CYBER SECURITY APPLIED IN SMART CITIES

Thanga Dharsni I[1] , Divyam Nayyar[2] , Pratyush Kaushal[3], Rohit Kumar Pathak[4], Ajay Kumar Pal[5]
[1]Asst. Professor, ECE Dept, MVJCE, [2,3,4,5]Student ECE Dept, MVJCE

Abstract

Implementation of smart Technologies leads to serious risks, threats in the physical security and privacy of the citizens. Smart cities implement emerging networking, embedded electronics, communication Technologies we discuss various vulnerability and security issues related to connected world and security solution for better deployment and accessibility of the technologies. Cyberthreats related to smart connected devices, internet of things and smart cities solutions.

Keywords: Cybersecurity, smart city solutions, privacy Threat Modelling

I.INTRODUCTION

The world is witnessing rapid urbanization, hitherto unseen. currently, more than 50% the world population lives in cities, and this figure is expected to grow up to 70% population growth, cities have embraced advanced information and communication technology(ICT)-based solutions to provide smart services to their citizen. Today, several countries are working toward the development of smart cities that will offer citizen-centric smart services in an efficient and cost-effective manner.

There is no universally accepted definition of a smart city, till date. The idea of a smart city may vary, depending on the level of development, willingness to change and reform, resources, and aspirations of the city resident Most of the smart services are provided through the use of cyber–physical technologies. Traditionally, cyber and physical systems have been independent of each other. Perturbation in either cyber or physical systems is contained within the respective domains. In cyber–physical systems these two domains are tightly integrated, which opens up opportunities for newer type attacks through exploitation of vulnerabilities individual domains[1]. Moreover, ensuring the security resources and privacy of citizens' data is a major concern in any smart city solution. With the growing number of attacks in the cyber space, it is expected that a large attack surface of smart cities will aid cyber criminals to launch large-scale attacks so as to breach security and privacy of resources and data. Hence, planning and implementation of cybersecurity measures is of utmost importance in the case of smart cities.

Historically, it has emerged that any cyber security program consists of both managerial and technical measures. This find support in existing cyber security laws and regulations which differ in scope and intensity between nations and business sectors. Inter connected infrastructure in smart cities gives rise to scenarios where an attack on one sector may cause an unrelated, but connected, sector to be compromised as well. Hence, it is extremely important to study and analyze the security requirements of smart cities, keeping in mind both the physical (due to common infrastructure) and logical (intra- or inter-sector) dependencies of different sectors. Based on these requirements, a detailed risk assessment may be undertaken to identify, analyze evaluate the security risks within the cyber space of a smart city.

The identified risks will enable the design of smart security measures to help prevent, detect, and/or recover from those risks. However, it should be borne in mind that, like all other security programs, implementation of cybersecurity for smart cities is not a onetime affair. Security concerns evolve continuously with changes in infrastructure, discovery of new vulnerabilities, emergence of new threats, and enhancements in the regulatory framework. Hence, we propose a life-cycle approach to manage the various phases of cybersecurity of smart cities. It begins with the establishment of scope and boundaries of the proposed security implementation. This is followed by the identification of security requirements, keeping

in mind applicable laws and regulations and specific security concerns and expectations of various smart cities[7].

II. SMART SERVICES SECURITY ISSUES

A smart country get the data from its embedded systems and the sensors implanted in it. It shares those data via a smart communications system that is typically a combination of wired and wireless infrastructure. It is the smart software engines to make smart decisions for enhanced service performances. Cybersecurity of smart cities means protection of systems, and infrastructure responsible for the city' so operations and for the stability and livelihood of its citizens The very nature of smart city cyber–physical infrastructure opens up a huge attack surface, which is the aggregation of all known and unknown vulnerabilities, taking into consideration existing security controls across all subsystems and networks[2].

The following paragraphs highlight some of the security issues associated with smart city services. In smart transportation sector, the design of automotive vehicle architectures is still mainly driven by safety and cost factors rather than security. In most of the cases, the current state-of-the-art industry practices for establishing communication between embedded subsystems in automotive cars do not follow standard computer security principles This renders those autonomous vehicles prone to theft and remote attacks. Moreover, in-vehicle wireless sensor networks, used in applications like tire-pressure monitoring systems (TPMSs), do not employ any cryptographic algorithms for protecting their communications.

An in-depth understanding of the vulnerabilities, threats, and attacks is necessary for the development of any defense mechanism Moreover, solutions based on cryptographic mechanisms should be suitable for resource-constrained embedded systems. Some of the potential attack scenarios are enumerated below:

• Autonomous vehicles are vulnerable to remotely executed attacks. Attackers able to control one or more autonomous vehicles could cause the crash.

• Unlike general purpose computing devices, installing system updates or security patches for a car may be expensive and complicated, rendering them vulnerable to zero-day attacks.

• Features like access to Internet while traveling greatly increases a vehicle's attack surface.

• The use of cellular and Bluetooth technology in modern cars also increases the risk of remote attacks.

• Devices in autonomous vehicles that receive external inputs, such as GPS, are vulnerable to signal jamming.

• An attacker could intercept and modify safety-related data as it is communicated over V2V networks, leaving neighboring vehicles blind to actions like sudden braking, acceleration, lane changes, or turning.

Smart grid significantly depends on intelligent and secure communication infrastructures for its operation.

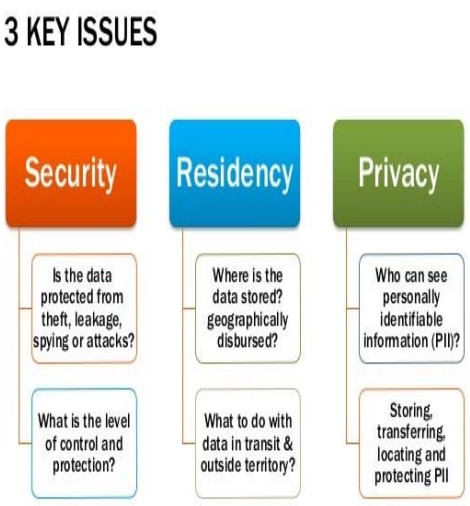

Fig 1. Three Security Issues

Many of the communications technologies currently used in smart grid have known vulnerabilities, which, when exploited, could lead to unreliable system operations, affecting both utilities and consumers The automated meter reading(AMR)technology widely used in smart grid lacks basic security measures to ensure privacy, integrity, and authenticity of data[5].

Moreover, some AMR meters periodically broadcast their energy usage data over insecure wireless links. Attackers can capture this data with modest technical effort and identify unoccupied residences or citizens' routines SCADA systems are widely used in water distribution systems and sewage treatment plants. These systems are designed primarily to maximize functionality, not security. Attackers with little effort can capture/modify traffic between the central control unit and on-field units such as the pumping stations and valves.

Another threat to this system is the theft of sensitive information regarding site maps, details of chemical processes, site security plans, and so on. This renders such SCADA control networks vulnerable to disruption of service, eventually leading to public safety concerns [. In the famous Maroochy Shire incidence in Australia in 2000 an attacker penetrated into the SCADA system and caused a large volume of untreated sewage to be released in public places[3]. Huge amount of citizen information captured in smart city services can endanger the privacy of its citizens For instance, smart health services might help to mitigate many health-related issues; its ability to gather unprecedented amounts of information could end anger the privacy of citizens. Moreover, from the data collected in a smart city, it would be possible to infer citizens' habits, their social status, and even their religion. All information are very sensitive, and when they are combined with health information, the result is even more severe. In a nutshell, protecting the privacy of citizen data and securing the infrastructure is an uphill challenge currently faced by the research community. Thus, it calls for proper management of cybersecurity in the context of smart cities.

smart city, it would be possible to infer citizens' habits, their social status, and even their religion. All information are very sensitive, and when they are combined with health information, the result is even more severe. In a nutshell, protecting the privacy of citizen data and securing the infrastructure is an uphill challenge currently faced by the research community. Thus, it calls for proper management of cybersecurity in the context of smart cities.

III. MANAGEMENT OF CYBERSECURITY IN SMART CITIES

Ensuring the security of resources and privacy of citizen data is a major concern in any smart city project. The cyberspace is infested with malware and novel and damaging attacks expected that the total connectivity of smart cities will aid cybercriminals to launch large-scale attacks so as to breach security and privacy of resources and data. Hence, design and implementation of cyber security measures is of utmost importance in the case of smart cities. However, it is almost impossible to achieve absolute security[4]. Cyber security can be visualized as a spectrum that runs from very insecure to very secure It is a balancing act that requires the deployment of "proportion at e-defense." The controls that are implemented should be proportional to the risk. It is important to determine relevant controls by comparing the cost of security with the value of services they are protecting, privacy needs of citizens' data, and efficiency needs of systems. In other words, implementation of cyber security measures is a management issue, where a fine balance is to be drawn between system efficiency, security expenses, and data protection. However, cyber security needs of a smart city are not static; they evolve continuously with changes in services and assets, discovery of new vulnerabilities, and emergence of new threats.

Moreover, changes in laws, regulations, and contractual obligations also lead to new security requirements. Hence, the process of developing and deploying a proper cybersecurity program for a smart city is not a one-time affair; rather it is a continual process of analysis, design, implementation, monitoring, and adaptation to changing needs. Considering the above requirements, we propose a life-cycle approach to manage the various phases of cyber security of smart cities. Different phases of this life cycle are detailed in the following subsections

IV. PRIVACY PROTECTION IN SMART CITIES

For any technology, the rights of citizens should be guaranteed anywhere and anytime. Despite the benefits of smart cities services, privacy breaches are becoming worrisome within the context of smart cities. In fact, most services of a smart city are based on ICT. Sometimes users (especially adolescents and the elderly) are not familiar with security issues, and they become

perfect targets for attackers when they interact with many smart cities services through their smartphones, tablets, and computers, revealing personal data such as gender, age, and location.

Thus, this section focuses on privacy issues within smart cities. We first define privacy issues; then we present and compare different privacy models. Finally, we briefly discuss current privacy regulations in different countries. Privacy issue. To understand the significance of privacy challenges n smart cities, we use the following example. A vehicle's license plate can be connected to the vehicle owner's identity. Hence, the trajectory of a vehicle can easily be traced even if all communications between the vehicle and infrastructure are encrypted and each device is authenticated by others. In a smart city, future vehicles will have various communication capabilities that include Internet access, GPS, an electronic tolling system, and RFID. Connected devices in a vehicle will store lots of personal information and have various communication capabilities[3]. In a smart city, the number of connected devices will be very high. We have proposed a new approach to assess threats to smart city systems by gathering hundreds of features from system architecture, networks, operating systems, database schemas, encryption techniques, security policies, business operations, and corporate data. This Hardware, intelligence, Software, Policies and Operation (Hi SPO) approach uses an algorithm we developed to calculate threat factors automatically based on those features. The threat factor gives us how robust a smart city system is facing the cyber threats. installation policy, workstation security, privacy protection policy, web application security policy and compliances.

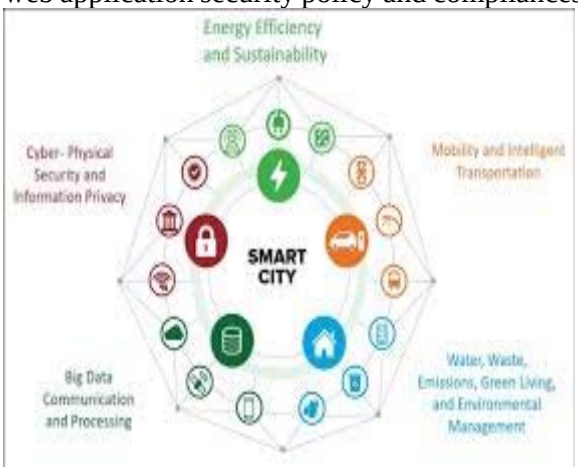

Fig-2. Threat Assessment and Risk Mitigation

Inspecting operational security is to analyzing systems without updated virus definitions, insider threats, security policy enforcement, account managements, authorized connections on firewall, restricted/banned site access attempts, etc. In addition, the Hi SPO approach also integrates data from public and commercial threat analysis and threat intelligence systems including PASTA (Process for Attack Simulation and Threat Analysis), CVSS (Common Vulnerability Scoring System), NRAT (Network risk Assessment Tool), WASC (Web Application Security consortium), and Fire Eye as a service to get more up-to date threat data.

V. THREAT MODELLING

Threat modeling process starts with gathering information in network and system architecture, operating systems and updates, components and configurations of applications, data and data storage, database schemas, services and roles, encryptions and external dependencies. Then we look at the business objectives, security policies, procedures and compliance with interviews from executives ranging from CISO and IT managers[8]. After this step, we look at the business operations of the company and interview top executives including CIO, COO and CEO. Next, we conduct a series of vulnerability assessments. Based on the data collected, we start modeling threats to the company.

The Hi SPO algorithm considers threats and risks of most security areas including hardware, software, policies and business operations [4]. So the threat factor provides an overall view of security of smart city systems. Reducing the threat factor will in return enhance the security and reduce the risks of data breaches to smart city systems.

VI. THREAT REPORT

Threat report contains threat modeling executive summary, model name, owner, reviewer, contributors, description, and model diagram. It also lists a detailed description about name and nature of the threat, actions that have been taken and data flow diagram that corresponding to the threat surface. The report also contains vulnerability assessment results with data

discovered during the process. The final report gives threat factors that were calculated before mitigation and after the assessment and mitigation period. For the system we worked on, the first month of assessment and mitigation leads to the threat factor dropping down from originally 0.71 to 0.38. After the first round, many areas of the smart city systems were secured. The blue-hat team was still able to reveal data from the system. The second round of assessment and mitigations took additional three months. When it was done, the threat factor was further reduced to 0.18. At this point, our blue-hat team was no longer able to find any data from the system. Based on the threat factors that were calculated before and after the assessment, we provide mitigation strategies that would improve overall security of the smart city systems[6].

VII. CONCLUSION

Adoption of smart city model is inevitable to cope up with the unprecedented urban population growth. Wide deployment of cyber–physical infrastructures, for realizing smart city services, poses as a great threat for city administrators. Managing the cybersecurity is vital for smooth functioning of smart city operations. In this chapter, we have proposed a life-cycle approach to manage the various phases of cyber security of smart cities. This provides approach toward managing threats, vulnerabilities, and risks of a city based on perception of security of city administration and the citizens.

VIII. REFRENCES

[1] Cybersecurity for smart city architecture (2015). National Institute of Standard and Technology (NIST). Retrieved from http://nist.gov/cps/cybersec_smartcities.cfm

[2] City Science (2015). Massachusetts Institute of Technology (MIT). Retrieved from http://cities.media.mit.edu/

[3] PASTA. (2016). Process for Attack Simulation and Threat Analysis Risk-Centric Threat Modeling. OWASP. Retrieve from https://www.owasp.org/images/a/aa/AppSecEU2012_PASTA.pdf

[4] FIRST. (2016). Common Vulnerability Score System v3.0. Retrieved from https://www.first.org/cvss/cvss-guide

[5] WASC Threat Classification v2.0. (2017). Web Application Consortium. Retrieved from http://projects.webappsec.org/w/page/13246978/Threat%20Classification.

[6] Cybersecurity for smart city architecture (2015). National Institute of Standard and Technology (NIST). Retrieved from http://nist.gov/cps/cybersec_smartcities.cfm

[7] City Science (2015). Massachusetts Institute of Technology (MIT). Retrieved from http://cities.media.mit.edu/

[8] K. Waedt, Y. Ding, Y. Gao, X. Xie: I&C Modeling for Cybersecurity Analyses, 1st TÜV Rheinland China Symposium - Functional Safety in Nuclear and Industrial Applications, Shanghai, October 2015.

[9] P. Leibold, Adaptive City Mobility (ACM) blazes new paths for competitive electric mobility, http://adaptive-city-mobility.de, 2016-06.

[10] P. Kulkarni, T. Farnham: Smart City Wireless Connectivity Considerations and Cost Analysis: Lessons Learnt From Smart Water Case Studies, IEEE Access, March 9th, 2016.