of adding the receiver's name in the second message of the protocol. Denning and Sacco showed that there is a possibility of a parallel attack. This

attack can be disabled by adding a random number of the receiver in the second message. Denning and Saccos have suggested another solution, which is the usage of timestamps. Like all server protocols, this one is also subject to be attacked on its own server.

3.4 Otway- Rees

This protocol uses symmetric keys, random numbers, indexes and authentication server. The protocol is subject to man - in - the middle attack.[5] There is a possibility that the intruder gets a new session key from the server, which the intruder can use to present himself as the receiver to the sender. In this case the intruder uses two different keys to communicate with the receiver and sender. There is a possibility of a type attack when the intruder plants the name of the sender, receiver and the index as the session key.[6] Another attack is a replay attack, when the intruder uses old random numbers in order to deceive the receiver and initiate communication.

3.5 Kerberos

Kerberos is simultaneously an authentication protocol and KDC, too. Kerberos can be described as a safe authentication protocol that uses a Single Sign On login type, which ensures high efficiency. Users are allowed to sign on the system only once, and have access to system or network resources, depending on their authority. Communication between entities within the Kerberos protocol is based on the tickets exchange. A ticket represents a type of encrypted data that is transmitted through the network, and delivered to the client who saves them and uses it later as a pass for establishing communication with the appropriate server. While encrypting messages / tickets, Kerberos protocol uses symmetric DES algorithm or its variants such as 3DES, and Kerberos Version 5 uses AES algorithm only. Kerberos environment consists of two servers as follows: authentication server AS and Ticket-Granting Server.

3.5.1 Kerberos thread-safety

There is a possibility of cache and repeating old Authenticators. Although the timestamps should prevent it, the repetition can be made until the expiration time of the ticket. Servers are supposed to store all valid tickets in order to prevent repeating, but it is not always possible to do so. In addition, the lifetime of tickets can be quite long, and it is usually about 8 hours long. Authenticators rely on the fact that all the clocks in the network are more or less synchronized. If it is possible to trick the server in terms of the time, then the old Authenticator can be

repeated without any problems at all. Most network time protocols are unsafe, so this could be a serious problem. Kerberos is subject to password guessing attack. The intruder can obtain tickets and then try to decrypt them. It is known that the average user usually does not choose good passwords. If the intruder has collected enough tickets, he has a good chance to find out the password. Probably, the most serious attack is the one involving malicious software. Kerberos protocols rely on the fact that the programs are reliable. Kerberos improvements are being worked on, including the implementation of public key cryptography and application of smart cards for key management. Kerberos version 4 used symmetrical DES encryption system which wasn't reliable and it is replaced with the 3DES system, and in Kerberos version 5, AES system is commonly used because it is more reliable.

3.6 Neuman – Stubblebine

Due to system errors or diversions, clocks can become unsynchronized. If this happens, it is possible to attack the majority of these protocols. If the sender's clock isn't synchronized within configured limits with the receiver's clock, the intruder can intercept the sender's message and repeat it later, when timestamp matches the current time on the computer of the receiver. This attack is called suppress-replay attack and it can have serious consequences. This protocol tries to repel suppress-replay attack but it is subject to type attack [7] by replacing keys with random numbers. There is a possibility of parallel attack, too. [8]

3.7 Denning-Sacco

This protocol uses timestamps and public key signatures. It is a modified version of Needham - Schroeder protocol with symmetric key. In Denning Protocol, timestamps are applied instead of random numbers in order to eliminate the risk of freshness attack, which was a problem in the Needham - Schroeder protocol. Timestamps entail a problem of clock synchronization. There is a possibility of parallel attack on this protocol. In the original protocol, the receiver has no way to verify if he really receives a message from the sender. The intruder is thus enabled to start a parallel session and send to the receiver an intercepted message from the sender-receiver communication. Lowe is in his work provide a solution to this problem. [9]

3.8 Woo-Lam

This protocol uses public keys, random numbers and signatures. It can be attacked by parallel attacks. The attack is carried out in a way that an intruder presents himself to the receiver as being the server, and convinces him to continue communicating. As an answer to this threat it is necessary to take certain measures, such as: each message should contain session number, accept the session only if the last message session has passed. All these measures taken do not mean that we have eliminated the possibility of other attacks. Another type of attack that is possible, on this protocol, is type attack. An intruder, using an incorrect message, can get the session key. The only way to prevent this is to analyze all the messages and reject those that do not match the characteristics of the protocol. [10]

4. COMPARATIVE PROTOCOLS' ANALYSIS

From the Table 1 we can see that most of the steps are performed in Woo-Lam Protocol. All the protocols, with the exception of Wide - Mouth Frog, use the services of KDC (Key Distribution Center). An equal number of protocols use random numbers, which are used only once, and timestamps, in order to prevent a replay attack. Only Neuman-Strubbine uses both. Only Otway- Rees uses indexes. Most protocols are with symmetric keys. The protocols with asymmetric keys use signature as additional way of protection.

Table 1. Protocols' properties

	Number of steps	Keys control	Random number	timestamp	Index	Symmetric keys	Asymmetric keys	Signature
Wide - Mouth Frog	2	sender		x		x		
Yahalom	5	server	X			x		
Needham-Schroeder	6	server	X			x	x	
Otway-Rees	5	server	X		x	x		
Kerberos	4	server		x		x		
Neuman-Stubblebine	5	server	X	x		x		
Denning-Sacco	4	server		x			x	x
Woo-Lam	8	server	x				x	x

The Table 2 shows that all the protocols are the most subject to parallel attacks, and the least to freshness attacks. Needham- Schroeder and Otway- Rees protocols are the most subject to a number of different attacks whereas Kerberos is the least subject to any. The table

shows that there is no a completely safe protocol. There is always a possibility of an attack.

Table 2. Protocols' attacks addressed in the literature

	Freshness	Man-in-the middle	Type	Replay	Parallel
Wide - Mouth Frog		[13]		[6],[15]	
Yahalom			[17]	[19]	[1]
Needham-Schroeder	[11]	[17]		[9], [17]	[9]
Otway- Rees		[16]	[10],[11]	[23]	[24]
Kerberos				[22]	
Neuman-Stubblebine		[18]	[19]		[20]
Denning-Sacco	[21]				[15]
Woo-Lam			[10]		[14]

5. CONCLUSION

The disadvantage with Wide-Mouthed Frog protocol is that the sender devises a session key. This protocol is subject to replay attack. Another flaw is the absence of authentication during random numbers exchange. The good side of this Protocol is its simplicity. Yahalom protocol's main flaw is the possibility to run parallel sessions. Furthermore, all the systems that use the services of KDC are subject to possible attacks on the system whether the attack aims to get the passwords or to prevent communication with KDC, which disables the entire system. In Needham-Schroeder protocol we have a problem with the old session keys and the possibility of starting attack through them. This protocol is subject to "man in the middle" attack. There is a version of this protocol with a public key, which has solved this type of problem. In the Otway-Rees protocol an intruder can communicate both, with the sender and receiver, by using two different session keys. The problem with the old keys appears as well. Kerberos could be attacked in the cases of user's mistake or by taking weak passwords. Furthermore, in this protocol there is a problem with clocks synchronization, as with all other protocols that rely on timestamps. Kerberos version 4 used symmetrical DES encryption system that was not reliable and it is replaced by somewhat better 3DES system, but version 5 with AES system is considered to be more reliable. Another protocol that relies on timestamps, which is possibly its main flaw, is Neuman - Stubblebine protocol. This protocol is subject to replay and "man in the middle" attacks. Attack on Denning-Sacco protocol is possible if

the attacker presents himself as being the sender and sends his session key to the receiver. The problem with Woo-Lam Protocol is a possibility for an attacker to run parallel sessions. BAN Logic program is used for Cryptographic Protocols Analysis and detecting their flaws. The problem of establishing secure session keys between pairs of computers (and people) on the network is so significant that it prompted a very extensive research towards the development of new and debugging the old protocols.

REFERENCES

- [1] M. Burrows, M. Abadi, and R. M. Needham. A logic of authentication. Proceedings of the Royal Society of London, 426:233–271, 1989.
- [2] Aditya Bagchi, Vijayalakshmi Atluri, Information Systems Security: Second International Conference, ICISS 2006, st.196.
- [3] Pieter Ceelen, Sjouke Mauw, Sasa Radomirovi. Chosen-name Attacks: An Overlooked Class of Type-flaw Attacks. Université du Luxembourg Faculté des Sciences, de la Technologie et de la Communication
- [4] James Heather, Gavin Lowe, and Steve Schneider. How to prevent type flaw attacks on security protocols. J. Comput. Secur., 11(2):217–244, 2003.
- [5] Frédéric Massicot, Man-in-the-middle attack against the initiator of Otway-Rees Key Exchange Protocol, SANS Institute, 2000.
- [6] J. Clark, Attacking Authentication Protocols, 1996
- [7] Graham J. Steel, Discovering Attacks on Security Protocols by Refuting Incorrect Inductive Conjectures, University of Edinburgh, 2003., 101 st.
- [8] Gavin Lowe, Some New Attacks upon Security Protocols, Oxford University Computing Laboratory, Wolfson Building, October 1, 1996
- [9] G. Lowe, "A family of attacks upon authentication protocols," Department of Mathematics and Computer Science, University of Leicester, Leicester, 1997.
- [10] James Heather, Gavin Lowe, Steve Schneider, How to Prevent Type Flaw Attacks on Security Protocols
- [11] Graham J. Steel, Discovering Attacks on Security Protocols by Refuting Incorrect Inductive Conjectures
- [12] Jeremy BRUN-NOUVION, Hicham HOSSAYNI, Security models, 1st Semester 2010/2011
- [13] John Kelsey, Bruce Schneier, David Wagner, Protocol Interactions and the Chosen Protocol Attack, U.C. Berkeley, 2005
- [14] Anca Jurcut, Tom Coffey, Reiner Dojen, Robert Gyrodi, Security Protocol Design: A Case Study Using Key Distribution Protocols, Department of Electronic & Computer Engineering, University of Limerick, Ireland.
- [15] Reiner Dojen, Anca Jurcut, Tom Coffey, Cornelia Györfi: On Establishing and Fixing a Parallel Session Attack in a Security Protocol. Intelligent Distributed Computing, Systems and Applications. Springer Berlin / Heidelberg, Vol. 162, pp. 239-244, September 2008.
- [16] M. Panti L. Spalazzi S. Taoni, Attacks on Cryptographic Protocols: A Survey, Istituto di Informatica, University of Ancona
- [17] G. Lowe, A Family of Attacks upon Authentication Protocols, Technical Report, Department of Mathematics and Computer Science, University of Leicester, 1997.
- [18] Frederic Massicot, Man in the middle attack against security protocol, SANS Institute Ottawa, 2002
- [19] Alexander Marsalek, A review of attacks found and fixed, University of Technology Graz, Institute for Applied Information Processing and Communications, Graz, Austria
- [20] Lowe, Gavin, "An attack on the Needham-Schroeder public key authentication protocol." Information Processing Letters, November 1995
- [21] Paul Syverson, A Taxonomy of Replay Attacks, Naval Research Laboratory Washington,
- [22] Tzonelih Hwang, Narn-Yih Lee, Chuan-Ming Li, Ming-Yung Ko, Yung-Hsiang Chen, Two attacks on Neuman—Stubblebine authentication protocols, Institute of Information Engineering, National Chen-Kung University, Tainan, Taiwan, 1993
- [23] Gavin Lowe. A family of attacks upon authentication protocols. Technical Report 1997
- [24] Gagan Dua, Nitin Gautam, Dharmendar Sharma, Ankit Arora, Replay attack prevention in kerberos authentication protocol using triple password, Department of Computer Engineering, National Institute of Technology, Kurukshetra, India, 2013
- [25] Lambert M. Surhone, Mariam T. Tennoe, Susan F. Henssonow, Otway-Rees Protocol: Computer Network, Authentication, Communications Protocol, Internet, Replay Attack, Eavesdropping, Security Protocol Notation, Cryptographic Nonce, Tapa blanda – 16 sep 2010
- [26] Horea Oros, Florian Boian, Spi Calculus Analysis of Otway-Rees Protocol, Int. J. of Computers, Communications & Control, ISSN 1841-9836, E-ISSN 1841-9844 Vol. III (2008), Suppl. issue: Proceedings of ICCCC 2008, pp. 427-432

MODERN BUSINESS ENVIRONMENT: INFORMATION TECHNOLOGY AS A SHIELD AGAINST CYBER SECURITY THREATS

NENAD BIGA

Graduate School of Business, La Salle University (Philadelphia, United States), and JPMorgan Chase & Co. (New York, United States), nenad.bigajpmchase.com

MILOŠ JOVANOVIĆ

Business School, Middlesex University London (London, United Kingdom), Faculty of Organizational Sciences, University of Belgrade (Belgrade, Serbia), Faculty of Informatics and Computing, Singidunum University (Belgrade, Serbia), and OpenLink Group (Belgrade, Serbia), mjovanovic@openlink.rs

MARIJA PERKOVIĆ

Royal Holloway, University of London (London, United Kingdom), Faculty of Philosophy, University of Belgrade (Belgrade, Serbia), and OpenLink Group (Belgrade, Serbia), mperkovic@openlink.rs

DRAGAN MITIĆ

Faculty of Information Technologies, Metropolitan University (Niš/Belgrade, Serbia), and OpenLink Group (Belgrade, Serbia), dmitic@openlink.rs

Abstract: *The impact of information and communication technologies on modern business is undeniable. While it is a source of unlimited number of opportunities for progress, it also comes with some disadvantages. Security problems have been in focus for the past ten years, and for sure will be in the future too. Unfortunately, current situation is not very bright as there are still many undiscovered areas and preventive measures are far from being sufficient. This paper present the biggest challenges in cyber security.*

Keywords: *modern business, information technology, cyber security, vulnerabilities*

1. INTRODUCTION

In the early 1990s numerous authors and practitioners forsee extensive changes which were going to happen due to technology development [1], [2]. The expectations were that the change would exert its influence at the level of business processes [2]. It was evident that redesign of business processes was inevitable and it was welcomed in the academic circles [2].

There is still lack of sufficient understanding how technology and mainly computers change the business world. People wrongly assume that it is all about speeding up the processes, without realizing that the change is not quantitative, but qualitative as well. A rather different way to view this problem is to see companies and markets as information processors [3]. Without technological advances, information processing was slow, costly, and at times impossible. Investments in IT structure contributed to reductions in costs which were so significant that they influenced restructuring of the economy [3].

Technology did not influence just the business sphere, but its progressive nature posed some challenges for its own development. The exponential expansion of the internet made it harder to keep the technology relevant and useful. Another problem is the increase in number of security

issues related to IT structure management [4]. Governemnts teamed up with companies in order to protect informaton and a great number of cyber laws has been enacted [4]. However, the problem still remains and it is more relevant than ever. This paper will assess the importance of data and information security in the modern business world and it will also tackle the general importance of technology (especially cloud technology) regarding security issues.

2. CYBER ATTACKS: A SNAPSHOT

Trends in 2015

As cyber attacks are part of the modern business everyday reality, a huge amount of reports can be found covering this problem. According to several different resources, this year has been fruitful when it comes to cyber attacks ranging from data breaches to digital extortion [5]. Symantec Corporation, a company which has built its business on researching and tracking problems regarding IT security reported that during 2015 there was over 1 million of cyber attacks each day [5].

Another piece of information which excellently paints the picture about current problems is that a new zero-day

vulnerability was uncovered each week during 2015. (Zero-day vulnerability is defined as a hole in software that is unknown to the vendor which is usually exploited by hackers.) The more concerning piece of information is that the number of uncovered zero-day vulnerabilities increased for 125% during the period from 2014 to 2015 [5].

Types of Data breaches and Occurrence Rates

A report published by State of California Department of Justice from January 2015 shows a detailed breakdown of the data breach statistics. The relevant results are presented in the Image 1.

	2012	2013	2014
Number of breaches reported ¹	131	167	187
Number of records affected ²	2.5 Million	18.5 Million	12.7 Million
Type of Breach³			
Physical Theft or Loss	27%	26%	19%
Malware & Hacking	45%	53%	60%
Misuse (Intentional)	10%	4%	5%
Errors (Unintentional)	18%	18%	16%
	100%	100%	100%
Industry Sectors⁴			
Retail	26%	26%	26%
Finance	22%	20%	16%
Health Care	15%	15%	17%
Professional Services	5%	8%	6%
Government	8%	7%	3%
Hospitality	2%	5%	4%
Education	8%	3%	4%
Other	14%	17%	24%
	100%	100%	100%

Image 1: Type of Breach and Breaches per Industry Sectors

It is observable that malware and hacking is most common, followed by physical theft or loss, unintentional loss, and intentional misuse [6]. Physical theft or loss was defined as “unencrypted data stored on laptop, thumb drive or other device removed from owner’s control” [6]. Malware and hacking was defined as “intentional unauthorized intrusions into computer systems containing data” [6]. Misuse was defined as “intentional abuse of access privileges by insider” [6]. Errors were defined as “anything unintentionally done or left undone that exposes data to unauthorized individuals” [6].

The classification was also made based on the industry sectors. As the table shows, the highest number of data breaches is in the retail, closely followed by finance and health care [6].

Current situation in Serbia

This negative trend affected companies in Serbia as well. In July 2016 several domestic newspapers reported an official announcement of the Police Department that more than 1 million EUR has been stolen during cyber attacks [7]. To the knowledge of the Police Department of Serbia, small and medium enterprises are usually chosen as targets. These attacks are rather simple, as intruders present themselves as companies with which a target company already has an established business connection. Legitimate messages with payment instructions are then altered and new IBAN number is sent to targeted companies. These scams are usually uncovered 3 to 6

days later which leaves plenty of time for the criminals to withdraw money from foreign accounts and delete all piece of evidence (such as false email, false website, etc.) [7].

Previously described attacks lack the sophistications of cyber attacks encountered in other countries. RHEA group listed three biggest cyber attacks in 2016 which show extremely high level of sophistication. These include a cyber attack on the Ukrainian power grid when 225 000 people were left without power [8]. The second mentioned attack is the one in which the Central Bank of Bangladesh was targeted and the losses amounted to USD 81 million, while USD 850 million couldn’t be processed [8]. The third highly sophisticated attack was directed towards payroll company ADP. The damage still hasn’t been estimated exactly, as hackers didn’t still money but payroll, tax and benefits information from nearly 640 000 companies among which is the US National Bank as well [8].

3. SECURITY AND SOFTWARE VULNERABILITIES AND CYBER CRIMES

Finding definitions of security and software vulnerabilities may be quite a challenge since it is assumed that everybody knows what it is. However, a blog run by one the giants of IT industry – Microsoft – draws attention to the need to define term security vulnerability in order to know how to fight related problems. The definition they offer is that “a security vulnerability is a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product” [9]. Importance of this problem and its consequences are better understood when they are expressed in numbers. According to the extensive primary research conducted by the Kaspersky Lab, security breaches are a common problem as 90% of the companies at some point experiences this type of trouble [10]. The estimation showed that small to medium enterprises, on average, incur costs of 38 000 USD due to security breaches, while large enterprises spend more than half a million dollars to cover the damage [10]. These numbers show direct costs of security breaches, but additional indirect costs exist as well. For small to medium enterprises indirect costs amount to 8 000 USD, while for large enterprises these are, on average, 69 000 USD [10]. The main sources of security breach-related costs for large enterprises are summarized in the Image 2, while the Image 3 shows the same type of information but for small to medium enterprises.

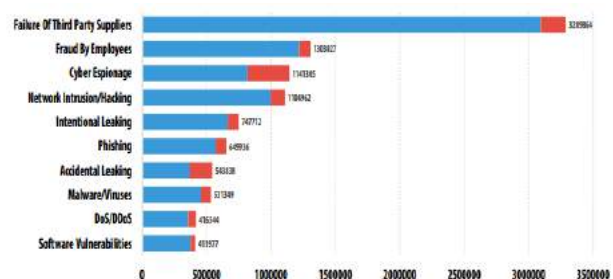


Image 2. Total impact of security incidents for large enterprises [10]

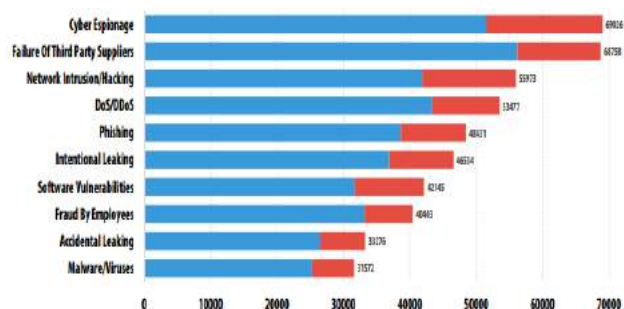


Image 3. Total impact of security incidents for small to medium enterprises [10]

When these numbers are viewed, it is understandable why security budgets are spiraling during the last few years. It is also relevant for this topic why the costs of security breaches are so high. Following is the list of the most serious and costly consequences which were outlined by managers [10]:

- Temporary loss of access to business critical information (50%)
- Loss of credibility/damage to company reputation (43%)
- Temporary loss of ability to trade (38%)
- Loss of contracts/ business opportunities in the future (30%)
- Costs associated with professional help to remedy loss (e.g. legal costs) (25%)
- Cost of additional software/infrastructure to prevent future problems (24%)
- Competitors obtaining previously confidential data (e.g. financial, strategic, IP) (20%)
- Financial losses caused by reimbursing/compensating clients (19%)
- Damage to credit rating (18%)
- Additional staffing/training costs (17%)
- Increased insurance premiums (13%)

Having in mind all of the previously outlined data, it comes as a surprise that there is almost no information about procedures which should be implemented once a software vulnerability is detected [11]. Same research gap is present in the area of detecting vulnerabilities [11]. Recently, there have been some advances in this field and security risk analysis models have been offered to the public [12]. We find it rather important to contribute to this topic by adding a short overview of significant software vulnerabilities which were discovered during the period from 2014 to 2015. Summary of the research results is presented in Table 1.

Once when vulnerabilities are spotted, they should be fixed before they are exploited by hackers. Steps which are undertaken can be labeled as preventive measures, which is exactly our last topic in this paper.

Table 1. Software vulnerabilities summary

CVE	Name	Discovered	Software	Use consequences
2014 - 0160	Heartbleed	2014	OpenSSL	Reading confidential data from system memory, downloading cryptographic keys
2014 - 6271	Shellshock	2014	Bash	Execution of arbitrary code, unauthorized access to the remote computer system
2014 - 3566	POODLE	2014	SSLv3	Decoding messages
2015 - 0235	GHOST	2015	glibc	Overtaking control over remote Linux system
2015 - 0204	FREAK	2015	SSL/TLS	Data theft using cryptanalyses based on intruding short RSA keys

4. PREVENTIVE MEASURES AGAINST CYBER ATTACKS

When it comes to prevention of cyber attacks, there are numerous methods, but none of them guarantees success. For example, one of the recent findings is a network security metric for measuring the risk of unknown vulnerabilities [13]. As this system is dealing with zero-day vulnerabilities, it does not provide any guidance on solving the actual problems, but according to authors, it does give a good basis for building knowledge about system's faults [13].

There are other methods which indeed predict exact files which may be source of vulnerability. An empirical study confirmed that CCD metrics are successful in making a distinction between vulnerable and non-vulnerable files [14]. In general, vulnerability inspection efforts are significantly decreased when code churn, developer

activity, and combined CCD metrics are applied at once [14].

Automatic testing is another tool which is available for predicting problems which may arise from software vulnerabilities. However, these tools are not used as often as they should be. The problem lies in the fact that prevention of software vulnerabilities related problems requires a lot of time and continuous effort and often the pace of work does not allow investing extra time.

5. CONCLUSION

The strong relationship between modern business entities and technology is undeniable. While it is a source of unlimited number of opportunities for progress, it also comes with some disadvantages. Security problems have been in focus for the past ten years, and as hackers are becoming more and more sophisticated, it seems that in the future academia and professional circles will be still trying to find ways to protect data and information.

Unfortunately, current situation is not very bright as there are still many undiscovered areas and preventive measures are far from being sufficient. The number of cyber attacks (which is constantly growing) confirms this statement. Apparently, future development in this area should take two roads simultaneously: developing more advanced software systems, but at the same time developing more sophisticated measures for protecting vendors and users in the first place.

REFERENCES

- [1]G. Smith, "Business process re-engineering: the use of process redesign and IT to transform corporate performance", *J Inf Technol*, vol. 8, no. 3, pp. 201-202, 1993.
- [2]V. Grover, "Information technology enabled business process redesign: An integrated planning framework", *Omega*, vol. 21, no. 4, pp. 433-447, 1993.
- [3]E. Brynjolfsson and L. Hitt, "Beyond Computation: Information Technology, Organizational Transformation and Business Performance", *Journal of Economic Perspectives*, vol. 14, no. 4, pp. 23-48, 2000.
- [4]H. Cavusoglu, B. Mishra and S. Raghunathan, "The Value of Intrusion Detection Systems in Information Technology Security Architecture", *Information Systems Research*, vol. 16, no. 1, pp. 28-46, 2005.
- [5] Symantec, "Symantec Cyber Attacks Report", *Resource.elq.symantec.com*, 2016. [Online]. Available: [https://resource.elq.symantec.com/LP=2899?inid=symc_threat-report_istr_to_leadgen_form_LP-](https://resource.elq.symantec.com/LP=2899?inid=symc_threat-report_istr_to_leadgen_form_LP-2899_ISTR21-report-main)
- [6] Oag.ca.gov, "State of California - Department of Justice - California Data Breach Statistics", *Oag.ca.gov*, 2016. [Online]. Available: <https://oag.ca.gov>. [Accessed: 08- Oct-2016].
- [7] Press Online, "MUP upozorava preduzeća na prevare preko interneta", *Press Online*, 2016. [Online]. Available: <http://www.pressonline.rs/info/hronika/377514/mup-upozorava-preduzeca-na-prevare-preko-interneta.html>. [Accessed: 10- Oct- 2016].
- [8] RHEA Group, "The three biggest cyber-attacks of 2016", *RHEA Group*, 2016. [Online]. Available: <http://www.rheagroup.com/three-biggest-cyber-attacks-2016/>. [Accessed: 10- Oct- 2016].
- [9]"Definition of a Security Vulnerability", *Msdn.microsoft.com*, 2016. [Online]. Available: <https://msdn.microsoft.com/en-us/library/cc751383.aspx>. [Accessed: 10- Oct-2016].
- [10] Kaspersky Lab, "Damage Control: The Cost Of Security Breaches", *Kaspersky Lab*, 2016.
- [11]M. Hafiz and M. Fang, "Game of detections: how are security vulnerabilities discovered in the wild?", *Empirical Software Engineering*, vol. 21, no. 5, pp. 1920-1959, 2015.
- [12]N. Feng, H. Wang and M. Li, "A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis", *Information Sciences*, vol. 256, pp. 57-73, 2014.
- [13]L. Wang, S. Jajodia, A. Singhal, P. Cheng and S. Noel, "k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities", *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 1, pp. 30-44, 2014.
- [14]Y. Shin, A. Meneely, L. Williams and J. Osborne, "Evaluating Complexity, Code Churn, and Developer Activity Metrics as Indicators of Software Vulnerabilities", *IEEE Transactions on Software Engineering*, vol. 37, no. 6, pp. 772-787, 2011.

CIP - Каталогизacija у публикацији -
Народна библиотека Србије, Београд

007:004.056.5(082)

659.23:004.056.5(082)

004.738(082)

INTERNATIONAL Conference on Business Information Security BISEC (8 ; 2016
; Beograd)

Proceedings / The Eighth International Conference on Business
Information Security BISEC, Belgrade, 15th October 2016. ; [editor Igor
Franc, Tanja Ćirić]. - Belgrade : Belgrade Metropolitan University, 2016
(Kruševac : Sigraf). - ilustr. - 108 str. ; 30 cm

Tiraž 100. - Napomene i bibliografske reference uz tekst. - Bibliografija
uz svaki rad.

ISBN 978-86-89755-10-7

a) Информациона технологија - Безбедност - Зборници b) Пословне
информације - Заштита - Зборници c) Електронски уређаји - Повезивање -
Интернет - Зборници
COBISS.SR-ID 226642700

