Credit: 1 PDH

Course Title:

The Importance of Internet of Things Security for Smart Cities

Approved for Credit in All 50 States

Visit epdhonline.com for state specific information including Ohio's required timing feature.

3 Easy Steps to Complete the Course:

1. Read the Course PDF
2. Purchase the Course Online & Take the Final Exam
3. Print Your Certificate

Chapter 1

The Importance of Internet of Things Security for Smart Cities

Mircea Georgescu and Daniela Popescul

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/65206

Abstract

The purpose of this chapter is to provide an extensive overview of security-related problems in the context of smart cities. The impressive heterogeneity, ubiquity, miniaturization, autonomous and unpredictable behaviour of objects interconnected in Internet of Things, the real data deluges generated by them and, on the other side, the new hacking methods based on sensors and short-range communication technologies transform smart cities in complex environments in which the already-existing security analyses are not useful anymore. Specific security vulnerabilities, threats and solutions are approached from different areas of the smart cities' infrastructure. As urban management should pay close attention to security and privacy protection, network protocols, identity management, standardization, trusted architecture, etc., this chapter will serve them as a start point for better decisions in security design and management.

Keywords: Internet of Things, smart cities, Internet of Things security, attacks in Internet of Things, smart cities security

1. Introduction

During the history of mankind, cities have been trying to offer their residents a better quality of life, a safe and comfortable environment and economic prosperity. Nowadays, citizens expect from their cities fluid transportation, clean air, responsible consumption of utilities, constant interaction with city administrators, transparent governance, good health and educational systems and significant cultural facilities. In order to answer these requests, a city needs to become smarter and smarter, continuously improving its status quo. For the purpose of this chapter, we define a smart city as 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]. Summarizing the opinions expressed in [2–10], the relevant goals for a smart city are:

- Smart mobility (traffic management, bike/car/van sharing, multimodal transport, road conditioning monitoring, parking system, route planning, electric car gearing services);
- Smart grid/energy (power generation/distribution/storage, energy management, smart metering, street lightening optimization);
- Public safety (video/radar/satellite surveillance, environmental and territorial monitoring, children protection—e.g. safer home-school journeys for children, emergency solutions, waste management, smart air quality, weather data for snow cleaning);
- Smart governance (transparent decisional process, a greater involvement of citizens in legislative initiatives, public-private partnerships, online taxing systems);
- Smart economy (high-level jobs, competitiveness, entrepreneurial spirit, innovation and research in the field) and
- Smart life (cultural and educational facilities, meaningful events, entertainment and guided tours, access to cultural sights and historical monuments, good conditions for health).

An essential element of a smart city, often neglected when focus is placed on infrastructure, is the self-decisive, independent and aware citizen. In [11], humans are seen as sensors, with a direct and active public participation, strongly facilitated by information and communication technologies (ICT). According to [12], the relationship between the city and the smart citizen should be characterized by urban openness, defined as systems' capacity to enable user-driven innovation in existing and new services, participatory service design and open data platform availability. Also, service innovation, partnership formation and urban proactiveness (the extent to which smart city services are moving towards sustainable energy use as well as ICT-enabled services) are mandatory.

In recent years, the fulfilment of these goals depends more and more on technology, especially ICT. In consequence, one of the essential nuances of the term "smart city" is given by the ICT incorporation in urban infrastructure, with solutions as 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, various smartphone apps and sharing economy platforms, etc. [12–15].

Internet of Things (IoT) has a central place among these technologies. In IoT, the physical things connect to other physical and virtual things, using wireless communication and offering contextual services. IoT is based on a global infrastructure network which connects uniquely identified objects, by exploiting the data captured by the sensors and actuators, and the equipment used for communication and localization. The radio-frequency identification

http://dx.doi.org/10.5772/65206

(RFID) lies at the basis of this development, but the IoT has developed by incorporating technologies such as sensors, printed electronic or codes, PLC, EnOcean, GPS, mobile (2G/GSM, 3G, 4G/LTE, GPRS) and short-range (NFC, Bluetooth, ZigBee, Wi-Fi, ANT, Z-Wave, IEEE 802.15.4) communications. The collaboration of the cyber-real artefacts is changing the city infrastructure, and their autonomous and nomad characteristics might lead to serious security problems that must be understood and solved in good time. A key challenge for IoT towards smart city applications is ensuring their reliability, incorporating the issues of ethics, security (confidentiality/integrity/availability), robustness and flexibility to rapidly changing environmental conditions. Without guarantees that the interconnected objects are accurately sensing the environment and are exchanging the data and information in a secure way, users are reluctant to adopt this new technology. The people's trustful acceptance of IoT components in a smart city is closely related to the notions of risk, security and ensuring private life which must be properly addressed by urban management.

2. Security challenges in Internet of Things

The aspects related to ethics and security in ICT have been a subject of study for the academic world and the wide public since the appearance of computers and the prefiguration of artificial intelligence. Thus, it is said that ICTs are of an emergent and creative nature and, explicitly or implicitly, they overtake some of our tasks and delicately induce certain moods or even force behaviour patterns, following their own development and functioning logic, imperatively heading the humankind to its maximum efficiency. Society can only answer to this by adapting and accepting the situation. Over the time, security in ICT has been treated from a historical perspective, at the organizational level, from a hacker's point of view or from a technical one. Currently, researchers approach the so-called green technologies, calm technologies, cloud computing, the impact of social media on people and communities and especially IoT, which raises a great number of security questions.

Difficulties in approaching IoT security are brought at least by the following elements:

- While city security is addressed primarily by city managers, IoT is rather understood by engineers. These two sides must dialogue and transfer knowledge both ways, a process which is not necessarily easy. If the authors of norms, standards, programs and security policies lag behind technical experts, the digital divide may deepen a lot and collaboration may prove difficult.
- One of the information security truisms says that the attackers are always one step ahead the "good guys". But while current, "classical" Internet attacks may cause damages to the information confidentiality, integrity and accessibility, similar actions in IoT can lead even to the loss of human lives. As shown in [16], there have already been demonstrations of hackers' interferences in the on-board computers of cars/planes and attacks in surgery rooms or on patients with implanted insulin pumps or other medical devices. As the list of vulnerable systems includes electric heating systems, food distribution networks, hospitals, traffic lights systems, transport networks, which are strongly interconnected in a smart city,

the attack scenarios which might be envisaged starting from here are truly scaring. In consequence, the importance of security measures increases greatly in the IoT.

- Besides attackers, the autonomous behaviour of things that invisible communicate to each other can affect our lives, in ways still difficult to predict. Anticipating dangers in IoT through a serious vulnerability scan becomes a necessity, but the process is difficult and can be done only with a sustained research and practice effort.
- IoT landscape is fragmented, because its applications are based on different architectures, standards and software platforms of significant complexity. Each smart city develops proprietary technological solutions, in response to its own problems and opportunities. In many situations the connected things, technologies and their firmware are protected by trade secrets. Legal framework is not yet appropriate, and legal responsibilities are not clear enough. Existing solutions are not interconnected and standardized, creating so-called technological silos; also, a lot of actors are involved, and various regions of the systems are controlled by different organizations.

Even this non-exhaustive presentation of the IoT-related security issues is an alarm sign that, in a smart city, every inhabitant should be assured he/she is protected by efficient technical, economic, legal and social actions. In what follows, the above mentioned problems are going to be approached in a framework in which smart cities are seen as a synergetic sum of smart devices that generate huge amounts of data while working for the smart citizens' benefit.

2.1. Security vulnerabilities in Internet of Things

The most important vulnerabilities in IoT are determined by the special nature of interconnected objects and the great variety and sensitiveness of the data collected.

2.1.1. Not-so-smart things

The objects interconnected in IoT and used in smart cities are characterized by ubiquity, miniaturization, autonomy, unpredictable behaviour and difficult identification. Their heterogeneity is impressive, ranging from tiny/invisible objects to very sophisticated embedded systems. In the same city, we can easily identify sensors used to monitor pollution and air quality, traffic and the greater road infrastructure, public and private safety, energy and water consumption, waste management, etc.; wearable sensors, placed into clothing or under the skin; usual things such as keys, watches, coffee filters, fridges, domestic heating controllers, books, doors, etc. and devices with a lot of computing power such as smartphones, tablets, printers, TVs, medical devices, SCADA (supervisory control and data acquisition) systems, cars, etc. Their number increases on a daily basis, and so do the connections between them. According to [16], all these things can be very smart in some situations and quite stupid in others: for example, smart in the sense that they collect, transmit, process and respond to various data, but stupid when there is a need to protect them. In [17], software, hardware and network constraints that restrict the inclusion of adequate security mechanisms (e.g. cryptography) directly in smart objects are identified. For this reason, security measures are usually

http://dx.doi.org/10.5772/65206

left aside, and the exposure to attacks is high. A Hewlett-Packard study is mentioned in [18] —it shows 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.

2.1.2. Deluges of sensitive data and information

Data collected by smart things are at the heart of smart cities. The problem is that they are sensitive data, often gathered without citizens' explicit consent. For example, messages, medical and academic records, personal pictures, appointments, bank account information, contacts and others can be used by the smart cities' infrastructure, with more or less security measures put in place. Safely combining IoT data from different sources is a serious issue in a smart city, since there is no guaranteed trusted relationship between the parties involved. As regards the property right on data and information, the difficulties appear from the correct identification of the authors—for example, an answer to the question "Who is the owner of data retrieved by sensors connected in IoT?" is hard to imagine at this point. When the information is personal or financial, things get more serious. The IoT omnipresence will make the boundaries between the public and private space invisible, and people will not know where their information security ends up. The Big Brother type surveillance, namely monitoring the individuals without them being aware of it, will be possible.

User privacy is strongly affected by the fact that the objects are equipped with sensors which will allow them to "see", "hear" or even "smell". The data registered by the sensors are sent in great quantities and in different ways through networks, and this can prejudice the individual's private life. According to [19], today's average smart mobile devices and applications are capable of recording user mileage, blood pressure, pulse and other intimate medical data that can be stored or sent to points of interest without the explicit user consent. These facts combined with the estimate that in 2020 the number of interconnected devices from IoT will exceed 25 billion can have devastating consequences. By means of RFID, GPS and NFC technologies, the geographic position of where a person is and his/her movements from one place to another can be easily found without his/her knowledge.

At a supra-level, smart spaces want to know everything about their inhabitants. As presented in [12], various technologies capture personally identifiable information 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. For example, a smart building is sensitive in terms of environmental condition (temperature, humidity, smoke, CO_2, extreme light, air pollution, external presences) and is 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 drivers/passengers and with pedestrians. As shown in [19], 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 the driver's identity. According to [20], 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.

2.2. Security threats in Internet-of-Things

Security threats can be divided, according to their nature, into three major categories: natural factors, based on hazard; threats caused by incidents that appeared in the system (errors); threats on systems caused by human-intended action (attacks).

2.2.1. Natural factors

The natural causes based on hazard, that can affect the IoT implementations in a smart city, can be divided into *special environment conditions* and *natural calamities or disasters*. The first category includes extremely high or low temperatures, excessive humidity or an excessively dusty environment which, in time, can determine IoT devices to break down. In the second case, the smart city infrastructure can be affected by fires, floods, strong winds, storms or earthquakes.

2.2.2. Incidents/errors

One of the most frequent *human errors* that can emerge when using IoT devices is the improper configuration, ignoring the activation of the login function or of other security mechanisms. The devices are not configured in an adequate manner, implicit factory settings are used and this is especially dangerous when passwords are involved. Proper authentication settings are not put in place, terms and conditions are not read/understood and there is no knowledge about the data collected by applications and the way of using them by third parties. Also, people give the same treatment to all the data stored in the device—without taking into account the fact that certain data, when loaded onto IoT devices, can require extra security measures. Unaware citizens are easily fooled through social engineering, spam emails, data streaming and other malicious methods. More severe are the errors that appear in the configuration of networks. The causes of errors are the "classic" ones—insufficient qualification/thoughtlessness, people's involvement in problems that are out of their competences (either due to curiosity, or from an exaggerated reliability in their own power to solve certain things), ignorance (we shouldn't expect users to use a system correctly if they haven't been trained to do so) and lack of interest in performing certain actions.

The *problems related to the software* are much more numerous in the IoT environment as compared to the classical environment, as a result of the juvenile character of IoT applications. Producers have difficulties in developing software which functions properly on all customized models. Even more challenging is the problem of portability for those who develop software for the whole range of devices found on the market. The significant software complexity involved by IoT, the requirement that each object/device must have a unique

http://dx.doi.org/10.5772/65206

identity and the large code base cause difficult testing and validation procedures. In a more specific manner, [21] shows that encryption is not used to fetch updates, update files are not properly encrypted, updates are not verified before upload and firmware usually contains sensitive information.

For various reasons, the services offered by IoT providers do not function in normal terms all the time and *communication line breakdowns/lack of signal/connexion errors* occurs. A malfunctioning at the level of a network, either from a provider or from within an organization, can result in the blocking of the infrastructure in a certain area of the city. Wireless networks are more vulnerable than the wired ones, due to interferences, frequent disconnections, broadcast transmission of data, low capacity and great mobility of devices. In consequence, the wireless channels are more susceptible to errors and this may lead to the degradation of security services, easier data interception and difficult use of advanced encrypting schemes. The physical security of objects is not guaranteed and their identification and authentication are problematic, 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.

2.2.3. Attacks

In a smart city, the attack surface is an extended one. Usual problems refer to device deliberate damage/theft, attacks on devices/components intended for recycling, malware and phishing attacks, network spoofing attacks or social engineering (e.g. apps repackaging—a malware writer takes a legitimate application, modifies it to include malicious code, then sets as available for download—or attacks using a newer version of software—creator of the malicious software sets a newer version of the app, infected with malware to the smart device user). But there are also numerous novel problems that make the attack scenarios inexhaustible.

First of all, we notice a large and increasing number of *sensor-based attacks*. To start from our pockets, we must admit that the inventory of sensors in a smartphone is intimidating: GPS chips, microphones, cameras, accelerometers, gyroscopes, the proximity sensors, magnetometers, ambient light sensors, fingerprint scanners, barometers, thermometers, pedometers, heart rate monitors, sensors capable to detect harmful radiation, back illuminated sensor, RGB light sensors, hall sensors [22]. Such sensors detect location of the mobile phone, in this way helping users to navigate in cities by maps/pictures, measure the position, tilt, shock, vibration and acceleration (the rate in change of velocity), rotations/twists, detect the presence of nearby objects without any physical contact, capture how bright the ambient light is, measure atmospheric pressure, deliver altitude data, detect the minute pulsations of the blood vessels into one's fingers and calculate one's pulse. They can capture location, movements, time stamps, even private conversations and background noises. As a result, a smartphone can be used to keep a targeted individual under surveillance. This, combined with the possibility of installing third-party software and the fact that a smartphone is closely associated with an individual, makes it a useful *spying tool*.

From a different point of view, 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 [23], video and pictures can reveal the social circle and behaviour of a citizen in a completely unexpected manner; in addition, according to [24], smartphones are more and more targeted by *malware* which accesses the microphone, cameras and other sensors. The book mentions Soundcomber, a proof-of-concept Trojan horse application that records the sounds made when digits are pressed, identifies them and tries to reveal typed PINs or passwords.

In another academic demonstration described in [25], when users placed their smartphone next to the keyboard, the deviations of accelerometer were measured. In this way, entire sequences of entered text on a smartphone touch screen keyboard were intercepted. In [26] and [27] similar successes are presented: using the motion sensors (accelerometers and gyroscopes), keystrokes (four-digit PINs and swiping patterns) were inferred from touch screens of smartphones and tablets with various operating systems. Also, in [28] it is showed that the gyroscope can be used to eavesdrop on speech in the vicinity of the phone.

From another range of IoT 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.

Various new attacks are also permitted by *short-range communication technology*. ZigBee is a global standard and protocol developed as a light wireless communication for helping the smart objects to address one to each other in a common and easy way. With low costs and good efficiency, ZigBee technologies are used in many scopes such as home automation, industrial control or medical data collection. ZigBee-enabled systems are vulnerable to security threats, such as traffic sniffing (eavesdropping), packet decoding and data manipulation/injection. Moving on to Bluetooth, some blue-prefix attacks are bluejacking (spamming nearby object users with unsolicited messages), bluesnarfing (stealing the contact information found on vulnerable devices) and bluebugging (accessing smart objects' commands without notifying or alerting their user). Also, anyone with a Bluetooth-enabled device and software for discovering passwords via multiple variants (brute force) could connect to road sensor, etc. Regarding Near Field Communication, possible security attacks include eavesdropping, data corruption or modification, interception attacks and physical thefts. At a 2012 BlackHat conference, a researcher presented his findings on how he hacked smart devices to take advantage of a variety of exploits [29].

2.3. Living in a smart city—some risky scenarios

If we take into consideration the smart cities' dimension, we can imagine a multitude of scenarios as effects of the previously mentioned vulnerabilities and threats.

http://dx.doi.org/10.5772/65206

According to Bettina Tratz-Ryan, research vice president at Gartner, "smart commercial buildings will be the highest user of IoT until 2017, after which smart homes will take the lead with just over 1 billion connected things in 2018" [30]. *Smart buildings* increasingly use technology to control aspects such as heating, lighting and physical access control—all of which are potential vectors for attackers to target. A building automation system (BAS) controls sensors and thermostats. Several areas of concern were found in the BAS architecture that could allow hackers to take control, not only of the individual building system but also of the central server, which could then be a springboard to attack other buildings. After this proof-of-concept, IBM X-Force ethical hacking team leader Paul Ionescu said that the exercise proved that very little attention was being paid to IoT in smart buildings as these devices fell outside the scope of traditional ICTs [31].

In an attempt to explore security issues in *smart city transport infrastructure* and give recommendations on how to address them, presented in [32], a Kaspersky Lab Global Research & Analysis Team (GReAT) expert has conducted field research into the specific type of road sensors that gather information about city traffic flow. Team demonstrated that information gathered by these devices, delivered and analysed in real time by the special city authorities, can be intercepted and misused, in scenarios as demolishing expensive equipment and sabotaging the work of the city authority's services. In [33], some attacks which enable the hackers to stop the engine during the travel or opening the doors of the car into the parking lot are presented. From a different point of view, [34] showed that, in public transportation, screen reflected in sunglasses were filmed and, with a special software, password entered by users were discovered.

Another example in [34] demonstrates that the mobile infrastructure used by *the police forces in a smart city* is vulnerable. With low costs and large-available equipment (including a GirlTech IMME toy instant messenger of 15$), denial-of-service and interception attacks were proved as possible. Captured clear text data included identifying features of targets and undercover agents, plans for forthcoming operations, wide range of crimes, etc.

Denial-of-service attacks can be trivially launched by malicious entities against a wireless-based communication infrastructure. In the context of a *smart grid*, such attacks have potential to disrupt smart grid functions such as smart metering, demand response and outage management, thus impacting its overall resiliency [35].

In the *health area*, [24] presents a science-fiction scenario, in which Brain-computer interfaces (BCI)-based games could provide their users stimuli that generate subconscious thoughts (e.g. part of a PIN number, passwords, financial data). These thoughts are captured by the BCI device and sent to the attacker, who analyses them, searching for sensitive information.

As presented in [16], attacks in these zones can provoke compromising entire systems, 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", has been sold on the black market since 2013. The experts in ICT 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. Another 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. In an analysis on industrial control systems (SIEMENS S7, MODBUS, DNP3, BACNET) security made at Romania's level, [35] showed that most vulnerabilities were found in GSM towers, utilities providers, furnaces and data centres. 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.

3. IoT-related security measures for a safer smart city

In an IoT-based smart city architecture, development and progress are not possible without trust. Security of each device, sensor and solution is not optional; it definitely must be taken into consideration from the very beginning. On the above presented quicksands, the need to rethink the "classical" security measures appears as mandatory. Also, specific novel measures are needed from various actors.

3.1. Legal/governmental actions

Through vast regulations and proper financing, European Union (EU) made an impressive start in the smart cities' security field. EU leaders affirm that security 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 [36]. Alliance for Internet of Things Innovation (AIOTI), an organization founded by the European Commission and various IoT key players in 2015, strongly recommends the principles of "privacy by design" (inclusion of proper security measures at the earliest stage in technological design) and "privacy by default" (no unnecessary data are collected and used) [37]. Under this umbrella, partners with different backgrounds—local authorities, telecom operators, universities, companies, small and medium enterprises—bring together their complementary legal, academic, societal, technical and business expertise and implement powerful projects. Some of the (intended) results of selected projects are presented in **Figure 1**.

Also, most European government affirm a strong interest in securing IoT, which is, in their opinion, an important factor for innovation and growth.

http://dx.doi.org/10.5772/65206

3.2. City managers

In a smart city, programs, policies, procedures, safety standards, best practices, security incidents and event management systems need to be developed and put in place. This is the attribution of the city administrator; cooperation with private sector is also mandatory. Proper audit trail mechanisms are needed in order to ensure that no limits are crossed by service providers. Because the smart cities grow, the infrastructure becomes more interconnected and risks are multiplying. A coherent and stable digital architecture must be maintained. 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.

Figure 1. Smart city–related security results in EU-funded projects.

ICT departments of the public administration have to educate the citizens in a proper way. They can use social media tools in order to provide increased awareness and control and to empower citizens to easily manage access to IoT devices and information, while allowing IoT-enabled, citizen-centric services to be created through open community APIs. No doubts regarding the collection of data and misunderstandings of legal framework are allowed to occur—inhabitants must be informed directly of any risk related to their privacy and security. Secure exchange of in-transit and at-rest data is required between IoT devices, cities and

citizens. The ultimate goal is a more self-aware behaviour of users, e.g. use of two steps of authentication on devices—at minimum, default passwords should be replaced with stronger ones; password encryption, or constant software updates.

3.3. Producers/security providers/software developers

Producers have to provide secure design and development of hardware—security methods should be built into the IoT equipment and network at the very beginning of the process, and not after its implementation. The cooperation with security providers/researchers is mandatory—they 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, also they can help producers to find and patch all the vulnerabilities before it's too late.

At the device level, information about the default names, MAC and IP addresses, ports, technological processes used in production phase, even the producer/vendor's name should be kept confidential; if the attacker has this information, he can easily find online tools for hacking the device and can obtain control on management systems of smart infrastructure. Better user configuration capabilities are necessary, as the number and the complexity of systems make it necessary to provide mechanisms allowing the users to configure the systems themselves. Feedback should be required from the users in a coherent way; consumers' opinion must be taken into consideration when devices/networks are redesigned.

In software development, testing should receive proper attention—good security scanning before launching the code is a common sense request. Also, better controls on who has access to software are needed, preventing leakage of information about passwords. 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.

4. Conclusions

In a smart city, IoT interferes strongly with inhabitants' lives. IoT, which is no more in its infancy, presents various vulnerabilities and threats, caused by technological advances and proliferated through lack of users' awareness. They are augmented by the extended use of new technologies as RFID, NFC, ZigBee, sensors, 3G and 4G that bring along the adjustment of the traditional information security threats to this new environment, as well as the emergence of new dangers. The problems treated here are of interest both for each of us, as citizens, and for the city managers, national and international regulators, especially in a world in which the borderline between the physical and virtual life is becoming more and more difficult to draw.

In this context, urban managers have to address carefully the notions of trust, risk, security and privacy. The city authority have to be well informed about all the problems related to smart

things, spaces, services and citizen security; also, the solutions offered by the security providers have to be known and chosen with maximum discernment.

The chapter 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.

Author details

Mircea Georgescu* and Daniela Popescul

*Address all correspondence to: mirceag@uaic.ro

"Alexandru Ioan Cuza" University, Iași, Romania

References

[1] Georgescu, M, Păvăloaia, VD, Popescul D, Țugui, A. The race for making up the list of emergent smart cities. An Eastern European country's approach. Transformations in Business & Economics. 2015;14(2A (35A)):529-549.

[2] Cook, DJ, Das, SK. How smart are our environments? An updated look at the state of the art. Journal Pervasive and Mobile Computing. 2007;3(2):53-73.

[3] Caragliu, A, Del Bo, C, Nijkamp, P. Smart Cities in Europe. Series Research Memoranda. University Amsterdam, Faculty of Economics, Business Administration and Econometrics. 2009;48:45-59.

[4] Gharavi, H, Ghafurian, R. Smart grid: the electric energy system of the future. Proceedings of the IEEE. 2011;99(6):917-921.

[5] Giffinger, R, Gudrun, H. Smart cities ranking: an effective instrument for the positioning of the cities?. ACE: Architecture, City and Environment. 2010;4(12):7-26.

[6] Airinei, D, Grama, A, Fotache, D, Georgescu, M, Munteanu, A, Dospinescu, O, Păvăloaia, VD, Popescul, D. The Use of Information and Communication Technologies in Organizations. Iași: Editura Universității Alexandru Ioan Cuza; 2013. 465 p.

[7] Borja, R, de la Pinta, JR, Álvarez, A, Maestre, JM. Integration of service robots in the smart home by means of UPnP: a surveillance robot case study. Robotics and Autonomous Systems. 2013;61(2):153-160.

[8] Neirotti, P, De Marco, A, Cagliano, AC, Mangano, G, Scorrano, F. Current trends in smart city initiatives: some stylised smart facts. Cities. 2014;38:25-36.

[9] Lee, JH, Hancock, MC, Hu, MC. Towards an effective framework for building smart cities: lessons from Seoul and San Francisco. Technological Forecasting and Social Change. 2014;89:80-99.

[10] Radu, LD. Green ICTs potential in emerging economies. Procedia Economics and Finance. 2014;15:430-436.

[11] Balena, P, Bonifazi, A, Mangialardi, G. Smart Communities Meet Urban Management: Harnessing the Potential of Open Data and Public/Private Partnerships through Innovative E-Governance Applications", Computational Science and Its Applications. Lecture Notes in Computer Science– ICCSA 2013. 2013;7974:528-540.

[12] Kitchin, R. Getting Smarter about Smart Cities: Improving Data Privacy and Data Security. Dublin, Ireland: Data Protection Unit, Department of the Taoiseach; 2016.

[13] Vermesan, O, Friess, P, editors. Internet of Things—From Research and Innovation to Market Deployment. Denmark: River Publisher; 2013.

[14] Camarinha-Matos, L, Afsarmanesh, H. Collaborative systems for smart environments: trends and challenges. Collaborative Systems for Smart Networked Environments, IFIP Series. 2014;434:3-14.

[15] Borgia, E. The Internet of Things vision: key features, application and open issues. Computer Communications. 2014;54(1):1-31.

[16] Popescul, D, Radu, LD. Data security in smart cities: challenges and solutions. Informatica Economică. 2016;20(1):29-39.

[17] Hossain, M, Fotouhi, M, Hasan, R. 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); June 27-July 2; New York. 2015. p. 21-28.

[18] Hewlett-Packard Enterprise. Internet of Things Research Study [Internet]. 2014. Available from: http://www8.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf [Accessed: 4 May 2016]

[19] Bertolucci, J. Big Data Drives the Smart Car [Internet]. 18 March 2014.Available from: http://www.informationweek.com/big-data/big-data-analytics/big-data-drives-the-smart-car/d/d-id/1127767 [Accessed: 5 May 2016]

[20] Maglaras, LA, Al-Bayatti, AH, He, Y, Wagner, I, Janicke, H. Social internet of vehicles for smart cities. Journal of Sensors and Actuators Networks. 2016;5(3).

[21] Muller, M. IoT Security: The Ugly Truth [Internet]. 25 September 2015.Available from: https://www.youtube.com/watch?v=j2qAkWDSDkg [Accessed: 10 May 2016]

[22] Agarwal, D. Testing Mobile Apps: Smartphones Sensors List [Internet]. 17 February 2016.Available from: https://testingmobileapps.wordpress.com/2016/02/17/smartphones-sensors-list/ [Accessed: 20 May 2016]

[23] Cilliers, L, Flowerday, S. Information security in a public safety, participatory crowd-sourcing smart city project. In: Proceedings of World Congress on Internet Security (WorldCIS-2014); 2014; New York, USA: Curran Associates, Inc. London, UK. p. 36-41.

[24] Loukas, G. Cyber-Physical Attacks: A Growing Invisible Threat. Elsevier; 2015.

[25] Owusu, E, Han, J, Das, S, Perrig, A, Zhang, J. ACCessory: password inference using accelerometers on smartphones. In: Proceedings of the Twelfth Workshop on Mobile Computing Systems & Applications; 2012; p. 9-15.

[26] Al-Haiqi, A, Ismail, M, Nordin, R. On the Best Sensor for Keystrokes Inference Attack on Android. In: The 4th International Conference on Electrical Engineering and Informatics (ICEEI 2013); 2013.

[27] Xu, Z, Bai, K, Zhu, S. Taplogger: inferring user inputs on smartphone touchscreens using on-board motion sensors. In: Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks; 2012. p. 113-124.

[28] Michalevsky, Y, Boneh, D, Nakibly, G. Gyrophone: recognizing speech from gyroscope signals. In: Proceedings of the 23rd USENIX Security Symposium; 20-22 August; 2014.

[29] Appleby, T. Is NFC Still a Vulnerable Technology? [Internet]. 17 June 2013.Available from: https://securityintelligence.com/is-nfc-still-a-vulnerable-technology [Accessed: 15 April 2016]

[30] Gartner. Next year, smart cities will use 1.6 billion connected things [Internet]. 10 December 2015.Available from: https://www.helpnetsecurity.com/2015/12/10/next-year-smart-cities-will-use-16-billion-connected-things/ [Accessed: 14 May 2016]

[31] Millman, R. How Vulnerable are Smart Buildings to Cyber Hacks? [Internet]. 29 March 2016.Available from: http://www.ifsecglobal.com/how-vulnerable-are-smart-buildings-to-cyber-hacks [Accessed: 1 May 2016]

[32] Kaspersky Lab. Traffic Jams: Kaspersky Lab Discovers Security Issues in Smart Transport Monitoring System [Internet]. 18 April 2016.Available from: http://www.kaspersky.com/about/news/virus/2016/Traffic-Jams [Accessed: 18 May 2016]

[33] Popa, M, Cartas, C. OBD2 IoT device proof of concept for the insurance companies connected cars. In: Proceedings of the 15th International Conference on Informatics in Economy (IE 2016)—Education, Research & Business Technologies; 2-5 June; Cluj-Napoca, Romania. Cluj-Napoca, Romania: Bucharest University of Economic Studies Press; 2016. p.103-107.

[34] Rubin, A. All your Devices can be Hacked [Internet]. October 2011.Available from: https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked [Accessed: 10 May 2016].

[35] Sechel, S. Information insecurity: an assessment of the Romanian cyberspace. In: Proceedings of the 15th International Conference on Informatics in Economy (IE 2016)

—Education, Research & Business Technologies; 2-5 June; Cluj-Napoca, Romania. Cluj-Napoca, Romania: Bucharest University of Economic Studies Press; 2016. p. 314-320.

[36] European Union. Online Privacy [Internet]. [Updated: 11 April 2016]. Available from: https://ec.europa.eu/digital-single-market/node/39821 [Accessed: 13 May 2016].

[37] 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 [Internet]. 27 April 2016. Available from: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 [Accessed: 20 May 2016].