Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 109C (2017) 1086–1091

Procedia Computer Science

www.elsevier.com/locate/procedia

The International Workshop on Smart Cities Systems Engineering (SCE 2017)

Cyber Security Attacks on Smart Cities and Associated Mobile Technologies

Anwaar AlDairi and Lo'ai Tawalbeh*

Computer Engineering Department,
College of Computer and Informatino Systems, Makkah, Saudi Arabia

Abstract

Smart City refer to the city that integrates modern technologies for automated and efficient service providing to enhance citizens' lifestyle. Latest studies show that like 60 present of the whole world's population will be living in urban environments by the year 2030. This massively growing population in urban environments leads to the need of advanced management approaches that use latest IT platforms and techniques for smartening every city-related service. Such emergent integration of technologies faces several security- related challenges because of not considering security tests of new deployed technologies, in addition to not engaging other system parties with security incidents due to the huge communication. On the other side, high complexity, high interdependency and intensive communication lead to unbounded attack surface and cryptography-related issues. In our paper, we intend to provide detailed overview based on literature of smart cities' major security problems and current solutions. Moreover, we present several influencing factors that affect data and information security in smart cities.

Peer-review under responsibility of the Conference Program Chairs.

Keywords: Smart Cities Technologies, Cloud Computing, Mobile Devices, Cyber Security.

1. Introduction

There is no specific and universal definition for the concept smart city as countries and their governments determine how far they go for smartening according to their willingness to change, resource limitations and financial status [1]. However, we generally use the concept smart city for the integration between traditional infrastructure and

* Corresponding author. Lo'ai A. Tawalbeh Tel.: +966-553-506-982; fax: +0-000-000-0000 .
E-mail address: LATAWALBEH@uqu.edu.sa

Peer-review under responsibility of the Conference Program Chairs.
10.1016/j.procs.2017.05.391

latest technologies of information and communication to create an entire system for resource-efficient and real time city-related service providing in urban environments.

There are five main components that are essentially required to be in a smart city: modern information and communication technologies, buildings, utilities and infrastructure, transportation and traffic management and the city itself[2]. Technically, smart city is about the cooperation between governance institutes and public and private foundations to implement and deploy long-term computerized platforms that impose using modern technologies including mobile cloud computing[3], electronic objects, networks and intelligent decision-making methodologies. Smart cities worldwide aim generally to handle the main challenges that currently face the globe such as climate changes, limited resources, Urbanization and high population growth. Moreover, smart cities aim to secure economic competitiveness in urban spaces and let urban citizens experience classier lifestyles[4]. Concepts to become smart are as different as cities themselves. In General, there are six dimensions or areas where cities can become smarter: smart governance, smart economy, smart people, smart mobility, smart living and environment[5] (Figure 1).

Smart city is not only about deploying smart platforms to perform city-related services efficiently, but it is a huge concept that comprises several physical and electronic objects that interact and communicate

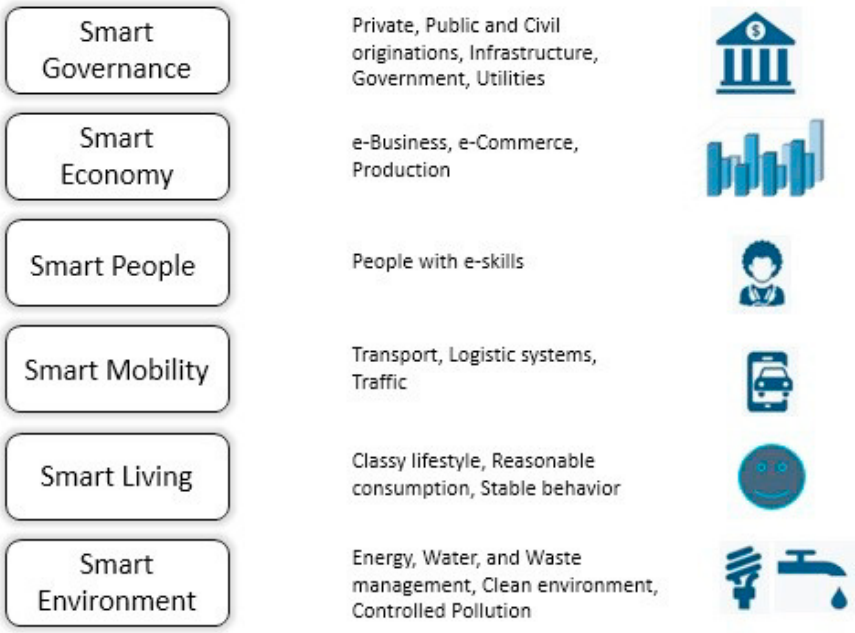

Fig. 1. Dimensions of Smart Cities

through wired and wireless networks. On the other side smart city is about several computer-related sciences that are used along the whole smartening process such as artificial intelligence, cloud computing, embedded computing and biometrics. In addition to the hired modern technologies that are considered the core of smart city entire regulation such as RFID (Radio Frequency Identification System) and smart hand held devices (phones, laptops, tablets, etc.). Clearly, smart cities are complex and interdependent huge systems and this leads to several political, social, economic, and technical problems and challenges. Costs and funding, continuously changing population's needs, collaboration among stakeholders, people-friendly interfaces, interoperability, security and privacy are examples for problems that face smart cities. In this paper, we focus on the security and privacy of smart cities since Information security and data privacy are critical challenges that cause real harms if not well considered.

Insuring security in smart cities indicates protecting data, information and network from any attack and malicious activity. However, there are security-related challenges that complicate security maturity in smart cities. Deployed hardware and software to smart cities are usually released from their vendors without sufficient testing for cyber

security. Using such insecure products may cause several hacks leading to filling the system with fake data, which causes systems shutting down and service termination. To measure how smart a city is, we look at the level of automation and computer systems it uses, in addition to the integration between its systems. This high integration leads to operational interdependencies from the most critical systems to the simplest ones causing huge cascade attack that can damage the whole infrastructure and communication. On the other side, smart cities face problems in vulnerabilities assessment and response and recovering plans. Finally, taking care of security is costly and getting enough budget requires long process in public sectors.

To sum up, security-related problems in smart cities are real and current and need instant considering and analyzing. Thus, security, privacy and related issues are hot topics especially that smart city's technologies and systems are becoming very important to optimize cities and enhance the quality of life. In our paper, we are considering several security and privacy concerns in smart cities. By data security, we mean data tendency to be accidentally or intentionally affected by technical failures caused by attacks or malicious activities; and by data privacy, we mean the ability to protect data from unauthorized accessing or re-using in addition to protect their collection processes and all operations being run on them.

2. Related Works

Security and privacy are always hot topics to discuss. For smart city, security and privacy concerns are even more important than they are for any technological phenomena because number of smart cities is increasing rapidly worldwide. Thus, researchers must pay more attention so security and privacy concerns in smart cities in order to enrich literature with more researches and studies in this regard. For our paper, we reviewed several valuable researches that discuss security and privacy challenges and related issues.

In[6], the authors present smart cities as state of the art gathering of information and communication technologies and they discuss current urban problems and urban modern technologies. In addition to that, they clarify current risks and uncertainties in smart cities by defining six scenarios of cities that are stated smart. The work in[7] provides information about requirements, benefits and challenges in the smart city research area. It also talks about the new vision of Cloud of Things (CoT), which is the integration between the technology Internet of Things and the science of Cloud Computing CC[8]; and it discusses how smart cities services can be provided based on Cloud of Things.

In [9], the authors examined security and privacy concerns through providing a model that represents the major elements of smart cities (servers, people and things) and the interaction among them. In[10], the authors discuss the regulations on security and privacy violations and they state that these regulations do not suit the importance and criticality of security and privacy issues.

It is known that smart cities provide huge benefits to the users, but at the same the users concern about their data privacy that is transferred over non-secure channels. So, it is a must to secure the communication channels in order to provide safe media to move data specially over wireless networks[11, 12]. In[13], the authors discuss privacy trade-off with smart city. They converse the down sides that smart cities might bring into our lives regarding the violations of privacy that may occur. Users must pay huge attention to what they share and must know that once they share any piece of personal data, it will not disappear. It is important to alert planners and analysts for the necessity of thinking about protection against security vulnerabilities during the design of smart city. The cyber-infrastructure technologies must be determined during design process to predict the smart city response.

3. Security in Smart City

We mentioned that to mature a specific city from being connected to being smart is quite tricky and challenging security-wise process as it implicates high level of dependency and connectivity across its layers (data/information, technology, application, and infrastructure). In this section, we present main security challenges and related violations that may occur in every layer of smartening a city.

3.1. Infrastructure Security

Several vulnerabilities and risks face cyber-physical infrastructure used in city smartening. However these modern cyber-physical infrastructure systems are massively used, there is no satisfying insight for their vulnerabilities and threats. Generally, intentional and accidental threats on smart city infrastructure-related security cause different serious consequences according to city's maturity and smartness. Thus, we present main encountered infrastructure security-related threats and challenges. Urban infrastructure such as electricity supply, water distribution, streets, buildings and others face several security threats in their specific cyber-physical components and systems such as:

- cameras: cities are full of private and public cameras which both are protected variably using encryption protection and username/password protection. Reaching private or public cameras and having access on them cause violation to individuals' privacy and spying on governmental concerns.
- communication networks: cyber-physical objects are connected together along the smart city using several communication technologies such as WiFi, 4G, RFID, GSM and others. Each of which has specific security concerns that must be perceived during deployment and use of communication technologies.
- building management systems: designers and developers of such systems usually concentrate on the service provided and disregard cyber security related issues. Thus, manufacturers of such systems do not uphold these systems with notification options to notify users about security violations and do not respond to vulnerabilities, which result in building management systems that are insecure and weakly protected;
- transport management systems: such systems face the most critical hacks as they cause catastrophes especially when they happen to air traffic systems or trains control systems. Moreover, they cause huge traffic jams that may last for hours by hacking control systems of traffic lights and their sequencing, road signs and speed limit signs.

Basically, urban infrastructure is a combination of cyber physical systems that are integrated to physical independent components. CPSs comprise of interconnected physical objects such as sensors, computing elements, networking objects etc. In smart Cities, CPSs must accomplish main three tasks, which are collecting data, deciding which efficient processes have to be run and controlling physical components. Following we present briefly the main threats that intimidate urban infrastructure's integrity:

- Eavesdropping: implant eavesdropping tools in specific network for spying on communication channels, capturing the network traffic behavior and getting the network map. Eavesdropping is dangerous threat that leads to break down the integrity and confidentiality which causes financial and personal failures.
- Theft: it affects urban infrastructure by stealing intangible stuff such as sensitive data, information, credentials, software and cryptographic keys; and by stealing tangible physical objects such as hand held devices (smartphones, laptops, and tablets, etc.) and technological equipment. It breaks down systems' availability and confidentiality, which causes financial shortages and reputational loose.
- Denial of Service DoS: is to overflow connections until services and devices relying on this connection are blocked. DoS attacks affect the availability of systems or connections.
- Other threats can be caused accidentally by hardware failure, software crashing, environment and nature behavior and vendors and manufacturer end of support. Such threats affect the availability and integrity of infrastructure systems, which causes deficiency in production and service providing.

3.2. Data/Information Privacy in Smart Cities

Smart Cities deal with huge quantities of real time data and related technologies that is data-driven technologies that act on, generate, process, run, and produce data. Smart Cities have many resources producing different types of data. Among these resources are systems that continuously produce fine-scaled and exclusive data. These systems are widespread in smart cities and the data they produce are called big data[14,15]. Other systems transform small and traditional data into infrastructure datasets that are used in several ways. There are systems that make locked data available for public- called open data. One more systems are machine learning related systems that develop new data and data analytics. All these urban data are used to run smart city technologies, so it is important to keep these vast amounts of data and information secure. Moreover, it is necessary to maintain the privacy of locked data and personal data and to make sure that they are not intentionally or accidentally reached or accessed. Privacy is ensured by protecting five privacy related issues: protecting identities that indicate protecting personnel and their confidential data; protecting people areas that indicate to protect each one's space and properties; protecting locations which indicate preventing spatial tracking; communication protection which indicate not to eavesdrop any kind of conversations; and finally, transactions protection that protect every single purchase, exchange and query. The privacy related issues can be classified in to three categories of privacy: communication, individual and business privacy[16] (Table 1).

Table 1.Privacy-related challenges and violations

Category	Privacy-Related Challenge	Violations	Description
Communication Privacy	• M2M communication • Citizen to smart city communication	Eavesdropping	To spy on all kinds of conversations and recordings and to listen to communication channels; or we may say reading data by unauthorized readers[17].
		DOS	To block all system's operations by using its radio signals for broadcasting devices for malicious purposes; or we may say to blind smart cities[18].
		Man-in-the-Middle attack	Intercept communication channels to manipulate transmitted data, and falsified operators' actions [16]
		Side Channel Attacks	To use whatever reached information about the physical implementation of computing tasks such as power consumption and execution time [19, 20]
		Identification	Linking data and information to whom they belong.
		Secondary use	Using data and information collected according to specific permission and particular use for another unpermitted purposes.
Business Privacy	• Banking • E-commerce	Phishing	To impersonate trusted reputable party for gaining critical information such as passwords and credit cards n40bers via emails and instant messages [21].
		Spoofing	To duplicate data by third malicious and send it to the reader after revealing the security protocol[16].
		Attacks to data integrity	Get information about customers and networks and inject false data to system's monitoring centre[22].

4. Conclusion

Smart City's cyber security is very important issue that involves considering several security concerns about technology, applications, infrastructure and information/data. Mainly cyber security is affected by the emergent integration of technologies and the resulted intensive communication, high complexity and high interdependency, which leads to unbounded attack surface and cryptography-related issues. Cyber security of smart cities is an important issue that needs international collaboration, which includes experts from all over the world.

Acknowledgment

This work is funded by grant number (13-INF2526-10) from the Long-Term National Science Technology and Innovation Plan (LT-NSTIP), the King Abdul-Aziz City for Science and Technology (KACST), Kingdom of Saudi Arabia.We thank the Science and Technology Unit at Umm Al-Qura University for their continued logistics support.

References

1. SIEMENS. Available from: <http://www.siemens.com/innovation/en/home/pictures-of-the-future/infrastructure-and-finance/smart-cities-facts-and-forecasts.html>. [Jan 2017]
2. FORBES. Available from: < http://www.forbes.com/sites/peterhigh/2015/03/09/the-top-five-smart-cities-in-the-worl/#5715497d5a0e> [Dec 2016]
3. Tawalbeh LA, Alassaf N, Bakheder W, Tawalbeh A. Resilience Mobile Cloud Computing: Features, Applications and Challenges. In 2015 Fifth International Conference on e-Learning (econf) 2015 Oct 18 (pp. 280-284). IEEE.
4. Lo'ai AT, Basalamah A, Mehmood R, Tawalbeh H. Greener and smarter phones for future cities: Characterizing the impact of GPS signal strength on power consumption. IEEE Access. 2016;4:858-68.
5. Vanolo A. Smartmentality: The smart city as disciplinary strategy. Urban Studies. 2013 Jul 11:0042098013494427.
6. Batty M, Axhausen KW, Giannotti F, Pozdnoukhov A, Bazzani A, Wachowicz M, Ouzounis G, Portugali Y. Smart cities of the future. The European Physical Journal Special Topics. 2012 Nov 1;214(1):481-518.
7. Petrolo R, Loscrì V, Mitton N. Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms. Transactions on Emerging Telecommunications Technologies. 2015 Feb 1.
8. Tawalbeh LA, Haddad Y, Khamis O, Aldosari F, Benkhelifa E. Efficient software-based mobile cloud computing framework. InCloud Engineering (IC2E), 2015 IEEE International Conference on 2015 Mar 9 (pp. 317-322). IEEE.
9. Elmaghraby AS, Losavio MM. Cyber security challenges in Smart Cities: Safety, security and privacy. Journal of advanced research. 2014 Jul 31;5(4):491-497.
10. Bartoli A, Hernandez-Serrano J, Soriano M, Dohler M, Kountouris A, Barthel D. On the Ineffectiveness of Today's Privacy Regulations for Secure Smart City Networks. Smart Cities Council, Washington, DC. 2012 Nov.
11. Sklavos N, Zhang X. Handbook of Wireless Security: From Specifications to Implementations. CRC-Press, A Taylor and Francis Group, ISBN X. 2007;84938771:2007.
12. Moh'd A, Aslam N, Marzi H, Tawalbeh LA. Hardware implementations of secure hashing functions on FPGAs for WSNs. InProceedings of the 3rd International Conference on the Applications of Digital Information and Web Technologies (ICADIWT 2010 Jul.
13. Ahmed KB, Bouhorma M, Ahmed MB. Age of big data and smart cities: privacy trade-off. arXiv preprint arXiv:1411.0087. 2014 Nov
14. Lo'ai AT, Bakheder W, Song H. A mobile cloud computing model using the cloudlet scheme for big data applications. InConnected Health: Applications, Systems and Engineering Technologies (CHASE), 2016 IEEE First International Conference on 2016 Jun 27 (pp. 73-77). IEEE.
15. Lo'ai AT, Mehmood R, Benkhlifa E, Song H. Mobile cloud computing model and big data analysis for healthcare applications. IEEE Access. 2016;4:6171-80.
16. Ijaz, Sidra, Munam Ali Shah, Abid Khan, and Mansoor Ahmed. "Smart Cities: A Survey on Security Concerns." INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS 7, no. 2 (2016): 612-625.
17. Cédric, LÉVY-BENCHETON, Eleni DARRA, Daniel Bachlechner, Michael Friedewald, Timothy MITCHENER-NISSEN, Monica LAGAZIO, and K. U. N. G. Antonio. "Cyber Security for Smart Cities-an Architecture Model for Public Transport. pdf." (2015).
18. Oliveira LM, Rodrigues JJ, Sousa AF, Lloret J. Denial of service mitigation approach for IPv6- enabled smart object networks. Concurrency and Computation: Practice and Experience. 2013 Jan 1;25(1):129-42
19. Lo'ai AT, Somani TF. More Secure Internet of Things Using Robust Encryption Algorithms Against Side Channel Attacks.
20. Lo'ai AT, Somani TF, Houssain H. Towards secure communications: Review of side channel attacks and countermeasures on ECC. In Internet Technology and Secured Transactions (ICITST), 2016 11th International Conference for 2016 Dec 5 (pp. 87-91). IEEE
21. TechTarget. Available from < http://searchsecurity.techtarget.com/definition/phishing> [Jan 207]
22. Nanni G. (2013/. Transformational 'smart cities': cyber security and resilience. Symantec, Mountain View, CA.