Cybersecurity for Smart Cities: A Brief Review

Armin Alibasic, Reem Al Junaibi, Zeyar Aung*, Wei Lee Woon, and Mohammad Atif Omar

Institute Center for Smart and Sustainable Systems (iSmart),
Masdar Institute of Science and Technology,
Abu Dhabi, United Arab Emirates
{aalibasic,raljunaibi,zaung,wwoon,momar}@masdar.ac.ae

Abstract. By leveraging advancements in information and communications technology (ICT), Smart Cities offer many potential benefits like improved energy efficiency, management and personal security. However, this dependence on ICT also makes smart cities prone to cyber attacks. In this paper, we investigate the topic of cybersecurity for smart cities. We show how the specific characteristics of smart cities give rise to cybersecurity challenges, and review the different threats faced. Finally, we review some of the more important cybersecurity solutions for smart cities that have been proposed.

Keywords: Cybersecurity, Cyber Threats, Smart City, Smart Grid, Internet of Things

1 Introduction

Rapid advances in ICT have been exploited to streamline the design, operation and management of urban environments in a variety of ways. For example, it is now possible to monitor and manage energy consumption patterns in real time with smart meters, use this information to coordinate generation and distribution resources via the smart grid, continuously track traffic congestion and road hazards and communicate this automatically to vehicles and commuters. Progress in these areas have helped to cut costs, increase efficiency, bring about greater safety and convenience, and reduce pollution and greenhouse gas emissions.

A smart city can be defined as: "*A smart city uses digital technologies or information and communication technologies (ICT) to enhance quality and performance of urban services, to reduce costs and resource consumption, and to engage more effectively and actively with its citizens. Sectors that have been developing smart city technology include government services, transport and traffic management, energy, health care, water and waste.*" [23].

According to well-known urban strategist Boyd Cohen, smart cities can be divided into six key components: (1) Smart Economy, (2) Smart Environment, (3) Smart Government, (4) Smart Living, (5) Smart Mobility, and (6) Smart People. Table 1 shows the six key components for smart cities [12].

* Corresponding author.

Component	Indicators and Benefits
Smart Economy	Entrepreneurship & Innovation, Productivity, Local and Global Interconnectedness
Smart Government	Supply and Demand Side policies, ICT, E-Government Application, Transparency, Open Data
Smart Living	Culturally vibrant, happiness, health and safety
Smart Mobility	Connected, ICT, Support for clean and non-motorized options, mixed modalities
Smart People	Creative, Inclusive, Emphasis on educational excellence

Table 1. Key smart city components

While many of the "flagship" smart city developments have been designed from the ground up, the concept stands to make the most impact in situations where ICT technology is progressively integrated into the operations of existing urban areas. Cities can become "smart" by adopting modern technologies for transportation, traffic control, disaster response and security, resource management and other aspects of city management.

These enhancements are extremely valuable do carry a number of inherent risks. These tend to be rooted in the fact that a smart city often entails many new systems and devices being deployed in novel circumstances and often without adequate security testing. Many of these technologies are wireless and so depend on custom protocols and encryption platforms. Even seemingly minor bugs can cause very serious problems. For example in May 2012 the placer county courthouse system in California accidentally summoned 1,200 people to jury duty on the same morning, an incident which resulted in severe traffic jams throughout the city [6]. In this particular case, the event was the result of an unintentional computer glitch, but it would not be difficult to envision a situation where a hostile party could intentionally create a similar "glitch" to disrupt public life in a similar way.

Of even greater concern is the fact that many smart cities have yet to develop action plans which outline responses to possible cyber attacks which target the city's services, infrastructure and ICT systems. Because all systems are fundamentally interconnected, weaknesses in any one element can have wide-ranging consequences. For example, encryption problems can result in a compromised wireless network, which in turn can be exploited by hackers to attack a city's

electricity or water supply. It is clear that cyber threats to smart cities need to be taken extremely seriously.

Possible solutions include:

1. Creation and use of security check lists for encryption, authentication, authorization, and software updates while implementing new systems
2. Implementation of failsafes and manual overrides on all city systems
3. Development of action plans and procedures for responding to cyber attacks

We will focus more on these solutions in the evaluation section of this paper. According to Gartner [5], by the end of 2020 there will be 25 billion connected devices. Other projections [4] indicate that 70% of the world's population is expected to live in urban environments by 2050. The rapid growth in the worldwide urban population, as well as the increasing interconnectedness of this demographic makes the cybersecurity of cities incredibly important, and the situation will only become even more pressing with the introduction of ever more intelligent and connected devices and infrastructure.

A wide variety of systems, ranging from home appliances to medical devices in hospitals to air defense systems, will be affected by a single cyber attack which targets the energy grid. The weapon of choice in this modern age is no longer a bomb, but rather malicious software (known as malware) designed to destroy, disrupt or take control of the complex systems which control the operation of smart grids. In addition, the immense complexity and scale of a smart city would mean that these issues need to addressed as early as possible, and that, in the case of many existing cities, it may already be too late to incorporate adequate cybersecurity measures.

The cyber threat landscape is extremely fluid. The last few years have seen an exponential growth in the number of potential threats. In a 2012 report, McAfee Labs stated that, "*For the year, new malware sample discoveries increased 50 percent with more than 120 million samples now in the McAfee Labs 'zoo'* " [17]. The specific nature of the threats themselves are also evolving and are increasing in sophistication. Advanced persistent threats (APT), where an unauthorized entity gains and retains access to a network, are a good example of this trend. In many cases, the attackers are no longer "script kiddies", but are highly skilled and organized professionals who are able to deploy a variety of sophisticated techniques to launch complex and coordinated attacks. Examples of well-known cyber threats include:

- Hackers
- Malware
- Zero days
- Botnets
- Denial of service (DOS)
- Distributed denial of service (DDOS)

While all these terms are by now quite widely known, the scope of the attacks have now broadened and include industrial control systems, as was demonstrated in 2010 with Stuxnet [24].

2 Smart City Cyber Challenges

There is an extensive body literature on the topic of smart cities. Some papers [18, 13] provide useful guidelines for policy makers and city managers seeking to better define and drive their smart city strategy and planning actions towards the most appropriate domains of implementation. Other papers [19, 25] have described the deployment and experimentation architecture of the Internet of Things (IoT) so they can provide a suitable platform for large scale experimentation and evaluation of IoT concepts under real-life conditions. Some authors [14] apply a Quality Function Deployment (QFD) method to establish interconnections between services and devices, and between devices and technologies for smart cities.

However none of above mentioned papers emphasized cybersecurity. Seto et al. [20] discussed the privacy risks associated with advances in the standardization of the smart grid, whose technology is at the core of the smart city. They verified the effectiveness of privacy impact assessment, with reference to privacy risks in the smart city, where all kinds of user data are stored in electronic devices, thus making everything intelligent. Yibin et al. [15] presented a mobile-cloud-based smart city framework, which is an active approach to avoid data over-collection. By putting all of the users' data into the cloud, the security of users' data can be greatly improved.

Matuszak et al. [16] and Wang et al. [22] carried out a series of studies on reducing the risks of cyber intrusions and detecting various types of attacks on the smart grid, which can be regarded as a subset of the smart city, and developed algorithms and visualization techniques for cyber trust in a smart grid system. Cyber trust was evaluated in terms of a mathematical model consisting of availability, detection and false alarm trust values, as well as a model of predictability.

In addition to the above theoretical studies, researchers have also performed experiments on real-world scenarios. Research conducted by Hioureas and Kinsey [11] proved how surveillance technology systems could also be used in a harmful way. They performed man-in-the-middle attack by using methods such as Address Resolution Protocol (ARP) poisoning. That enabled them to alter any data sent to and from the router. Figure 1 shows an attacker who tells the user he is the router, and tells the router he is the user, thus intercepting traffic to and from the web server is easy.

Cerrudo [7] provided an overview of current cybersecurity problems affecting cities as well as real threats and possible cyber attacks that could have a huge impact on cities. Some of possible weak points mentioned were:

- Traffic Control Systems
- Smart Street Lighting
- City Management Systems
- Sensors
- Public Data
- Mobile Applications

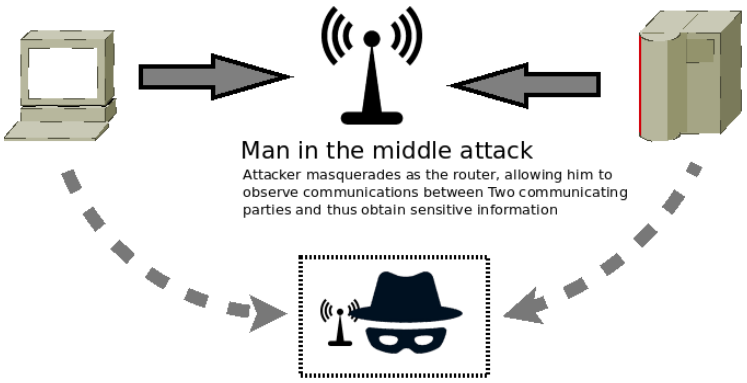

Fig. 1. An attacker masquerades as the router to gain access to sensitive communication

- Cloud and Software as a Service (SaaS) Solutions
- Smart Grid
- Public Transportation
- Cameras
- Social Media
- Location-based Services

One example that was mentioned pertained to an attack on sensors, which form the backbone of the smart city: "*Attackers could even fake an earthquake, tunnel, or bridge breakage, flood, gun shooting, and so on, raising alarms and causing general panic. An attacker could launch a nuisance attack by faking data from smell or rubbish level sensors in empty garbage containers, to make garbage collectors waste time and resources. Keep in mind that many systems and services from cities rely on sensors, including smart waste and water management, smart parking, traffic control, and public transport. Hacking wireless sensors is an easy way to remotely launch cyber attacks over a city's critical infrastructure.*" [7].

According to a poll conducted by researchers at the Morning Consult firm [2], nearly 36 percent of voters consider acts of terrorism as the main security threat to the USA, followed by cyber-attacks at 32 percent, while "war with a large military power" was perceived as the third greatest threat with 12.1% of the vote (see Fig. 2). With all this in mind and from analyzing the papers cited above, we can see the importance of devoting additional resources and attention to securing smart cities from cyber attacks.

3 Proposed Solutions

One of many possible smart city cybersecurity solutions was proposed by Cerrudo et al. [8]. In their report, the authors provided guidelines for the organizations responsible for selecting and testing the technologies which would be

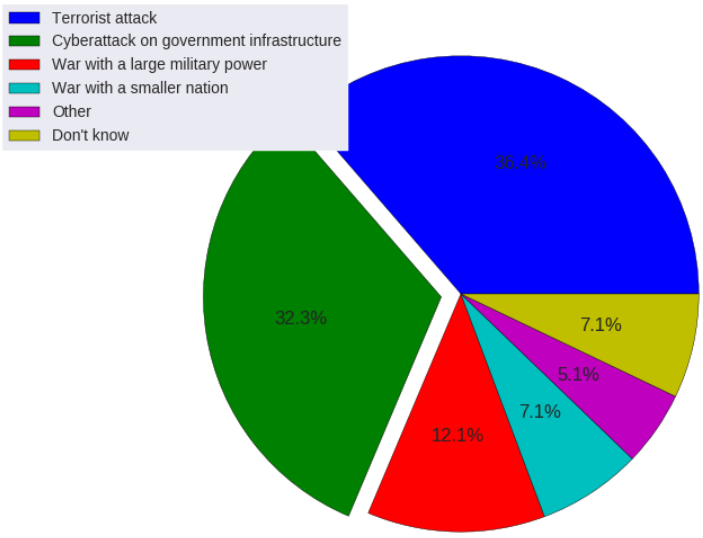

Fig. 2. Perceived US security threats [3]

deployed in a smart city. The focus was on appropriate testing and assessment strategies to be followed when selecting these technologies as well as the respective vendors.

Firstly, the importance of a structured and well thought out technology selection process cannot be understated. In particular, it must be stressed that issues of cybersecurity should be taken into account right from this early stage. In the context of a smart city, all systems are inter-dependent and weak services can cause large-scale damage and even affect national stability and security. A smart city requires new levels of confidentiality, integrity, availability and defense. All wired and wireless communications (data in transit) should be properly protected with strong encryption. The solution should support strong authentications mechanism (one-time passwords, certificate or biometric-based authentication etc.). All functionality should require and enforce proper permissions (authorization) before performing any action. Updates of software, firmware, etc. should be automatic and secure. Logs must also be saved securely against tampering. Devices should have a mechanism to prevent tampering by unauthorized sources. In the case of a system malfunctioning or crash, the system should remain secure and security protections remain enforced. Solutions should come with a secure configuration by default. All of these their recommendations are for Technology Selection.

The second is the recommendations for technology implementation, operation and maintenance. For implementation technology should pass selection phase security test; technology should be securely delivered; enable strong encryption;

secure system administration; set strong passwords; remove unnecessary user accounts; disable unused functionality and services; enable auditing of security events, etc. For operation and maintenance technology should pass monitoring, patching, regular assessment and auditing, protection of logging environment, access control, cyber-threat intelligence, compromise reaction and recovery.

The third is the recommendations for technology disposal. We should avoid repurposing technology, all data should be erased securely and if that is done by vendors then they should do the same.

Cerrudo et al. [8] also proposed a checklist of security related steps that smart city operators and administrators should consider implementing.

- Create a simple checklist-type cybersecurity review. Check for proper encryption, authentication, and authorization and make sure the systems can be easily updated.
- Ask all vendors to provide all security documentation. Make sure Service Level Agreements include on-time patching of vulnerabilities and 24/7 response in case of incidents.
- Fix security issues as soon as they are discovered. A city can continuously be under attack if issues are not fixed as soon as possible.
- Create specific city CERTs that can deal with cybersecurity incidents, vulnerability reporting and patching, coordination, information sharing, etc.
- Implement and make known to city workers secondary services/procedures in case of cyber attacks, and define formal communication channels.
- Implement fail safe and manual overrides on all system services. Don't depend solely on the smart technology.
- Restrict access in some way to public data. Request registration and approval for using it, and track and monitor access and usage.
- Regularly run penetration tests on all city systems and networks.
- Finally, prepare for the worst and create a threat model for everything.

Gurgen et al. [10] suggested smart city objectives should encourage self-awareness and provided a set of guidelines and recommendations to achieve this. One of the most frequently adopted models for realizing an autonomic system is the MAPE-K model (see Fig. 3), which consists of a control loop with four phases (Monitor, Analyze, Plan, and Execute) built on an underlying knowledge base, and which interacts with the surrounding physical environment using sensors and actuators.

Dong [9] employed complex networks theory and data mining to identify vulnerabilities in the physical power system of a smart grid, which is a critical component in a smart city. The proposed cyber system models was designed to be used alongside existing power system models to analyze the complex interactions between the cyber and physical parts of a smart grid. The author also proposed advanced modeling tools to model cyber attacks and to evaluate how they could affect smart grid security.

For a broader review of information security issues, which encompasses all ICT-based systems, including the smart city, readers are referred to [21], which

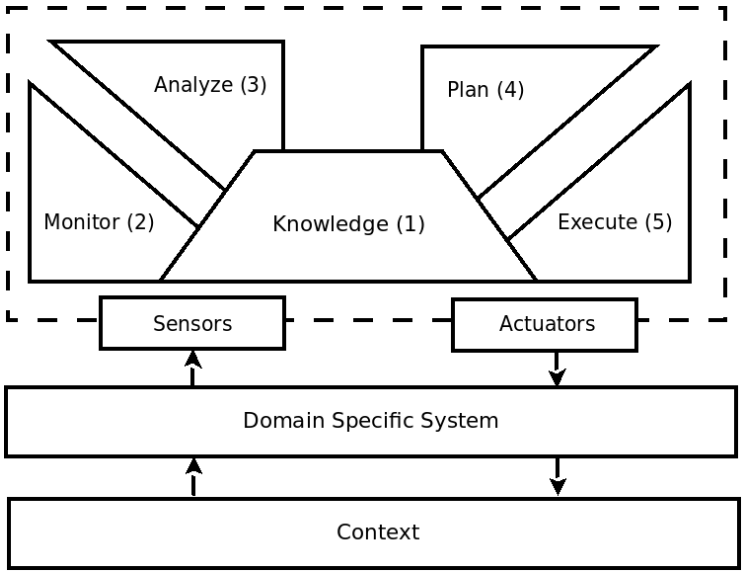

Fig. 3. The MAPE-K model [10]

explains the fundamentals of information security in a very accessible manner. Topics addressed include CIA (Confidentiality, Integrity, and Availability), cryptography, cryptanalysis, access control, security protocols, and various aspects of software security.

4 Conclusion

In this paper, we discussed the concept of smart cities and their cybersecurity challenges and possible solutions. The area of smart city cybersecurity is still in its infancy, and many more policy, architectural, design, and technical solutions are anticipated in this very important domain. We would like to conclude this paper with the words of the renowned security expert Eugene Kaspersky [1]: "*Smart technologies and interconnectivity should be improving lives around the world. But with all the opportunities they create, it is a challenge to stop people with malicious intent exploiting them. we are confident that it is possible to meet the challenge, but it requires a lot of hard work from governments, software and equipment developers, and IT security companies. We are just starting out on this path, but follow it we must — to ultimately build a safe and secure digital world for all.*"

References

1. http://gulfnews.com/business/sectors/technology/cybersecurity-challenges-in-smart-cities-development-1.1613223

2. http://resources.infosecinstitute.com/cyber-attacks-on-power-grid-the-specter-of-total-paralysis/
3. http://securityaffairs.co/wordpress/wp-content/uploads/2015/07/power-grid-attack-scenario-2.jpg
4. https://www.qualcomm.com/products/smart-cities
5. http://www.gartner.com/newsroom/id/2905717
6. http://www.npr.org/2012/05/03/151919620/computer-glitch-summons-too-many-jurors
7. Cerrudo, C.: An emerging US (and world) threat: Cities wide open to cyber attacks. Tech. rep., Securing Smart Cities (2015)
8. Cerrudo, C., Hasbini, A., Russell, B.: Cyber security guidelines for smart city technology adoption. Tech. rep., Securing Smart Cities, Cloud Security Alliance (2015)
9. Dong, Z.: Smart grid cyber security. In: Proceedings of the 2014 13th International Conference on Control Automation Robotics and Vision. pp. 1–2 (2014)
10. Gurgen, L., Gunalp, O., Benazzouz, Y., Gallissot, M.: Self-aware cyber-physical systems and applications in smart buildings and cities. In: Proceedings of the Conference on Design, Automation and Test in Europe. pp. 1149–1154 (2013)
11. Hioureas, V., Kinsey, T.: Does CCTV put the public at risk of cyberattack? how insecure surveillance technology is working against you. Tech. rep., Securing Smart Cities (2015)
12. Institute for Sustainable Communities, et al.: Getting smart about smart cities: USDN resource guide. Tech. rep., Institute for Sustainable Communities, Nutter Consulting, and Urban Sustainability Directors Network (2015?)
13. Lazaroiu, G.C., Roscia, M.: Definition methodology for the smart cities model. Energy 47, 326–332 (2012)
14. Lee, J.H., Phaal, R., Lee, S.H.: An integrated service-device-technology roadmap for smart city development. Technological Forecasting and Social Change 80, 286–306 (2013)
15. Li, Y., Dai, W., Ming, Z., Qiu, M.: Privacy protection for preventing data over-collection in smart city. IEEE Transactions on Computers 65, 1339–1350 (2015)
16. Matuszak, W.J., DiPippo, L., Sun, Y.L.: CyberSAVe: Situational awareness visualization for cyber security of smart grid systems. In: Proceedings of the 10th Workshop on Visualization for Cyber Security. pp. 25–32 (2013)
17. McAfee Labs: McAfee threats report: Fourth quarter 2012 executive summary. Tech. rep., McAfee, Intel Security Group (2013)
18. Neirotti, P., De Marco, A., Cagliano, A.C., Mangano, G., Scorrano, F.: Current trends in smart city initiatives: Some stylised facts. Cities 38, 25–36 (2014)
19. Sanchez, L., Munoz, L., Galache, J.A., et al.: SmartSantander: IoT experimentation over a smart city testbed. Computer Networks 61, 217–238 (2014)
20. Seto, Y.: Application of privacy impact assessment in the smart city. Electronics and Communications in Japan 98, 52–61 (2015)
21. Stamp, M.: Information Security: Principles and Practice. John Wiley & Sons, second edn. (2011)
22. Wang, P., Ali, A., Kelly, W.: Data security and threat modeling for smart city infrastructure. In: Proceedings of the 2015 International Conference on in Cyber Security of Smart Cities, Industrial Control System and Communications. pp. 1–6 (2015)
23. Wikipedia.org: Smart city (2016), https://en.wikipedia.org/wiki/Smart_city
24. Wikipedia.org: Stuxnet (2016), http://en.wikipedia.org/wiki/Stuxnet

25. Yin, C., Xiong, Z., Chen, H., Wang, J., Cooper, D., David, B.: A literature survey on smart cities. Science China Information Sciences 58, 1–18 (2015)