BELGRADE
METROPOLITAN
UNIVERSITY

BISEC

BUSINESS INFORMATION SECURITY CONFERENCE

Univerzitet Metropolitan Beograd
20. oktobar 2018.godine

www.bisec.metropolitan.ac.rs

PROCEEDINGS

The Tenth International Conference on Business Information Security

BISEC

INTERNATIONAL CONFERENCE ON
BUSINESS INFORMATION SECURITY

Belgrade Metropolitan University

Belgrade, 20th October 2018.

www.**metropolitan**.ac.rs

Publisher

Belgrade Metropolitan University
Tadeuša Košćuška 63, Belgrade, Serbia
http://www.metropolitan.ac.rs

For Publisher

Prof. Dr Dragan Domazet

Editor

Doc. Dr Igor Franc
MSc Bojana Trebinjac

Chair of Organizing Committee

Doc. Dr Igor Franc

Conference Secretariat:

MSc Bojana Trebinjac

Printing

Copy Planet Beograd

Design

Petar Cvetković

Year of publication

2019.

Circulation

60

CONTENT

Organizer

UNIVERZITET
METROPOLITAN
BEOGRAD

Co-Organizer

Математички
институт
САНУ

ESIGURNOST
INFORMATION
SECURITY

The 10th International Conference on Business Information Security (BISEC-2018), 20th October 2018, Belgrade, Serbia

DATA RELATIVITIES IN THE TRANSCENDING DIGITAL FUTURE

ZLATOGOR MINCHEV
Joint Training Simulation and Analysis Center, Institute of ICT,
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, zlatogor@bas.bg

Abstract: *Modern world is constantly evolving due to the new transcending digital reality influence, encompassing both human and technologies into a generically new intelligent and autonomous transhuman society. The future civilization digital unfolding is expected to give life-like characteristics to machines that will also create multiple uncertainties and relativities to the upcoming rich data handlings, concerning issues like: 'value', 'ownership', 'endurance', 'privacy' and 'security'. The paper studies the problem, establishing a system-of-systems transcending future modelling outlook and analytical assessment from data relativities' perspective. This assures a plausible view to the near future technological developments related to data dynamics. An experimental interactive validations is also provided, adding comprehensiveness to the presented findings.*

Keywords: *Data Relativities, Digital Future, Analytical Modelling, Experimental Validation*

1. INTRODUCTION

Digitalization has already transcend our future, giving the machines new, smart development outlook [1], [2]. The transhumanization idea [3] though quite arguable from the current ethical perspective is already getting support in the context of augmenting human capabilities from the present IoT & AI booming [4]. This however creates an innovative future influenced by the informational revolution that goes beyond our current imagination, mostly inspired through the previous industrial society, controlled by people that uses machines just as tools for human potential support [5]. The future world will also become rather pluralistic, parallelized, polyarchic, polycentric and difficult to accept from transformational and organizational points. In this new order of constantly evolving machine autonomization the biggest unknowns for the digital future are emerging from the new understandings towards the roles of humans and machines that are expected to become somewhat mixed and overlaid [6]. Such kind of an outspringing progress is naturally creating a competition that puts the human aspect of our society in conflict with the technological ones, generating new, advanced roles for the machines. The result of this upcoming transcending future is naturally setting up questions and disputes for: 'What makes us humans?', 'Aren't we just code with the same origin, like machines, but not that limited?' or 'Is our world just simulation directed from another level?' [7]. This gives the future AI designers unbelievable energy of ingenious innovations dreaming, which however are 'compromised-by-design' as their first-level creators are humans. So the 'singularity' idea [8] is somewhat fictional one because people and their programs are naturally implementing errors. Apart of this, the humans are not perfect enough as a rule and are getting motivation by emotions in their actions. So, we need certain evolution time for adequate adaptation and proper understanding or at least accepting the new transcending social outlook.

The rich sensors data arrays [9] stored in distributed huge databases [10] behind the modern digital transformation are having a mixed and heterogeneous origin of both human and machines, getting a relativistic nature that needs to be deeply explored. Presently, the privacy discussions and regulations are just the beginning of the problem [11], but luckily create a fruitful soil for surveying the digital future ecosystem transformation [12].
Further the paper is structured as follows: initially a system-of-systems analytical modelling of the data relativities digital effectiveness change is given in Section 2, followed by experimental results mixed (human-machines) smart validation in Section 3. Finally, some concluding remarks and future effects of digital transformation present acceptances and plausible future beliefs are outlined in the discussion part.

2. ANALYTICAL MODELLING

Deeper understanding of future data relativities trends could be obtained by probabilistic effectiveness assessment, implementing 'system-of-systems' modelling paradigm into a graph-based interpretation of the 'Entity – Relationship' representation, successfully realized in I–SCIP-EA software environment [13]. Here it should be noted that 'Entities' (marked with labelled round rectangles) actually encompass a set of objects or agents, having own properties and behaviour but capable to communicate with others via the multiple 'Relations' generalization (marked with bi-directional arrows). What need to be added also in this short description is the assessment of the model relations based on the Bayesian approach in accordance with a selected scenario objective. Both 'Risk' and 'Utility' are used for 'Effectiveness' assessment. The results are aggregated visually into a 'System Effectiveness Diagram' – 'SE Diagrams', providing a 3D entities' effectiveness visualization (noting 'Perpetual' vs 'Intermittent' entities' dual behaviour representation, graphically divided by the NW/SE diagonal plane), defining both active (white) and passive (grey) ones in each of the two subclasses), in accordance with the relations' probabilistic weights as follows: *Ef* – forward entities relationship effectiveness, *Eb* – backward entities relationship effectiveness, *Es* – resulting, generalized system effectiveness [11]. The present model creation was supported with some young researchers and expert data gathered from the working discussions among more than 350 participants from 17 nations throughout the world (including: Austria, Belgium, Bulgaria, Canada, Cyprus, Germany, Greece, Italy, Macedonia, Serbia, Spain, Sweden, Switzerland, Turkey, Ukraine, UK & USA) during: 'Future Digital Society Resilience in the New Digital Age' Joint Research & Industrial Expert Forum [14],'e-IRG Workshop' [15] and 'STO HFM-288 Research Workshop on Integrated Approach to Cyber Defence: Human in the Loop' [16].

The model results from Figure 1 (encompassing 10 entities and 24 bi-directional relations with the relevant SE Diagrams) for the present – year 2018 and future expectations towards year 2028, regarding the data relativities' plausible digital transformation could be summarized as follows:

2018:

Perpetual: active: 6 – 'Digital Transcends', 7 – 'E-Credentials', 10 – 'Smart Content'.

Intermittent: active: 1 – 'Human Factor', 2 – 'Mobile Data Sources', 3 – 'Storage Services', 4 – 'Legal Regulations'; passive: 5 – 'Data Compromising', 8 – 'Tech Singularity', 9 – 'Advanced Interfacing'.

2028:

Perpetual: active: 3 – 'Storage Services', 6 – 'Digital Transcends', 7 – 'E-Credentials'; passive: 9 – 'Advanced Interfacing', 10– 'Smart Content'.

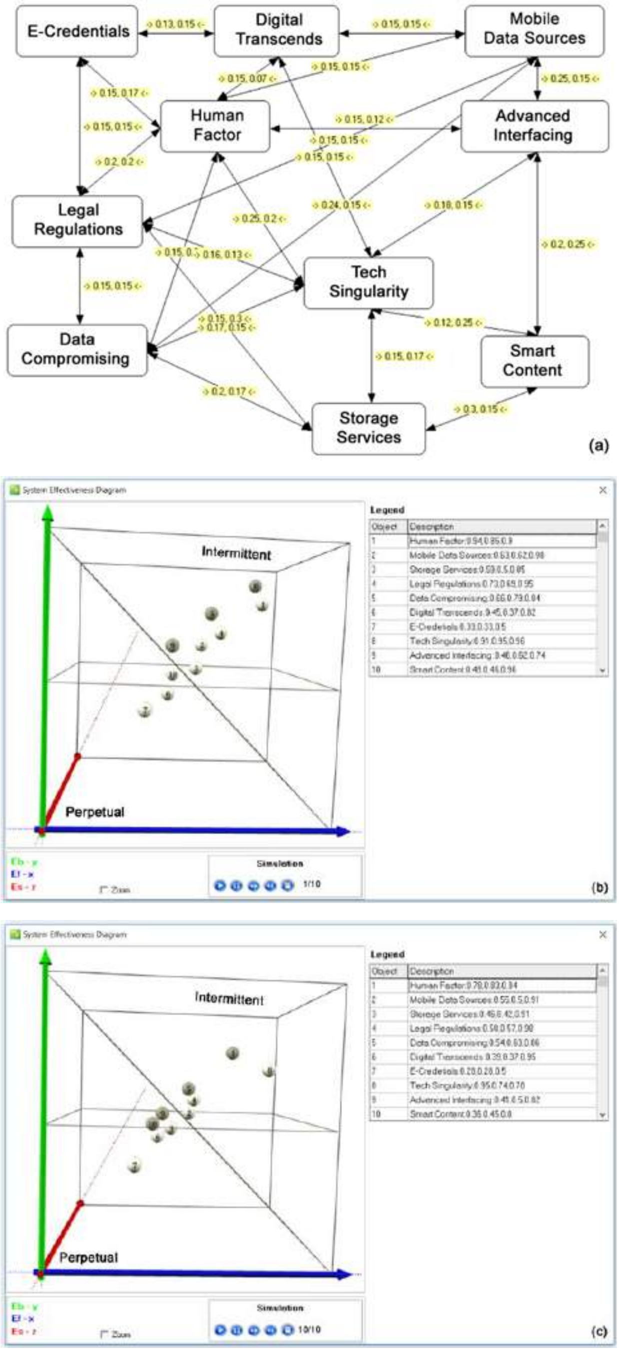
Intermittent: active: 2 – 'Mobile Data Sources', 4 – 'Legal Regulations', 8 – 'Tech Singularity'; passive: 1 – 'Human Factor', 5 – 'Data Compromising'.

The obtained results could be further explained in details (taking into account the perpetual scenarios parts for our digital society, influenced by climate change dynamics [17] expectations) around several key outlines and findings:

(i) Multiple rich data sources (mainly mobile sensor meshes, multimedia, biometrics, unstructured & semistructured messages, advanced social activities, etc.) accuracy, dynamics and data digital life endurance will continue to grow and are going to embed smart generating, processing, searching and connectivity;

(ii) The expected plausible technological progress will give a new impulse towards the technological singularity vs human ones, creating new ultra- speed and scale, highly distributed storage services for the smart digital context generated from (i). This however will also create and uncertain data booming with new social dynamics, originating from the human factor natural subjective striving to control and dominate over the newly transformed mixed world;

(iii) The near future will also establish and innovative e-credentials (personal, working and ad-hoc established, e.g. the 'virtual avatars' or 'virtual wallets' in the digital space) understanding with more flexible regulations, related to an intuitive human-machine and machine-to-machine advanced (multi biometric & smart protocol) interfacing and communication.



Legend

Object	Description
1	Human Factor:0.94,0.95,0.9
2	Mobile Data Sources:0.63,0.62,0.98
3	Storage Services:0.59,0.5,0.85
4	Legal Regulations:0.73,0.69,0.95
5	Data Compromising:0.66,0.79,0.84
6	Digital Transcends:0.45,0.37,0.82
7	E-Credentials:0.33,0.33,0.5
8	Tech Singularity:0.91,0.95,0.96
9	Advanced Interfacing:0.46,0.62,0.74
10	Smart Content:0.48,0.46,0.96

Legend

Object	Description
1	Human Factor:0.79,0.93,0.34
2	Mobile Data Sources:0.55,0.5,0.91
3	Storage Services:0.46,0.42,0.91
4	Legal Regulations:0.58,0.57,0.98
5	Data Compromising:0.54,0.63,0.86
6	Digital Transcends:0.39,0.37,0.95
7	E-Credentials:0.28,0.28,0.5
8	Tech Singularity:0.95,0.74,0.78
9	Advanced Interfacing:0.45,0.5,0.82
10	Smart Content:0.36,0.45,0.8

Figure 1: Data relativities dynamics modelling (a) and effectiveness assessment results, concerning technological progress scenario for the current (2018 – (b)) and future (2028 – (c)) time horizon

The future e-credentials will transcend the human factor role in the newly established modern world from both positive and negative perspectives, giving augmented capabilities for parallel work and producing also cognitive disambiguates;

(iv) This new, transcending digital world will however stay also security uncertain, concerning the upcoming technological developments due to its rather complex nature, scale and errors presence both with machine and human nature. The, future smart malware solutions, attacks and data breaches will emerge from the mixed digital environment, addressing both humans and machines. The phenomenon is expected to be a natural effect of the early transhumanization objective accomplishment, related to technological experimental implantations, tattoos, autonomous AI & IoT developments with multiplatform integrations;

(v) All these digital transformations will finally establish a rather relativistic mixed data environment with arguable dynamic stability, where it is going to be difficult to define clear certain digital personalities' ownership and engagements between human and machines from nowadays perspective.

Being plausible by nature, the presented expert results generalizations for the near future (up to year 2028) digital transformations from data perspective were further empirically validated, implementing futuristic experimental environment with user response multilayered monitoring.

3. EMPIRICAL VALIDATION

Experiment Setting Up

The validation of the accomplished analytical modelling findings (see Section 2) was further conducted empirically, implementing a transformed reality interactive simulation, organized in the framework of CYREX 2018 [18].
Using a fictitious scenario events script, played (for about 180 minutes) from the trainees in several multirole teams, an exploration of digital transformation plausible future data relativities dynamics was performed.
The scenario architecture included four key attack vectors (social engineering, industrial espionage, malware & targeted attacks) and seven main teams, organized as follows: a start-up company – 'Digital Creativity', developing a payment solution, based on human capabilities digital copying. The innovative results are bought from a larger corporation – 'Moon Digital Solutions', which has some invading plans on the 'New Life' planet colony. A hacker group 'Stellar Ghost' is also involved, modifying the 'Digital Creativity' work, swapping the data with aggressive dictatorship and fighting skills for the robots at 'New Life'. Other exercise participants were: 'Galactic World' – an intergalactic association responsible for digital techs regulation, using another small company – 'QHR Selection' to interfere in the situation and stop the hackers' terrorist plans, giving the 'New Life' colony robots fast food skills instead of aggressive ones. Finally, a PR body – 'Stellar Media' is involved for assuring public announcements of the situational dynamics. The participants used several device types: phablets, tablets, desktop and mobile computers, numerous open cloud services (data storage and sharing, encryption, chats, social media, multimedia messaging, e-mail accounting and participants DLP multi asset configurable monitoring) some accessed directly or with encrypted QR codes. The exercise was mainly organized in a closed Facebook social network group, partially implementing also WhatsApp & Viber, while participants' network access to the used cloud services was organized via a VPN. The players' behaviour was explored and archived remotely, using response time monitoring, video recording (similar to CYREX 2017 [11]) and COTS DLP solution CoSoSys My Endpoint Protector, v. 4.7.4.7 [19]. The DLP environment is capable to control 'Data-in-Motion' and 'Data-in-Rest' types of data. Based on client-server architecture the environment is providing client agents, installed on the users' endpoint devices, archived in a remote server. These agents are practically capable to control all the communication channels used in the exercise. The accomplished DLP solution is able to detect the content of the data and to compare it with preliminary defined keyword dictionaries, distinguishing sensitive data, whilst coping multiple I/O interface devices and allowing ad-hoc security policy definitions. The implemented users' monitoring approach provided an opportunity for deeper trainees' analysis, concerning their cognitive and behavioural responses.

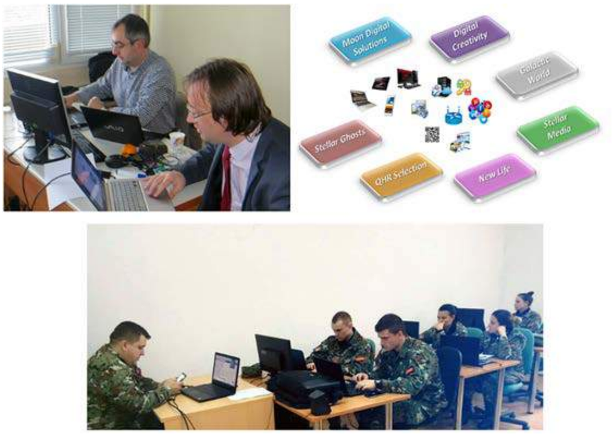


Figure 2: Moments and architecture of CYREX 2018, exploring data relativities digital transcending [18]

Results Assessment

Having empirical nature, the accomplished framework of CYREX 2018 was quantitatively assessed (see Figure 3) from the participants (using trained teams inputs of both 'Positive' and 'Indefinite' indicators' percentage measures and the ideas marked in [11]), regarding five key parameters: 'Environment Adequacy', 'Scenario Complexity', 'Technological Effects', 'Human Factor Effects' & 'Training Satisfaction'. Additionally, DLP monitoring data log leakages aggregated and normalized results distribution is also given, regarding seven of the exercise monitored attacks: 'Unauthorized Devices Connection', 'Targeted Attacks', 'Marked Key Words', 'Malware', 'Delayed Responses', 'Social Engineering' and 'Equipment Fails'. The obtained validation results are addressing obvious successful understanding for CYREX 2018, compared to CYREX 2017 [11], giving only a diminished mark for the 'Human Factor Effects' asset (<< 70%) due to the hidden participants monitoring that was not preliminary announced. Similar is the situation with the data leaks results, using insiders for installing specific key words in the teams communication language, together with provoking unexpected equipment fails and DDoS targeted attacks that were however indirectly successful (<< 10%), providing (>> 20%) visible delays towards the scenario scripts and unauthorized equipment (USB sticks and other peripheral devices with storage functionality) usage. Being more visible the malware and social engineering attempts in CYREX 2018 were getting better visibility (>> 15%), providing successful coverage for the unnoticed data leaks.

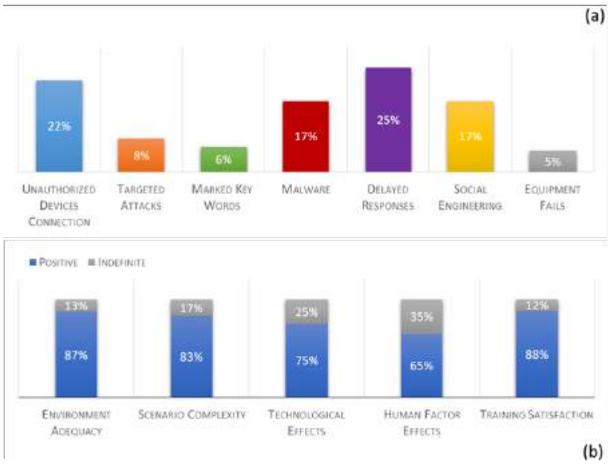


Figure 3: CYREX 2018 data leakage assets (a) and event aggregated assessment (b) results

4. DISCUSSION

The new age of digital transformation is shaping both humans and machines evolution, establishing an innovative but somewhat uncertain mixed social environment with numerous opportunities and adversaries. Proper analytical coping of this problem area evidently requires a multiaspect approaching that gathers expert, users and experimental interactive validations with the upcoming technological developments that though claiming to become smarter and miniaturized are still quite limited. Future data will become more fluid and relative than ever before, regarding the present ideas and understanding of ownership, endurance and privacy. What however stays unchanged is the natural human objective to dominate on the situation, being non-rationally but emotionally motivated and will provoke in the future conflicts, uncertainties and mistakes with the transhumanization and machines intelligent autonomization development plans. Evidently the machines and their software will become flooded with rich data sources, requiring fast and smart processing and functional response. This in fact is establishing a new transcending, highly dynamic, ultra- scaled & connected, largely distributed mixed environment. A fruitful soil that normally will grow new, unforeseen human-machine better interactions, producing at the same time smart data leakages, transcending security challenges and innovative knowledge extractions capabilities. This digital data transformation will establish and a conceptually different multiple data assets value that continuously grows, creating also a disruptive economic environment due to its relativistic nature. Most important in this rather uncertain digital future is the plausible adaptation and advanced resilience of the new human society that hopefully will create and cultivate different digital and cognitive skills for successful meeting the overlaid mixed environment transcending changes.

REFERENCES

[1] G. Wahlers (Ed), “The Digital Future, International Reports”, Konrad Adenauer Stiftung, no. 1, 2018, https://goo.gl/8CLcvn

[2] Secure Digital Future 21 Web Forum, http://securedfuture21.net

[3] Trippett, D. “What is Transhumanism and How Does It Affect You?”, April, 2018, https://goo.gl/Fnhbtb

[4] R. Sirius & J. Cornell, “Transcendence: The Disinformation Encyclopedia of Transhumanism and the Singularity”, Disinformation Books, 2015

[5] K. Schwab, “The Fourth Industrial Revolution: What It Means, How to Respond”, World Economic Forum, May 9, 2017, https://goo.gl/e1Kc3F

[6] M. Borders, “The Social Singularity: How Decentralization will Allow us to Transcend Politics, Create Global Prosperity, and Avoid the Robot Apocalypse”, Social Evolution, 2018

[7] G. Leonhard, “Technology vs. Humanity: The Coming Clash Between Man and Machine”, Fast Future Publishing, 2016

[8] M. Shanahan, “The Technological Singularity”, MIT Press, 2015

[9] The Complete Guide to Machine Learning for Sensors and Signal Data, Reality AI, 2018

[10] G. Drakos, “The New Era of Huge Data”, August, 2018, https://goo.gl/AKvLrN

[11] Z. Minchev, L. Boyanov, A. Georgiev, & A. Tsvetanov, “An Analytical Outlook towards Digital Training Security Transformations”, In Proc. of ICAICTSEE – 2017, UNWE, Sofia, Nov 3-4, 2017, https://dx.doi.org/10.13140/RG.2.2.20333.28645

[12] Z. Minchev, “Security Challenges to Digital Ecosystems Dynamic Transformation”, In Proc. of BISEC 2017, Belgrade, Serbia, 2017, pp. 6-10

[13] Z. Minchev, “Digital Security Future Objectives Foresight Modelling and Analytical Assessment”, Extended Abstracts from 12th Annual Meeting of BGSIAM, Sofia, December 20-22, 2017, pp. 76

[14] Joint Research & Industrial Expert Forum - Future Digital Society Resilience in the New Digital Age, http://it4sec.org/news/forum-future-digital-society-resilience-new-digital-age

[15] e-IRG Workshop Web Page, http://e-irg.eu/e-irg-workshop-may-2018

[16] STO HFM-288 Research Workshop on Integrated Approach to Cyber Defence: Human in the Loop, FB News Feed, https://goo.gl/HmUtbr

[17] A. Frank, J. Carroll-Nellenback, M. Alberti, & A. Kleidon, “The Anthropocene Generalized: Evolution of Exo-Civilizations and Their Planetary Feedback”, Astrobiology, vol. 18, no. 5, May, 2018, https://doi.org/10.1089/ast.2017.1671

[18] Cyber Research Exercise - CYREX 2018 Web Page, http://cleverstance.com/CYREX_2018/cyrex_2018.html

[19] CoSoSys My Endpoint Protector Web Page, www.endpointprotector.com

VIRTUAL ENTERPRISE DATA PROTECTION:

FRAMEWORK IMPLEMENTATION WITH PRACTICAL VALIDATION

IVAN GAIDARSKI
Joint Training Simulation and Analysis Center, Institute of ICT,
Bulgarian Academy of Sciences, i.gaidarski@isdip.bas.bg

ZLATOGOR MINCHEV
Joint Training Simulation and Analysis Center, Institute of ICT,
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, zlatogor@bas.bg

Abstract: *Modern data protection combines multilevel measures and compliances, implementing different regulations, standards and policies that become vital in the new digital world. The paper outlines component-based architecture framework for ISS of virtual organization and the data protection components, covering multiple data sources, states and roles. Other important aspect is the classification of the different types of data, their owner, the data users, the location of data, the direction it moves inside and outside of the system, the data protection methods and where exactly we should apply these methods. Further the presented idea is experimentally validated within interactive mixed environment simulation. Monitoring with access control of the exchanged data flows and used devices is also accomplished, using COTS DLP system. A concluding results discussion with enterprise data protection policies recommendations is finally presented.*

Keywords: *Enterprise Data Protection, Architecture Framework, Interactive Validation, DLP Systems, Data Protection Policies Recommendation*

1. INTRODUCTION

Today the information, owned by enterprises and organizations in general is their most important and valuable asset in the digital era.

This gives them competitive advantage and differentiates the market. Information ownership and handling are already the high octane fuel for the day-to-day operations and is prerequisite to the successful wholesale performance.

Information and data loss, leakage/bridge or unauthorized access can lead to serious damages for todays' organization, failure of competitive advantages, and even dropping out of the market.

Recently organizations from practically all sectors have become victims of attacks to their data and information [1]. These incidents cost millions and can cause collateral damages to brand and reputation of the organizations.

There are different types of data loss incidents, including theft of trade information, sales of customer details to external parties, loss of USB sticks, laptops or mobile devices. The majority of these incidents resulted from the actions of internal users or trusted third parties [2].

The field of security deals with the protection of assets. The following assets can be protected by Information Security Systems:

- Data Assets;
- Software Assets;
- Hardware Assets;
- Networking Assets.

The protection of information in all its forms is the main goal of Information Security. The best approach is to consider every asset and relationships between assets in the context of its associated risk for loss and value.

Information Security can be divided into different categories, depending on the protected asset:

- Data Protection;
- Infrastructure Protection;
- Software Protection;
- Hardware Protection;
- Network Protection.

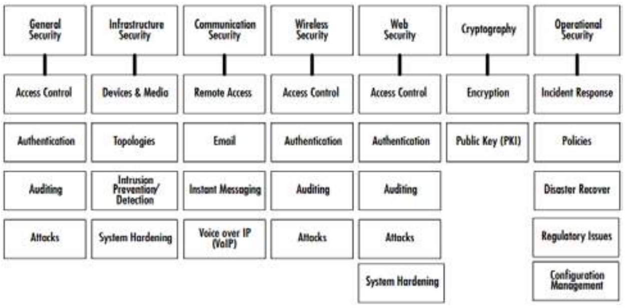


Figure1: Information Security categories

The main objective of Information Security System (ISS) is securing the information in the organization. It can combine different security controls – firewalls, IDS, IPS, DLP and others.

To protect the information, enterprises need also to establish information security policies that are supported by standards, procedures and guidelines.

Data Protection as part of Information Security System can be defined as technical and managerial controls and procedures for protection of the confidentiality and integrity of personal information [3].

The paper outlines component-based architecture framework for ISS of virtual enterprise organization and the data protection components, covering multiple data sources, states and roles.

Other important aspect is the classification of the different types of data, their owner, the data users, the location of data, the direction it moves inside and outside of the system, the data protection methods and where exactly we should apply these methods. Further the presented idea is experimentally validated within interactive mixed environment simulation. Monitoring with access control of the exchanged data flows and used devices is also accomplished, using COTS DLP system. A concluding results discussion with enterprise data protection policies recommendations is finally presented.

2. ARCHITECTURE FRAMEWORK FOR ISS

The traditional approaches for development of ISS do not realize a reference methodology for system implementation. In this paper, we present an approach for conceptual modelling of ISS, which is based on description of system's architecture. This solution gives us a possibility for achieving some important goals as: interoperability, reusability, easy deployment and scalability, producing as final results – reference templates for building ISS, according to the organization of interest specifics. The approach is based on the framework of architectural description of systems defined in the standards IEEE 1471[4] and IEEE 42010 [5].

According to the standards, the basic concepts that define the framework of architecture description of a system (see Figure 2) are:

- *Environment* – determined by all influences upon a system that are categorized as concerns. This is the base that contains all domains, in which the system is considered.
- *Viewpoint* – captures the conventions for constructing, interpreting and modelling a type of view that is in relation to a specific Model Kind.
- *View* – representation of the system from the perspective of a related set of concerns: each view corresponds to exactly one viewpoint and is addressed to identify system stakeholders and answers their identified concerns. A view is comprised of architecture models.
- *Stakeholders* – individuals, groups and organizations with interests to the system;
- *Concerns* – A concern space is formed from the union of all stakeholder concerns [6], [7].

To achieve effective data protection, we suggest a multi-layered conceptual model of ISS, organized around the viewpoints "Information Security" – first layer, and "Information Processing" – second layer.

The stakeholders related to the "Information Security" viewpoint are developers and integrators. Their concerns are conceptual integrity, deployment, scalability, reusability, structure and system properties. The "Information Processing" viewpoint focuses on information processing, semantic of information and relationships between information objects [21].

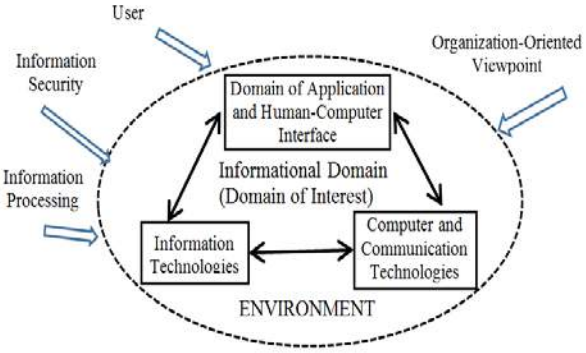

User
Information Security
Organization-Oriented Viewpoint
Information Processing
Domain of Application and Human-Computer Interface
Informational Domain (Domain of Interest)
Information Technologies
Computer and Communication Technologies
ENVIRONMENT

Figure 2: An architectural framework for ISS description

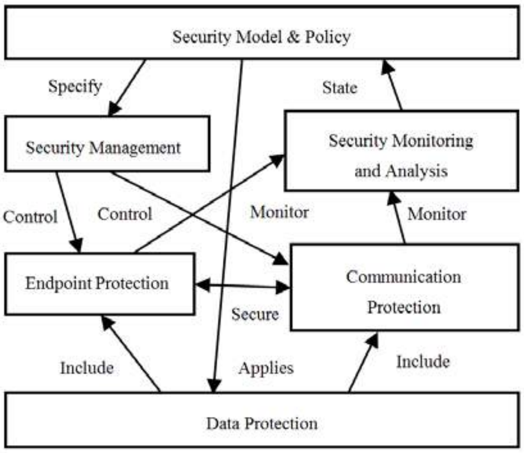


Figure 3: Meta-model of "Information Security" viewpoint

The main questions to the Information Security Systems are "What", "How" and "Why" to protect.

The suggested meta-model of "Information Security" consists of six components (Figure 3), each of them provides different functionalities [21]:

- *Endpoint Protection* ("What") defends the endpoints (any element of ISS with computational and communication capabilities) – identity, access control, cyber and physical security;
- *Communications Protection* ("What") protects the communication between the endpoints via authentication/authorization of the traffic, cryptographic and information flow control techniques;
- *Security Monitoring & Analysis* ("How") preserves the state of the system by monitoring and analyzing the other components of the system;
- *Security Management* ("How") controls the other components of the system;

- *Security Model & Policy* (“Why”) – implements the security policies and directs all other components to ensure the security of the data;
- *Data Protection* (“Why”) – The protection of the data in the system – the protected data, the system management data, the configuration data and the data collected as part of the monitoring and analysis function [18].

The second meta-model “Information Security” represents the three types of data states that result from the work of available systems and devices (Figure 4) [21]:

- *Data-at-Rest* – Inactive data, stored within the IT infrastructure or on media – databases, servers, intranet sites, workstations, laptops, mobile devices, portable storage, removable media, cloud storage.
- *Data-in-Use* – Active data that is being printed, copied, accessed or used by a system and processed in application.
- *Data-in-Motion* – Data transmitted by the networks or endpoints.

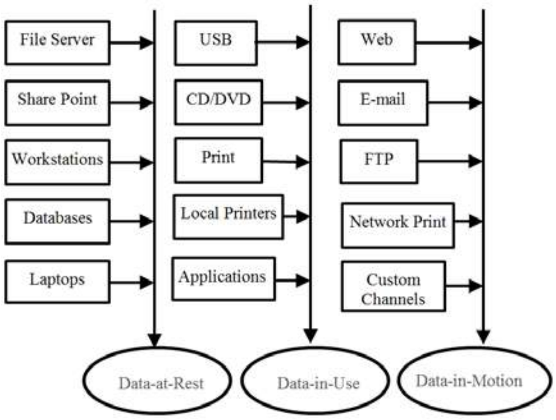


Figure 4: Meta-model of “Information Processing” viewpoint

In order to protect the specific types of data in a system, it is also necessary to implement specific Information Security Techniques (IST) in the basic components from the “Information Security” meta-model. The data have to be protected against loss, theft, unauthorized access and changes by applying IST such as confidentiality controls, integrity controls, access control, isolation and replication [2].

Figure 5 shows a multi-layered conceptual model of ISS, which contains the meta-models representing “Information Security”, “Information Processing” viewpoints and the relations between them:

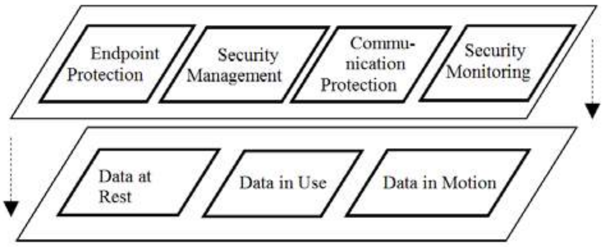


Figure 5: Two-Layered conceptual model of ISS

- *Endpoint Protection* component protects “Data-at-Rest” and “Data-in-Use” of the endpoints through relevant IST, as access control, passwords, antivirus, audit trails, physical security measures, etc.;
- *Communications Protection* component protects “Data-in-Motion”, using cryptographic techniques, network segmentation, perimeter protection, gateways, firewalls, intrusion detection, network access control, deep packet inspection and network log analysis;
- *Security Management* component protects all configuration, monitoring, and operational data, using cryptography.
- *Security Monitoring & Analysis* component is responsible for the protection of the data for current system state, the monitoring of key system parameters and indicators. The typical ISTs in this component are cryptographic techniques.

3. GOVERNANCE AND CLASSIFICATION OF THE PROTECTED DATA

To achieve effective data protection, it is necessary to classify the different types of data, their owner, the data users, the location of data, the direction it moves inside and outside of the system. It is also important to classify the different types of threats to the data, taking into account the risks associated with them, and the relevant techniques for reduction or neutralization of threats.

Some activities have also to be performed in order to identify the sensitive data for an organization, gaining understating “What” is the most important data, which must be protected, “Where” it resides and “Where” it is going.

The data is inevitable to be also classified and from a business perspective. There is no a universal description of what is the organization’s most important data. This depends on the specific type of activities it performs. There should be understanding about the specific types of data held by the organization and used in day-to-day operations. The vital data, which organization cannot afford to lose is the data that is required to be protected.

Very important is to consider the risk of leaking that data to unauthorized parties. The results can be severe for the organization – direct financial losses, business disruption, damage to reputation and brand, regulatory violations and fines [8].

The risk assessment of the organization’s sensitive data includes:

- The value of internal data;
- Whether the data is protected by regulations;
- Impact on brand and reputation;
- Loss of competitive advantage;
- Direct impact to business partners and customers.

After the data is identified, next step is to discover where exactly it resides within the IT infrastructure. It can be everywhere – databases, cloud, servers, workstations, mobile devices or flash drives. There are two high-level repositories to store the data:

***Structured repositories**:* The data is stored in databases. The strategies for identifying sensitive data in structured repositories include working with the business and IT staff and usage of interviews and questionnaires, business process walk-throughs, reviews of the organization's documentation – application descriptions and data flow diagrams.

***Unstructured repositories**:* The data is stored in less controlled repositories such as workstations, laptops, removable devices and network shares. They are usually chaotic and stored by end users without complying with any rules. The strategies for identifying the sensitive data include inquiry of business users and IT personnel, including provision of useful information about the data stores. Due to the nature of the unstructured data, the usage of special Data Discovery tools is needed. They perform scanning with the help of specially designed dictionaries and rules for detection of sensitive data. Data Discovery tools can identify sensitive data on:

- Network segments, undocumented shared drives, servers and databases;
- Network shares, databases with different levels of access privileges, intranet sites;
- User's workstations and laptops with sensitive data stored on local drives.

Providing complete view of the location of the sensitive data is not enough. The organization must be aware "Where" and "How" the data is transferred inside and outside the organization. Special monitoring tools can be used for complete picture of the data transfers.

Another important understanding is what sensitive data is accessible or exchanged with third parties. Controls have to be implemented to secure the third-party access, including:

- Secure data transmissions;
- Controlled access to company networks and data;
- Monitoring of third-party access to company resources;
- Third-party due diligence/information security assurance.

With the knowledge of the sensitive data, "How" are they used and by "Whom", Data Protection Policies have to be developed in the organization, in order to document all the security requirements.

The policies must comply with Data Protection Regulations, Standards and Policies, which concern that particular organization – ISO 27000 [9], [10], ISACA's COBIT [11], [12], NIST "800 series" [13], special sector-specific regulations – the Gramm-Leach-Bliley Act (GLBA) [14] for the financial sector, Sarbanes-Oxley Act (SOX) [15], [16] for US public companies, Health Insurance Portability and Accountability Act (HIPAA) [17] and Payment Security Industry (PCI) Data Security Standard (DSS) [18], the new 2018 EU General Data Protection Regulation (GDPR) [19].

4. DATA PROTECTION TOOLS AND THEIR DEPLOYMENT AS PART OF THE ISS

There are many traditional network- and infrastructure-centric security solutions for protection of the confidentiality, integrity and availability of the data: gateways, firewalls, cryptographic techniques, network segmentation, intrusion detection, network access control, deep packet inspection, network log analysis and many others. They are designed for protection, monitoring or control of the traditional outside-inside vectors of attack, but when it comes to protection of sensitive information, they are not enough. We need tools, which are capable on protecting the data from inside, which requires a new approach.

Such solutions, which leverage data-centric approach, are the Data Leak Protection (DLP) systems. They are designed to stop data leakages from inside to the outside, no matter it is intentional or unintentional, being a result of a human errors – Figure 6. DLP systems are capable on preventing the attempts to steal, modify, prohibit, destroy or obtain unauthorized access to the data, by detecting its content and enforce protective actions based on the value and level of importance.

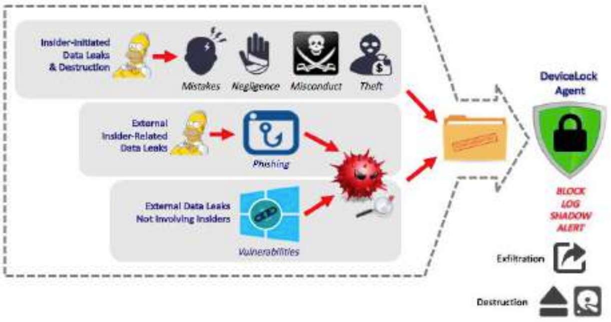


Figure 6: Prevented data breach types

One of the defining characteristic of DLP solutions is their ability to analyse the content and context of the data. DLP can analyse deep content using a variety of techniques, such as: rule-based/regular expression, database fingerprinting, exact file matching, partial document matching, statistical analysis, conceptual/lexicon and categories. The context analysis, include characteristics such as source, destination, size, recipients, sender, header information, metadata, time, format.

The main goal of DLP is to stop the data before it leaves protected environment of the organization, providing information for:

- Identification of the threats and vulnerabilities to the data;
- Violations of the security policies and procedures in the organization;
- Discovering and identifying the sensitive information in the organization.

One of the biggest advantages of the DLP systems is their ability to protect the data according to the behaviour of different users and to achieve compatibility with different security standards, internal rules and security policies.

DLP systems can be focused on servers, global communications and data channels of the organization.

They can control email communications and file transfers from file servers.

DLP also can protect endpoints and local data channels – workstations, laptops, mobile devices – tablets and phones. Controlled channels in this case include all possible physical ports, personal emails, file transfer to cloud services and more (Figure 7) [20].

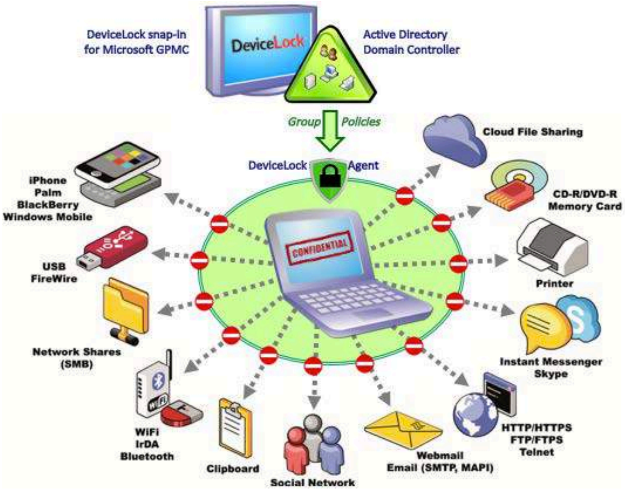


Figure 7: DeviceLock EndPoint DLP Suite – How it works

5. EMPIRICAL VALIDATION

The validation of the accomplished ISS conceptual modelling and DLP functionalities was further conducted empirically, implementing a transformed reality interactive simulation, organized in the framework of CYREX 2018, using the material from [23]. An implementation of a fictitious scenario events script, played (for about 180 minutes) from the trainees in several multirole teams, an exploration of digital transformation plausible future data relativities dynamics was performed.

The scenario architecture included four attacking vectors (social engineering, industrial espionage, malware & targeted attacks) and seven main teams, organized in the following scenario idea: a start-up company – "Digital Creativity", creating cloning human skills payment approach and a larger corporation – "Moon Digital Solutions", approaching the "New Life" planet colony. A hacker group "Stellar Ghost", modifying the "Digital Creativity" work. Other exercise participants were: "Galactic World" – a digital techs regulation association, using a smaller company – "QHR Selection" to stop "Stellar Ghost" terrorist plans, changing the invading data with fast food cooking skills for the "New Life" robots. Additional PR body – "Stellar Media" is also involved for giving publicity to the situational dynamics.

The participants' teams used several mobile device types with different open cloud services (data storage and sharing, encryption, chats, social media, multimedia messaging, e-mail accounting and participants DLP multi asset configurable monitoring) accessed directly or with encrypted QR codes. The exercise was mainly organized in a closed Facebook social network group, with WhatsApp & Viber elements, giving trainees network access via a VPN. The players' behaviour was explored and archived remotely, using response time monitoring, video recording (similar to [24]) and COTS DLP solution CoSoSys My Endpoint Protector, v. 4.7.4.7.

The DLP environment is capable to control "Data-in-Motion" and "Data-in-Rest" types of data. Based on client-server architecture the environment is providing client agents, installed on the users' endpoint devices, archived in a remote server. These agents are practically capable to control all the communication channels used in the exercise. They can intercept information from the corresponding data channel (USB, Bluetooth, I/O ports, Wi-Fi, LAN Network, etc.) and send it to the cloud, to control the relevant operations (read/write/copy) and to apply the adjusted policy to the endpoints. The DLP solution can control different users and endpoints, making possible to assign an IT security policy for the different users in the organization. The accomplished solution is also able to detect the content of the data and to compare it with preliminary defined keyword dictionaries, distinguishing sensitive data, whilst coping multiple I/O interface devices and allowing ad-hoc security policy definitions. With full control capabilities, the DLP solution can stop the leak of sensitive information, before it happens.

The implemented users' monitoring approach provided an opportunity for deeper trainees' analysis, concerning their cognitive and behavioural responses.

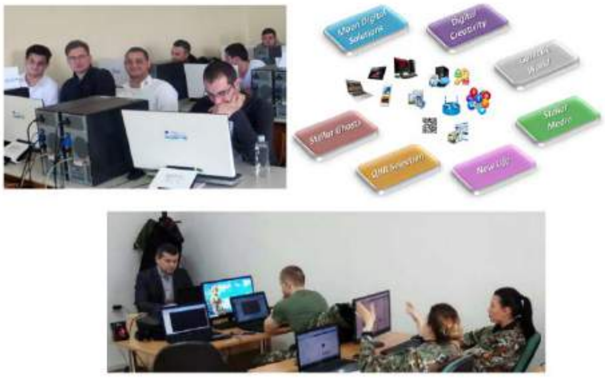


Figure 8: Moments and architecture of CYREX 2018, exploring data relativities digital transcending [22]

Results Assessment

Having empirical nature, CYREX 2018 framework was quantitatively assessed (see Figure 9), using trained participants inputs (both "Positive" and "Indefinite" indicators' percentage measures and the ideas marked in [24]), on five key parameters: "Environment Adequacy", "Scenario Complexity", "Technological Effects", "Human Factor Effects" & "Training Satisfaction". Additionally, DLP monitoring data log leakages aggregated and normalized results distribution is also given, concerning seven of the exercise monitored attack vectors: "Unauthorized Devices Connection", "Targeted Attacks", "Marked Key Words", "Malware", "Delayed Responses", "Social Engineering" and "Equipment Fails".

The obtained results are addressing some successful understanding for CYREX 2018, but giving a diminished mark (compared to CYREX 2017, [24]) for the "Human Factor Effects" asset (<< 70%) due to the hidden participants monitoring that was not preliminary announced. Similar is the situation with the data leaks results, using insiders for installing specific key words in the teams communication language, together with provoking unexpected equipment fails and DDoS targeted attacks that were however indirectly successful (<< 10%), providing (>> 20%) visible delays towards the scenario scripts and unauthorized equipment (USB sticks and other peripheral devices with storage functionality) usage. Being more visible the malware and social engineering attempts in CYREX 2018 were getting better visibility (>> 15%) providing successful coverage for the unnoticed data leaks.

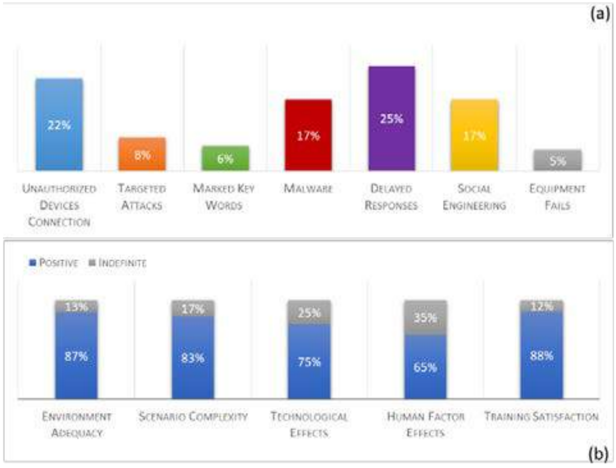


Figure 9: CYREX 2018 data leakage assets (a) and event aggregated assessment (b) results

6. CONCLUSION

In this paper is presented an architectural description of Information Security Systems (ISS) with some methods for conceptual modeling. The goal of architecture model construction is to ensure scalability, usability, interoperability, easy deployment and ease-of-use templates of ISS across organizations of different types and sectors of work. Using this approach allows us to achieve model independence when changing external or internal conditions.

As the data protection is one of the major components of ISS, we review specific data-centric protection tools, such as Data Leak Protection (DLP) systems and their experimental deployment as part of the ISS. One of the biggest advantages of the DLP systems is their capabilities to protect data according to the behavior of different users and to achieve compatibility with multiple security standards, internal rules and security policies. These hopefully will provide a more secure working services and environment in the new digital era.

7. ACKNOWLEDGEMENT

This study is partially supported by a research project grant “Modelling the Architecture of Information Security Systems in Organizations”, Ref. No: 72-00-40-230/10.05.2017, ICT Sciences & Technologies Panel, Program for Young Scientists and PhD Students Support – 2017, Bulgarian Academy of Sciences.

REFERENCES

[1] 2018 Data Breach Investigations Report, 11th Edition, Verizon, https://goo.gl/NtpXQ1

[2] M. Rhodes-Ousley, “Information Security – The Complete Reference”, 2nd Edition, The McGraw-Hill, 2013

[3] M. Whitman, & H. Mattord, “Principles of Information Security”, Fourth Edition. Course Technology, Cengage Learning, 2012

[4] IEEE Std 1471, IEEE Recommended Practice for Architectural Description of Software-Intensive Systems, 2000

[5] ISO/IEC/IEEE 42010:2011 - Systems and software engineering – Architecture description, https://www.iso.org

[6] R. Hilliard, “Aspects, Concerns, Subjects, Views”, In Proc. of OOPSLA’99 Workshop on Multi- Dimensional Separation of Concerns in Object-Oriented Systems, 1999

[7] R. Hilliard, “Viewpoint Modeling”, In Proc. of First ICSE Workshop on Describing Software Architecture with UML, Position paper, May, 2001

[8] Data Loss Prevention – Insights on Governance, Risk and Compliance, Ernst and Young, DLP conceptual model_EY_Data_Loss_Prevention.pdf

[9] J. Hintzbergen, & K. Hintzbergen, “Foundations of Information Security Based on ISO27001 and ISO27002”, Van Haren, 2010

[10] ISO 27001 Official Page, https://www.iso.org/isoiec-27001-information-security.html

[11] COBIT Security Baseline: An Information Survival Kit, 2nd ed. IT Governance Institute, 2007

[12] COBIT resources, http://www.isaca.org/COBIT/Pages/default.aspx

[13] NIST Special Publications (800 Series), http://www.csrc.nist.gov/publications/PubsSPs.html

[14] Gramm-Leach-Bliley Act (GLBA) resources: https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

[15] S. Anand, “Sarbanes-Oxley Guide for Finance and Information Technology Professionals”, Wiley, 2006

[16] Sarbanes-Oxley Act, https://www.sec.gov/about/laws/soa2002.pdf

[17] K. Beaver, & R. Herold, “The Practical Guide to HIPAA Privacy and Security Compliance”, 2nd ed, Auerbach, 2011

[18] PCI Security Standards, https://www.pcisecuritystandards.org/pci_security/

[19] EU General Data Protection Regulation Official Page, http://ec.europa.eu/justice/data-protection/reform/index_en.htm

[20] DeviceLock, www.devicelock.com/products/

[21] I., Gaydarski, & Z. Minchev, “Conceptual Modeling of Information Security System and Its Validation Through DLP Systems”, In. Proc. of BISEC 2017, Belgrade Metropolitan University, 2017, pp. 36-40

[22] Cososys Endpoint Protector, www.endpointprotector.com

[23] Z. Minchev, “Data Relativities in the Transcending Digital Future”, Keynote Paper, In Proc. of BISEC 2018, Belgrade Metropolitan University, 2018.

[24] Z. Minchev, L. Boyanov, A. Georgiev, A., Tsvetanov, “An Analytical Outlook towards Digital Training Security Transformations”, In Proc. of ICAICTSEE – 2017, UNWE, Nov 3-4, Sofia, Bulgaria, 2017, https://dx.doi.org/10.13140/RG.2.2.20333.28645

BIOMETRIC CRYPTOSYSTEMS – APPROACHES TO BIOMETRIC KEY-BINDING AND KEY-GENERATION

NEMANJA MAČEK
School of Electrical and Computer Engineering of Applied Studies, Belgrade; Graduate School of Computer Sciences, Megatrend University, Belgrade; SECIT Security Consulting; macek.nemanja@gmail.com

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

MILAN GNJATOVIĆ
University of Novi Sad, Faculty of Technical Sciences; milangnjatovic@uns.ac.rs

BRANIMIR TRENKIĆ
School of Electrical and Computer Engineering of Applied Studies, Belgrade; btrenkic@viser.edu.rs

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

ACA ALEKSIĆ
Belgrade Metropolitan University, Faculty of Information Technologies; aca.aleksic@metropolitan.ac.rs

Abstract: *Biometric cryptosystems are emerging technology that allow user to generate or unlock cryptographic key using biometric data, such as iris or fingerprint. In other words, biometric cryptosystems provide mechanisms for biometric-dependent key-release. A comprehensive survey of biometric cryptosystems is presented in this paper, i.e. state of the art approaches, such as fuzzy commitment, fuzzy vault are reviewed and discussed. Finally, a brief discussion of biometric cryptosystems security is given as a concluding remark to this paper.*

Keywords: *Biometry, Cryptosystems, Key Binding, Key Generation*

1. INTRODUCTION

Biometric cryptosystems require the storage of public information that is dependent on biometrics. This information is applied to retrieve or generate keys, which is referred to as helper data [1]. Due to biometric variance (see Image 1) it is not feasible to extract keys from biometric characteristics directly.

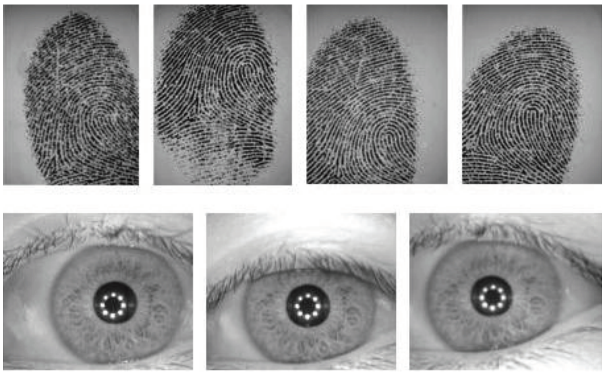


Image 1: Biometric invariance (samples originating from FCV and CASIA databases)

Helper data, which does not reveal significant information about original biometric templates is therefore used to reconstruct cryptographic keys. Biometric comparisons are performed indirectly by verifying key validities, where the output of an authentication process is either a key or a message about failure. Since the verification of keys represents a biometric comparison in encrypted domain [2], biometric cryptosystems are applied as a means of biometric template protection, in addition to providing biometric-dependent keyrelease.

Within biometric cryptosystems acceptance requires the generation or retrieval of hundred percent correct keys, while conventional biometric systems response with “Yes” or “No”.

In addition, the majority of biometric cryptosystems introduce a higher degree of quantization at feature extraction, compared to conventional biometric systems, which are capable of setting more precise thresholds to adjust recognition rates.

There are two types of biometric cryptosystems, depending on how helper data are derived: key-binding systems and key-generation systems. More detailed information on those are given in sections 2 and 3 of this paper.

2. KEY-BINDING SYSTEMS

In key-binding systems, helper data are obtained by binding a chosen key to a biometric template. As a result of the binding process a fusion of the secret key and the biometric template is stored as helper data. Applying an appropriate key retrieval algorithm, keys are obtained from the helper data at authentication [3]. Since cryptographic keys are independent of biometric features these are revocable while an update of the key usually requires re-enrolment in order to generate new helper data.

Several approaches to biometric key-binding will be briefly discussed in this paper: Mytec1 and Mytec2, fuzzy commitment scheme and fuzzy vault.

The first sophisticated approach to biometric key-binding based on fingerprints was proposed in [4-6]. The presented system was called Mytec2, a successor of Mytec1 [7], which was the first biometric cryptosystem but turned out to be impractical in terms of accuracy and security. The basis of the Mytec2 (and Mytec1) algorithm is the mechanism of correlation. The algorithm behind Mytec2 was summarized in a patent [8], which includes explanations of how to apply the algorithm to other biometric characteristics such as iris. However, no performance measurements are reported in publications.

Juels and Wattenberg [9] combined techniques from the area of error correcting codes and cryptography to achieve a type of cryptographic primitive referred to as fuzzy commitment scheme.

A fuzzy commitment scheme consists of a function F, used to commit a codeword $c \in C$ and a witness $x \in \{0,1\}n$. The set C is a set of error correcting codewords c of length n and x represents a bitstream of length n, termed witness (biometric data). The difference vector of c and x, $\delta \in \{0,1\}n$, where $x = c + \delta$, and a hash value $h(c)$ are stored as the commitment termed $F(c,x)$ (helper data). Each x', which is sufficiently "close" to x, according to an appropriate metric, should be able to reconstruct c using the difference vector δ to translate x' in the direction of x. A hash of the result is tested against $h(c)$. With respect to biometric key-binding the system acquires a witness x at enrolment, selects a codeword $c \in C$, calculates and stores the commitment $(c,)$ (δ and $h(c)$). At the time of authentication, a witness x' is acquired and the system checks whether x' yields a successful de-commitment. Enrolment and authentication phases are depicted on Images 2 and 3, respectively.

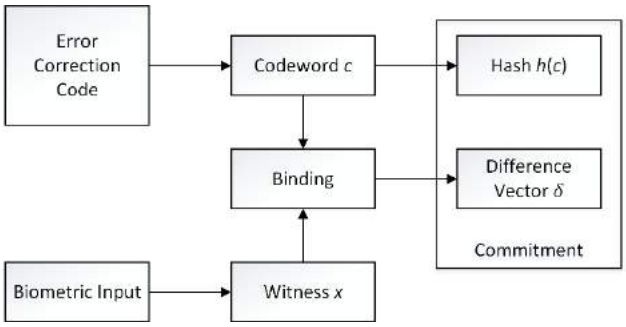


Image 2: Fuzzy commitment scheme (enrolment phase)

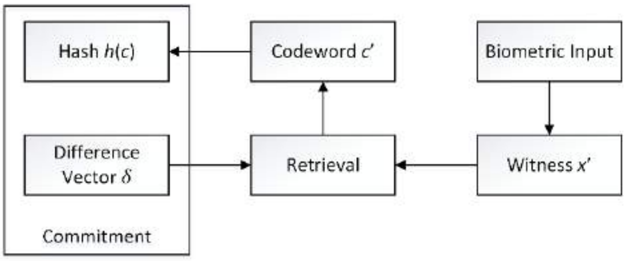


Image 3: Fuzzy commitment scheme (authentication phase)

Fuzzy Vault is an encryption scheme proposed by Juels and Sudan [10] which leverages some of the concepts of error-correcting codes, to encode information in such a way as to be difficult to obtain without the "key" used to encode it, even if the methods used for encoding are publicly known. Although this approach can work with any code, the Fuzzy Vault scheme is often used with Reed-Solomon codes, so we will focus on them for this exposition. A secret is encoded using a set of values (the "key"), and can then be unlocked with another set of values only if it has substantial overlap with the set used to lock it. This approach offers order invariance, meaning that the sets used to lock and unlock the secret are unordered. Because of this property, the Fuzzy Vault scheme has been seen application in biometric encryption [11], namely fingerprint authentication.

Reed-Solomon codes work by encoding the values in a message as the coefficients of a polynomial and then evaluating that polynomial at a set of points to obtain the codeword for that message. By using a number of evaluation points greater than the degree of the polynomial, it will be possible to obtain the polynomial (and therefore the message) by interpolation even in the presence of missing or erroneous values. However, if there are too many errors, there will not be a unique interpolating polynomial of the proper degree. These properties are leveraged in the Fuzzy Vault scheme.

Numerous enhancements to the original concept of the fuzzy vault have been introduced. Moon et al. [12], for example, suggest to use an adaptive degree of the polynomial. Nagar and Chaudhury [13] arrange encoded keys and biometric data of fingerprints in the same order into separate grids, which form the vault. Chaff values are inserted into these grids in appropriate range to hide information.

3. KEY-GENERATION SYSTEMS

In key-generation systems, helper data is derived only from the biometric template. Keys are directly generated from the helper data and a given biometric sample. While the storage of helper data are not obligatory the majority of proposed key-generation schemes does store helper data (if key-generation schemes extract keys without the use of any helper data these are not updatable in case of compromise).

The prior idea of generating keys directly out of biometric templates was presented in a patent by Bodo [14]. An implementation of this scheme does not exist and it is expected that most biometric characteristics do not provide enough information to reliably extract a sufficiently long and updatable key without the use of any helper data.

Helper data-based key-generation schemes are also referred to as “fuzzy extractors” or “secure sketches”, for both primitives formalisms (and further extensions) are defined in [15, 16]. A fuzzy extractor reliably extracts a uniformly random string from a biometric input while stored helper data assist the reconstruction. In contrast, in a secure sketch, helper data are applied to recover the original biometric template.

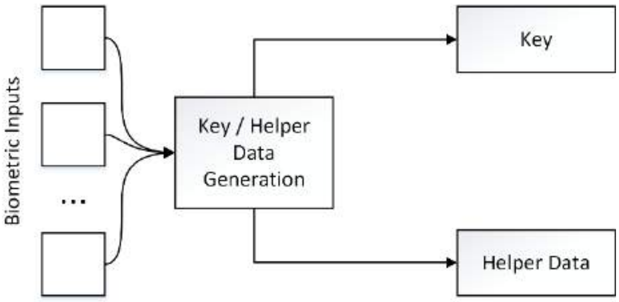


Image 4: Key-generation system (enrolment phase)

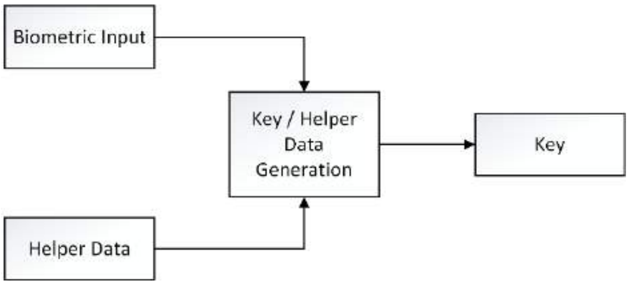


Image 5: Key-generation system (authentication phase)

There are two schemes that employ helper data. The private template scheme, based on iris, was proposed by Davida et al. [17, 18] in which the biometric template itself (or a hash value of it) serves as a secret key. The storage of helper data which are error correction check bits are required to correct faulty bits of given iris-codes. In another group of schemes, called quantization schemes, helper data are constructed in a way that is assists in a quantization of biometric features in order to obtain stable keys.

5. CONCLUSION

Concluding remarks are focused on the security of biometric cryptosystems. Most biometric cryptosystems aim at binding or generating keys, long enough to be applied in a generic cryptographic system (for example, at least 128-bit length of keys for AES algorithm). To prevent biometric keys from being guessed or brute-forced, these need to exhibit sufficient size and entropy. System performance of biometric cryptosystems is mostly reported in terms of false reject and false acceptance rates, since both metrics and key entropy depend on the tolerance levels allowed at comparison, these three quantities are highly interrelated. A second factor which affects the security of biometric cryptosystems is privacy leakage, i.e., the information that the helper data contain (leak) about biometric data. Ideally, privacy leakage should be minimized (for a given key length), to avoid identity fraud. The requirements on key size and privacy leakage define a fundamental trade-off within approaches to biometric cryptosystems, which is rarely estimated (this trade-off is studied from in an information-theoretical prospective). Additionally, stored helper data have to provide unlinkability. However, attacks on biometric cryptosystems are much more complex when compared to traditional biometric authentication. The goal is to reduce the search space, obtain the key or create a masquerade version of biometrics.

REFERENCES

[1] A. K. Jain, K. Nandakumar, A. Nagar, “Biometric template security”, EURASIP J, Adv Signal Process 2008, pp. 1-17.

[2] A. K. Jain, A. Ross, U. Uludag, “Biometric template security” Challenges and solutions”, In Proc. of European Signal Processing Conf (EUSIPCO) 2005.

[3] U. Uludag, S. Pankant, S. Prabhakar, A. K. Jain, “Biometric cryptosystems: issues and challenges”, In Proc. IEEE 2004, 92 (6), pp. 948-960.

[4] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. V. Kumar, “Biometric encryption–enrollment and verification procedures”, In Proc. SPIE, Optical Pattern Recognition IX 1998, 3386, pp. 24-35.

[5] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy R, B. V. Kumar, “Biometric encryption using image processing”, In Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II 1998, 3314, pp. 178-188.

[6] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy R, B. V. Kumar, “Biometric encryption”, ICSA Guide to Cryptography, 1999.

[7] C. Soutar, G. J. Tomko, G. J. Schmidt, “Fingerprint controlled public key cryptographic system”, US Patent 1996, 5541994.

[8] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy R, B. V. Kumar, “Method for secure key management using a biometrics”, US Patent 2001, 6219794.

[9] A. Juels, M. Wattenberg, “A fuzzy commitment scheme”, In Proc. 6th ACM Conf on Computer and Communications Security 1999, pp. 28-36.

[10] A. Juels A, M. Sudan, “A fuzzy vault scheme”, In Proc. 2002 IEEE Int. Symp. On Information Theory 2002, 408.

[11] K. Nandakumar K, A. K. Jain, S. Pankanti, “Fingerprint-based fuzzy vault: implementation and performance”, IEEE Trans. Inf. Forensic. Secur. 2007, Vol 2, pp. 744-757.

[12] D. Moon D, W-Y. Choi, K. Moon, Y. Chung, “Fuzzy fingerprint vault using multiple polynomials”, IEEE 13th Int Symposium on Consumer Electronics, ISCE ‘09 2009, pp. 290-293.

[13] A. Nagar, S. Chaudhury, “Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme”, In Proc. 18th Int. Conf. on Pattern Recognition (ICPR’06) 2006, ICPR 4, pp. 537-540.

[14] A. Bodo A, “Method for producing a digital signature with aid of a biometric feature”, German patent DE 4243908 A1 1994.

[15] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, “Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data”, In Proc. Eurocrypt 2004, pp. 523-540, (LNCS: 3027).

[16] E. A. Verbitskiy, P. Tuyls, C. Obi, B. Schoenmakers, B. Ŝkorić, “Key extraction from general nondiscrete signals. IEEE Trans Inf Forensic Secur 2010, 5(2):269-279.

[17] G. Davida, Y. Frankel, B. Matt, “On enabling secure applications through offline biometric identification”, In Proc. of IEEE, Symp on Security and Privacy 1998, pp. 148-157.

[18] G. Davida, Y. Frankel, B. Matt, “On the relation of error correction and cryptography to an off line biometric based identication scheme” In Proc. of WCC99, Workshop on Coding and Cryptography 1999, pp. 129-138.

ARTIFICIALLY INTELLIGENT CLOUD COMPUTING – THE ABILITY TO PREVENT ERRORS

DRAGAN ĐOKIĆ
Belgrade Metropolitan University, Faculty of Information Technology, Belgrade, Serbia,
dragan.djokic@metropolitan.ac.rs

MILOŠ JOVANOVIĆ
OpenLink Global Ltd., London, United Kingdom, milos.jovanovic@openlinkgroup.com

ACA ALEKSIĆ
Belgrade Metropolitan University, Faculty of Information Technology, Belgrade, Serbia,
aca.aleksic@metropolitan.ac.rs

DRAGAN VALENTIROVIĆ
Faculty of Mechanical Engineering, University of Belgrade, Belgrade, Serbia, dvalentirovic@gmail.com

DRAGAN MITIĆ
Belgrade Metropolitan University, Faculty of Information Technology, Belgrade, Serbia, miticdjd@gmail.com

Abstract: *This paper explores the possibilities and existing achievements of the integration of artificial intelligence and cloud-based storing solutions. A brief explanation of both technologies is provided, followed by a broader approach to the benefits they achieve together. Throughout the work is shown that AI helps the user and provides him security from the most sensitive link in the chain: man. An analysis of social and financial benefits is presented as well. We have approached such possibilities and indicated the ways in which artificial intelligence can be fused with cloud storage. Solutions to overcoming obstacles to the said technologies are suggested through their examination. The risks and dangers that accompany this area have been touched upon. Further research and development options are submitted while instructing caution to the damage artificial intelligence and cloud could do together.*

Keywords: *Artificially Intelligence, Cloud Computing, Efficiency, Productivity, Innovation*

1. INTRODUCTION

Challenges over the precious and economical storage of data, but also with their organization and accessibility, posed a problem to corporations until the introduction of cloud storage. Such a solution was not immediately accepted as a serious way to disengage the aforementioned problem. The cloud worked its way up to becoming one of the most important and fundamental technologies on which a large number of citizens, as well as business people trust. Besides backup, high level of organization was essential for big databases.

Artificial intelligence found its place firstly in organizational matters of the cloud and then became essential to it. Currently, most advanced cloud platforms are those fused with the power offered by artificial intelligence. Big data is becoming a serious standalone term that exists because of the advancement of the mentioned two technologies. Uncountable units of data are exchanged in real time, not to mention historically. This information is invaluable if approached correctly, and room for improvement of societies' standards is huge, but the focus remains on getting more for less.

The Cloud and AI provide societies with much more for the same price. Specifically, better organization, access to information that had not been accessible before, and keeping people safer are the goals of the technologies that serve as the pillars of today's world of information technology. Cloud computing and AI are bringing major changes in the corporate world and their fusion is believed and known to be the coming future of technology.

2. BACKGROUND

Cloud

Earlier, many were worried about the introduction of "newbies" like cloud technology. However, some other relatively new phenomena, related AI and cloud, such as the use of mobile phones in place of computers, have positively, improving impact on cloud technology.

Elementary use of cloud services comes down to the scalability of data storage; any required capacity can be achieved without planning and at any point in time. This eliminates a number of servers and the capacity to predict their numbers. This is largely due to the fact that service providers always offer the possibility to increase, or if necessary, decrease the capacity of the storage and manage other services that the client is paying for. Cloud platforms have a much higher potential than just storing data due to distributed computing power.

More importantly, an essential part of any cloud's scalability is its competence to distribute more hardware resources to a specific user and do so when the user needs it. Such situations occur when a user needs to write more data or needs more processing power from a service. Users only have to pay for the resources that they have used; if such resources are merely storage or power related, and most of the services are migrated to the cloud, this could result in great reductions in costs. Servers and their corresponding equipment are very expensive, especially when it comes to bigger operations. Moreover, the implementation of the cloud removes the need for a server economy.

Productivity and efficiency benefits are paramount when considering the advantages that the cloud offers. Vast benefits include: accessible data at all times, which provides the flexibility to make support services more available and remove limits from using only the on-premises equipment; having access to provided services at all times requires distribution of information to more than one cloud server, and that redundancy is one more service that is achieved through cloud backup. Containerization of applications is another focal cloud service. Instead of virtualizing entire operating systems, containers are made from the application layer. This allows for the easy application distribution through the cloud. As machine learning became more sophisticated, it started offering opportunities for cloud servers to be exploited as well as artificial intelligence.

Artificial Intelligence

Artificial intelligence is becoming sophisticated, and as it improves it poses a greater threat to humans should it get out of control. AI is the capability of a robot controlled by a computer or a digital computer that carry out tasks that are usually linked with intelligent beings. It allows machines to act, react, think and learn the way people work.

AI helps different machines in learning and analyzing historical data, making decisions and identifying patterns. This process helps to eradicate the chances of human error. Therefore, AI increases the decision-making process of different organizations. Systems of this type are able to learn from their mistakes and adapt to different problems that are presented to them. The learning process concerning artificial intelligence is called machine learning, or on a higher level, the evolution of machine learning: the deep learning. Machine learning is primitive in comparison to deep learning and consists of algorithms that analyze data, extract knowledge from it, and then present solutions to the given problem [1]. This process produces a trained machine capable of completing the task that would otherwise require hours of coding. Some of the learning methods include decision-tree based learning, as well as inductive logic programming, clustering, and reinforcement learning.

The difference with deep learning is that it layers algorithms with the goal of creating an artificial neural network. What neural networks do is attempt to imitate the human neural system with the emphasis on the way human neurons connect with each other. In comparison to natural neural networks, artificial ones are made of layers, connections, and directions of data propagation. Artificial neurons carry a factor of correctness concerning the data they analyze. When every neuron is put into the equation, the total outcome is calculated through the feedback of each neuron.

None of these methods have achieved the goal of a general AI qualified for completing any type of task. It strives for the automatization of as many jobs as possible – especially those that are hazardous and have led to the implementation of AI in robots. AIs are superior to humans when it comes to carrying out defined tasks, but they are not immaculate. Their performance depends on the level of training they have received and the time they have spent in the training.

The learning process, put simply, would be to tell the AIs where they went wrong and to let them figure out on their own how to overcome the error. The danger of having everything automated continues to frighten societies but is also what everybody wants. Many professions will go extinct but the machines working for us should not be considered immoral. This field is not fully explored nor defined. Standards need to be applied but that is only possible when a complete understanding of artificial intelligence is achieved.

It is advisable to mention that AI can also benefit from cloud technology. This is reflected in the provision of information for the learning process which may have inconceivable AI benefits for various potential applications.

3. SYMBIOSIS OF AI AND CLOUD

Artificial intelligence needs to learn and to be trained, and there are two methods on how to go about the process: supervised and unsupervised learning [2]. In supervised learning, AIs are presented with training datasets, which serve as boundaries of the correct outcome of the operation. The structure of a dataset consists of basic facts about the objects in the problem. Should a returned value appear incorrect, a supervisor will intervene and direct the AI to the correct solution of the problem.

The difference concerning unsupervised learning is that training datasets and outcomes are not defined. Their purpose is to solve complex problems with binary logic while only using the submitted data. Returned values are not systemized as exclusively correct or incorrect answers. Every answer is calculated to a degree of probability and semi-supervised learning (most of the time) is a realistic solution to the user's needs. This occurs due to the incomplete or inaccurate data on the matter. The combination enables usage of reference data when it is available and calculates probability when such data is non-existent.

Various roles [3] can be assigned to an AI in retail, supply chains, news, financial services, healthcare, etc., but what is undoubtedly needed are massive amounts of data [4]. The adaptation of advertisement contents is a need of every user, the optimization of routes and prediction of changes in demand are data-demanding processes, but the greatest potential and the highest requirements are held by the healthcare industry. AI integration with smart scanners could provide automatized visual diagnoses, reduce maintenance expenses, reduce human error, enable robotized surgical assistance, and improve data keeping.

Possibilities of connecting an AI to a cloud have various benefits to both sides. Cloud servers hold a lot of data and that is an invaluable resource to any AI, but if more AIs are connected, they can learn from each other's mistakes. When one particular AI learns a process, it can easily transfer the knowledge to another AI, which drastically increases the potential of such symbiosis. In the past, AI's growth was hindered due to limited datasets, it was unable to analyze all real-time data. Big data is the fuel that powers AI. The advancement of big data analytics has removed such obstacles. Tools have been created to enable rapid analysis and technology is now agile enough to access colossal datasets.

Due to a cloud's scalability, AI services provided from the cloud are also scalable. When an enterprise wants to expand AI related projects, the cloud permits adding computing power or requesting more hours of full capacity of servers from the providers [5]. Renting AIs is a great way of getting access to advanced computing power while minimizing the costs on the infrastructure, thereby accomplishing the highest efficiency because of paying only for the time or percentage of the power used.

Cloud AI is easier to use because AIs require training, and as the argument in previous paragraphs has shown, the development process is very expensive. The goal is thus to implement AI wherever it can increase efficiency. All around us, AIs are great assistants in any task. However, they are only good at performing one task at a time. The most popular use of AIs is in tremendously large databases. Huge databases need sorting, which calls for machine learning. Analytics tools offer classification and superior organization. Prior to the implementation of artificial intelligence with data analysis methods, analysts used to spend more time preparing the data than on the analysis itself. The innovation that AI brought with itself is the automatic ingestion of data, classification, and organization of all data sources.

4. SITUATION AND EXAMPLES TODAY

Although the work with cloud technology is desirable because it brings a lot of money, it quickly crystallized that it is extremely expensive for small business organizations to develop cloud technology. One of the reasons is that training algorithms take a lot of computing power. Large companies like Microsoft, Amazon, Google do not have such problems because with a large human and material capital they can not only maintain, but also improve their position in the market by continuously improving their high-tech services. It is therefore logical that they are the leaders of AI-based cloud development, as an economical solution for software development. Previously listed companies have a turnover of $40 billion in the market for these technologies [6].

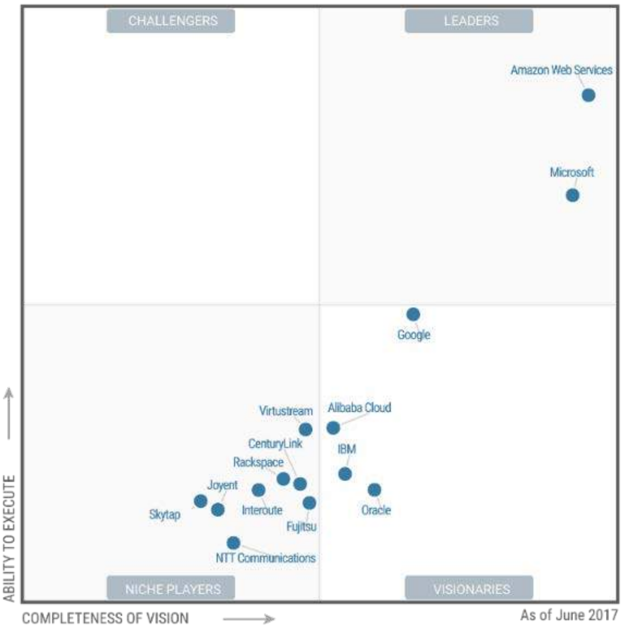


Figure 1: Magic Quadrant for Cloud Infrastructure as a Service, Worldwide [7]

By owning AWS Amazon Cloud, Amazon as a company is the prime. That confirms freshly presented version No. 9, an integrated development environment (IDE) which can immediately plug into a cloud platform. Recently developed AI tools, for example, allow converting speech from audio files into text, translation, following people, activities, objects, etc. Besides mentioned, unique chips have been produced by this company. They are named Tensor Processing Units (TPUs) for the reason that they effectively process TensorFlow and reduce the needs of energy.

A bit similar to TensorFlow is Gluon - the open-source deep-learning library. This is a project by Amazon and Microsoft, joined together. The second one is making an effort in designing low-power chips for running servers, too. The capacity of those chips is still sort of an enigma, even for the specialists. In order to keep up with innovations companies should select their provider as clever as they can. For example, hyperscale cloud providers are presenting a variety of AI services. On the other hand, Amazon Web Services (AWS) launched Amazon Lex (a conversational engine), Amazon Polly (voice-like output generator), Amazon Rekognition (computer vision solutions builder) and Amazon Machine Learning (ameliorates machines' abilities to predict better) [8].

5. OBSTACLES FOR FUTURE IMPROVEMENT

Technical

The increase in efficiency and innovation potentials have been noted after AI and cloud computing were combined [5]. While operations expand, larger data workloads are worked with, and possibilities are perceived to reduce the expenses. Intelligent data storage layer on the cloud offers high efficiency and scalability, both of which are mandatory solutions to this problem. The cloud has a vast set of tools that are striving to analyze data economically and securely. Distinct ways [9] of data processing offer different results in prioritizing real-time data or being as accurate as possible.

It is difficult, even for the most advanced systems, to keep up with the amounts of data generated at the moment, and it is even more time-consuming to analyze all the data on a certain subject [10]. The main goal remains to ensure the management of exponential data growth in a scalable and efficient way, which is why datasets are put together. The purpose of a dataset is to contain analyzed data only on the matter that is of interest at that moment. AI can have a massive impact on the preparation of datasets and simplifying the job for humans.

More powerful infrastructure is required for fine-tuned results and that is why computing power is a serious obstacle for artificial intelligence and the cloud as well. Both branches need very sophisticated infrastructure to provide the services they offer, especially if such systems are developed privately. Establishing private AI integrated cloud networks – besides the infrastructure costs – yields high costs in human resources. Regular maintenance and supervision crews are also expensive due to the essential ‘always-online’ support. Moreover, the expenses multiply when a group of experts is assigned to train an AI.

Creating a general AI has been attempted, and the closest the society has come to achieving that goal was the creation of the multitasking [11] methods, which are divided by the ways in which they connect tasks to each other. Tasks can be divided after connecting all the data to them, or conversely, the data on each task can be divided and later connected once the tasks are completed separately.

AI’s biggest disadvantage currently is its inability to deal with different occupations. General artificial intelligence is what is thought of when talked about AIs. Currently, the AIs that are available exist in the form of very sophisticated algorithms with a possibility of expansion under certain conditions, which is the main reason why the actual perfect assistant cannot yet be made.

Legal

Artificial intelligence has been encountering problems with various governments. The law is getting twisted when it comes to criminal liability and prospective jurisdiction [12]. Some have redefined their laws according to AI, but those regulations are only a work in progress. Legal workers have been battling to achieve controlled access to permissions that the AI technologies need without violating human rights [13]. Examples of practical usage include image processing, geotagging [14], three-dimensional environment processing, speech analysis and data mining. The examples listed above need access to cameras, microphones and a lot of historical data.

Algorithms are used to analyze images to extract information and in real time with autonomous vehicles that require radar and laser data to understand three-dimensional geometries. Text analysis has even more application because of the massive amounts of data being generated daily. It is used to obtain information, apply a classification, or extract particular pieces of data. This type of analysis is also considered to be data mining. Large quantities of data are needed to reap the full benefits of the analytics tools. Individual’s security is questioned when a great amount of data is analyzed, especially since confidential data is required for some analysis.

Especially a big fear may arise in the economy. A group of data that is stored and processed by cloud technologies and AIs are also large groups of important ones, such as, for example, confidential finance documents or documents from the domain of intellectual property.

The general impression is that even the most advanced countries in the world do not give enough support to new trends, because laws often come with delays and major deficiencies. In the case of stress situations (abuse), there is a big dilemma whether the guilt can be proven. The sensitive analyzed data is valuable to hackers, and if stored and used carelessly, it can become a threat. In certain cases, storing that kind of data on the cloud is unpermitted and there are also limitations as to where the data is stored geographically.

6. CONCLUSION

Innovation that combines cloud computing and artificial intelligence can be of great importance to society. Raising the standard for human lives is a philanthropic deed that we should all commit to. With present-day devices and with sophisticated software growing and multiplying exponentially, ample data is injected into the systems. The corporate world has a wide playing field of opportunities that would not be presented to them if it were not for the analysis of massive amounts of information. For some time, it has been a common practice to resort to cloud storing of the entire data an operation has generated. Artificial intelligence gives wings to the organization and classification methods of that very storage.

Inventors should continue perfecting the solutions that are currently used, and with great effort, a general AI could see the light of day. That is why the legal regulations should be prepared even before. This is highly risky, but it cannot be said with certainty that it will generate a high reward as well [15]. AI must not be underestimated and neglected, for at this moment, it is a double-edged sword. Cloud, when it is alone, has the ability to become significant computer hardware in several areas. However, cloud computing integration of AI will improve its market demands. With the big steps that exist in the growth of clouds and artificial intelligence, it seems that their future is very closely related. Cloud computing becomes very easy to protect, scan and handle artificial intelligence.

Above all, the more companies become on the cloud, more need to integrate with AI in order to achieve efficiency. The point will come when there is no cloud technology without artificial intelligence. Starting from the assumption that a modern business environment requires complex solutions in the field of data analysis and data protection, it is absolutely and without any doubt that progress in this field will precisely preclude the development of artificial intelligence, machine learning, deep learning, logic algorithms and neural networks in the cloud – whether it is services, platforms or infrastructure. Also, the availability of these technologies at the lowest levels will surely contribute to a rapidly changing business environment and affect the change and automation of most business processes.

The next generation of services in the cloud environment can represent an intersection of innovative business processes and technological innovations, which can lead to the need for support in the field of intelligent processes automation – where AI finds the right application.

REFERENCES

[1] J. Le, "The 10 Deep Learning Methods AI Practitioners Need to Apply," Medium, Nov. 2017. [Online]

[2] P. Mell, T. Grance, "The NIST Definition of Cloud Computing", NIST, Sep. 2011.

[3] H. Motahari-Nezhad, B. Stephenson, S. Singhal, "Outsourcing Business to Cloud Computing Services: Opportunities and Challenges", HP Laboratories, 2009.

[4] S. Pearson, "Taking Account of Privacy when Designing Cloud Computing Services", HP Laboratories, 2009.

[5] C. Harvey, "AI in the Cloud Boosts Cloud Performance", Datamation, Jan. 2018. [Online]

[6] J. Snow. "2017: The year AI floated into the cloud.", MIT Technology Review, 2018. [Online]

[7] L. Leong, R. Bala, C. Lowery and D. Smith, "Magic Quadrant for Cloud Infrastructure as a Service, Worldwide", Gartner, 2017. [Online]

[8] M. Kralj, "How cloud serves as the foundation of AI", InfoWorld, 2017. [Online]

[9] A. Impacts, "Trends in the cost of computing", 2015.

[10] S. Riesen, "The challenges of artificial intelligence", Technologist magazine

[11] S. Ruder, "An Overview of Multi-Task Learning in Deep Neural Networks", arXiv, Jun. 2017. [Online]

[12] B. Buchanant, T. Headrickt, "Some Speculation About Artificial Intelligence and Legal Reasoning", Board of Trustees of the Leland Stanford Junior University, Stanford Law Review, Volume 23, No. 1, Nov. 1970.

[13] Enterprise Innovation editors, "2018: The rise of AI, hybrid cloud and digital human rights issues", Enterprise Innovation magazine, 2018.

[14] S. Agarwal, J. Dunagan, N. Jain, S. Saroiu, A. Wolman, "Volley: Automated Data Placement for Geo-Distributed Cloud Services", University of Toronto and Microsoft Research, 2010.

[15] M. Kosoff, "THE WORLD'S A.I. PROBLEMS ARE ONLY GOING TO GET WORSE", Vanity Fair, Feb. 2018.

The 10th International Conference on Business Information Security (BISEC-2018), 20th October 2018, Belgrade, Serbia

E-MAIL FORENSICS: TECHNIQUES AND TOOLS FOR FORENSIC INVESTIGATION

LJUBOMIR LAZIĆ
Belgrade Metropolitan University, Faculty of Information Technologies, ljubomir.lazic@metropolitan.ac.rs

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

Abstract: *E-mail has emerged as the most important application on Internet for communication of messages, delivery of documents and carrying out of transactions and is used not only from computers but many other electronic gadgets like mobile phones. This paper is an attempt to illustrate e-mail architecture from forensics perspective. Also, paper projects the need for e-mail forensic investigation and lists various methods and tools used for its realization. A detailed header analysis of a multiple tactic spoofed e-mail message is carried out in this paper. It also discusses various possibilities for detection of spoofed headers and identification of its originator. Further, difficulties that may be faced by investigators during forensic investigation of an e-mail message have been discussed along with their possible solutions. Our focus is on email header analysis phase offered by the tools. We examine the capability of a particular tools such as:EmailTrackerPro and aid4mail in action.*

Keywords: *E-mail forensic, header analysis, E-mail message as evidence*

1. INTRODUCTION

Modern time communication is impossible without emails. In the field of business communication, emails are considered as its integral part. At the same time, emails are also being used by criminals [1,3,5]. In digital forensics, emails are considered as evidence and Email Header Analysis has become important to collect evidence during forensics process [1,2]. Email clients are computer programs that allow users to send and receive emails. Over time, different types of email clients have been invented for the convenience of email users. We will discuss different types of email clients now. Broadly, email clients are divided into two types based on email saving location. They are – web-based email clients and desktop-based email clients.

a) Web-based Email Clients: Web-based email clients save all their data to its web server. Some web-based clients are Gmail, Yahoo Mail, Hotmail, etc. The benefit of using web-based email clients is it can be accessed from anywhere in the world, using Username and Password. One of its disadvantages is users do not know where their data is being stored.

b) Desktop-based Email Clients: Desktop-based email clients are opposite of web-based clients. Outlook, Thunderbird, Mail Bird are some examples of desktop-based email clients. All data of desktop-based web browser is stored in the system of its users. Thus, users do not have to worry about data security. The same point can be considered as a disadvantage in some cases. Especially, when it is used in criminal activities, and the evidence cannot be collected from the server [3,5]. E-mail messages include transit handling envelope and trace information in the form of structured fields which are not stripped after messages are delivered, leaving a detailed record of e-mail transactions. A detailed header analysis can be used to map the networks traversed by messages, including information on the messaging software and patching policies of clients and gateways, etc. Over a period of year's e-mail protocols have been secured through several security extensions and producers, however, cybercriminals continue to misuse it for illegitimate purposes by sending spam, phishing e-mails, distributing child pornography, and hate e-mails besides propagating viruses, worms, hoaxes and Trojan horses. Further, Internet infrastructure misuse through denial of service, waste of storage space and computational resources are costing every Internet user directly or indirectly.

E-mail forensic analysis is used to study the source and content of e-mail message as evidence, identifying the actual sender, recipient and date and time it was sent, etc. to collect credible evidence to bring criminals to justice [1-5]. This paper is an attempt to illustrate e-mail architecture from forensics perspective. It describes roles and responsibilities of different e-mail actors and components, itemizes meta-data contained in e-mail headers, and lists protocols and ports used in it. It further describes various tools and techniques currently employed to carry out forensic investigation of an e-mail message.

This paper projects the need for e-mail forensic investigation and lists various methods and tools used for its realization. A detailed header analysis of a multiple tactic spoofed e-mail message is carried out in this paper. It also discusses various possibilities for detection of spoofed headers and identification of its originator. Further, difficulties that may be faced by investigators during forensic investigation of an e-mail message have been discussed along with their possible solutions [3,4].

Also, this paper will discuss tracing e-mail headers and issues associated with it. It will address both HTTP & SMTP initiated e-mails. It will discuss different ways used by e-mail senders to evade tracing and workarounds used by investigators to combat them. It will also discuss advanced measures and techniques used by investigators to track emails [5]. In The paper we will discuss particular tools such as: *EmailTrackerPro* and *aid4mail* in action.

2. E-MAIL SERVICE ARCHITECTURE

E-mail system comprises of various hardware and software components that include sender's client and server computers and receiver's client and server computers with required software and services installed on each. Besides these, it uses various systems and services of the Internet. The sending and receiving servers are always connected to the Internet but the sender's and receiver's client connects to the Internet as and when required [1, 2]. E-mail is a highly distributed service that involves several actors which play different roles to accomplish end-to-end e-mail exchange [1]. These actors fall under three groups namely User Actors, Message Handling Service (MHS) Actors and ADministrative Management Domain (ADMD) Actors. User Actors are Authors, Recipients, Return Handlers and Mediators which represent people, organizations or processes that serve as sources or sinks of messages. They can generate, modify or look at the whole message. Message Handling Service (MHS) Actors are Originators, Relays, Gateways and Receivers which are responsible for end-to-end transfer of messages. These Actors can generate, modify or look at only transfer data in the message. ADministrative Management Domain (ADMD) Actors are Edges, Consumers and Transits which are associated with different organizations and have their own administrative authority, operating policies and trust-based decision making [2].

E-mail system is an integration of several hardware & software components, services and protocols, which provide interoperability between its users and among the components along the path of transfer. The system includes sender's client and server computers and receiver's client and server computers with required software and services installed on each. Besides, it uses various systems and services of the Internet [1].

The sending and receiving servers are always connected to the Internet but the sender's and receiver's client connects to the Internet as and when required. An e-mail communication, for example, between a sender 'Alice' having e-mail address 'alice@a.com' and recipient 'Bob' having e-mail address 'bob@b.com' is shown in figure 1.

'Alice' composes an e-mail message on her computer called client for 'Bob' and sends it to her sending server 'smtp.a.org' using SMTP protocol. Sending server performs a lookup for the mail exchange record of receiving server 'b.org' through Domain Name System (DNS) protocol on DNS server [1] 'dns.b.org'. The DNS server responds with the highest priority mail exchange server 'mx.b.org' for the domain 'b.org'. Sending server establishes SMTP connection with the receiving server and delivers the e-mail message to the mailbox of 'Bob' on the receiving server. 'Bob' downloads the message from his mailbox on receiving server to local mailbox on his client computer using POP3 [2] or IMAP [3] protocols. Optionally, 'Bob' can also read the message stored in his server mailbox without downloading it to the local mailbox by using a Webmail program.

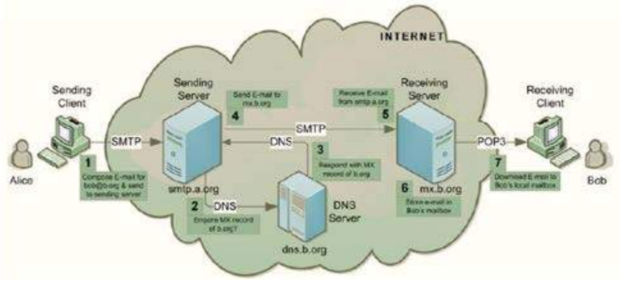

INTERNET
Sending Client
Sending Server
Receiving Server
Receiving Client
Alice
Bob
SMTP
SMTP
DNS
DNS
POP3
1
Compose E-mail for bob@b.org & send to sending server
2
Enquire MX record of b.org?
3
Respond with MX record of b.org
4
Send E-mail to mx.b.org
5
Receive E-mail from smtp.a.org
6
Store e-mail in Bob's mailbox
7
Download E-mail to Bob's local mailbox
smtp.a.org
mx.b.org
DNS Server
dns.b.org

Image 1: E-mail communication between a sender 'Alice' and recipient 'Bob' [2]

E-mail system is an integration of several hardware and software components, services and protocols which provide interoperability between its users and among the components along the path of transfer. The e-mail architecture shown in figure 2 below specifies the relationship between its logical components for creation, submission, transmission, delivery and reading processes of an e-mail message. Several communicating entities called e-mail nodes which are essentially software units working on application layer of TCP/IP model are involved in the process of e-mail delivery. Nodes working on lower layers such as routers and bridges represent options to send e-mail without using SMTP are not considered in this architecture because almost all e-mail communication uses SMTP directly or indirectly. Further, proprietary nodes used for internal deliveries at sending and receiving servers are also not considered in this architecture.

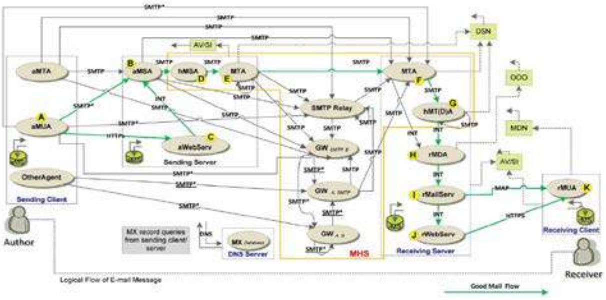


Image 2: E-mail Architecture [2]

A mail message from Author to Receiver that traverses through aMUA, aMSA, hMSA, MTA (outbound), MTA (Inbound), hMDA, rMDA, rMailServ and rMUA is considered as good mail by the Sender Policy Forum (SPF). Mails following through other paths are either fully or partially non-SMTP based or uses non-standard transfer modes which are often suspected to contain viruses and spam. Delivery Status Notification (DSN) messages are generated by some components of MHS (MSA, MTA, or MDA) which provide information about transfer errors or successful deliveries and are sent to MailFrom addresses. Message Disposition Notification (MDN) messages are generated by rMUA which provide information about post-delivery processing are sent to Disposition-Notification-To address. Out Of Office (OOO) messages are sent by rMDA to return address [1].

E-mail forensic investigation techniques

E-mail forensics refers to the study of source and content of e-mail as evidence to identify the actual sender and recipient of a message, data/time of transmission, detailed record of e-mail transaction, intent of the sender, etc. This study involves investigation of metadata, keyword searching, port scanning, etc. for authorship attribution and identification of e-mail scams.

Various approaches that are used for e-mail forensic are described in [3] and are briefly defined below. E-mail forensic include header analysis, bait tactics, server investigations, and network device investigation. Besides mandatory headers, custom and MIME headers appearing in the body of the message are also analysed for sender mailer fingerprints and software embedded identifiers.

Email Forensics Analysis Steps

A forensic investigation of e-mail can examine both email header and body. This paper will look at header examination.
According to [3] an investigation should have the following:
- Examining sender's e-mail address
- Examining message initiation protocol (HTTP, SMTP)
- Examining Message ID
- Examining sender's IP address

Some other aspects that controls forensics step include the following properties (Image 3):

1) Storage format of email: Server side storage format may include maildir (each email is kept separate in a file, for each user), mbox format (all email files are in a single text file). Server-side stores email in SQL Server databases. Reading different types of formats can be done for forensics analysis by using notepad editor and applying regular expression-based searches [4]. At the client-side, an email is stored as mbox format (Thunderbird) [4]. Client side may also store emails as .PST (MSOutlook), and NSF (Lotus Notes) files.

2) Availability of backup copy of email: When checking from the serve side, all copies are transferred to the client. This requires seizing the client computer. For webmail, copies are always saved at the server side [**4**].

3) Protocol used to transport email: Email can be initiated and transported based on SMTP or HTTP [1] depending on the email server applications.

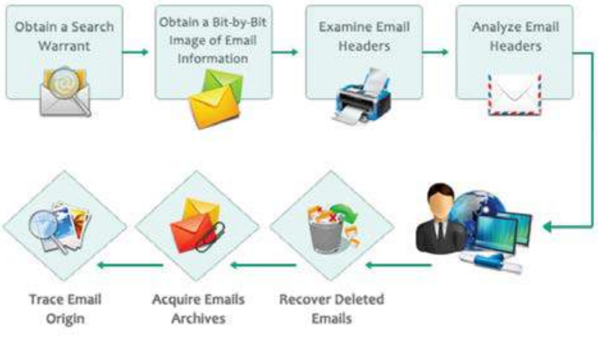


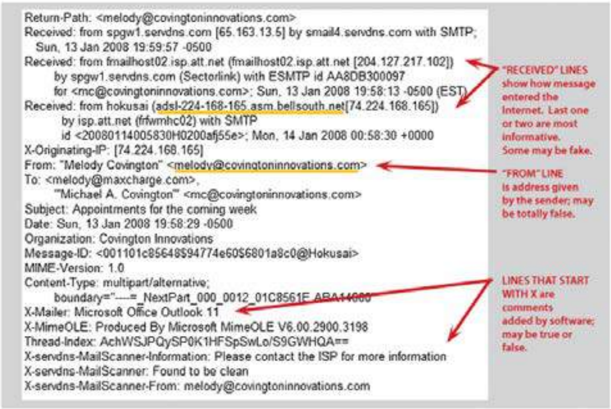
Image 3: Broad steps in email forensics for investigator

Header Analysis

Meta data in the e-mail message in the form of control information i.e. envelope and headers including headers in the message body contain information about the sender and/or the path along which the message has traversed. Some of these may be spoofed to conceal the identity of the sender. A detailed analysis of these headers and their correlation is performed in header analysis. Besides header analysis various other approaches that can be used for e-mail forensics include bait tactics, server investigations, and network device investigation. Custom and MIME headers appearing in the body of the message are also analysed for sender mailer fingerprints and software embedded identifiers [3].

Relevance of Headers & Components

Email header forensics basically denotes the examination done on the email message body and the source and path followed by it. This also includes the identification of genuine sender, time, or recipient of the emails. The email header forensic analysis can bring out the candid evidences from various components included in the header part. Let us see which components are helpful for header forensics;



```
Return-Path: <melody@covingtoninnovations.com>
Received: from spgw1.servdns.com [65.163.13.5] by smail4.servdns.com with SMTP;
   Sun, 13 Jan 2008 19:59:57 -0500
Received: from fmailhost02.isp.att.net (fmailhost02.isp.att.net [204.127.217.102])
        by spgw1.servdns.com (Sectorlink) with ESMTP id AA8DB300097
        for <mc@covingtoninnovations.com>; Sun, 13 Jan 2008 19:58:13 -0500 (EST)
Received: from hokusai (adsl-224-168-165.asm.bellsouth.net[74.224.168.165])
         by isp.att.net (frfwmhc02) with SMTP
         id <20080114005830H0200afj55e>; Mon, 14 Jan 2008 00:58:30 +0000
X-Originating-IP: [74.224.168.165]
From: "Melody Covington" <melody@covingtoninnovations.com>
To: <melody@maxcharge.com>,
        "'Michael A. Covington'" <mc@covingtoninnovations.com>
Subject: Appointments for the coming week
Date: Sun, 13 Jan 2008 19:58:29 -0500
Organization: Covington Innovations
Message-ID: <001101c85648$94774e60$6801a8c0@Hokusai>
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_NextPart_000_0012_01C8561E.ABA14060"
X-Mailer: Microsoft Office Outlook 11
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3198
Thread-Index: AchWSJPQySP0K1HFSpSwLo/S9GWHQA==
X-servdns-MailScanner-Information: Please contact the ISP for more information
X-servdns-MailScanner: Found to be clean
X-servdns-MailScanner-From: melody@covingtoninnovations.com
```

"RECEIVED" LINES show how message entered the Internet. Last one or two are most informative. Some may be fake.

"FROM" LINE is address given by the sender; may be totally false.

LINES THAT START WITH X are comments added by software; may be true or false.

Image 4: A typical E-mail header

`X-Apparently-To:` It will reveal recipient's email address while investigating. This can be the validation field for checking email service provider. Generally this field is referred to as "BCC, CC, or To" and is not restricted to "To".

`Delivery To:` This shows the address of the auto-mailer.

`Return-Path:` This field is used for the bounces of email messages. In case the mail server is sending the message and it cannot be delivered.

`Received-SPF:` During email header forensics, this field shows the information of email service used for the sending of mails. It is also having an ID number which is important for log examination for determining the validity of an email. In case of unavailability of the ID, the email must have been spoofed.

`Message ID:` This is a globally used unique identification ID which refers to the genuine time of the emails and version of message. It is highly important to know if investigators want to know whether spoofing is done to the email or not.

MIME Version: It stands for Multipurpose Internet Mail Extensions and is an Internet Standard which extends format of message.

Content-type: This shows the type of content or format used for the message like; XLML, Text, or HTML.

X-Mailer: It displays the email client which is used for sending the message.

X-Originating-IP&Received: This is an important field for tracing the IP address used for sending the email. This is the most important message when it comes to the email header forensic analysis as it has to be examined where the mail arrived from.

DKIM-Signature: This field stores the signature of an email and all key-fetching information in simple "tag=value" syntax. It is a crucial field to validate the domain name and identity allied to the message via cryptographic authentication.

3. EXAMINING E-MAIL FORNSIC TOOLS: CASE STUDIES

Email analysis, as we already mention, is the task performed in the network forensics. Email analysis is the process which involves analysis of emails sent and received at different ends. In current era, there are very less ways to analyse emails. Most widely accepted method is the Manual Method of Email Analysis [4,5]. Although there have been many attempts into securing e-mail systems, most are still inadequately secured. Installing antiviruses, filters, firewalls and scanners is simply not enough to secure e-mail communications. Some common examples of illegitimate uses of emails are spam, phishing, cyber bullying, botnets, disclosure of confidential information, child pornography and sexual harassment. The anonymity factor of e-mail has made it difficult for digital forensic investigators to identify the authorship of an email, and to compound this problem further; there is no standardised procedure to follow.

Therefore, a forensic investigator needs efficient tools and techniques to perform the analysis with a high degree of accuracy and in a timely fashion. It is evident that an email forensic tool may only assist the investigator during a specific stage of analysis [4,5].

While preforming manual method for email analysis, we try to spot spoofed messages which are sent through SMTP (Simple Mail Transfer Protocol). By analysing them we can decode the message being sent. After decoding, all IP addresses are analysed and their location is traced. A timeline of all event is made (in universal standard time) and is checked further for suspicious behaviour. Server logs are checked at the same time to ensure that all the activities are mentioned in the timeline so formed. If any suspicious activity is found, the mails are recovered and can be used as evidence against the sender. Email is extracted from the client server which keeps a copy of sent mails until a specific number.

First case study

First, we will describe a well-known case in court practice i.e. a case study involving the use of Manual Method for Email Analysis [4] using a whaling attack which is a spear-phishing attack directed specifically at high-profile targets like C-level executives, politicians and celebrities:

- An email attached to a $20 million dollar lawsuit purported to be from the CEO of "`tech.com`" to a venture capital broker. The message outlined guaranteed "warrants" on the next round of finding for the broker.
- "`tech.com`" filled counter claim and claimed the email was *forgery*. Their law firm engaged a team to determine the validity of the message.
- The team imaged all of the CEO's computers at his office and his home. Email server backup tapes were recalled from the client servers.
- All hard drivers and email servers were searched for "questioned" message. There were no traces of any such mail on any of the hard drive or mail spool.
- When the time stamps and message id's were compared with the server logs then it was found that the "questioned" message have not gone through either "`tech.com`'s" webmail or mail server at the time indicated by the date/time stamp on the message.
- Based on the analysis the defendants filed motion to image and examine broker's computers.
- Federal judge issued subpoena and the team arrived at the broker's business, he refused to allow his system to image.
- Broker's lawyer went into the state court, on a companion case, and got judge to issue an order for a new court appointed examiner.
- The examination revealed direct proof of the alteration of a valid message's header to create a "questioned" email.

The allegedly received email

Here is the header of problematic e-mail is presented.

```
Return-Path: CEO Good_Guy@tech.com
Received: from mail.tech.com
(mail.tech.com [201.10.20.152])
by hedgefund.fund.com (8.11.0/8.11.0)
ESMTP id e73MfZ331592; Thu, 3 Aug 2000
15:45:31 -0400
Received: from webmail.tech.com
(webmail.tech.com
[10.27.30.190]) by mail.tech.com
(Switch-2.0.1/Switch-2.0.1) ESMTP id
e73MfW903843; Thu, 3 Aug 2000 14:41:32
-0500
Received: from tech.com
(ostrich.tech.com [10.27.20.190])
by webmail.tech.com (8.8.8+Sun/8.8.8)
with ESMTP id RAA01318; Thu, 3 Aug
2000 14:41:31 -0500
content-class: urn:content-
classes:message
Subject: Warrants on $25 Million
Funding
Date: Thu, 3 Aug 2000 14:43:47 -0500
MIME-Version: 1.0
Content-Type: application/ms-tnef;
```

```
name="winmail.dat"
Content-Transfer-Encoding: binary
Message-ID:
<3989e793.87BDEEE2@tech.com>
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
<3989e793.87BDEEE2@tech.com>
Thread-Topic: Warrants on $25 Million
Funding
Thread-Index:
AcHatCZUSkaLe0ajEdaelQACpYcy8A==
From: "CEO Good_Guy@tech.com"
<ceo_good_guy@tech.com >
To: "Bad_Guy_Broker"
<bad_guy@fund.com>
```

Information contained in the header can aid investigators in tracing the sender of the e-mail. A thorough investigation of e-mail headers should include examination of the sender's e-mail address and IP address, examination of the message ID as well as the messaging initiation protocol (HTTP or SMTP). To determine the source of the e-mail, *investigators must first examine the received section at the bottom of the header and work their way up in a bottom to top approach.*

It is also important that e-mail cases examine the logs of all servers in the received chain as soon as possible. Time is very important in e-mail cases as HTTP and SMTP logs are archived frequently; especially by large ISPs. If a log is archived, it could take time and effort to retrieve and decompress the log files needed to trace e-mails. Some e-mails have fake/forged headers in order to deceive investigators, so extreme caution and careful scrutiny should be practiced in investigating every part of the e-mail header.

Now, this is quite a bit long and tiring procedure which would involve too many mails to be analysed which would be too much time consuming. Time being the most expensive entity, we need to save the time as much as we can. To save this time certain tools are present which helps to reduce the work burden. So, we need a software tools, such as eMailTrackerPro (http://www.emailtrackerpro.com/) and Aid4Mail Forensic (http://www.aid4mail.com/) that are discussed in the next section.
In this case investigator should look at ESMTP id which is a unique identification assigned by each intermediate relay or gateway server. This id is usually in a hexadecimal string that is reset each day. Resulting in an id that can be resolved to a time window on a particular server. Investigator, also, should, compare header information against server logs: `webmail@tech.com`. Analysis of the webmail server logs revealed several issues regarding the validity of the suspect message:

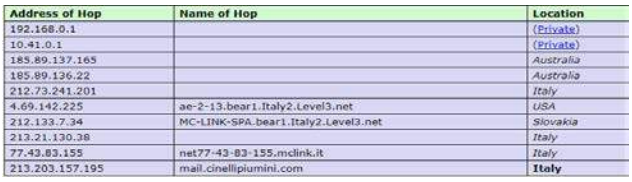
- Matching trace header timestamps and ESMTP ids revealed that RAA01318 was issued at 17:41:31 to the authentic message
- Comparing the 14:41:31 timestamp of the suspect message with the log revealed the server was assigning ESMTP ids beginning with "OAA" not "RRA" as represented in the header.

Analysis of the mail server logs confirmed that the suspect message was not authentic:

- Matching trace header timestamps and ESMTP ids revealed that the authentic Message-ID was logged at 17:41:32 and assigned ESMTP id e73MfW903843 then it was sent to the `hedgefund@fund.com` server and it was assigned a new ESMTP id e73MfZ331592
- Comparing the 14:41:32 timestamp of the suspect message with the log revealed there were no messages for over an hour during that time frame.

Second case study

This section describes the court case of cybercrime so called "identity theft in Internet communication by electronic mail by two business entities". Based on the analysis of the method of communication (e-mails, SMS messages and voice), languages in business correspondence, frequency of transactions, problems in business, ways of solving them in over 100 collected e-mails in communication between two companies during three years successful cooperation, the author of the work came to indisputable indicators of cybercrime [5]. Theft of identity of e-mail addresses and false communications with a foreign company was carried out in order to indicate that a cash transaction of around EUR 100,000 was paid to the account of NN strikers in the London bank, and not to the account in the domestic Serbian bank to which the money was paid up to then in the process of electronic payment of goods and services between the parties to the dispute. The process of examining e-mails is described using the *eMailTrackerPro* tool in the event of identity theft by an NN person (attacker, hacker), an e-mail forensic investigation plan, restrictions, an attacker detection process as the third NN person in an email communication, Man-in-the-Middle Attack experiment that served as the basis for forensic analysis of e-mail in the case study. As for this case, it is necessary to see from which address the hacker sent a message, and through which hopes (jumps through the Internet) a message was sent to reach its destination, as can be seen in the following image [5].



Address of Hop	Name of Hop	Location
192.168.0.1		(Private)
10.41.0.1		(Private)
185.89.137.165		Australia
185.89.136.22		Australia
212.73.241.201		Italy
4.69.142.225	ae-2-13.bear1.Italy2.Level3.net	USA
212.133.7.34	MC-LINK-SPA.bear1.Italy2.Level3.net	Slovakia
213.21.130.38		Italy
77.43.83.155	net77-43-83-155.mclink.it	Italy
213.203.157.195	mail.cinellipiumini.com	Italy

Image 5: Hopes through which the hacker's mail passed

As far as the hopes through which the message goes, we can see that it is a little unusual that everything is going from Italy, going to the server in Slovakia, to the US (forged email address of `xxxxx@yahoo.com`), then back to Italy and then to Australia. The following figure will show the path on the map as the message was traveling.

Italy
Australia

Image 6: Path on the map the message travelled

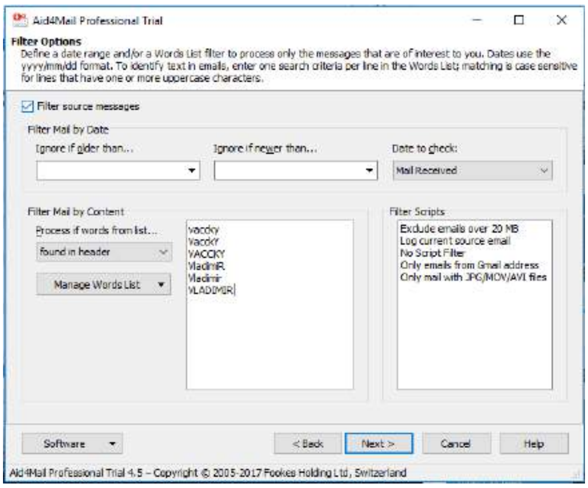
After this knowledge, it was necessary to analyse other suspicious e-mails, as well as the email server on the victim's side, as we described earlier. It was found that during the time of the hacker attack, the actual sender did not send any messages. There are many tools which may assist in the study of source and content of e-mail message so that an attack or malicious intent of the intrusions may be investigated. This section introduces some of these tools: eMailTrackerPro and Aid4Mail Forensic.

Software eMailTrackerPro [4] is a proprietary email forensic solution that analyses email files stored in local disk and supports automatic email analysis for the identification of spamming incidents. eMailTrackerPro is capable of recovering the IP address that sends the message along with its associated geographical location (city) to determine the threat level or validity of an e-mail message. It can find the network service provider (ISP) of the sender. A routing table is provided to identify the path between the sender and receiver of an email. It also can check a suspected email against Domain Name Server blacklists to safeguard against spam.

The *disadvantage* associated with this software is that it would be unable to find a spammer which is not blacklisted into its database.

Add4Mail forensic software tool

Another tool developed for helping in the mail sorting purpose only. This software can find emails which can be searched by any particular keyword. As with *EmailTrackerPro* and on this tool, we need to configure our mail ie. Let's choose which mail we will use for analysis. In this case, we will use gmail. Once we have completed the mail configuration, we are going to the next step that allows us to select the time frame in which we want to search for mail by keywords, and in the window where Vaccky, VacckY, etc., are located. It's actually a keyword search box.


Aid4Mail Professional Trial

Filter Options
Define a date range and/or a Words List filter to process only the messages that are of interest to you. Dates use the yyyy/mm/dd format. To identify text in emails, enter one search criteria per line in the Words List; matching is case sensitive for lines that have one or more uppercase characters.

☑ Filter source messages

Filter Mail by Date
Ignore if older than...
Ignore if newer than...
Date to check: Mail Received

Filter Mail by Content
Process if words from list... found in header

```
vaccky
VacckY
VACCKY
VladimiR
Vladimir
VLADIMIR
```

Filter Scripts

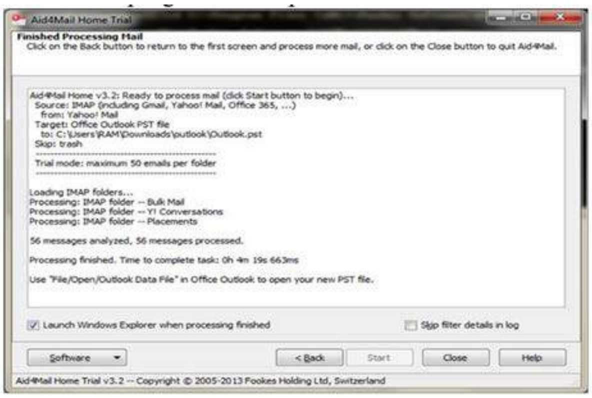
```
Exclude emails over 20 MB
Log current source email
No Script Filter
Only emails from Gmail address
Only mail with JPG/MOV/AVI files
```

Aid4Mail Professional Trial 4.5 – Copyright © 2005-2017 Fookes Holding Ltd, Switzerland

Image 7: Example: Search keywords for a mailbox by Add4Mail

The output provided by this software program is the message written in the email along with the date, time and other information specific to the mail as in image 8.

This software program can also be used to fetch some deleted mails from their trash folder. Unlike email tracker pro, this tool does not only serve to track the message, but also for detailed forensic mail analysis. This tool can be found at http://www.aid4mail.com/, but like *EmailTrackerPro* is not an open source, but you must purchase a license.


Aid4Mail Home Trial

Finished Processing Mail
Click on the Back button to return to the first screen and process more mail, or click on the Close button to quit Aid4Mail.

```
Aid4Mail Home v3.2: Ready to process mail (click Start button to begin)...
  Source: IMAP (including Gmail, Yahoo! Mail, Office 365, ...)
    from: Yahoo! Mail
  Target: Office Outlook PST file
    to: C:\Users\RAM\Downloads\outlook\Outlook.pst
  Skip: trash
  ------------------------------------------------
  Trial mode: maximum 50 emails per folder
  ------------------------------------------------

Loading IMAP folders...
Processing: IMAP folder -- Bulk Mail
Processing: IMAP folder -- Y! Conversations
Processing: IMAP folder -- Placements

56 messages analyzed, 56 messages processed.

Processing finished. Time to complete task: 0h 4m 19s 663ms

Use "File/Open/Outlook Data File" in Office Outlook to open your new PST file.
```

☑ Launch Windows Explorer when processing finished
□ Skip filter details in log

Aid4Mail Home Trial v3.2 -- Copyright © 2005-2013 Fookes Holding Ltd, Switzerland

Image 8: Example of processing mail by Add4Mail

The major *disadvantage* of this software is that it can just find keywords which the user search for. It has no artificial intelligence and so is completely a manual software program developed to sort and find mails.

5. CONCLUSION

Digital forensic analysis is a complex and time consuming process which involves the analysis of digital evidence. Emails might contain valuable information that could lead investigators to the identity and/or location of the offender. Additionally, email forensic tools through email header analysis may even reveal information related to the host machine used during the composition of the message. In this paper, we have discussed key information related to email forensic analysis as well as important aspects of header tracing. Finally, we demonstrated two forensic tools that can be utilised for email analysis emphasising on their key features in an effort to assist investigators in the selection of the appropriate tools.

ACKNOWLEDGEMENTS

This research was financially supported by the Ministry of Science and Technological Development of the Republic of Serbia, as part of the TR35026 "Software Environment for the optimal management of the quality software development process" project.

REFERENCES

[1] M. T. Banday, “Analysing E-Mail Headers for Forensic Investigation”, Journal of Digital Forensics, Security and Law, Vol. 6(2), 2011.

[2] M. T. Banday, “Techniques and Tools for Forensic Investigation of E-mail, International Journal of Network Security & Its Applications, Vol. 3, No. 6, 2011.

[3] M. Al-Zarouni, “Tracing E-mail Headers”, Australian Computer, Network & Information Forensics Conference. 2004, pp. 16–30.

[4] Mrityunjay, U. Chauhan, and S. Gupta, “Novel Approach for Email Forensics”, International Journal of Engineering Research & Technology (IJERT), Special Issue 2017.

[5] Lj. Lazic, “E-Mail Forensics: The Case From The Court Practice Of Theft Of Identity”, Conference: ITeO2018, 28. September, Banjaluka, 2018, pp. 368- 383.

The 10th International Conference on Business Information Security (BISEC-2018), 20th October 2018, Belgrade, Serbia

BISEC
BUSINESS INFORMATION SECURITY CONFERENCE

CAN SUPPORT VECTORS DETECT EXPLOITS?

NEMANJA MAČEK
School of Electrical and Computer Engineering of Applied Studies, Belgrade; Graduate School of Computer Sciences, Megatrend University, Belgrade; SECIT Security Consulting; macek.nemanja@gmail.com

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

MILAN GNJATOVIĆ
University of Novi Sad, Faculty of Technical Sciences; milangnjatovic@uns.ac.rs

BRANIMIR TRENKIĆ
School of Electrical and Computer Engineering of Applied Studies, Belgrade; btrenkic@viser.edu.rs

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

ACA ALEKSIĆ
Belgrade Metropolitan University, Faculty of Information Technologies; aca.aleksic@metropolitan.ac.rs

Abstract: *An exploit is software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in operating system or other software products to cause unintended or unanticipated behaviour of computer software, hardware, or other electronic devices. Such behaviour includes actions like unauthorized gaining control of a computer system, unauthorized privilege escalation, or a denial-of-service attack. Although anti-malware products and signature-based intrusion detection systems provide reasonable level of security, they will not detect and prevent execution of new exploits or exploits that tend to evolve, as there is no signature in the anti-malware or intrusion detection database. To raise the overall level of security we have introduced one kernel-based machine learning method, named support vector machines, into an intrusion detection system that is capable of detecting exploits without employing signature database. Experimental evaluation of our solution is conducted on the custom dataset generated in isolated environment.*

Keywords: *Exploits, Machine learning, Support Vector Machines*

1. INTRODUCTION

There is no concise definition of malicious software, frequently referred to as malware in the literature. Malware can roughly be defined as any software intentionally designed with the goal to cause damage to a computer, computer network or anything controlled by a computer system, even industrial power-plants. There are various types of malware, such as computer viruses, worms, Trojan horses, logic bombs, ransomware and cyber-weapons. Malware evolved from early infectious programs, which were written as academic experiments or pranks. Although most of those were typically harmless, they have set a solid ground for development of harmful ones. Today, malware is used by black hats and governments, to steal financial or business information, perform industrial espionage, etc. Further, malware is even used to perform attacks on antagonist country ran industrial plants. One of the first attempts of such activities is the infamous Stuxnet, which was designed to target SCADA systems and is believed to be responsible for causing substantial damage to Iran's nuclear program – over 58% of target system in the early days of infection resides in Iran. Due to the complexity of the malware itself, it is believed that it was built jointly by the United States of America and Israeli government institutions, yet neither country has admitted responsibility for the Stuxnet creation ever since.

Malware does the damage after it is implanted or introduced in some way into a target's computer and can take the form of executable code, scripts, active content, and other software [1]. The authors of malware seek out vulnerabilities in operating systems or computer software, such as buffer-overflow vulnerability that can be exploited. Therefore, one may say that malware is based on exploits, i.e. carefully crafted software chunks that exploit aforementioned vulnerabilities. After exploit is executed on the target system, attacker can take control over the victim, raise privileges, or run the payload attached to the malware, e.g. ransomware encryption module.

A very detailed list of remote exploits, Web application exploits, local and privilege escalation exploits, denial of service and proof of concept exploits is available on Offensive Security's Exploit Database Archive [2]. On July 7, 2018, there were 39,630 exploits archived in the database. Each exploit is very well documented (i.e. which target it exploits, on which platform, who is the author, etc.), and available for free download as source code (in C, Python, Ruby, etc.)

Although this database may help anti-malware software vendors to write signatures that will help the security software detect an exploit, there are two major issues open: (1) will signature based anti-malware software or intrusion detection system detect exploit-based malware that evolves, and (2) will signature based anti-malware software or intrusion detection system detect zero day exploits? The answer to both questions is, unfortunately, negative.

Having that said, simple anti-malware software or intrusion detection system obviously do not provide sufficient level of defense, meaning that there is a need for additional security mechanisms. One way to add another layer of defense is to employ semi-supervised anomaly detection on the host. This process is based on training the learner with normal behavioral patterns. Although applicable in theory, there are several problems with this approach: it is very hard to obtain all records of normal behavior and draw the exact line between normal behavior and anomaly, normal behavior tends to evolve with time, a noise may exist in the data, etc. Having that said, one may conclude that this approach would lead to a large number of false positives, i.e. legitimate activities that are detected as anomalous.

Another approach is to employ supervised machine learning methods, i.e. systems that are trained with both normal and exploitation data. Although this type of security mechanism can be implemented as host-based intrusion detection system, i.e. system that monitors activities like frequency of system calls and critical system infrastructures, one should note that remote exploit works over a network and exploits the security vulnerability without any prior access to the vulnerable system. Having that said, it is necessary to implement this security countermeasure on the network-level, i.e. create a network-based intrusion detection system trained with data containing of labelled network traffic containing both exploits and normal traffic. As a machine learning classification algorithm we have chosen kernel-based method named Support Vector Machines.

2. MACHINE LEARNING IN INTRUSION AND EXPLOITATION DETECTION

Machine learning algorithms independently collect knowledge from the machine readable information, i.e. they learn from data. Such algorithms build a model from training inputs and use it to make decisions, or predictions [3]. Tom Mitchell provided a widely quoted, formal definition of machine learning: “A computer program is said to learn from experience *E* with respect to some class of tasks *T* and performance measure *P*, if its performance at tasks in *T*, as measured by *P*, improves with experience E” [4]. According to this formal definition, an intrusion detection system (IDS), which we employ to detect exploits, learns to classify events (task T); performance measure P of this task is the classification accuracy, and the experience E is the training set. Mitchell states that machine learning is suitable for application in software engineering when it is necessary to extract knowledge from large databases and when a high degree of adaptation to user needs is required. If we take into account the fact that IDS analyses a large set of events and that it is necessary to adapt IDS to the environment it protects, it can be concluded that machine learning is suitable for use in intrusion detection.

There are two types of machine learning algorithms: unsupervised (no "teachers") and supervised (with "teachers"). Unsupervised algorithms learn from unlabelled examples; the objective of unsupervised learning may be to cluster examples together on the basis of their similarity [5]. Unsupervised learning is suitable for finding patterns in the data. 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, on the basis of the trained model. Class labels assigned to instances in data sets that are used to train supervised learning based IDS indicate legitimate activities or certain types of intrusions.

Machine learning methods used for classification can be divided into [6]: basic methods (artificial neural networks [7], Support Vector Machines [8], decision trees [9, 10], naive Bayes [11]), 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 [12]), incremental methods (naive Bayes updatable), hybrid incremental methods (Hoeffding Tree [13]), basic ensembles (Random Forest [14]), hybrid ensembles (stacking) and hybrid incremental ensembles (Ada Hoeffding option tree). There is a large number of studies reported in the literature that investigate the performances of intrusion detection systems with classifiers based on artificial neural networks (multilayer perceptrons and self-organizing maps), Support Vector Machines, decision trees, Random Forest, Bayesian networks, naive Bayes, hidden Markov models, inductive learning, clustering and nearest neighbors. For more details on findings reported in aforementioned literature, reader may consult [15].

One should note that the nature of input data will influence the choice of classifiers. For example, dimensionality of class label will lead to exclusion of linear regression, multiple linear regression and Support Vector Machines (SVMs), while orientation towards creating simple models lead to exclusion of artificial neural network [10].

3. SUPPORT VECTOR MACHINES

Support Vector Machines are linear learning methods that seek out the decision function in the set of functions (hypothesis) that are linear combinations of input values. The data that is not linearly separable in the original input space is cast into high-dimensional feature space where it is linearly separable. The transformation from the input into the feature space increases the expressiveness of linear methods, but also leads to an increased risk of overfitting. The statistical learning theory [16] defines which parameters should be controlled in order to achieve an appropriate level of generalization and reduce the risk of overfitting. Maximum margin classifier does not allow learning examples to be misclassified and can only be used with a data set that is linearly separable in the feature space. This constraint motivated the development of soft-margin classifier [17], a modified maximum margin idea that allows examples to be mislabelled.

Support vector machines can be defined as "(1) learning algorithm that uses linear methods (2) in kernel induced feature space, (3) statistical learning theory to control generalization error and (4) optimization theory to solve convex quadratic programming problem; solving this problem equals learning with SVM."

4. FEATURE SELECTION

Feature selection (e.g. features that describe the network connections in the training set) affects the classifier's performance. Although each feature contains a certain amount of knowledge that has an impact towards detection, two facts should be taken into account when selecting features that will be used to form a training set: (1) some features contribute significantly to the classification accuracy, while the influence of others might be almost negligible; (2) system based on an excessive number of features will most probably be CPU-demanding and practically useless if the network flow is heavy.

IDS can be adapted to detect specific categories of attacks by re-adjusting feature weights. There are several methods that can be used to determine feature weights. One feature weight calculation method is based on that idea: the weight of feature is calculated according to the accuracy change of the classifier trained with a set from which feature is removed, compared to the classifier that takes all features in consideration. Another feature weights calculation method is based on F-score. Based on statistic characteristics, it is independent of the classifiers. F-score is a simple technique that measures the discrimination between a feature and the label. Feature's F-score is a ratio of discrimination between the positive and negative sets and discrimination within each of the two sets. The larger the F-score is, the more likely this feature is more discriminative.

To design a high sensitivity exploit detection system based on support vectors, one should follow these steps: pre-process the data (convert the features and normalize feature values), determine optimal hyper-parameters of the original model (optimal hyper-parameters provide a classifier that will predict unknown data most accurately), train the classifier, calculate feature weights, scale training and test set with feature weights (thus the relevance of features towards classification will be incorporated into a model that is trained in the final training step), determine optimal hyper-parameters of the new model, train the classifier with the scaled training set and finally test it.

5. GENERATING THE DATASET

The dataset used in this research is built from traffic captured on the simulated network, consisting of three computers. One computer was used as attacker, the other one as a Linux router which also captured the network traffic using PCAP library, while the third was used as a victim, running Windows and Linux operating systems and software that was found exploitable on Offensive Security's Exploit Database Archive [2]. Synthetic dataset consists of normal, healthy traffic recorded during one day period and variety of simulated attacks, generated by compiled exploits from Exploit Database Archive, fired up 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 certain incompleteness of the dataset. Since Support Vector Machines operate with numerical data, all features must be converted to numerical (scaled to range [0,1]) without missing values. This leaves a Support Vector Machine learner to be trained and evaluated with incomplete datasets, i.e. with some features removed.

6. PERFORMANCE METRICS

The efficiency of our exploit detection system is given by detection accuracy and false negative rates. True alarm (True Positive, TP) indicates that the system successfully detected the intrusion. False alarm (False Positive, FP) indicates that the system incorrectly identified legitimate activity, recognizing it as an intrusion. Missed alarm (False Negative, FN) indicates that the system incorrectly identified an intrusion, recognizing it as a legitimate activity. True Negative (TN) indicates that the system successfully identified the legitimate activity.

Detection accuracy depends on all positive and negative results of the system and is defined as follows:

$$a = \frac{TP + TN}{TP + TP + FP + FN} \tag{1}$$

False Negative Rate (FNR) is the ratio of false negatives and the sum of true positives and false negatives:

$$FPR = \frac{FP}{TP + FN} = 1 - sensitivity \tag{2}$$

Low incidence of false negative alarms indicates that a small amount of exploits is incorrectly identified as legitimate activities. System with low FNR can be used in critical areas of computer networks where an exploitation attempt may not pass undetected, as it may produce significant damage, while discrimination of legitimate activities can easily be corrected (for example, in a corporate network).

7. EXPERIMENTAL EVALUATION

Performance of the algorithms is experimentally evaluated using MATLAB R2016a with Statistical and Machine Learning Toolbox, version 10.2. Within this research the following algorithms have been evaluated: Support Vector Machines on incomplete dataset and adaptive models based on Support Vectors built by empirical and F-score based re-weighting on incomplete dataset. Training datasets consisting of five thousand instances with 41 features (incomplete) and 54 features (complete) were used for five-fold cross validation. Balanced sets with thousand instances were used as test-sets. Results for each classifier were listed in Table 1 (results of five-fold cross validation) and Table 2 (results on the test set).

Table 1: Five-fold cross validation results (accuracy and false negative rates)

Classifier	Accuracy (%)	FNR (%)
SVM	92.81%	3.39%
SVM (empirical)	94.38%	2.65%
SVM (F-score)	94.76%	2.41%

Table 2: Test results (accuracy and false negative rates)

Classifier	Accuracy (%)	FNR (%)
SVM	89.12%	4.27%
SVM (empirical)	93.67%	3.11%
SVM (F-score)	94.61%	3.07%

5. CONCLUSION

This paper evaluated the possibility of Support Vector Machines to discriminate exploitation code in network traffic from the rest of the data. The dataset for network-based exploit detection was created on the basis of normal, healthy traffic, and exploits, downloaded and run from Offensive Security Database of Exploits. Due to irresolvable incompleteness problem, support vectors were trained with incomplete dataset with several features removed. By boosting feature weights we have managed to increase detection accuracy and reduce false negative rates. However, by doing so, we have introduced adversarial learning issue – overemphasized weights.

REFERENCES

[1] T. Nash, “An Undirected Attack Against Critical Infrastructure, Vulnerability & Risk Assessment Program” (VRAP), Lawrence Livermore National Laboratory, retrieved July 7, 2018.

[2] Offensive Security’s Exploit Database Archive, https://www.exploit-db.com, last time visited October 15, 2018.

[3] M. A. Hall, L. A. Smith, “Practical feature subset selection for machine learning”, In C. McDonald (Ed.), Computer Science ’98 Proceedings of the 21st Australasian Computer Science Conference ACSC’98, Perth, 4-6 February, pp. 181-191, 1998, Berlin: Springer.

[4]. T. Mitchell, “Machine Learning”, McGraw-Hill Science/Engineering/Math, page 2, 1997.

[5] Z. Ghahramani, “Unsupervised Learning”, In Bousquet, O. et al. (Eds.), Machine Learning 2003, LNAI 3176, Springer-Verlag Berlin Heidelberg.

[6] V. Miškovic, 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, pp. VII2.3.1-6, 2014.

[7] S. Haykin, “Neural Networks: A Comprehensive Foundation”, 2nd edition, Prentice Hall, 1998.

[8] V. Shawe-Taylor, N. Cristianini, “Kernel Methods for Pattern Analysis”, Cambridge University Press, 2004.

[9] L. Breiman, J. H. Friedman, R. A. Olshen, C. J. Stone, “Classification and Regression Trees”, Wadsworth, Belmont.

[10] B. Predić, G. Dimić, D. Rančić, P. Štrbac, N. Maček, “Improving Final Grade Prediction Accuracy in Blended Learning Environment Using Voting Ensembles”, Computer Applications in Engineering Education, accepted for publication, in press.

[11] V. Cherkassky, F. M. Mulier, “Learning from Data: Concepts, Theory and Methods”, 2nd ed., John Wiley - IEEE Press, 2007.

[12] R. Kohavi, “Scaling Up the Accuracy of Naive-Bayes Classifiers: A Decision-Tree Hybrid”, In KDD, pp. 202-207, 1996.

[13] 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.

[14] L. Breiman, “Random Forests”, Machine learning, 45(1), pp. 5-32, 2001.

[15] N. Maček, “One class of adaptive network intrusion detection systems”, Doctoral dissertation, Faculty of informatics and computing, Singidunum University, 2013.

[16] V. Vapnik, “Statistical Learning Theory”, John Wiley & Sons, 1998.

[17] C. Cortes, V. Vapnik, “Support-vector networks”, Machine learning, 20(3), pp. 273-297, 1995.

BIOMETRIC SECURITY LEVEL FINGERPRINT vs. IRIS AND FORMING PERIOD AT HUMANS

KOMLEN LALOVIĆ

Visoka škola strukovnih studija za Informacione tehnologije - Beograd, komlen.lalovic@its.edu.rs

TOT IVAN

Univerzitet odbrane, Vojna akademija Beograd, ivan.tot@va.mod.gov.rs

Abstract: *This work present comparative analysis between fingerprint and iris biometrics formed on human kind. It shows in detail advantages and disadvantages both of them and providing science all relevant data when it can be used and acquired to enable top level security.*

Keywords:

Biometrics, Fingerprint, Iris Patent, Pseudo-Code.

I INTRODUCTION

Biometry is scientific discipline and technology that measures and analyzes biological characteristics of people. It is a part of advanced security systems widely used in today's modern society and protection systems.

The highest in persistence in Biometry and the lowest possibility of interrupt data is fingerprint and minutiae, so that the aim of this work and Patent device is that kind of Biometry.

Main difference between fingerprint and iris at humans is forming period and it is various. Fingerprint is formed prenatal before baby is born and iris and pigmentation is formed from 2nd until 4th year at children. This is crucial for understanding security systems that can be created and used based on this two biometric.

II TECHNOLOGY OVERVIEW

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. [8]

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. [5]

In the issued Patent confirmation **П-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. [8]

III DISCUSION

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***[1]). [1]

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 new-born baby. [2]

.

IV ESSENCE OF TWO BIOMETRICS

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] [2] [3]

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 foots 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. [3] [4]

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 (n=32). [6]

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 midwifes 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 PIN[2] code that only they possess for their data. [2] [7]

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 it’s backup copy are always in encrypted form and there is no

[1] **Minutiae** – fingerprint specific points visible on a finger image

[2] **PIN** – Personal Identification Number

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. [6]

It prevents any possible theft or replacing the baby’s identity, which has unfortunately being 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 Heath care system of each Country.

V RESEARCH

Figure 1 shows one of Fingerprint.

Figure 1

As we can see clearly that ridges and valley are made and scanned with one of existing fingerprint scanners. We have various such as: optical, capacitive, thermal, pressure etc. All of them poses its advantages and disadvantages depend on purpose and fingers which is scanned.

Figure 2 shows one of Iris biometrics recognition

Figure 2

We can see that both of the system provides high level of protection by using it. It depends of the purpose and age of humans.

VI FURTHER DEVELOPMENT

Both of the biometric systems have huge potential of making serious security systems, they provide it even today. We can say for sure it will be future of security systems and biometrics development.

VII CONCLUSION

Each Biometry tries to minimize **FAR**[3] and to maximize **FRR**[4] in attempt to be much more accurate and secure. This device has accomplished that part since it combines two scanned data and its accuracy grows exponentially.

Every biometric systems have huge potential of making serious security systems, they provide it even today. We can say for sure that fingerprint and iris recognition will be future of security systems and biometrics development.

REFERENCES

Books:

[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

Articles from Conference Proceedings (published):

[3] Biometric verification of a subject through eye movements, Martti Juhola, Youming Zhang, Jyrki Rasku, Computers in Biology and Medicine, Vol. 43, Issue 1, p42–50, Published in issue: January 01, 2013

[4] Komlen Lalović, Doctoral thesis “New system of identification newborn babies and parenthood guarantee based on Biometry”, University of Singidunum, July 2016.

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

[6] 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*

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

[8] NIST publishes compression guidance for fingerprint, Journal Elsevier - Biometric Technology Today, Volume 2014 Issue 4, April 2014, Pages 12

[3] **FAR** – False Accept Rate

[4] **FRR** – False Reject Rate

LEGISLATIVE ISSUES ANALYTICAL MODELLING FOR DATA SECURITY BREACHES PREVENTION

NIKOLA SARANOV
UnitedLex Ltd., Sofia Bulgaria, nikola.saranov@unitedlex.com

ZLATOGOR MINCHEV
Joint Training Simulation and Analysis Center, Institute of ICT,
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, zlatogor@bas.bg

STOYAN PORYAZOV
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, stoyan@cc.bas.bg

EMILIYA SARANOVA
Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, emiliya@cc.bas.bg

Abstract: *A number of vague terms and uncertainties could be found in the recent data protection legislation, concerning the field of data breaches. Specific interest are opening the issues of qualitative and quantitative understandings of terms like: 'risk to the rights and freedoms of natural persons', 'criteria for data security', 'appropriate technical and organisational measures for data protection'. The paper provides an analytical modelling approach that gives some assessments for achieving a better understanding towards the legal necessities and measures on countering data breaches. The obtained results will provide some practical support to the strategic and operational implementations preventive framework development.*

Keywords: *Data Protection, Data Breaching, Data Security, Analytical Modelling, Preventive Framework Development*

1. INTRODUCTION

For the data breaches prevention process, it is highly important to have a properly built Incident Response and Management Plan, which takes under consideration all the specifics of the business environment and the services or products provided. A workflow-based system for security operations must provide full visibility – from alert collection and escalation, through mitigation, containment, analysis and remediation.

The new conditions in the EU Data Protection Legislation require more and more attention to be paid on creation and implementation of such plan, due to the constantly increasing need of adequate protection of personal data. The undertakings that grant such protection are the so called Technical and Organizational Measures (TOMs).

2. LEGAL REQUIREMENT FOR SECURE DATA PROCESSING

The Federal Data Protection Committee in Switzerland [1] provides appropriate definition of TOMs, separating them in technical on one hand and on the other hand, organizational measures. The Swiss Statutory Supervisor defines the Technical Measures as "those that directly involve IT Systems" and the organizational are "related to the systems environment and particularly to the people using it". The definition is followed by a very important note: "Only an interplay of both types of measures can prevent data to be destroyed or lost and mistakes, fakes and unauthorized access from occurring"

Article 5 (1) (f) from the General Data Protection Regulation (GDPR, EU 679/2016) outlines the meaning of "integrity & confidentiality" of personal data:

"Processed in a manner that ensures appropriate security of the personal data and against accidental loss, destruction or damage, using appropriate TOMs"

This is how the GDPR outlines the requirement for secure processing through using of appropriate Technical and Organizational measures. It is important to outline the difference between the GDPR's personal data security and the Cybersecurity concept for information security.

TOMs are being described as measures for protection of personal data, which is stored within computers and networks. Therefore, from the IT point of view, Technical Measures for data security may be accepted as Cybersecurity. This is complex technical matter, which is constantly evolving, due to the evolution of the complexity of threats and vulnerabilities.

According to the UK's National Cyber Security Center (NCSC) [2], the factors that should be taken into consideration when applying cyber security measures are:

- System security – the security of network and information systems, including those which process personal data;
- Data security – the security of data held within certain system, e. g. ensuring appropriate access controls are in pace and that data is stored securely;
- Online security – the security of your website and any other online service or application;

- Device security – including policies on Bring-Your-Own-Device (BOYD).

It is apparent that GDPR reflects the wide concept of Information Security, but while the Information Security is considered partially as Cybersecurity, it also covers much wider range of security measures, like physical for example. From here, the accent of Information Security is to keep harmless the networks, the devices and the information stored within them, while GDPR's TOMs and its fundamental "Security Principle" are more focused on the specifics of every particular kind of processing of data. The "Security Principle" [3] goes beyond the way you store or transfer information. Every aspect of processing of personal data is covered, not just cyber security. This principle is a warrant to the "confidentiality, integrity and availability" of the data as obligations under GDPR. According to Art. 32 (1), "Security Principle" means the following:

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity of the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk"

This article clearly outlines that when creating a data protection policy within an organization, or when defining and implementing the Technical and Organizational measures, the very first thing to be taken under consideration is the *appropriateness* of the level of security to the risks behind the respective processing. Here GDPR emphases on the level of security of processing with respect to the state of the art and cost of implementation, as well as the nature, scope and purpose of processing.

Therefore, when defining the criteria for data security [4], two pillars laid in the GDPR must always be taken into strong consideration:

- Risk-based approach – the term "risk" can be defined as a "combination of the likelihood of an adverse event (hazard, harm) occurring and of the potential magnitude of the damage caused" (the incident itself, the number of people affected and the severity of the damage for each) [5].
  Considering the aforementioned factors, organizations should understand that the risk-based approach is a quantitative methodology that will not eliminate the risk; however, it will enable the understanding of risks with the aim of mitigating the impact which requires identification of risk factors for the entire information system of the organization, classification of the data and scoring the effectiveness of the incident response plan respectively for every risk per processing activity.
- No one-size-fits-all solutions – GDPR compliance requires comprehensive approach. Organizations analyze which gaps they need to fill to meet the minimum standards. Both technical and organizational measures should be assessed. Specific industries, dealing with large amount of personal data are generally more affected

These pillars on one hand provide freedom of how a company will organize its data processing security measures but leave a gap in defining their *appropriateness*. Hence, the *appropriateness* of the measures taken must be based on the assessment of data security potential risks. This includes the following factors:

- Review of the personal data involved in the processing in order to assess how valuable, sensitive or confidential it is, having in mind the data and information structure implemented in the company systems; state of the art technologies and costs for their implementation; business specifics (transfers; BOYD, etc.)
- The damage or distress that may be caused if the data was compromised, having in mind the potential risk for the freedoms and rights of the natural persons.

Article 33 of the GDPR further refers into Article 34 of the Regulation which states that if the rights and freedoms of the natural persons are threatened majorly, the controller shall communicate in clear and plain language the nature of the personal data breach to the data subject without undue delay. However, the notification to the data subjects is not required if:

- The controller has implemented appropriate technical and organizational protection measures in respect of the personal data affected by the breach (such as encryption);
- The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of individuals is no longer likely to arise;
- It would involve disproportionate effort [6].

3. ANALYSIS AND OPEN LEGAL ISSUES

GDPR has not specifically answered the following questions:

- What would constitute "undue delay" under article 33?
- What are the criteria to determine "feasibility" under article 33?
- What factors would establish "high risk to rights and freedoms of individual" for the purpose of Article 33 and 34?
- What would be considered as "disproportionate effort" under Article 34?

Unfortunately, the GDPR does not give a clear explanation of what is meant under "rights and freedoms of the natural persons". According to Article 1 of the Regulation: (1) This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data. (2) This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

Based on the Chapter 3 from GDPR (Rights of the Data Subjects), a list of rights available when a person or organization collects and records personal details could be outlined:

- Right to be aware of the reasons that require data communication and the ways these data are used;
- Right to free access to all the gathered data and the chance to transfer all of his personal data to other services suppliers (data portability);
- Right to ask for modifications, cancellation or removal of the data, with the same effort that takes to give the consent;
- Right to be informed in case of a personal data breach;
- Right to be sure that all laws are enforced, mainly on data transfer outside the EU [7].

Taking into consideration the term “Freedom”, things are becoming more complicated. Freedom is very complex category, which should be considered only in the context of data protection. The European Convention on Human Rights (ECHR) [8] defines fundamental freedom as: “Those which are the foundation of justice and peace in the world and are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which they depend”.

Article 8 (1) of ECHR states: “Everyone has the right to respect for his private and family life, his home and his correspondence”. In the context of data processing, in Case “Von Hanover vs. Germany” ECHR [9], the court suggests: “Increased vigilance in protecting private life is necessary to contend with the new communication technologies which make it possible to store and reproduce personal data”.

In the EU, the Charter of Fundamental Rights [10], freedoms receive more amplified consideration.

Article 8 “Protection of personal data”:

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

Those principles are laid down in the Treaty on the Functioning of the European Union [11]:

“Article 16 (ex Article 286 TEC)

1. Everyone has the right to the protection of personal data concerning them.

2. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.”

These provide a very brief definitional outline of rights and freedoms as they relate to personal data and requires special consideration when implementing security measures in an organization and eventually responds to a data security incident.

Having these determined, a **Personal Data Security** in the perspective of GDPR could be defined as *referring to all the measures implemented as to protect the characteristics of the processed data (accuracy and precision; legitimacy and validity; reliability and consistency; timeliness and relevance; completeness and comprehensiveness; availability and accessibility; granularity and uniqueness) with respect to the fundamental rights and freedoms of the natural persons as defined in the Data Protection Legislation (GDPR, Chart of Fundamental Rights, The European Convention on Human Rights, etc.).*

Under Directive 95/46EC, data controllers were obliged to notify the processing of personal data to supervisory authorities. This notification obligation was abolished in the new GDPR and was replaced by other mechanisms which are likely to result in a high risk to the rights and freedoms of natural persons, one of these new mechanisms is called Data Protection Impact Assessment.

In order to assess the severity of high data security risks, the data controller is obliged to carry out a DPIA prior to the processing.

Article 35 (1) of the GDPR requires a DPIA only when a processing is “likely to result in a high risk to the rights and freedoms of natural persons”. Article 35 (3) provides a non-exhaustive list of circumstances for which the data controller is required to perform a DPIA. These are particular examples of when DPIA will be required where, when taking into account the nature, scope, context and purposes of the processing, the processing operations is likely to result in high risks to the rights and freedoms of natural persons [12]:

- A systematic and extensive evaluation of personal data based on automated processing including profiling, on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
- Processing, on a large scale, of special categories of data (concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, or data concerning health or data concerning natural person’s sex life or sexual orientation) or of personal data relating to criminal convictions and offences;
- A systematic monitoring of a publicly accessible area on a large scale.

The Article 29 Working Party now clarifies the indicators of high risk. It has published guidelines on DPIAs (the “Guidelines”) [13], following its consultation on a draft version published in 2017. The Guidelines provide nine criteria which should be considered when assessing whether processing operations are likely to result in a high risk to natural persons. For the Article 29 Working Party, a situation only requires a DPIA, if it covers up more than two criteria. Nonetheless this is not an absolute rule, because it is also possible that in a certain situation, one criterion is dominant enough to require a DPIA.

In order to determine whether a DPIA is necessary, due to the inherent high risk of the processing operation, the following criteria should be considered:

- Evaluation or scoring.

The risk of the processing operation is high, when there is a situation of evaluation or scoring and this because of the processing of "aspects concerning the data subject's performance at work, health, economic situation, personal preferences or interests, reliability of behaviour, location or movements" (recitals 71 and 91). This is for example the case for a processing operation in which private companies generating profiles for contract directories use public social media profiles data.

Automated-decision making with legal or similar significant effects: Automated-decisions have legal or similar significant effects on individuals, therefore they constitute a high risk for these individuals. This is for example the case in a process that leads to discrimination against individuals:

- Systematic monitoring;
- Processing sensitive data;
- Data processed on a large scale;
- Datasets matched or combined;
- Data concerning vulnerable data subjects; Applying technological or organizational solution.

The use of a new technology can create the need to carry out a DPIA. It can involve forms of data collection and usage with a high risk to individuals' rights and freedoms and this because of the innovation in technology. This innovation brings development, but the personal and social consequences are unknown:

- Data transfer across borders outside the European Union;
- When the processing prevents that data subjects can exercise a right or use a service/contract.

The consequences of non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA where necessary, carrying out DPIA in an incorrect way, failing to consult the competent supervisory authority where required, are all breaches of the GDPR that could each result in fines of 10 million Euro or up to 2% of the total worldwide annual turnover, whichever is higher. Article 79 sets out the factors authorities must consider when imposing penalties for violations of the GDPR. In all circumstances, the remedy should be "effective, proportionate and dissuasive" [14]. When deciding whether to impose a fine and what amount, the supervisory authority must consider "the degree of responsibility of controller or processor having regard to technical and organizational measures implemented pursuant to Articles 23 and 30". These articles outline the data protection by design and data security requirements, which require controllers to tailor protective measures to the risk of a processing activity.

Recital 75 of the GDPR further identifies processing activities that pose a risk to data subjects. These are activities "where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analyzing or prediction of aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects".

Recital 75 provides general insight into the nature of the harms that the GDPR seeks to avoid. According to the Regulation "harm" is defined as "physical, material or moral damage". It is particularly concerned with processing activities that could lead to "discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorized reversal of pseudonymization, or any other significant economic or social disadvantage".

In Article 4 (2) GDPR provides definition of the term "processing", which is a major part of the data lifecycle:

"processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"

The first vulnerability in the data lifecycle is at the point of data capture, it is essential to prevent incomplete or incorrect data from being captured. During subsequent processing this could result in a misleading picture which in turn, could result in wrong production and decision being made. It is therefore important to develop mechanisms to minimize the risk of errors during the data processing in each of the phases.

The Swiss Data Protection Law provides a clear approach to the organizations in establishing a clear and consistent processing activities plan. The so called Data Processing Policy ensures the necessary transparency in the development and administration of personal data files. Along with the Incident Response Plan, these are the two critical acts each organization must have in place as to ensure not only compliance, but a truly effective organization in regard of personal data processing activities.

Apart of defining the TOMs, the Data Processing Policy summarizes and centralizes the manner of controlling the documents and information produced by the various units conducting the project. It therefore provides the system operators and those in charge of data protection with a complete set of documentation which enables them to look up and apply proven practices of the organization.

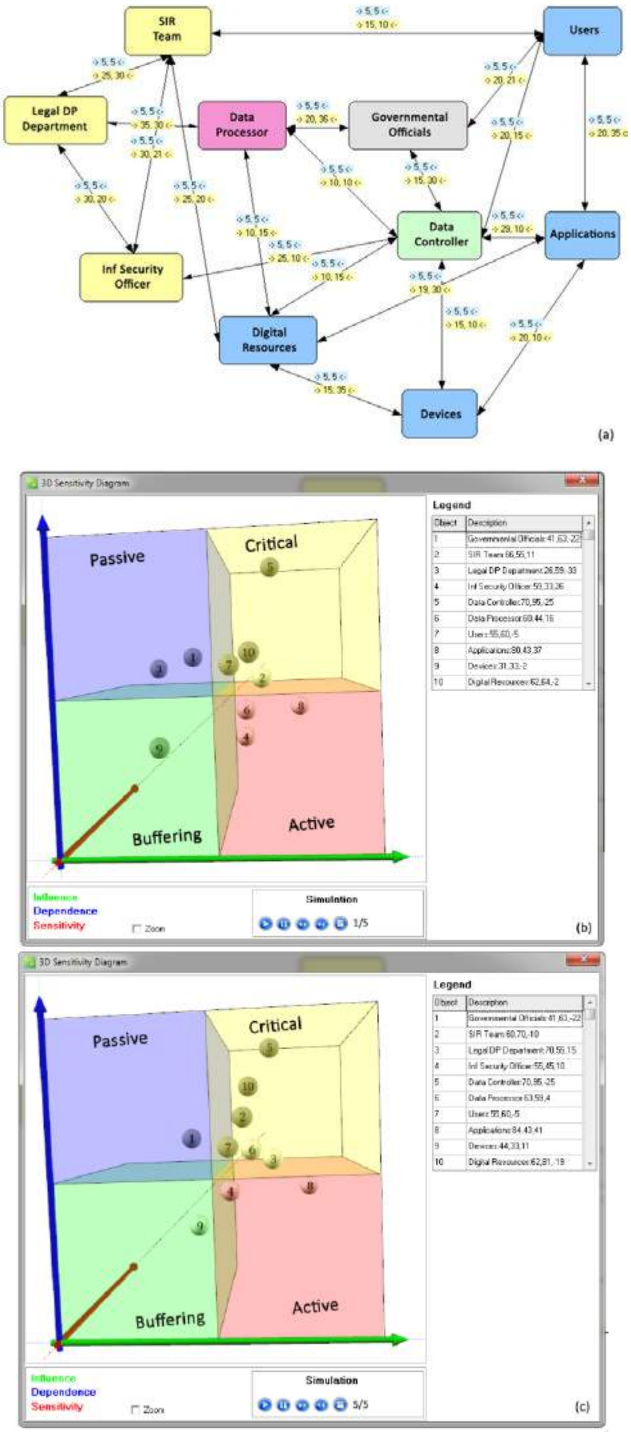
The principle is that the data processing policy must be written by the Data Controller and directly applied to the Data Processing Agreements with the data processing organization, reflecting all requirements of the particular activity and the data protection legislation. It is a well-known truth that the majority of Data Controllers rely on ad-hoc decisions and negotiating the TOMs and the manner of processing and don't have clear and documented position on the matter.

By defining the responsibility of the controller for having Data Processing Policy, the Swiss Data Protection Law differs the individual from federal controller. In the cases where the controller is individual, the requirement depends on the sensitiveness of the data, as well as the entities that will have access to it. In the cases where the controller is a federal body, the content of the processing policy is very precisely defined:

- The internal organization i.e. the operations performed by the system and the organizational structure must be documented. In particular, the various responsibilities (data protection, list of processing etc.) must be listed;
- The documents on the planning implementation and operation of the IT resources must be transparently structured;
- An overview if the Technical and Organizational measure shows which ones have been already taken;
- The origins and processing purpose of the data must be described;
- The reporting obligation is described with all the required information;
- An access matrix to show the organizational units and persons who have access to the data;
- The measures to facilitate the right to information are defined;
- The configuration of the IT resources lists all the software and hardware used.

4. DYNAMIC ENTITY – RELATIONSHIP MODEL OF DATA BREACH RESPONSE

The idea of this section is to present a system model for analytical modeling of data security breaches analysis that will support the identification of possible breaches sources, implementing: legal, organizational and technological aspects of the problem at hand, whilst assessing their sensitivity from a holistic perspective. The working hypothesis is following Vester's interpretation of complex discrete dynamic systems [15], practically incorporated with I-SCIP-SA environment. This solution has numerous proven successful stories during the last 10 years with different problem areas, mainly from the security area [16]. The model is presented in Figure 1a using an Entity-Relationship causality paradigm over a weighted graph with ten nodes and 20 dual arcs. Entities are presented as labeled round rectangles, while relations are uni- or bi-directional headed arrows (noting Influence - forward x relation and Dependence – backward y relation). Sensitivity – z is also calculated via Influence/Dependence ratio, noting both active (positive, white) and passive (negative, light grey) indexed entities.



Legend

Object	Description
1	Governmental Officials:41,63,-22
2	SIR Team:66,55,11
3	Legal DP Department:26,59,-33
4	Inf Security Officer:59,33,26
5	Data Controller:70,95,-25
6	Data Processor:60,44,16
7	Users:55,60,-5
8	Applications:80,43,37
9	Devices:31,33,-2
10	Digital Resources:62,64,-2

Legend

Object	Description
1	Governmental Officials:41,63,-22
2	SIR Team:60,70,-10
3	Legal DP Department:70,55,15
4	Inf Security Officer:55,45,10
5	Data Controller:70,95,-25
6	Data Processor:63,59,4
7	Users:55,60,-5
8	Applications:84,43,41
9	Devices:44,33,11
10	Digital Resources:62,81,-19

Figure 1: E-R causality model for data security breaches analysis (a) and resulting 3D Sensitivity Diagrams, concerning the system states before (b) and after (c) a security breaching incident in I-SCIP-SA environment.

Model relations are weighted either with singular or multiple array values, marked with two separate labels for their number – M (the upper ones, marked with small inscribed blue rectangles, M=5 for the present model, having dynamic representation that is concerning both the moments before and after a security breaching incidents of different type [17], assuming minimal necessity of five-steps handling) and weight – W (the bottom ones, marked with yellow, W is measured in percentages from the interval [0, 1]).

Resulting entities classification is visualized after Influence, Dependence and Sensitivity parameters values in a cubic 3D Sensitivity Diagram (see Figure 1b & Figure 1c), incorporating four sectors: Active, Passive, Critical and Buffering.

The presented model entities are outlining the following allocations before a security data breaching incident (see Figure 1b): Active: 'Inf Security Officer' – 4, 'Data Processor' – 6, 'Applications' – 8, with $z > 0$; Passive: 'Governmental Officials' – 1, 'Legal DP Department' – 3, with $z <0$; Critical: 'Data Controller' – 5, 'Users' – 7, 'Digital Resources' – 10 with $z < 0$ & 'SIR Team' – 2, with $z >0$; Buffering: 'Devices' – 9, with $z <0$.

The resulting entities predispositions after a security data breaching incident (see Figure 1c) could be assumed as follows: Active: 'Inf Security Officer' – 4, 'Applications' – 8, with $z > 0$; Passive: 'Governmental Officials' – 1, with $z <0$; Critical: 'SIR Team' – 2, 'Data Controller' – 5, 'Users' – 7, 'Digital Resources' – 10 with $z < 0$ &, 'Legal DP Department' – 3, 'Data Processor' – 6 with $z >0$; Buffering: 'Devices' – 9, with $z >0$.

5. CONCLUSION

The analysis of the concept "high risk to rights and freedoms of individual" outlined the most valuable considerations, which should be taken into account during the processes of incident responding and addressing number of issues around the risk assessment and creation of organization's policies.

Three more issues in the data breach response and prevention legislation were pointed out and remains to be further clarified. They require deeper consideration in the organization's process setting.

The analysis of the legal requirements for secure data processing resulted in defining the concept of Personal Data Security.

The obtained results from the system analysis are raising generalized attention towards possible data breaches from multiple modern accessed devices, giving critical role to Legal Data Processing Department and Data Processor towards increased active role for the Information Security Officer with SIR Team negative balance and slightly changed significance for the Digital Resources securing. This illustrates the need of more precision and extensive regulation of the crucial and active roles in the context of personal data breach response.

REFERENCES

[1] The Federal Data Protection and Information Commissioner (FDPIC) Switzerland, "A Guide for Technical and Organizational Measures", August 2015, pp. 11-12

[2] Information Commissioner Office (ICO) UK, "Guide to the General Data Protection Regulation", Security, 2018

[3] National Cyber Security Center (NCSC) UK, "GDPR Security Outcomes", 2018

[4] G. Maldov, "The Risk-Based Approach in the GDPR", IAPP 2018

[5] F. Blanc, & E. Franco-Temple, "Introducing a Risk-Based Approach to Regulate Businesses", World Bank Group, 2014

[6] Data Protection: Better Rules for Small Business, https://ec.europa.eu/justice/smedataprotect/index_en.htm#mobile-menu

[7] M. O'Dwyer, "GDPR Data Breach: Rights and Freedoms of a Natural Person", DataLex Consultancy, 2018

[8] "Convention for the Protection of Human Rights and Fundamental Freedoms", Rome, 1950

[9] "Von Hannover v. Germany" 59320/00 [2004] ECHR, 294, 2004

[10] "Charter of Fundamental Rights of the European Union", 2012/ C326/02

[11] Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the EU, Official Journal C326, 26.10.2012

[12] Y. S. Sype, & M. Sudnik, "When to Perform a Data Protection Impact Assessment", KU Leuven, 2017

[13] Article 29 Data Protection Working Party, "GDPR Guidelines on Data Protection Impact Assessment", 2017

[14] M. Staples, & J. Adams, "Privacy and Data Security Due Diligence", 2015

[15] F. Vester, "The Art of Interconnected Thinking – Ideas and Tools for Dealing with Complexity", München: MCB – Verlag, 2007

[16] 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

[17] 2018 Data Breach Investigations Report, Verizon, https://www.verizonenterprise.com/verizon-insights-lab/dbir/

The 10th International Conference on Business Information Security (BISEC-2018), 20th October 2018, Belgrade, Serbia

BUSINESS INFORMATION SECURITY CONFERENCE

ROLE OF THE BIG DATA IN DIGITAL MARKETING – CONTEXT OF THE SECURITY FRAMEWORK

MILOŠ JOVANOVIĆ
OpenLink Global Ltd., London, United Kingdom, milos.jovanovic@openlinkgroup.com

UROŠ PINTERIČ
Faculty of Organisation Studies in Novo Mesto, Novo Mesto, Slovenia, uros.pinteric@fos-unm.si

DRAGAN VALENTIROVIĆ
Faculty of Mechanical Engineering, University of Belgrade, Belgrade, Serbia, dvalentirovic@gmail.com

DRAGAN MITIĆ
Belgrade Metropolitan University, Faculty of Information Technology, Belgrade, Serbia, miticdjd@gmail.com

MILOŠ MILAŠINOVIĆ
Faculty of Technical Sciences, University of Novi Sad, Novi Sad, Serbia, misalin333@gmail.com

Abstract: *This work brings the research on digital marketing especially the new, an evolving branch that is changing the way marketing works; the big data and security in those area. One of the research questions was the correlation between companies marketing success and their big data usage. We present a review of applicable examples and tips of beneficial use in digital marketing. The main goal of this paper is to introduce us to big data and the good and bad sides of its influence on digital marketing. We reviewed current big data strategies, their advantages and disadvantages compared to common data, and their applicability in digital marketing. We analyzed and suggested processes and tools that could personalize the process of customer interactions, predict the future trends and enhance the loyalty of customers. Finally, we also suggest methods and tools which could possibly help businesses reach their marketing glance.*

Keywords: *Big Data, Digital Marketing, Analytics, Customers, Extraction, Personalization*

1. INTRODUCTION

Big data offers a possibility to collect all the data from the past work, to perceive past trends, and also to predict future ones. It is helping to understand the customer's behavior as well as to create opportunities for financial growth. We live in a digital era where everybody is connected. Smart gadgets, online carts/shopping, smart TVs, laptops, desktop computers, social networks, apps on cellphones and tablets are now a part of everyday life. Results of B2V predictive analytics technology forecast say that 36.8% of world high-growth companies are planning to invest in predictive analytics so they can successfully manage their marketing and sales campaigns.

Most of the companies are not introduced to this concept of digital marketing. This paper is bringing both theoretical and practical knowledge that can be implemented to increase user awareness and product sales. In addition to the increased number of competitors, companies must establish certain leverages which will bring them on top. Big data is providing an enormous amount of information by location, social networks, web, businesses etc. And it is all up to the companies and marketers on how they will use it. In order to make it simple and consume all the goods that big data provides and use it in marketing, it needs to be understood. The challenges and problems of big data are still backing companies to change their marketing strategies, but this paper also gives the exact guidelines and solutions to the main problems and concerns.

According to Advanced Performance Institute, from the very beginning till 2000 B.C., people produced information equivalent to information that we now produce in one minute. Companies are collecting data in order to improve their digital marketing. Taking the guesswork from the equation allows them to detect future trends and use them to make a targeted campaign. This gives them insights into important industry plan-points and new trends, whereby giving them a chance to preset and model their products or service towards better satisfaction of their customer's needs.

2. BACKGROUND

About Big Data and Digital Marketing

Big data is becoming essential for effective daily business performance. [1] Online sources are an invaluable asset for firms that have to collect/extract and process everything usable. This data includes information from user's social activities, web engine searches, online transactions, and other data. It is a large group of data that is analyzed to deliver results of current discovery.

Big data is playing a crucial role in companies digital marketing strategies and helps enterprises elevate their customer's behavior. Collecting, analyzing and maintaining big data will make marketing strategic decisions more accurate and precise. In addition to the ability to appoint the customer on large scale, big data can also be used to identify pertinent patterns of customer's behavior and create personalized campaigns on the individual level. Big data revamped the entire activity of sales and helped marketers to form more effective marketing strategies and models for their firms. [2]

Data Is Not Usable in Its Raw Form

Raw data is the data that has the potential to become information but has not been processed yet. The amount of memory of big data is presented in petabytes and exabytes, and the problem is how to extract meaningful information from that amount of data. The algorithm is to break this data into smaller pieces which are processed simultaneously in order to make the most effective decisions. The information being generated from big data can be extracted from few different sources and techniques.

There Is a Couple of Resources to Obtain Data

Data extracted from the web, for example, is the process that contains the compilation of data gathered by mining the web. This includes processes of discovering and extracting information from websites and servers, mining of unstructured data, server logs, browser activity or information extracted from the links and structure of the site. Data extracted from social networks through user's preferences, likes, shares, and comments, or the one gathered from the crowdsourcing, compiled from multiple sources like forums, surveys, pools and other types of user-generated media, provides a wide range of information about user's habits and needs. Companies conducting business create valuable data, financial, logistical or any business-related process involving certain activities such as purchases, requests, insurance claims, deposits, withdraws, flight reservations, credit card purchases, that can be used in a wide spectrum of marketing plans and strategies. However, the largest amount of data comes from the mobile phones. Constant progress of the smartphones helps the app to become more powerful so that more and more apps are gathering user information. Working in as the background service, apps collect our location, check-ins, e-mail addresses and other personals information.

3. THE CURRENT ROLE

Big Data in Predictive Analytics Have a Big Influence

Predictive analytics predict future events based on identified meaningful patterns of big data and estimate the allure of distinct options. Predictive analytics can be practiced on any type of unknown or unstructured data. Every aspect of a business that involves customers could benefit from big data: targeting in marketing, customer segmentation, recognition of the sales opportunities as well as business intelligence in general. The benefits of predictive analytics are having a stable, robust and flexible analytics model in place whereby assisting marketers to achieve the following benefits. In addition to regression analysis, predictive analytics also uses data mining and machine learning algorithms. Data mining is exactly what is important for analyzing large data sets, discovering common rules (patterns) and opening up and expanding new information we get from data. In addition, machine learning and innovation in the field of deep learning especially, open up significant opportunities when it comes to more precision analysis. By using sophisticated algorithms and neural networks, it is possible to analyze unformed and unstructured data sets considerably and much faster than using conventional methods, also with greater precision and with the possibility of making more precise conclusions in the end. It is quite clear that advancements in the development of solutions that enable increasing the accuracy of the information we receive during the analysis are essentially and the most important for the success of the digital marketing campaigns, generally speaking. The research reports that the top uses for big data in digital marketing include:

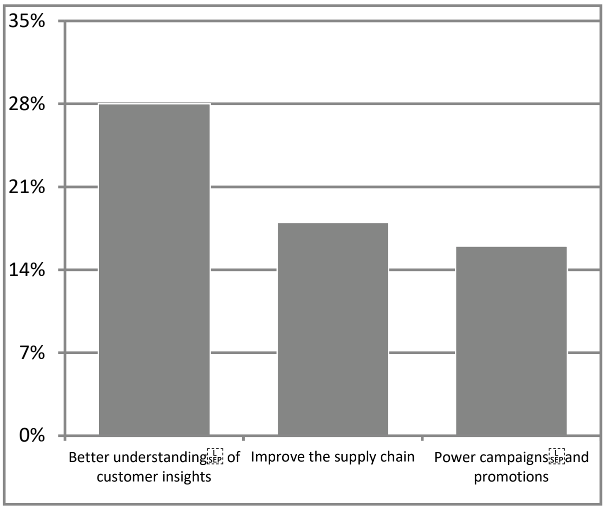


Fig. 1: Top uses for big data in digital marketing include [3] (values are presented in percentages)

Data Visualization Tools and Its Benefits

Data visualization tools are used to acquire given data and derive actionable insight. These may include investments, changes in shopping intervals and customer behaviors and desires. They help you to identify new patterns and trends and connect these discoveries with the decision makers. In addition, data visualization tools can understand and evaluate the results of data analyzing the process. [4] Visualization tactics include applications that can display real-time changes and more illustrative graphics, including personalization and animation. Data visualization has the ability to display unexpected findings in a clear and understandable manner. Those findings can separate companies from the competition and can be highly profitable. Advantages of data visualization and functional insights are that teams for customer relations can now read the data and can easier come to the desirable decisions. These decisions bring companies more customers and profit and are based on collective work and knowledge gathered to make compelling business improvements. [5]

Data Can Help You Plan for the Future

Analyzing data from the past can show you what marketing campaigns are working, which products are most popular, who's buying, when and how. Exploring analyzed data can show you what products are the most wanted and how to make more money. Data is in the past, but the strategy is in the future. Creating a strategy is taking results from the gathered data, making a plan and analyzing the outcome. Analyzing data without creating a plan of action is a waste of time. Using the approach driven by the data, marketers can analyze what's worked in the past so that they can make better decisions moving forward. Based on this obtained insight, they can plan their future marketing strategies and actions with a certain level of confidence. Especially important for constantly changing business offers that are trying to be more customer oriented. As a marketer, being data discerning is the only way to remain relevant in the digital marketing landscape. [6] Albeit the progress will seem rather slow in the beginning, companies willing to invest in big data and its visualization tools will gain, not only in profit but also in clients' satisfaction.

Real-Time Customer Experience Analytics Helps You Acquire More Clients

Clients' data analysis helps marketers to better respond to their demands and habits changes. Thanks to this, they can improve overall customer experience with their business. Considering every company and business, their eventual goal is to improve the customer experience and those customers are free to leave whenever they want to. Larger the company, larger the database and the amount of data they need to deal with. For these businesses, they face a challenge in making sense of huge amounts of data stored by the business and to know what to use and what to ignore. Data visualization software is used to illustrate relationships between data from various sources, mostly visualized through graphs, charts, and bars. This information can be the amount of time a user spent on site, a number of pages they visited or relevance of the next site they entered. It makes pages and sites easier to navigate and helps companies to create a happy and loyal clientele. Also assists marketers in making better strategies and advance user engagement. [7]

Customer Intelligence Optimization

Customer intelligence represents the collection of customer data which is analyzed to help businesses to interact with each customer in the best way possible. Digital era allows companies to gather customers' shared information whenever they reach out to their business: costumers needs, their interests, their wants. If marketers find ways to benefit from this data, they will be able to communicate with customers that every one of them feels like he is the only one and the one that matters them the most. This keeps the costumers loyal, develop better relationships, encourages clients to recommend the company and increase customers spends. There are few fundamental steps to a successful customer intelligence. The first step is the ability to efficiently and effectively gather the customer data into a unique repository that allow you to inspect it and interpret it. The second one is the infrastructure needed to inspect the data for the actionable insights. At the lowest level is the grouping the customers into categorized groups while some advanced technologies include customer behavior, predictive customer analytics, and machine learning. The third one is the skill to make the actions based on the analysis and to scope the results in order to improve future actions. [8] Combining predictive analytics with gathered clients' data helps companies build optimized experiences for each customer. Predictive analytics use reverse engineering, the processes of extracting knowledge or design information from anything made by customers and their past experience. The action is taken to pinpoint the exact marketing strategy and to take the right marketing initiatives. It gives marketers insights into industry convenience points and new trends that are budding and gives them the opportunity to tweak and model their product or service to suit the customer's requirements.

Data Analytics Does Not Have to Be Complex or Expensive

Apart from offering database management solutions, many remote service providers are now looking to offer data analytics as a service (DaaS). This is ideal for smaller businesses that also have large amounts of data but cannot afford the cash outlay required to purchase analytics tools and licenses. [9] This can be done through remote service applications, which allow clients to leverage various analytical tools on their data and pay according to data volumes processed. This can be also used to take advantage of interactive dashboards that are easier read by not-so technically skilled team members and help them get the insights they need from a data store. Data will, therefore, be hosted and reviewed remotely, and businesses receive login details allowing various levels of access according to permissions that are needed. Online data is the fuel that powers any successful digital marketing campaign. While marketing teams may already possess some offline data — purchaser names and addresses for instance — it pays off to consider that digital marketing channels are cheaper in the long term, especially if they make correct use of channels like email. There are also other forms of digital marketing, such as paid search, search engine optimization, and content marketing, and these have grown in popularity over the last few years. Marketing teams must be comfortable with every online marketing channel. This implies learning to use non-conventional data sources, such as search information, client transactions, social posts and other big data sources available online.

4. CHALLENGES, IMPACT, AND SECURITY

Challenges

Although using big data is looking like it lacks disadvantages, there is also the other side which brings some problems with it. Lots of collected data can be incomplete or invalid. Still, lots of companies use that kind of data and that makes them spend more time and money on sorting, storage, and maintenance the data. The problem with unreliable data is that it doesn't give you the right insights that provide value and you start falling behind the competition. This also contributes to the increase of security risk by not being able to distinguish the good data from the bad or outdated one. After the marketers separate the data, still there is a problem of their internal experience that they cannot draw insights from the data. Poorly interpreted data patterns and wrong connections and linking can lead marketers to bad conclusions. Sometimes analysts can be predetermined about what they are looking for, so they ignore real data insights that go against their expectations. Big data technology is still growing, and the marketers are still learning. There is a short supply of skilled data analysts and a company's profit increase is directly connected to them. Marketers are still not fully aware what data to gather. There are still not enough people capable of using this trend to its full potential. [10] Big data is growing at a stable rate and there is still a lot of unexplored markets, but lack of skill and a lot of analytic tools are the reasons why marketers are still refraining to get into big data analytics. There is also an internet problem because online ads costs are rapidly increasing.

Security in Nowadays

With the globalization of the internet and e-business, people are getting a lot of money by digital marketing and online product placement, so naturally, the online sites and social networks want their piece of that cake. Also, there is a problem that automatically implies to an answer. We are under-using our GPS location. Lots of people associate "local" with small business, but the location is all about getting customer behavior and measuring the difference between company's data and clients' actual location. Companies can use that to target-messages to purchasers at that specific location. [11] We can add one of the most recent cases to this: Facebook–Cambridge Analytica data scandal. It is known that Cambridge Analytica, firm that worked with Donald Trump's election team and the winning Brexit campaign harvested millions of Facebook profiles of US voters, in one of the tech giant's biggest ever data breaches, and used them to build a powerful software program to predict and influence choices at the ballot box. The data was collected through an app called thisisyourdigitallife, built by academic Aleksandr Kogan, separately from his work at Cambridge University. Through his company Global Science Research (GSR), in collaboration with Cambridge Analytica, hundreds of thousands of users were paid to take a personality test and agreed to have their data collected for academic use. However, the app also collected the information of the test-takers' Facebook friends, leading to the accumulation of a data pool tens of millions-strong. This big and recent example shows how the bid data sphere is sensitive, and how many citizens are poorly protected, and besides caution, there is little leftover. At the same time, laws that better describe such cases must be in correlation with the most expensive thing that businesses and users possess: trust.

The Impact Is Huge

The goal is to minimize the costs by switching from the traditional offline to online marketing, or a mix of both because customers move seamlessly across online and offline channels. The customers are right targeted more personally, the cost per unique client is decreased and it will lead to an increase in product sales. Marketers nowadays are crowded with information and there is so much data available, from all kind of sources. All this data should be utilized to inform marketers about client's behaviors and needs. There is a huge opportunity in cross-channel communications that should be used to increase relevancy to marketers. The ultimate goal is to build a deep and enduring relationship with clients over time. Every client needs to have personalized service and be given the exact information that it needs. But to improve that, marketers must evaluate an entire users' journeys and identify the points that can drive desired outcomes like additional sales, renewals, upsells, reviews or however they measure success. That can only be possible if they personalize every channel possible. Marketers need to find and satisfy those loyal users and not treat all customers the same. If done right, it will elicit the same loyalty and form a deeper relationship over time. Website personalization can be as personal as your email. Using real-time personalization tools, marketers can show personalized content even to anonymous visitors. [12]

5. CONCLUSION

Being able to target an audience made up of highly-qualified and purchase-ready prospects (and easily build them into loyal clients by anticipating their needs and hence offering true value) is the greatest goal of every marketing campaign. You can actually capture the attention of patrons looking at competitors' products/services in real-time by leveraging unique data sources. However, there is a long way to go and a lot of world scientists and marketers do not believe that big data can improve your digital marketing campaign or your business. The worlds ethical problem with adopting something new is present here as well so the great number of companies still rely on small and agile data. Also, there can be a common mistake in the understanding that having more data will deliver more client value. Well, it is not that simple. New value results from insights into customers, developing a strong relationship with them and understanding the true value and the potential in each of them. Proactively using this insight and treating each of them more personally is a real clients' value from the big data. Making the profiles of rich purchasers and tracking their response rates, marketing agents know exactly what to show and how will that affect certain segments of business in order to come to the best result possible. This also helps the companies cut down on research time and concentrate on a marketing branch with the best results. Massive marketing campaigns are costing companies lots of money and in lots of cases; they do not bring the expected results. Finding the right clientele allows marketers to do the right campaigns on the right people, thereby saving time and money. Ultimately, the value and effectiveness of big data depend on the human operators tasked with understanding the data and formulating the proper queries to direct big data projects. They must be able to extract the valuable data and need to have enough expertise to use and process that data. This helps the companies to scale the knowledge from the data analysis by making it more available. The process of using big data in digital marketing needs to be fluid and continuous – just because it was done once in the desired outcome, does not mean it should stop being used. The whole process should take time, thought and effort if you want to analyze and integrate it into your marketing campaigns the right way. What is relevant to clients, stakeholders, and business today may not be tomorrow. Constant progress and personalization with the user are the key elements to survive and succeed in these uncertain times. Big data is allowing us to listen to the clients' behaviors and needs, to build a deep and enduring relationship with the clients and to provide them an all-channel personalization that brings us a step ahead of the competition. Finally, given that users around the world generate extremely large amounts of data on a daily basis, and that this data is stored on different infrastructure and servers around the world, it is necessary to emphasize the importance of Big Data technology as a fundamental factor in the process of creating new information and hence knowledge. It should be mentioning possible troubles. For the company itself the damage is reflected in the loss of confidence (an example: Italy's UniCredit has stopped using Facebook for advertising and marketing campaigns until the U.S. giant improves its ethical standards [13]), the fall on the stock market, which in total makes a huge financial loss. But, perhaps more importantly, such events are brave those who want to abuse the sensitivity of our activities and trust among the citizens and companies that store their data for their own benefit. However, the dangers for citizens are even more serious. Troubles are manifested in the theft of personal, economic and any other important data that can be used for a wide range of abuses: from fraud to the formation of political discourse (which may be the most lucrative, since the citizen can be difficult to be aware of and caution enough to recognize this kind of manipulation.Precise analyses and application of appropriate analytical techniques can be highly reliable with an extremely important tool in the field of digital marketing. Bearing in mind the situation on a global level, especially when it comes to digital marketing and political campaigns, as well as the tendency of technology development, it is clear that good data analysis must lead to good decisions in terms of digital strategy. What certainly is a challenge is data privacy and data security in the context of complex big data analysis, as well as client confidence. It is necessary to take into account the legal framework that enables data analysis, but also the protection of clients whose data are analyzed.

REFERENCES

[1] SAS Insights, US, "Big Data Analytics — What it is and why it matters?". Retrieved from https://www.sas.com/en_us/insights/analytics/big-data-analytics.html

[2] [x]cubeLabs, "How Is Big data Influencing Digital Marketing Strategy?", Nov. 2017. Retrieved from https://www.xcubelabs.com/our-blog/how-is-big-data-influencing-digital-marketing-strategy/

[3] 2nd Watch Survey: "Big Data, IoT and Cloud Are Driving Digital Marketing", Jul. 2015

[4] Tom Soukup, Ian Davidson, "Visual data mining: techniques and tools for data visualization and mining", Canada: Wiley Computer Publishing, 2002

[5] D. Weisberg, *Think with Google*, "From Data to Insights: The Blueprint for Your Business", September 2014. Retrieved from https://www.thinkwithgoogle.com/marketing-resources/data-measurement/data-to-insights-blueprint-for-your-business/

[6] Dun & Bradstreet, *NetProspex*, Annual B2B Marketing Data Benchmark Report, "The State of Marketing Data", 2015

[7] P. Zikopoulos, C. Eaton, *IBM*, "Understanding Big Data: Analytics for Enterprise Class Hadoop and Streaming Data", 1st ed., McGraw-Hill, 2011

[8] *Optimove*, "Customer Intelligence", Jun. 2018. Retrieved from https://www.optimove.com/learning-center/customer-intelligence

[9] B. Marr, "The Next Big Thing In Big Data: BDaaS", Jul. 2015, LinkedIn.

[10] A. Gandomi, "Beyond the hype: Big data concepts, methods, and analytics", International Journal of Information Management, vol. 35, Apr. 2015, pp. 137-144.

[11] C. L. P. Chen, C. Y. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on Big Data", Information Sciences, vol 275, Aug. 2014, pp. 314-347.

[12] Kimberly Collins: "How to derive value from big data for customer relationship management", Gartner, Feb. 2013

[13] J. Mann, "UniCredit has stopped using Facebook for advertising: CEO", Aug. 2018. Retrieved from https://www.reuters.com/article/us-facebook-unicredit/unicredit-has-stopped-using-facebook-for-advertising-ceo-idUSKBN1KS1N5

SECURITY EVALUATION OF CANCELABLE BIOMETRICS

NEMANJA MAČEK
School of Electrical and Computer Engineering of Applied Studies, Belgrade; Graduate School of Computer Sciences, Megatrend University, Belgrade; SECIT Security Consulting; macek.nemanja@gmail.com

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

MILAN GNJATOVIĆ
University of Novi Sad, Faculty of Technical Sciences; milangnjatovic@uns.ac.rs

BRANIMIR TRENKIĆ
School of Electrical and Computer Engineering of Applied Studies, Belgrade; btrenkic@viser.edu.rs

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

Abstract: *Like any personal information, biometric templates can be intercepted, stolen, replayed or altered. Due to non-revocability of biometric data aforementioned attacks and may lead to identity theft. Having that said, it becomes clear that biometric systems operate with sensitive personal information and that biometric template security and privacy are important issues one should address while designing authentication systems. One approach to biometric template security and privacy is cancelable biometrics. Two main categories of cancelable biometrics can be distinguished: intentional distortion of biometric features with non-invertible transformations and biometric salting. State of the art approaches to cancelable biometrics are presented in this paper, as well as security evaluation of cancelable biometrics.*

Keywords: *Security, Cancelable Biometrics, Non-Invertible Transformations, Biometric Salting*

1. INTRODUCTION

“Cancelable biometrics consist of intentional, repeatable distortions of biometric signals based on transformations which provide a comparison of biometric templates in the transformed domain“ [1]. The inversion of such transformed biometric templates must not be feasible for potential imposters. In contrast to templates protected by standard encryption algorithms, transformed templates are never decrypted since the comparison of biometric templates is performed in transformed space which is the very essence of cancelable biometrics. The application of transformations provides irreversibility and unlinkability of biometric templates [2].

Cancelable biometric transformations are designed in a way that it should be computationally hard to recover the original biometric data. The intrinsic strength (individuality) of biometric characteristics should not be reduced applying transformations (constraint on FAR) while on the other hand transformations should be tolerant to intra-class variation (constraint on false rejection rate) [1]. In addition, correlation of several transformed templates must not reveal any information about the original biometrics (unlinkability). In case transformed biometric data are compromised, transformation parameters are changed, i.e., the biometric template is updated. To prevent impostors from tracking subjects by cross-matching databases it is suggested to apply different transformations for different applications.

Two main categories of cancelable biometrics are non-invertible transformations and biometric salting [3].

2. NON-INVERTIBLE TRANSFORMATIONS

Biometric data are transformed applying a non-invertible function. Image 1 depicts application of non-invertible transformation in face recognition process.

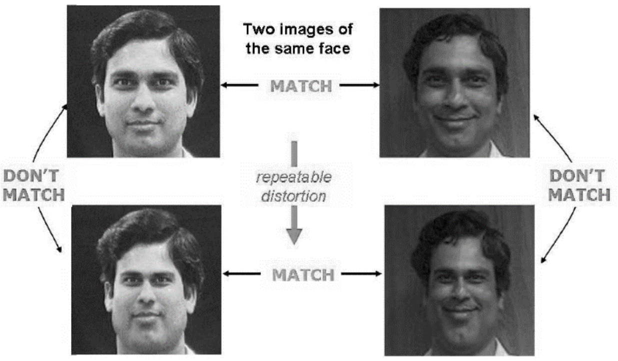


Image 1: Applying non-invertible transformation in face recognition (original image can be found in [4])

In order to provide updatable templates, parameters of the applied transformations are modified. The advantage of applying non-invertible transformations is that potential impostors are not able to reconstruct the entire biometric data even if transforms are compromised. However, applying non-invertible transformations mostly implies a loss of accuracy. Performance decrease is caused by the fact that transformed biometric templates are difficult to align (like in biometric cryptosystems) in order to perform a proper comparison and, in addition, information is reduced. For several approaches these effects have been observed [1, 5].

Ratha et al. [1] were the first to introduce the concept of cancelable biometrics applying non-invertible transformations. Generally, at enrollment, non-invertible transformatioms are applied to biometric inputs choosing application-dependent parameters. During authentication, biometric inputs are transformed and a comparison of transformed templates is performed.

Several types of transformations for constructing multiple cancelable biometrics from pre-aligned fingerprints and face biometrics have been introduced in [1, 4, 6] including Cartesian transform and functional transform. In further work [5], different techniques to create cancelable iris biometrics have been proposed. The authors suggest four different transforms applied in image and feature domain where only small performance drops are reported.

Hammerle-Uhl et al. [7] applied classic transformations suggested in [1] to iris biometrics. Furthermore, in [8] it is shown that applying both transformations to rectangular iris images, prior to preprocessing, does not work. Similar to [7] Rathgeb and Uhl [9] suggest to apply row permutations to iris-codes.

Maiorana et al. [10-12] apply non-invertible transformations to obtain cancelable templates from online signatures. In their approach, biometric templates, which represent a set of temporal sequences, are split into non-overlapping sequences of signature features according to a random vector which provides revocability. Subsequently, the transformed template is generated through linear convolution of sequences. The complexity of reconstructing the original data from the transformed template is computationally as hard as random guessing.

Boult et al. [13, 14] proposed cryptographically secure bio-tokens which they applied to face and fingerprints. In order to enhance security in biometric systems, bio-tokens, which they refer to as Biotope™, are adopted to existing recognition schemes (e.g., PCA for face).

3. BIOMETRIC SALTING

Biometric salting usually denotes transforms of biometric templates which are selected to be invertible. Any invertible transform of biometric feature vector elements represents an approach to biometric salting even if biometric templates have been extracted in a way that it is not feasible to reconstruct the original biometric signal [15]. As a consequence, the parameters of the transform have to be kept secret. In case user-specific transforms are applied, the parameters of the transform (which can be seen as a secret seed [16] have to be presented at each authentication. Impostors may be able to recover the original biometric template in case transform parameters are compromised, causing a potential performance decrease of the system in case underlying biometric algorithms do not provide high accuracy without secret transforms. While approaches to biometric salting may maintain the recognition performance of biometric systems non-invertible transforms provide higher security [4].

Savvides et al. [15] generate cancelable face biometrics by applying so-called minimum average correlation filters which provide non-invertibility. User-specific secret personal identification numbers (PINs) serve as seed for a random basis for the filters similar to [17].

Another approach to biometric salting was presented by Wang and Plataniotis [18] in which face features are transformed based on a secret key. Non-invertibility is achieved by means of quantization.

Ouda et al. [19, 20] propose a technique to obtain cancellable iris-codes. Out of several enrollment templates a vector of consistent bits (BioCode) and their positions are extracted. Revocability is provided by encoding the Bio-Code according to a selected random seed. Pillai et al. [21] achieve cancelable iris templates by applying sector random projection to iris images. Recognition performance is only maintained if user-specific random matrices are applied.

4. PERFORMANCE IMPLICATIONS

While in the majority of proposed approaches to cancellable biometrics template alignment is non-trivial and applied transformations are selected to be non-invertible, still some schemes [22, 16] report an increase in performance. In case user-specific transforms are applied at enrolment and authentication, by definition, two-factor authentication is yielded which may increase the security but does not affect the accuracy of biometric authentication.

A significant increase of recognition rates can be caused by unpractical assumptions during performance evaluations. If user-specific transforms are applied to achieve cancellable biometric these transforms have to be considered compromised during inter-class comparisons. Otherwise, biometrics becomes meaningless as the system could rely on secret tokens parameters without any risk [23]. Secret tokens, be it transform parameters, random numbers or any kind of passwords are easily compromised and must not be considered secure [24]. Thus, performance evaluations of approaches to cancellable biometrics have to be performed under the so-called “stolen-token scenario” where each impostor is in possession of valid secret tokens.

5. SECURITY EVALUATION

While in the vast majority of approaches, security is put on a level with obtained recognition accuracy according to a reference system, analysis with respect to irreversibility and unlinkability is rarely done. According to irreversibility, i.e., the possibility of inverting applied transformations to obtain the original biometric template, applied feature transformations have to be analysed in detail. For instance, if (invertible) block permutation of biometric data (e.g., fingerprints in [4] or iris in [7]) is utilized to generate cancelable templates the computational effort of reconstructing (parts of) the original biometric data has to be estimated. While for some approaches, analysis of irreversibility appear straight forward for others more sophisticated studies are required (e.g., in [11] irreversibility relies on the difficulty in solving a blind deconvolution problem).

In order to provide renewability of protected biometric templates, applied feature transformations are performed based on distinct parameters, i.e., employed parameters define a finite key space (which is rarely reported). In general, protected templates differ more as more distant the respective transformation parameters are [12]. To satisfy the property of unlinkability, different transformed templates, generated from a single biometric template applying different parameters, have to appear random to themselves (like templates of different subjects), i.e., the amount of applicable parameters (key space) is limited by the requirement of unlinkability.

The aim of attacking cancellable biometric systems is to expose the secret transformation (and parameters) applied to biometric templates. Thereby potential attackers are able to apply substitution attacks. If transforms are considered invertible, original biometric templates may be reconstructed. Since most approaches to biometric salting become highly vulnerable in case secret tokens are stolen [23], false accept attacks could be effectively applied. If the salting process is invertible, templates may be reconstructed and applied in masquerade attacks.

5. CONCLUSION

Cancelable biometrics is expected to increase the confidence in biometric authentication systems (trusted identification). This technology permanently protects biometric templates against unauthorized access or disclosure by providing biometric comparisons in the encrypted domain, preserving the privacy of biometric characteristics [25]. Cancelable biometrics keep biometric templates confidential meeting security requirements of irreversibility, and unlinkability.

REFERENCES

[1] N. K. Ratha, J. H. Connell, R. M. Bolle RM, “Enhancing security and privacy in biometrics-based authentication systems”, IBM Syst J 2001, 40:614-634.

[2] A. Cavoukian, A. Stoianov, “Biometric encryption”, in Encyclopedia of Biometrics Springer; 2009.

[3] A. Ross A, J. Shah, A. K. Jain, “From template to image: reconstructing fingerprints from minutiae points”, IEEE Trans Pattern Anal Mach Intell 2007, 29(4):544-560.

[4] N. K. Ratha, J. H. Connell, S. Chikkerur, “Generating cancelable fingerprint templates”, IEEE Trans Pattern Anal Mach Intell 2007, 29(4):561-572.

[5] J. Zuo, N. K. Ratha, J. H. Connel, “Cancelable iris biometric”, In Proc, of the 19th Int. Conf. on Pattern Recognition 2008 (ICPR’08) 2008, 1-4.

[6] N. K. Ratha, J. H. Connell, R. M. Bolle, S. Chikkerur, “Cancelable biometrics: a case study in fingerprints”, In Proc. of the 18th Int. Conf. on Pattern Recognition 2006, pp. 370-373.

[7] J. Hämmerle-Uhlr, E. Pschernig, A. Uhl, “Cancelable iris biometrics using block re-mapping and image warping”, In Proc. of the Information Security Conf. 2009 (ISC’09) LNCS 2009, 5735:135-142.

[8] P. Färberböck, J. Hämmerle-Uhl, D. Kaaser, E. Pschernig, A. Uhl, “Transforming rectangular and polar iris images to enable cancelable biometrics”, In Proc. of the Int. Conf. on Image Analysis and Recognition (ICIAR’10), Volume 6112. Springer LNCS; 2010:276-386.

[9] C. Rathgeb, A. Uhl, “Secure iris recognition based on local intensity variations”, In Proc. of the Int. Conf. on Image Analysis and Recognition (ICIAR’10). Volume 6112. Springer LNCS; 2010:266-275.

[10] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, A. Neri, “Template protection for HMM-based on-line signature authentication”, In Proc. Of Workshop Biometrics CVPR Conference 2008, 1-6.

[11] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, A. Neri, “Cancelable biometrics for hmm-based signature recognition”, In Proc of the 2nd IEEE Int. Conf. on Biometrics: Theory, applications and systems (BTAS’08) 2008, 1-6.

[12] E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, A. Neri, “Cancelable templates for sequence-based biometrics with application to on-line signature recognition”, Trans Syst Man Cybernet A Syst Hum 2010, 40(3):525-538.

[13] T. Boult, “Robust distance measures for face-recognition supporting revocable biometric tokens”, FGR ‘06: Proc. of the 7th Int. Conf. on Automatic Face and Gesture Recognition 2006, 560-566.

[14] T. Boult, W. Scheirer, R. Woodworth, “Revocable fingerprint biotokens: Accuracy and security analysis”, IEEE Computer Society Conference on Computer Vision and Pattern Recognition 2007, 1:1-8.

[15] M. Savvides, B. Kumar, P. Khosla, “Cancelable biometric filters for face recognition”, ICPR ‘04: Proc of the Pattern Recognition, 17th Int Conf on (ICPR’04) 2004, 3:922-925.

[16] A. B. J. Teoh, Y. W. Kuan, S. Lee, “Cancellable biometrics and annotations on biohash”, Pattern Recognition 2008, 41(6):2034-2044.

[17] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, B. V. Kumar, “Method for secure key management using a biometrics”, US Patent 2001, 6219794.

[18] Y. Wang, K. Plataniotis, “Face based biometric authentication with changeable and privacy preservable templates”, In Proc. of the IEEE Biometrics Symposium 2007, pp. 11-13.

[19] O. Ouda, N. Tsumura, T. Nakaguchi, “Bioencoding: a reliable tokenless cancelable biometrics scheme for protecting iris codes”, IEICE Trans Inf Syst 2010, E93.D:1878-1888.

[20]. O. Ouda, N. Tsumura, T. Nakaguchi, “Tokenless cancelable biometrics scheme for protecting iris codes”,

Proc of the 20th Int. Conf. on Pattern Recognition (ICPR'10) 2010, 882-885.

[21] J. K. Pillai, V. M. Patel, R. Chellappa, N. K. Ratha, "Sectored random projections for cancelable iris biometrics", In Proc. of the IEEE Int Conf. on Acoustics Speech and Signal Processing (ICASSP) 2010, 1838-1841.

[22] E. Reddy, I. Babu, "Performance of Iris Based Hard Fuzzy Vault", Int J Comput Sci Netw Secur (IJCSNS) 2008, 8(1):297-304.

[23] A. Kong, K-H Cheunga, D. Zhanga, M. Kamelb, J. Youa, "An analysis of BioHashing and its variants", Pattern Recognition 2006, 39:1359-1368.

[24] A. K. Jain, A. Ross, S. Prabhakar S, "An introduction to biometric recognition", IEEE Trans Circ Syst Video Technol 2004, 14:4-20.

[25] A. K. Jain, P. J. Flynn, A. A. Ross, "Handbook of Biometrics", Springer; 2008.

The 10th International Conference on Business Information Security (BISEC-2018), 20th October 2018, Belgrade, Serbia

BISEC
BUSINESS INFORMATION SECURITY CONFERENCE

GEOSPATIAL INTELLIGENCE AS A CHALLENGE FOR PERSONAL INTEGRITY IN CYBERSPACE

MIROSLAV D. STEVANOVIĆ
Academy of National Security, Republic of Serbia, mstvnv297@gmail.com

DRAGAN Ž. ĐURĐEVIĆ
Academy of National Security, Republic of Serbia, djurdjevic.dragan@gmail.com

Abstract: *In this article, we observe the use of technologies for collecting data with locational component, to acquire and manipulate information. We problematise geospatial intelligence from the aspect of providing integration of various cartographic data with those of intelligence agencies. By rapid integration of various indicators of human activity, metadata can be used to analyse relevant patterns, i.e. for human domain intelligence. Since this is not a regulated process, there is a risk that personal data can be targeted abusively. This technological possibility can be used for exerting behavioural and neurophysiologic influence. In this context, the metadata is instrumental to enable anticipation of relevant information. We find that the challenges for the safety of personal data from the geospatial intelligence are twofold. Structurally, the activity of actors with an access to data does not include informing of the public. Functionally, individuals are exposed to the clandestine influence of such actors.*

Keywords: *spatial pattern analysis, data integration, geographic information systems modelling, spatial data mining*

1. INTRODUCTION

Computer applications, devices and systems that are connected to the Internet or support online operation collect data that describe or provide information about other data (metadata). Metadata include factual background concerning, for example, the history of web browsing or activity on social networks, dates, times, locations, email exchanges, online transactions. When aggregated, this type of data can account for activities of user(s) on the Internet, but also provide a description of their real-life activities and interactions with others.

Metadata can also be collected with an additional locational, geospatial, component. This is technologically possible by web servers, firewalls, mobile or data network switches and mobile applications, through using cookies, event logging, traffic collection, or event reporting to a monitoring or surveillance system.

Technological systems for geospatial monitoring or information gathering can collect metadata for a variety of purposes. These include functions from managing or optimising network performance or troubleshooting service problems to conducting surveillance to combat terrorism or gathering intelligence to investigate cybercrimes. The doctrine has not, so far, identified compelling evidence that such activity has produced a relevant public benefit [1]. Even one of the most advanced bulk collecting programs, applied by the United States National Security Agency to use metadata, such as numbers called, IP addresses and call duration, to identify and capture terror suspects, as admitted, showed "minimal value in safeguarding the nation from terrorism” and not a single instance is identified in which the program made a substantial difference in the outcome of a counterterrorism investigation involving a threat to the U.S. [2].

The problem with geospatial intelligence spreads on several levels. Firstly, concerning the informed consent, i.e. has a commercial entity notified a specific Internet user that it is collecting metadata and requested an explicit permission to do so and, in relation to that, does a government agency need a permission by court or by law to collect metadata. Secondly, an issue of the use of metadata, i.e. a question of obligation of a commercial entity that collects metadata to publish a privacy policy or a notice that explains why the metadata is collected, how they shall be used, and whether they will be shared or sold to others, including with government law enforcement and intelligence agencies. Thirdly, an issue of expressed retention policy, i.e. how long an entity will store metadata, can they be used for different purposes over time, and whether the policies or metadata retention laws at the time of collection will remain over time. Fourthly, an issue of legality for government agencies to collect metadata about citizens as part of broad surveillance or intelligence gathering activities without warrants or in violation of constitutional or other citizens' rights.

The principle concern related to geospatial intelligence is possible manipulation against privacy. In that context, metadata can, by rapid integration of various indicators of individuals’ activities, be used to induce relevant patterns, namely for human domain intelligence [3]. This way, available metadata can be instrumentalised in the function of anticipation of certain kind of information and behavioral and neurophysiologic influence.

The challenges geospatial intelligence generates for the safety of personal data can be seen twofold. Structurally, the activity of actors with an access to data does not include informing of the public. Functionally, individuals are exposed to the clandestine influence of such actors [4].

2. RISKS CONCERNING PERSONAL METADATA

Metadata, generally, include specific details related to technical and business processes, data rules and constraints, and logical and physical data structures. They describe the data itself, the concepts the data represents, and the connections between the data and concepts. Metadata help in understanding data, systems and flows. This enables quality assessment of data and is thus integral in the management of databases and applications. Besides, they contribute to the ability to process, maintain, integrate, secure, audit and govern data.

Metadata related to a specific person allows deduction of the additional information about that person. Through them can be revealed nature, characteristics, behaviour and affinities within the available amount and range of metadata. This is the reason why metadata cannot be viewed and treated as the immanent neutral consequence of technology. Instead, this phenomenon requires societal answers to at least following issues: awareness of internet users, rights of data subjects, insights in processing data, assessment of impacts on privacy, privacy by design and by default, notification of any breach of personal data, data processing contracts, consent management.

There are critical ways in which these possibilities are generating a national security challenge. On one side, privacy is portrayed as an individual right, as opposed to the need for security which is collective. Protection of personal data is itself a fundamental right, while the significance of communications surveillance, especially since it was highlighted by the revelations of Edward Snowden, has triggered broader political and popular debate [5].

The focus of surveillance activities is, as much as on content, on metadata (or communications data in general). They operate based on gathering in bulk and in detail access. The principle question is whether this constitutes illegitimate mass surveillance. It is being done with participation of commercial data gatherers. What also makes this kind of surveillance new is the way that the Internet is used. Namely, the internet is used for almost every aspect of our lives and the implications of this are considerable, to the extent that although surveillance techniques are not all new, their relationship to people’s lives and their potential impact is. The growth of social networking sites and the development of profiling and behavioural tracking systems and their equivalents change the scope of the available information. It is not only the information deliberately imparted that is available, but also the information derived from analysis of that information and from our behaviour that can become available.

In parallel with this, technological developments have changed the nature of the data that can be obtained by surveillance. For example, the increased use of smartphones and related technologies provides new dimensions of data such as geolocation data and biometric data including facial recognition and fingerprints, and allows further levels of aggregation and analysis. The nature of the technology also implies that surveillance that would have been overwhelmingly expensive, as well as immensely challenging on a practical level, has now become relatively simple and inexpensive, and hence, attractive for governments.

Surveillance can be theoretically defined as ‘the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction’ [6] where automated algorithmic analysis is applied. What an algorithm does could be described as ‘focused, systematic and routine attention’ to data.

The power effects of surveillance illustrate three additional dangers of surveillance: blackmail, discrimination, and persuasion’ [7]

The conclusion drawn by the European Court of Human Rights (ECtHR), that ‘the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data’[8]. It is the development of systems and laws to allow the gathering of that data that produces the menace of surveillance, not that allows the examination or use of the data gathered. In the gathering stage, therefore, should start the rights-balancing efforts. This understanding is underlined by the subsequent rulings of the ECtHR [9] and the Court of Justice of the European Union [10].

Theory of emotional intelligence (how well we understand our emotions) show that everyone also has another diverse set of skills, i.e. the capacity, to solve problems (personal intelligence). On the Internet, personal data can be obtained. New technologies go further to enable an ontology-based framework for controlled release of personally identifiable information or sensitive personal information at policy writing as well as in evaluation.

The process of discovering interesting and previously unknown, potentially useful, intelligence from spatial databases (spatial data mining) is useful for extracting spatial patterns. Outputs could be in form of predictive models, spatial outliers, spatial co-location patterns, or spatial clustering. Their integration can lead to conclusions about meanings, i.e semantic, which can be done through algorithms. This introduces a further risk concerning individual’s freedoms. This personal security problem is generated by the capability to store metadata related to persons in a locational surrounding and stored in mediums, available for analysis and use against individuals [11]. Furthermore, for the security needs subsystems of exploitation of these outputs are designed, even when the law prohibits such use of metadata. As we noted in our previous works, on the general level, synthetic environment has a problematic approach to reality, to be suitable for every country’s national security needs. Application of simulation with such environment bears a risk that it may foster operational skills and disregard the role of previous knowledge for the perception of information in the context of threats for vital values [12].

3. PERSONAL INTEGRITY EXPOSED

Metadata related to activities of an individual online can be exposed in many aspects. It could be the reader database, voter records, personal information, large Internet panel surveys, availability of web services and subscriber databases, personal profiles etc. They offer a following potential for exploitation:

- personal data is used to determine the online experience;
- expose different sets of claims depending on the circumstances;
- handling information flows and social influence.

Furthermore, integration of various cartographic data (statistics etc) with remote-sensing data in cyberspace (also metadata) provides a suitable point for their fusion with conventional intelligence. Since the process of geospatial intelligence relies on most used online clicks of the users, i.e. their activity, to randomly figure the most favourable clicks, it is essentially activity based.

The data obtained through rapid integration of data from multiple sources provides for deriving patterns. These patterns concern human domain intelligence and the information can be implemented in line with behavioural and neurophysiological human characteristics [13]. In narrative shaping, position of corporate participate in the development of narratives, through the abuse of metadata, even though they appear to be neutral in such activity.

In this context, an example is provided in publicly exposed operations, known as "false flag", "black operation", "asymmetrical warfare" or "hybrid wars", which when viewed continuously represent a part of a integral operational military project within the North Atlantic Treaty Organisation [14]. Structurally, this indicates that there are Internet paramilitary echelons that are organised, logistically and operatively under the command of intelligence and other special services from the NATO structure. From this, it follows that the operation of these structures is carried out legally and non-transparently. In this context, direct problems, from a functional point of view, stem from agents of services in whose function they conduct activities in cyberspace.

Many of the software tools for Internet browsing, as a means of intelligence in cyberspace, have been developed within government agencies of the most developed countries. With the help of these tools online direct tasks are executed. This enables the ability to directly affect the flow, content or dynamics of information in the cyber space. Viewed from this aspect, the intelligence services of the countries with such capabilities can clandestinely conduct illegitimate information collection.

The tools for secret placing of false information on the Internet can, for example, include following goals: to change the results of online surveys; for mass delivery of email and/or SMS messages to support information campaigns; for targeted discovering targets and removal of content; for disturbing of video websites; within active Skype capabilities, such as delivering real-time call records (dialled fixed and mobile phone numbers from the VOIP network), messages being sent from both directions and contact list of the interlocutor; using "Skype resolver" comes to the account owner via: IP address, e-mail address, downloaded file; finds private photos of the target on Facebook; to remove permanent orders from the targeted computer and on behalf of the target; to visit specific web pages and increase or reduce visits to specific web pages; to spread creator/target messages on popular sites on behalf of the target/creator on YouTube; to deny Web server services; to deny distributed services using P2P protocols; to track the meta activities on eBay; to distribute the content from the creator/target email address to any address, and to send the content of the creator/target from someone else's email address; to connect two target phones to the call; to post on Facebook invisible to individual or all users in a country, as well as dozens of others.

It is significant that tools for secret data collection from the Internet browsing are not accompanied with reliable information. Reasons for this originate from limited scope of collection, inability to check, often the indirect nature of data collection, as well as, among else, the presence of other organised and unorganised online trolls. Individuals or organisations that make attacks towards this goal can easily be recognised, except of the secret services, which have vast resources, different IP addresses and the ability to manipulate data through many networks of computers where automated programs take place, which is difficult to identify (botnet). Botnet allows trolls to fall unnoticed and cannot be detected.

Integrity of personal security can, in the context of governance and the use of such tools, be viewed as (a) being consistent and coherent in principles, values, and action, (b) following regime values and rules, and (c) acting in accordance with relevant moral values, norms, and rules [15].

4. BROADER NATIONAL SECURITY CONCERNS

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 [16].

Technology and the largest tech firms are becoming increasingly controversial. Today, for example, there are growing evidence about third parties accessing and manipulating Facebook user data. While previously there was a wide spread debate about whether the government should be able to unlock devices belonging to individuals informally suspected of connection to terrorism or other crimes, today there is an open window of software opportunities to pursue new policies for the sector. If national security is viewed as the stability of basic values in a political community, this kind of technological advance introduces new challenges for national security systems.

The first is privacy. This matter is widely recognised through, for example, proposals to introduce an obligation for technological companies to obtain an affirmative opt-in from users before collecting their data and to allow users to retrieve or erase their data easily. So far, there are no conclusive evidence on how customers and companies, including new entrants, would react to such rules, so this question remains at the level of institutional perception of general threat to national security interests. From that aspect, it cannot be neglected that by collecting more data, companies may offer users inducements beyond the putatively free services they commercially provide, while on the other side, such rules have the potential to slow down the pace at which they can enhance services or add new features.

The second issue concerns the market power. In the early years of the Internet, tech industry pleaded for a hands-off approach to regulation and taxation. But now, as of 2017, among the largest US firms by market capitalisation are Apple, Alphabet (previously known as Google), Oracle Cisco, Facebook, Amazon, Twitter, all technological companies. Apple and Google have a duopoly on smartphone operating systems, yet they compete to improve their features and roll out new products. Meanwhile, Apple's iOS and Google's Android app stores have become a point of entry for new smartphone providers. Likewise, Facebook and Google dominate the digital advertising market but their profits allow them to offer ostensibly free email and social-media services that benefit consumers. Amazon is also dominant in online retail and data-centre infrastructure. The issue, therefore, is whether the current competition among the giants further multiplies their market power and influence.

A third issue concerns the control of information. Owing to the convenience and addictiveness of smartphones and social media, many people now get news exclusively from online platforms such as Facebook. Yet the microtargeted advertising model, as used by Google and Facebook, has disrupted print journalism's traditional source of revenue, along with coverage of state and local governments. Furthermore, social-media algorithms tend to amplify the most extreme material at the expense of more credible sources. Efforts to eliminate material viewed as extreme, as has become a practice by private technological monopolists without transparent procedure, practically raises the spectre of censorship possibilities. Especially, those who do not belong to the mainstream views fear that left-leaning companies in Silicon Valley can decide de facto limits of acceptable debate, disregarding the right to free speech.

The convergence of computers and telecommunications was anticipated as a means of linking computers and their users remotely. What has not been anticipated was the extent to which computation itself would fuse with communications. The movement of software to the World Wide Web (WWW), for example, is a sudden and unexpected development which was not considered outside of a hypothetical possibility even couple years ago.

At the practical level, what is currently happening is simply an extension of opening of software on the desktop to other software across the Internet. As the costs of memory are still dropping fast, and new memory is still soaking up ever more graphics, the trend of surveillance has migrated to networks. The fact that the Internet has been effectively free to users in educational environments, and low cost to others, has fostered a massive increase in shareware of a very high quality.

A practical new advance is the high quality 3-dimensional and multimedia software which is now available in the public domain and even threatening well established sellers of proprietary software. Three-dimensional graphics is being particularly taxed by these developments with the advent of virtual reality software over the Internet, but geographic information system (GIS) shareware is on the horizon as a variety of developers is beginning to develop graphical interfaces to locational data in the form of virtual reality interfaces such as animated maps.

These developments are fundamental leading to the beginning of changes in hardware itself. Several hardware-software companies have announced the network computer, which will function with no additional software compared to a web browser and some communications protocols. This way, desktop GIS will now have the possibility to be open to other kinds of software through dynamic data and other exchange mechanisms, and through the addition of programming languages within the GIS which opens it to other software on the same machine or network. Furthermore, what were once very different software packages are beginning to converge [17].

Concerning its application, GIS database can integrate many properties, variables, and themes through common geographic location. This qualitative leap enables spatial analysis. Namely, much socioeconomic indicators are collected in cross-section, and the construction of longitudinal series is permanently challenged by problems of continuity, budgets, and changing technology.

Spatial analysis, or spatial data analysis, comprises a set of techniques and tools designed to analyse data in spatial context. The result is a spatially explicit theory and modelling. Spatial interaction models can be implemented to anticipate choices made by consumers in targeted social groups, societies and even countries. This function can be multiplied through a variety of other forms of interaction over space as well, including telephone traffic, migration, and commuting.

Place-based analysis leads to development of principles that apply uniformly. As knowledge and policy are used inside the academic research and government agencies, corporations and NGOs to distinct between doctrinal and applied, or curiosity-based and problem-driven, it provides a connection between them, which is necessarily objective. Besides, as is noted in theory, place-based search, as representations of the entire surface within internal limits and sampled data, provides information only about a selection of places [18].

5. CONCLUSION

Generally, risks that can be associated with exposure of personal data, through metadata and geospatial intelligence, expose that organisational and corporate discourse today has the capacity to impose pseudo-moral. From the aspect of a state, as shown, this “illusionist” possibility, as an indeterminate catalyst or generator, are as a rule aimed to protect the existing concentration of power and capital.

On the functional level, non-transparent online exposure of personal integrity, viewed from the standpoint of the elaborated discourse of integrity, resembles obscuring rhetoric. Even though it was not a part of this analysis, this obscuring associate to mechanism of Orwellian newspeak. The analysis reveals in the case of private technological monopolists, corporate social responsibility in the cyberspace, as a public utility, or desired codes of ethics in such space, as a value itself, are sometimes used as a cover to conceal immoral, illegitimate or even legally disputable activities of big companies.

On the practical level, challenges for the safety of personal data from the geospatial intelligence are twofold. Firstly, structurally, the activity of actors with an access to data does not include informing of the public. Secondly, functionally, individuals are exposed to the clandestine influence of such actors.

As the problem of this analysis is the possible disturbing of social situation of moral integrity in condition of spreading of technological non-transparent use of metadata, counterfeit integrity that is exposed in this article, needs further critical thinking, when applied for the purpose of oppression and marginalisation of the population and individuals.

REFERENCES

[1] J. E. Mueller and M. G. Stewart, Chasing Ghosts: The Policing of Terrorism, Oxford: Oxford University Press, 2016, p. 185.

[2] D. Rudenstine, The Age of Deference: The Supreme Court, National Security, and the Constitutional Order, Oxford: Oxford University Press, 2016, p. 167.

[3] Office of Director of National Intelligence, Statistical Transparency Report Regarding Use of National Security Authorities-Calendar Year 2017, Washington: Office of Civil Liberties, Privacy, and Transparency, 2018. https://www.dni.gov/index.php/newsroom/press-releases/item/1867-odni-releases-annual-intelligence-community-transparency-report (26.08.2018.)

[4] B. Andrew, We're in This Together: Reframing EU Responses to Criminal Unauthorzed Disclosures of US Intelligence Activities, in: Russell A. Miller (ed.), Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair, Cambridge/New York: Cambridge University Press, 2017, pp. 229-256, p. 254.

[5] P. Bernal, Data Gathering, Surveillance and Human Rights: Recasting the Debate, Journal of Cyber Policy, 1:2/ 2016, pp. 243-264

[6] D. Lyon, Surveillance Studies: An Overview. Cambridge: Polity Press, 2007, p. 14.

[7] N. M. Richards, The Dangers of Surveillance, Harvard Law Review: 126:7/2013, pp. 1934–1965.

[8] ECtHR, S. and Marper v. UK, Apps. nos. 30562/04 & 30566/04, Judgement 4 December 2008, (2008) ECHR 1581, para 121.

[9] ECtHR, Zakharov v. Russia, App. no. 47143/06, Judgement 4 December 2015, (2015) ECHR 1065, para. 184.

[10] Court of Justice of the European Union, Maximillian Schrems v Data Protection Commissioner, Case C-362/14, Judgement 6 October 2015, para. 43.

[11] D. Li, S. Wang, D. Li, Spatial Data Mining: Theory and Application, Berlin/Heidelberg: Springer Verlag, 2015, p. 4.

[12] M. Stevanović and D. Đurđević, Computer Simulation in Domain of National Security: The Case of S.E.N.S.E., Proceedings The 9
th International Conference on Business Information Security (BISEC-2017), 18th October 2017, Belgrade, pp. 71-75.

[13] M. Stevanović and D. Đurđević, The Challenges of Shaping Narratives in Cyberspace for National Security, Paper presented at the International Scientific Conference "Freedom and Security in Real and Cyber Space", Belgrade, 9 June 2018. Proceedings of abstracts 10th International Scientific Conference "Freedom and Security in Real and Cyber Space, Belgrade, pp. 48-49.

[14] D. Đurđević and M. Stevanović, Internet as a Method of Trolling Offensive Intelligence Operations in Cyberspace, NBP – Journal of Criminalistics and Law, 14:2/2017, pp. 13-32.

[15] G. de Graaf, L. Huberts and T. Strüwer, Integrity Violations and Corruption in Western Public Governance: Empirical Evidence and Reflection from the Netherlands, Public Integrity, 20:2/2018, pp. 131-149.

[16] M. Stevanović and D. Đurđević, Internet of Things Challenges for Organised Societies, Proceedings The Eighth International Conference on Business Information Security (BISEC-2016), 15th October 2016, Belgrade, pp. 50-55.

[17]. M. Batty, New Technology and GIS, in: Geographical Information Systems: Principles, Techniques, Management and Applications, 2nd edition, P A Longley, M. F. Goodchild, D. J. Maguire, and D. W. Rhind (eds.), 2005, New Jersey: Wiley, pp. 309–316

[18] M. F. Goodchild, New Horizons for the Social Sciences: Geographic Information Systems, in. Social Sciences for a Digital World Building Infrastructure and Databases for the Future: Building Infrastructure and Databases for the Future, Paris: OECD, pp. 163-172.

007:004.056(082)

КОНФЕРЕНЦИЈА о безбедности информација (10 ; 2019 ; Београд)

Proceedings / The Tenth International Conference on Business Information Security - BISEC, Belgrade, 20th October 2018. ; [editors Igor Franc, Bojana Trebinjac]. - Belgrade : Metropolitan University, 2019 (Beograd : Copy Planet). - 59 str. : ilustr. ; 30 cm

Tiraž 60. - Bibliografija uz svaki rad.

ISBN 978-86-89755-17-6

а) Информације - Заштита - Зборници

COBISS.SR-ID 277900812

www.bisec.metropolitan.ac.rs
Belgrade Metropolitan University,
Tadeuša Košćuška 63, 11000 Belgrade, Serbia
+381 (11) 20 30 885, +381 (69) 20 30 885