Data Security in Smart Cities: Challenges and Solutions

Daniela POPESCUL, Laura Diana RADU
"Alexandru Ioan Cuza" University Iași
rdaniela@uaic.ro, glaura@uaic.ro

The purpose of this paper is to provide an extensive overview of security-related problems in the context of smart cities, seen as huge data consumers and producers. Trends as hyper connectivity, messy complexity, loss of boundary and industrialized hacking transform smart cities in complex environments in which the already-existing security analysis are not useful anymore. Specific data-security requirements and solutions are approached in a four-layer framework, with elements considered to be critical to the operation of a smart city: smart things, smart spaces, smart systems and smart citizens. As urban management should pay close attention to security and privacy protection, network protocols, identity management, standardization, trusted architecture etc., the paper will serve them as a start point for better decisions in security design and management.
Keywords: *Data security, Smart cities, Internet of Things, Smart things, ePrivacy*

1 Introduction

A smart city is a future, better state of an existing city, where the use and exploitation of both tangible (e.g. transport infrastructures, energy distribution networks, and natural resources) and intangible assets (e.g. human capital, intellectual capital of companies and organizational capital in public administration bodies) are optimized. [1] Advanced systems manage energy, water, transportation, traffic, healthcare and education. [2] In order to make them function as a whole for citizens' benefit, various smart cities technologies are used, including city operating systems, centralized control rooms, urban dashboards, intelligent transport systems, integrated travel ticketing, bike share schemes, real-time passenger information displays, logistics management systems, smart energy grids, controllable lighting, smart meters, sensor networks, building management systems, and an vast array of smartphone apps and sharing economy platforms. [3] From the IC&T point of view, these technologies are strongly based on smaller and smaller electronic chips and electro-mechanical devices, sensors, Internet IPv6 and wireless technologies, sensors, RFID (Radio Frequency Identification), localization technologies, NFC (Near Field Communication), Internet of Things (IoT) and Cloud Computing. [4]

In such a complex environment, all these interconnected cyber-physical devices and processes generate huge quantities of data, much of them in real-time and at a highly granular scale. [3] Data collection, processing, transfer and use enable smart living, instantaneous connection with/between every citizen, and create the possibility for the cities to be run more efficiently, productively, sustainably, fairly and transparently. [2], [3], [4] But, on the other side of the story, various problems occur in the huge data machinery that a smart city is: internal and external parties could not be trustable [4], new threats that affect data confidentiality, integrity, accessibility, protection and privacy are signaled continuously, smart cities technologies are still in their infancy, there are no standards of use and a lot of technical difficulties need to be defeated. [2], [4], [5], [6], [7], [8], [9]

In the rest of the paper, the above mentioned problems are going to be approached in a framework in which smart cities are seen as a synergetic sum of *smart things* and *smart spaces*, interconnected in *smart systems* (infrastructure and applications) that work for the *smart citizens*' benefit.

2 Data Vulnerabilities in a Smart City – A Four-Layer Analysis

2.1 Smart Things

DOI: 10.12948/issn14531305/20.1.2016.03

In a smart city, objects are connected in order to provide seamless communication and contextual services. A large variety of things are used in a smart city. Part of them are very sophisticated embedded systems – such as smart phones and TVs, tablets, printers, medical devices, SCADA (Supervisory Control and Data Acquisition) systems and so on, others are wearable (sensors placed on/under the skin or sewn into clothing that provide information about a person's vital signs), and many of them are usual things like keys, watches, coffee filters, fridges, domestic heating controllers, books, doors etc. Also, a lot of sensors are used to monitor air quality and pollution, auto and pedestrian traffic, bridges' resistance and road infrastructure in general, criminality rates and policing, energy and water consumption, waste management etc., forming a perceptual/recognition layer used to collect data and identify the physical world. On this layer, objects respond in numerous ways to their internal states and/or to external factors.

All this things can be very smart in some situations and quite stupid in others: for example, smart in the sense that they transmit/process/respond to various data, but stupid when there is a need to protect them. Smart things suffer from hardware limitations (computational and energy constraint, memory constraint, tamper resistant packaging), software restrictions (embedded software constraint, dynamic security patch), hard network-requirements (mobility, scalability, multiplicity of devices, multiplicity of communication medium, multi-protocol networking, dynamic network topology). [10] These resource-constraints restrict the inclusion of adequate security mechanisms (e.g., cryptography) directly in smart objects. In consequence, designers let the security aside, hoping it could be add later-on, and attack-resistance is usually losing the race against other design-factors, as good performance, small form, and low energy consumption. [11] In this sense, a Hewlett-Packard study showed that 80% of things in IoT fail to require passwords of a sufficient complexity and length, 70% enable an attacker to identify valid user accounts through account enumeration, 70% use unencrypted network services and 60% raise security concerns with their user interfaces. [12]

Data collected by smart things are at the heart of smart cities. The problem is that they are sensitive data, often gathered without our explicit consent. For example, messages, personal pictures, appointments, bank account information, contacts and others are stored in our smart phones in full awareness, with more or less security measures put in place. But an average smart phone comes with various sensors like gesture sensor, proximity sensor, RGB light sensor, gyro sensor, accelerometer, geomagnetic sensor, barometer, and hall sensor. Such sensors can capture location, movements, time stamps, even private conversations and background noises. The use of these sensors by different applications, the quantity and the purpose of collected data are not fully understood and controlled by their owners. For example, as shown in [13], video and pictures can reveal the social circle and behaviour of a citizen in a completely unexpected manner. From another range of devices, thermostats communicate their location (including the postcode), temperature data, humidity and ambient light data, the time and duration of activation – these data can be used to determine domestic habits of a citizen; medical bracelets store the heartbeat and sleeping patterns, collecting biometric and medical data that reveal individuals' physiological state. It is obvious that if these valuable data are not well treated, significant privacy problems may occur.

Furthermore, the majorities of things in a smart city are not personal and are unattended. Their physical security is not guaranteed, especially in the public networks, the control of the objects may be lost and cascade failures may appear, caused by the interconnectivity of a large number of devices, difficult to be protected simultaneously. Some connected things and their firmware are protected by trade secrets. Plus, the legal framework is not yet appropriate, and the legal responsibilities are not clear enough.

2.2 Smart Spaces

A smart space is described as a collection of smart things and other relatively powerful

DOI: 10.12948/issn14531305/20.1.2016.03

computers/gateways that manage and serve them; a merger of physical and digital spaces, that have some kinds of abilities of perception, cognition, analysis, reasoning and anticipation about a user's existence and surroundings, on which it can accordingly take proper actions. [7] In a smart space, smart things are put in context, they form ecosystems that monitor and control our physical environment and our actions. There are different spaces: smart buildings, like home and offices, smart hospitals, hotels and malls, smart cars, and even smart streets.

In order to bring us the desired comfort, smart spaces want to know everything about us. Various technologies capture personally identifiable information (PII) and household level data about citizens – their characteristics, their location and movements, and their activities – link these data together to produce new derived data, and use them to create profiles of people and places and to make decisions about them. [3] For example, a smart building is sensitive in terms of environmental condition (temperature, humidity, smoke, CO_2, extreme light, air pollution, external presences) and also able to determine a very accurate user profile based on his/her habits. Vehicles are active members of cities; they interact with each other, with driver/passengers and with pedestrians. As shown in [14], they have embedded computers, GPS receivers, short-range wireless network interfaces, and potentially access to in-car sensors and the Internet. The smart city infrastructure can read data about vehicles using radars, Bluetooth detectors, and license plate cameras. Speed, flow, and travel times are known this way and they can be associated with driver's identity. According to [15], tracking can reveal sensitive locations, such as home or work locations, along with the time and duration of each visit, effectively allowing one to infer the detailed behavioural profiles of drivers, information about safety-critical events, speed, destination, home and workplace addresses, time spent in a particular location and so on.

2.3 Smart Infrastructure

Smart cities are based on water and energy generation and transmission setups, transportation frameworks, waste disposal mechanisms, street and home lighting systems, connected healthcare, surveillance, and more. Huge amounts of data are produced by utility companies (use of electricity, gas, water, and lighting), transport providers (location/movement, traffic flow), mobile phone operators (location/movement, app use, and behaviour), travel and accommodation websites and smart hotels (reviews, location/movement, and consumption), Social Media sites (opinions, photos, personal info, location/movement), crowdsourcing and citizen science (maps, local knowledge, urban incidents, weather), government bodies and public administration (services, performance, surveys) [3] and transmitted through a wireless, mobile and Internet of Things (IoT) infrastructure. IoT has all the security problems of sensors and actuators, mobile networks and Internet, namely insecure web interface, insufficient authentication/authorization, insecure network services, lack of transport encryption, insecure cloud interface, insecure mobile interface, plus privacy issues (collection of unnecessary personal data). [16] [17] Data flows generated by the interaction between objects, between objects and individuals, between objects and back-end systems cannot be controlled with the classical tools. As services in a smart city are closely interconnected, if one smart service information system fails to provide relevant information to other connected smart services, it can lead to chaotic situations, which eventually may result in a complete breakdown. [2]

2.4 Smart Citizens

A smart city is about the relations between the everyday objects surrounding humans and humans themselves, and serving citizens is the main reason of a smart city. In consequence, a smart city will use e-government, will encourage individuals' participation in reporting issues and planning. But, as errare humanum est, people do a lot of mistakes in using the surrounding cyber-physical objects:

DOI: 10.12948/issn14531305/20.1.2016.03

- The devices are not configured in an adequate manner, implicit factory settings are used – this is especially dangerous when passwords are involved. Proper authentication settings are not put in place, terms and conditions are not read/understood, there is no knowledge about the data collected by applications and the way of using them;
- Devices are left unattended;
- Stored and transmitted data are treated in the same manner, the sensitive ones are not proper protected;
- People are easily fooled through social engineering, spam emails, data streaming, and other malicious methods.

Also, as previously shown, citizens have to self-report various data about themselves to the smart cities' managers – contact data, financial data, medical data, and emergency situations' data etc. The data collection, processing and transmission are not usually explained directly to the citizens, and they have to blindly trust the way in which data are used. A low-quality consent problem appears: in many cases the user is not aware of the data captured and processed by specific objects. In these situations, it is almost impossible to obtain the consent of collecting/processing data required by European legislation. If they are unhappy with these situations of uncertainty, the question of transmitting the data to untrusted third parties occurs, and suspicions about a Big Brother effect can determine the citizen not to share data to urban management anymore.

3. Attacks in a Smart City

In a smart city, the attack surface is an extended one, because of the great number of interconnected cyber-physical things, spaces, infrastructures and users. Violations of data security can provoke the compromising of entire system, and an infection can be easily transmitted between systems. This, in extremis, can determine an infection of the city itself, destroying even the physical infrastructure and threatening lives. This scenario seems to be a science-fiction one, but it's important to remember that *Stuxnet,* an "unprecedentedly masterful and malicious piece of code", according to [17], has been sold on the black market since 2013. The experts in IT&C security say it could be used to attack any physical target which is related to computers, and the list of vulnerable systems is almost endless – electric heating systems, food distribution networks, hospitals, traffic lights systems, transport networks etc. Other malware, such as *Linux.Darlloz* Worm, infects a wide range of home routers, set-top boxes, security cameras, and other consumer devices that are increasingly equipped with an Internet connection. In these conditions, the terrorist cyber-strikes against the utility and industrial infrastructure can no longer be dismissed as a spy movie scenario. [11] Intrusions in SCADA systems can lead to disruptions in the exchange of data between control centres and end-users. As a result, certain services provided to citizens (access to public health services in critical moments, the supply of electricity in some areas) will be compromised; certain areas of the city can be blocked by stopping traffic lights etc. Intruders can also install malware systems in data centres/user devices to obtain sensitive information about citizens and to use them for criminal purposes. Other examples of attacks are presented in figure 1.

DOI: 10.12948/issn14531305/20.1.2016.03

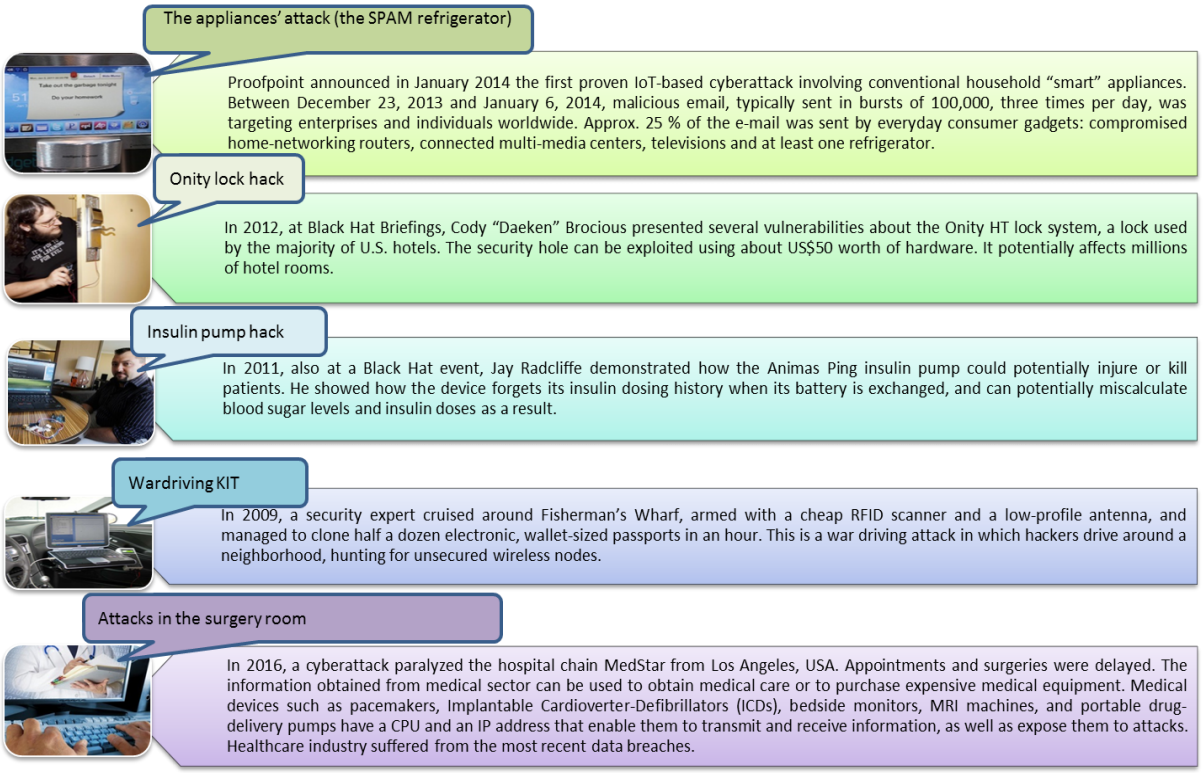

Fig. 1. Attacks in a smart city - some examples ([18], [19], [20], [21], [22], [23], [24])

In [10], Hossain et al. present a comprehensive classification of attacks in a smart city. They can be made with simpler or more complex devices, provoking losses of small/big size. Attacks can also be internal (the attacker is in the immediate proximity of the smart thing, in the same network with the victim) or external (the attacker is anywhere in the public network and access the victims' network in an unauthorized way). Attacks can be made in an active (illicit activities that disrupt the normal functioning of devices/networks) or passive (the attacker collects devices/networks data without interrupting the processes) mode. The attacks can compromise the user (stealing the passwords or access keys), the software (operating system, other applications in IoT nodes), or the hardware; they can be physical (determine physical damages or changing the smart things' settings or properties) or logical (create malfunctions in smart systems without physical damages).

Some attacks are recognized since 2014 at the European Union level. Opinion 8/2014 on the Recent Developments on the IoT published by European Union (EU) [29], lists the following situations:

- Inferences derived from data and repurposing of original processing: increasing the amount of data generated by IoT, in combination with modern methods of analysis and cross-matching, allow the use of data for purposes different than the originally established ones. These challenges calls for specific solutions, because, even if the user was comfortable with sharing the original information for one specific purpose, he/she may not want to share this secondary information that could be used for totally different purposes;
- Intrusive identification of behaviour patterns and user profiling: isolated data identified and collected by different objects can be combined to reveal important aspects of the habits, behaviours and preferences of individuals or social groups. Patterns of life and behaviour can be identified in this way. On the other hand, the continuous presence of sensors can put pressure on individuals and can limit their freedom;
- Limitations on the possibility of remaining anonymous when using service: the complete development of a smart city elimi-

DOI: 10.12948/issn14531305/20.1.2016.03

nates the citizens' possibility of using services in anonymous mode. The ubiquity of sensors makes it difficult to preserve privacy and poses significant data protection risks;

- Security risks: IoT has numerous security problems, with a risk that every object in the network becoming the target/source of an attack. Risks are therefore more serious those facing the Internet today. At least two issues should be considered in this case: (1) smart things security, the channels of communication between them and the storage infrastructure and (2) technologies used at different levels of data processing are designed and implemented by different suppliers, without the possibility of standardization and proper protection.

4. Security Measures in a Smart City – Another Onion Model

In order to adequately protect a smart city, a lot of measures provided by various actors are needed. An overall view of these solutions is presented in figure 2 and describe in the following part of the paper.

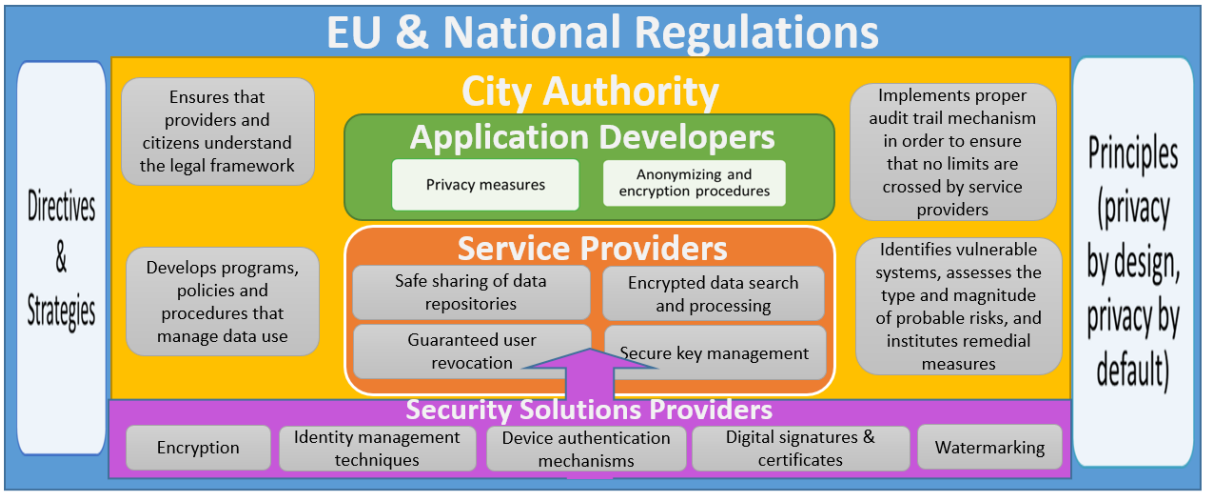

Fig. 2. Security measures for a smart city – an onion model

4.1 European Union Regulations

According to Digital Agenda for Europe, the smart environments created by merging physical and virtual worlds improve in a great extent EU citizens' lives. EU supports the implementation of smart city concept that permits better public services for citizens, better use of resources and less impact on the environment. In EU's opinion, in smart cities, digital technologies translate into better public services for citizens, better use of resources and less impact on the environment. [25] EU affirms that confidentiality and data privacy should play an important role in any smart city development strategy, taking into consideration those web-based attacks in IoT increased by 38% in 2015. [26] Otherwise, the introduction of these innovative technologies that access various data about people would not have their consent. Privacy-failures are considered one of the most important barriers to the development of smart cities by the Alliance for Internet of Things Innovation (AIOTI), an organization founded by the European Commission and various IoT key players in 2015. The principle of "privacy by design" is strongly recommended by AIOTI. According to this concept, the protection of privacy is embedded at the earliest stage in technological design. Another important principle is "privacy by default" - the controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. [27]

The important concepts of trust, security and

DOI: 10.12948/issn14531305/20.1.2016.03

privacy are treated in strategies as Digital Single Market Strategy, launched in 2015, EU Cybersecurity Strategy, adopted in 2013, European Agenda on Security adopted in 2015. A new term, ePrivacy, was coined for a distinct approach of confidentiality of online PII. In this domain, the main objective is the protection of the confidentiality and the security of individuals' communications in online environment, which is rooted in the fundamental right to the respect of private and family life. [28], [30] Online privacy is largely approached in the Data Protection Directive and in the ePrivacy Directive (Directive on Privacy and Electronic Communications), which try to ensure safe collection and processing of user data in IoT. Data can be obtained only under strict conditions and for legal purposes, issues that have to be guaranteed by organizations dealing with data collection. The problem is even more important in smart cities, where the volume of data is huge and concerns a wide range of activities in the life of the inhabitants of a city; here, unauthorized access to data can have important negative consequences on large groups of people. To protect them, the European Commission requires telecom operators and Internet Service Providers to report any "personal data breach" to the national authority and to inform the subscriber or individual directly of any risk related to personal data or privacy.

4.2 Other Stakeholders' Actions

Beside legal framework, proper governmental actions, technological solutions and education to increase users' awareness are needed to protect confidentiality, integrity and accessibility of data in a smart city. The convergent roles of different stakeholders in this area are presented in [6].

The *regulatory authority in the city* (governmental control domain) ensures that service providers and citizens understand the legal framework, develops programs, policies and procedures that manage data use, and implements proper audit trail mechanism in order to ensure that no limits are crossed by service providers. By identifying vulnerable systems, assessing the type and magnitude of probable risks, and instituting remedial measures, these bodies can fight cyber-physical-attacks and create risk-resilient smart services, maintaining the trust of their inhabitants that systems are safe and secure. Digital forensic capabilities are needed at this level. Because the smart cities grow, the infrastructure becomes more interconnected and risks are multiplying. A coherent and stable digital architecture must be put in place. [31] [32]

Application developers need to specify in a very clear way the measures they have taken before user's private and confidential data are accessed, and the anonymizing and encryption procedures used when data are in transit.

The *service providers* have to share their data repositories with other service providers, without compromising their security. Privacy measures, as encrypted data search and processing in untrusted domain, fine-grained controlled over shared data, guaranteed user revocation and secure key management, have to be employed to prevent illicit data access.

4.3 Security Providers

Based on the regulations and actions of the stakeholders presented above, the security providers need to adapt the "classical" security methods as encryption, identity management techniques, device authentication mechanisms, digital certificates, digital signatures and watermarking to the new environment, and to make them available for all entities interested in a proper data protection. According to [11], since attacks continue to increase in sophistication, the development of countermeasures remains a challenging and on-going exercise. The well-known truism of information security that *the attackers are always one step ahead of "the good guys"* is confirmed once again. Also, countermeasures applicable to one system/thing may not be applicable to other embedded systems. Thus, system-specific attack-resistance measures are crucial. The devices have to dynamically adapt to the situation - scalable security protocols are necessary.

5. Conclusions

DOI: 10.12948/issn14531305/20.1.2016.03

The people's acceptance of smart cities components and the trust in them are closely related to the notions of risk, security and ensuring private life, which must be studied carefully. At the same time, since the collaboration of the cyber-real artifacts will change the environment of all public organizations, and their autonomous and nomad characteristics might lead to serious security problems, we consider they will have to be addressed, understood and solved in good time. The city authority have to be well informed about all the problems related to smart things, spaces, services and citizen security; also, the solution offered by the security providers have to be known and chosen with maximum discernment. The paper offers only a non-exhaustive review of vulnerabilities, attacks and security measures, with the intention to raise awareness in this area of large public interest. Further in-depth analyses for each vulnerability, attack scenario and security measures adequacy are necessary.

References

[1] M. Georgescu, V. D. Păvăloaia, D. Popescul and A. Țugui, "The Race for Making up the List of Emergent Smart Cities. An Eastern European Country's Approach", *Transformations in Business & Economics*, vol. 14, no 2A (35A), pp. 529-549, 2015. Available: http://www.transformations.khf.vu.lt/35a/article/thera.

[2] A. Chaudhuri, "Cyber Risk Mitigation for Smart Cities", Whitepaper at TATA Consultancy Services, 2016. Available: https://www.researchgate.net/publication/293478570 _Cyber_Risk_Mitigation_for_Smart_Cities.

[3] R. Kitchin, "Getting Smarter about Smart Cities: Improving Data Privacy and Data Security", Data Protection Unit, Department of the Taoiseach, Dublin, Ireland, 2016. Available: http://www.taoiseach.gov.ie/eng/Publications/Publications_2016/Smart_Cities_Repo rt_January_2016.pdf.

[4] F. Silva Ferraz and C. A. Guimaraes Ferraz, "Smart City Security Issues: Depicting information security issues in the role of a urban environment", in *Proc. IEEE/ACM 7th International Conference on Utility and Cloud Computing*, London, UK, 2014, pp. 842-847. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7027604.

[5] M. S. John-Green and T. Watson, "Safety and Security of the Smart City – when our infrastructure goes online", in *Proc. The 9th International Conference on System Safety and Cyber Security Conference*, Session 4b: Cyber Physical Systems, Manchester, UK, 16 October 2014. Available: http://iettv.theiet.org/technology/infopro/40756.cfm.

[6] Z. Khan, Z. Pervez and A. Ghafoor, "Towards Cloud based Smart Cities Data Security and Privacy Management", in *Proc. IEEE/ACM 7th International Conference on Utility and Cloud Computing*, London, UK, 2014, pp. 806-811. Available: http://ieeexplore .ieee.org/xpl/articleDetails.jsp?arnumber=7027598.

[7] M. Jianhua, L. T. Yang, B. O. Apduhan, R. Huang, L. Barolli and M. Takizawa, "Towards a smart world and ubiquitous intelligence: A walkthrough from smart things to smart hyperspaces and UbicKids", *International Journal of Pervasive Computing and Communications*, vol. 1, issue 1, 2005. Available: http://dx.doi.org/10.1108/17427370580000113.

[8] S. Li, T. Tryfonas and H. Li, "The Internet of Things: a security point of view", *Internet Research*, vol. 26, issue 2, pp. 337 – 359, 2016. Available: http://dx.doi.org/10.1108/IntR-07-2014-0173.

[9] G. Gan, Z. Lu and J. Jiang, "Internet of Things Security Analysis", in *Proc. IEEE International Conference on Internet Technology and Applications (iTAP)*, 2011, pp. 1-4. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6006307.

DOI: 10.12948/issn14531305/20.1.2016.03

[10] M. Hossain, M. Fotouhi and R. Hasan, "Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things", in *Proc. IEEE 11th World Congress on Services (IEEE SERVICES 2015)*, New York, USA, June 27-July 2, pp. 21-28, 2015. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7196499.

[11] A. Ukil, J. Sen and S. Kolakonda, "Embedded Security for Internet of Things", in *Proc. of 2nd National Conference on Emerging Trends and Applications in Computer Science (NCETACS)*, Shillong, India, 2011, pp. 4-6. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=5751382.

[12] Hewlett-Packard Enterprise, "Internet of Things research study" 2014, accessed on 4-May-2016 [Online]. Available: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf.

[13] L. Cilliers and S. Flowerday, "Information Security in a Public Safety, Participatory Crowdsourcing Smart City Project", *Proc. of. World Congress on Internet Security (WorldCIS-2014)*, London, UK, 2014, pp. 36-41. Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7028163.

[14] J. Bertolucci, "Big Data Drives the Smart Car", *InformationWeek* [Online], 18 March 2014, http://www.informationweek.com/big-data/big-data-analytics/big-data-drives-the-smart-car/d/d-id/1127767.

[15] L. A. Maglaras, A. H. Al-Bayatti, Y. He, I. Wagner and H. Janicke, "Social Internet of Vehicles for Smart Cities", *Journal of Sensors and Actuators Networks*, vol. 5, issue 3, 2016. Available: https://www.researchgate.net/publication/292869605_Social_Internet_of_Vehicles_for_Smart_Cities.

[16] Q. Jing, V. A. Vasilakos, J. Wan, J. Lu and D. Qiu, "Security of the Internet of Things: Perspectives and Challenges", *Wireless Networks*, vol. 20, iss. 8, 2014, pp. 2481-2501. Available: http://link.springer.com/article/10.1007%2Fs11276-014-0761-7#/page-1.

[17] D. Kushner, "The Real Story of Stuxnet. How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program", IEEE Spectrum, 26 February 2013 [Online]. Available: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

[18] ***, "Proofpoint Uncovers Internet of Things (IoT) Cyberattack", 2014 [Online]. Available: http://www.proofpoint.com/about-us/press-releases/01162014.php.

[19] Goodin, D., "New Linux worm targets routers, cameras, "Internet of things" devices", 2013 [Online]. Available: http://arstechnica.com/security/2013/11/new-linux-worm-targets-routers-cameras-internet-of-things-devices/.

[20] D. Storm, "Electronic lock picking: Hotel heists allegedly exploited Onity keycard lock hack", 2012 [Online]. Available: http://blogs.computerworld.com/security/2140 4/electronic-lock-picking-hotel-heists-allegedly-exploited-onity-keycard-lock-hack.

[21] K. J. Higgins, „Drive-By 'War Cloning' Attack Hacks Electronic Passports, Driver's Licenses," Dark Reading, February 2, 2009 [Online]. Available: http://www.darkreading.com/risk/drive-by-war-cloning-attack-hacks-electronic-passports-drivers-licenses-/d/d-id/1130291

[22] K. Stammberger, „Current trends in cyber attacks on mobile and embedded systems," 2009, Embedded Computing Design [Online]. Available: http://embedded-computing.com/article-id/?4226=#

[23]***, „Hospital cyberattack highlights health care vulnerabilities," Chicago Tribune, 2016. [Online]. Available: http://www.chicagotribune.com/business/ct-hospital-cyberattack-vulnerabilities-20160330-story.html

DOI: 10.12948/issn14531305/20.1.2016.03

[24] Institute for Critical Infrastructure Technology, „Hacking Healthcare IT in 2016: Lessons the Healthcare Industry can Learn from the OPM Breach,", 2016. [Online]. Available: http://icitech.org/wp-content/uploads/2016/01/ICIT-Brief-Hacking-Healthcare-IT-in-2016.pdf

[25] ***, "Smart Cities", 2015 [Online]. Available: https://ec.europa.eu/digital-single-market/en/smart-cities.

[26] ***, "Cybersecurity and privacy", 2015 [Online]. Available: https://ec.europa.eu/digital-single-market/en/cyber-security-privacy.

[27] European Commission, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data", 2016 [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

[28] ***, "Online Privacy", 2016 [Online]. Available: https://ec.europa.eu/digital-single-market/node/39821.

[29] The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, „Opinion 8/2014 on the on Recent Developments on the Internet of Things", 16 September 2014, [Online]. Available: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

[30] Ș.V. Greavu, „Cloud Computing: Caracteristici și Modele," ASE Publishing House, București, 2015.

[31] O. Dospinescu, D. Fotache, A. Munteanu, "Architecture For Enterprise Mobile Services," in Proceeding of the 9th IBIMA International Business Information Management Conference, Marrakech, Morocco, 2008, pp. 985-991.

[32] D. Popescul, M. Georgescu, "Internet of Things – Some Ethical Issues," The USV Annals of Economics and Public Administration, vol. 13, 2013, pp. 210-216.

Daniela POPESCUL has a PhD in Cybernetics and Statistics since 2005 and is an Associate Professor at the „Alexandru Ioan Cuza" University of Iași, Faculty of Economics and Business Administration, Business Information System Dept. She is currently teaching and researching Information Security, Project Management, Information Systems, and Knowledge Management. She authored 13 books on Information Technology and more than 50 scientific papers. She presented more than 25 papers at international conferences.

Laura-Diana RADU received his BSc in Accounting and Information Systems (2001), M.Sc. in Business Information Systems (2003), PhD in Accounting (2006) from "Alexandru Ioan Cuza" University of Iasi. Now she is researcher in Research Department of Faculty of Economics and Business Administration. Her current research interests include Digital Accounting, XBRL, Financial Auditing, Green ICT, and Business Information Systems. She has participated in over 30 international conferences in Romania and abroad (Morocco, Czech Republic, Greece, Egypt, Spain, Turkey, Malaysia, Ireland and Italy) and is the author of more than 40 scientific papers published in journals, conference proceedings or as book chapters.

DOI: 10.12948/issn14531305/20.1.2016.03