Smart City Security

Shawn Ralko
Coastal Carolina University, seralko@g.coastal.edu

Sathish Kumar
Coastal Carolina University, skumar@coastal.edu

Abstract
With rapid growth of technology involved and the implementation of the smart city concept, it is becoming vital to identify and implement security controls for their secure operation. Smart city security is essential for a city to incorporate the technologies into smart city cyber infrastructure and to improve the conditions of life for its citizens. In this paper, we have discussed the growth of smart city concept, their security issues. We also discuss the security solutions that needs to be implemented to keep the smart city cyber infrastructure secure. We have also pointed out the recommendations on the open issues that the researchers and practitioners need to concentrate on.

Disciplines
Information Security | Management Information Systems | Technology and Innovation

INTRODUCTION

Smart cities are becoming a reality as part of our everyday lives. We as a society have become so dependent on them to run our cities we sometimes forget what would happen if the security that protects our smart cities was to fail what might happen. They run everything from our traffic patterns, security cams, water and so much more. If a whole network was to fail due to a cyber-attack the loss of data, damage and property and potential risk to lives due to disaster are astonishing. In this paper, we will discuss the overall growth of smart cities and how the security impacts it. With example scenarios, we have indicated what are the smart security issues and the potential problems that can happen with it. With every problem however there is always a solution. We have also discussed security options to help improve and solve some of the problems that are related to smarty city security.

BACKGROUND

Recently smart city security has become one of the important issue in the cyber security arena. Almost every developed country now has access to some type of device that can have access to the internet. In the earlier days, it was not always this way. Hence security for the smart cities has become an important requirement that was not needed earlier. for them was something that was nonexistent (Kumar, 2016).

The first true example of a smart city came about in the early 1970 when the analysis bureau would use computer data bases, cluster analysis and aerial photography to gather data on Los Angeles (Brasuell, James 2015). At this point in time smart cities where all based around the idea of data collection. They were looking at the rate of city growth, infrastructure and suburban growth as well. Noting as this time was being networked and controlled by a computer because this type of technology was not available to the public and didn't exist yet on a scale that was in remotely close to anything we have today. Simple as stated before smart cities where used for data collection. This was really the beginning of the smart city revolution and the security that would come with it. By the mid 1980`s we as a society started to see the spread of Local Area Networks, Client desktops and servers for educational, medical and military purposes. Advanced Research Projects Agency Network (ARPANET) was an early packet switching network and the first network to implement the TCP/IP standards. Originally ARPANET was funded by the United States department of defense and was used in military implications and research. However, the technology from this spawned the beginning of networks for the public use. Also in the 1980`s we started to see the Internet in its first forms begin to be used by networks.

Academic institutions such as schools and other facilities started setting up basic networks for sharing the information between research groups. ARPANET is one of the important factor that led to smart cities in their current form from the ground up.

Since then smart cities have in one form or another started exploding all over the world (Naphade, 2011). Any modern day city is run by some sort of a smart city cyber infrastructure (SCCI). To be specific, city and its resources such as water, traffic, and electricity utilization are all being controlled by the cyber infrastructure. Not only has the field of smart cities grown rapidly but the concerns due to security as well (Elmaghraby, 2014). The smart city security portfolio of the cybersecurity industry has poised to become one of the huge revenue generating area in next few years. Business Insider technology reports that within the next five years that the growth of the economic value of the smarty city security industry is to increase by five hundred billion dollars (Cerrudo, Cesar 2015). Given the expected expansion of the smart city initiatives and the smart city security concerns, it is very important to take the security issues seriously, explore and implement initiatives to protect the cities from security threats.

The concept of smart cities have become a part of our everyday lives. As a result, if a person lives in a smart city, he/she is becoming incredibly depend on it or are fully dependent on it already. For instance, smart cities have started to provide free wife for its residents. This is made possible by installing wireless routers on the street corners of cities and allowing the residents to access and use them. As a result, an important issue with this is the security threats behind it and how the citizens of the city can protect themselves when the city gives the Internet access to everyone for free (Lilian, 2015). The concept of smart cities is much more than just providing free Wi-Fi to its citizens. They now almost control every aspect of the functioning of citizen's daily life such as controlling the transmission of the utilities like water, electricity and so on.

Let's consider few scenarios that are controlled by a smart city cyberinfrastructure (SCCI). For example, a smart city citizen wakes up in the morning and turn on the water to brush his/her teeth and turn on the lights in their bathroom. Both these two items are probably controlled by the smart city grid (NIST, 2009). The city provides these facilities to the citizens and they are controlled by cyberinfrastructure. Next the citizen walks outside and hit the crosswalk button. For this to happen, traffic has to come to a stop and the crosswalk light has to become illuminated. Again all of this is controlled by a smart city. The traffic patterns, systems and pedestrian

walking signals are now all controlled by a smart city. Almost every aspect of a city is now being controlled by a SCCI. There is a need to discuss how more aspects than one may think are controlled by a smart city. For example, weather prediction and flood are all controlled by a SCCI. This means that if a natural disaster where to happen or a freak act of nature causes SCCI to fail and this would lead to catastrophic issues.

Smart city attackers have the power to get the information about all the citizens within a matter of minutes resulting in a potential threat to their well- being. A smart city also publishes open data such as information to the citizen about their city. For example, the information related to water consumption and electric energy consumption, the number of cars travelled in the road and the number of criminal acts take place in the city is being provided. These information is being used to have a more informed and educated resident in that city. They are involved in every aspect of it and we didn't even realize it was happening. This is not something to be scared of but rather to be embraced. They have impacted us in a way that is beneficial to use and is only going to improve the quality of life for all people in these smart cities. In this paper our intention is to point out the security issues of smart city cyberinfrastructure, such that the citizens can completely realize the benefits that the smart city can offer.

SMART CITY SECURITY ISSUES

Following are some of the important security issues associated with the smart city security. The first of these issues is that with the rapid growth of the technologies enabling the concept of smart city can the security with respect to those technologies can be maintained. New devices such as tablets, laptops, smartphones and more have made it easier for the potential attackers to find holes in the cyberinfrastructure. Also with the introduction of city wide Wi-Fi there is a constant internet access at any time in certain cities, threat level for an attack to happen has only increased

Another related issue is the training of employees who actually know how to secure a smart city network. With such rapid growth and expansion of smart cities there are few security professionals that have the qualification to actual maintain and support a smart city security system. The smart city security field is currently so understaffed that it is expected to become one of the top five most sought after and wanted jobs in the near future with respect to the technology market. Trained individuals in this field are in high demand. Without certified individuals, it would be difficult to address the security issues. Shortage of the security professionals makes it easy for

the attackers to identify and target more holes in the network so that threat turns into an attack.

Another issue is the patch deployment and security updates (Sen, 2013). For example, for every new update that takes place, there is going to be some new type of security hole that will open up in the cyber infrastructure. Also with such rapid growth of smart city initiatives, the updates are rushed out quickly. As a result, there are going to be openings for an attack such as a SQL injection. When software is not fully tested and published to the SCCI, it can have very real threats against it that can cause a big problem for the security side. Here are some examples of implications of simple issues in the code or if an attack takes place on the smart city security network. In May Of 2012 a county courthouse summoned 1,200 people to jury duty on accident because of a bug in the network. This caused a massive traffic jam. Another example was that in a number of 2013 attacks. A major service train system was shut down affecting 19 trains and leaving between 500 to 1,000 people stranded on board. Lastly in August of 2003 blackouts affected leaving millions of people in danger (Cerrudo, Cesar 2015).

Another problem that many people do not think about and it has a huge connection to smart cities is the budget for smart cities project. These smart cities are not being paid for by one person or a group of people. The money that is paying for these smart cities is coming from the city itself meaning the tax dollars that the cities collect. With the constant changing budget situations and how it is affect things like education, social programs and so on. The budget for a city has a direct relation to a smart city project because it dictates how much money a city will have to spend on their smart city security activities. Many times whatever issues a city is facing will be highlighted in the media and other such issues. They budget of that city will be shifted towards a larger percentage of that budget going towards that and other items that the city is paying for will receive less. As has been discussed so far in this paper a smart city can power almost everything that is running the daily needs of the city. For instance, smart city runs things like traffic cameras, water and sewage lines, and electrical plants and so on. If the appropriate budget is not given to the individuals, that are running these smart cities they will not be able to adequately protect these cities. A budget can be a silent killer of a smart city security initiative. Without having the proper budget, it can lead to situations such as lack of trained and certified security professionals as well as not having the proper resources in line to adequately protect a smart city. These can range from both hardware and software needs. For a smart city security initiative, it is extremely important these messages are relayed to the policy makers, administrators and make sure the issues of

a constantly changing budget are known to these leaders. Without a set budget that is discussed and planned out it can leave a smart city open to more threats and attacks then many would think to be possible.

SMART CITY SECURITY SOLUTIONS

While it may seem like there are an endless amount of problems with smart cities there are solutions out there and ways to improve on them. One such solution is the hardening of any systems network is virtually important to be it being successful. It doesn't matter if we are talking about software or hardware hardening any form of it is vital to keeping a smart city secure. One of the best things to do with solving smart city security issues is to do constant penetration testing. Constant penetration testing is vital to keep any smart city up and operational. Smart cities are always evolving and being updated in some form. So it is essential to make sure that you are constantly testing the network for new holes and ways to access it should be a first line of defense in preventing threats and attacks. Penetration testing is only one part of improve security measure.

Another issue to be considered is securing the ports. Some cities offer free Wi-Fi, which results in a large amount of traffic traveling going in and out of ports on a network every day. As a result of this port security can be a vital part as well in hardening and protecting your network. With port security, it is necessary to go through and find out which ones are being used for basic traffic and others are being left open but are of no use. Investing in a port scanner that can scan ports and packets on a network is an excellent way to solve the issue of ports and securing your smart city.

Furthermore, one of the most important steps in protecting a smart city by ways of improving security is hardware and software firewalls. Determining the type of traffic that is being allowed to pass through the firewall is one of the most important ways to defend the network from potential attack that can take place. A firewall is key to any network but in terms of a smart city and the security, a firewall is vital to the daily functions. Smart cities are constantly understock at all times but people looking to cause harm or gain finically from it. A firewall and having it set up correctly is one of the best way to improve the security around SCCI. However, even if one has all the hardware and software in the world to protect the smart city cyber infrastructure (SCCI), unless there are well trained and certified individuals to secure the SCCI they would be of no use.

We believe that one of the most important ways to secure the SCCI is to have trained and certified individuals developing, engineering and maintaining the SCCI. Another thing to be noted is while we have personnel that are

trained in Information technology fields does not mean they are versed in the security side of things. We believe that a person that is certified in SCCI security, should knows the nuts and bolts of how to secure the SCCI from potential attacks. SCCI is a very complex entity and having a team or an individual that is trained in securing them is crucial for them to be able to protect them from security attacks on a daily basis. If SCCI is down for just one day, the events would lead to catastrophic scenario.

Another solution that we have come up with is a variation of public Wi-Fi usage policy. Currently some cities are freely offering Wi-Fi to the mass public. Routers ae being placed on corners of the streets and the Wi-Fi is being used by the public. While this is a great idea, we believe this could solve multiple problems in one shot. By offering a small paid Wi-Fi service, we could reduce the overall traffic on the network by a large amount. As discussed earlier, one of the significant problem with smart cities is the amount of traffic a network can have on it at a given time. With a paid for service it would reduce the amount of traffic that is traveling on the network every day and as a result the security monitoring can be done more closely with the available resources. With a paid for service, smart city administration can also fix the issue of budget cuts by rolling that money right back into the smart city security fund. The city is already paying for the cost to install the routers and networks and by charging a small monthly fee the city should be able to gain money back on that investment as well as reroll that income into new security as well as decrease the overall traffic that is flowing on the network making the job of packet sniffers, firewalls and other security measures much easier. The paid for Wi-Fi service is a solution that has the potential to solve many problems that are typically associated with a smart city and thus it's a solution that is worth some thought among the smart city administrators and policy makers.

The last option we would like to explore is the evaluation of existing security products in the market that could be tailored to the needs of securing SCCI. Preferably the product should be pre designed with smart city security requirements (AGT, 2014). What this system should do is connects safety and security solutions to help protect against crime, terrorism and civil unrest. It should help the law enforcement and medical emergency services personnel by providing the response to calls and emergency quickly. The product should be able to control the flow of traffic and other variables since it is connected to SCCI. For example, in a large city like New York there are a constant threat of attacks from cyber threats and physical threats and this product should solve many problems associated with a smart city. There is a list of benefits that the recommended product

should provide to any smart city in order to improve the security problems associated with it. For example such a protected smart city can reduce crime, increase attractiveness to business and worked and improve resource allocation. The citizens of such a smart city also benefits by the safer streets and neighbors and the ability to report city safety incidents. Another important issue is to protect that security product or system to make sure that it does not fall into the wrong hands such that the product is full encompassing and perform the security goals completely.

FUTURE RESEARCH RECOMMENDATIONS

Following are the research and educational avenues that we recommend in order to address the security issues associated with the smart city security.

1. Since the most common threat for the SCCI is going to come from wireless devices, researchers and practitioners of SCCI security need to develop or customize the security system or product around hardening wireless ports, protocols and encryption.
2. Evaluate the options for training certified SCCI security professionals who have the ability to secure the smart city from external threats.
3. Analyze the policy implication of paid Wi-Fi service instead of free Wi-Fi in order to reduce smart cities network traffic as well as improving on overall security.
4. Identify and evaluate existing security products in the market that could be tailored to the needs of securing SCCI.

CONCLUSION

The concept of smart cities is changing the world. While we do not realize so many complex technologies has already integrated with the city infrastructure and there are numerous benefits associated with this concept, security is a major issue considering the vulnerabilities and several weak links in the SCCI. While there is considerable interest in the security of the smart cities, there is a lot of work need to be done so that the citizens can completely realize the benefits of the smart city. In this paper, we have discussed several security threats associated with the smart city through example scenarios. We have also discussed some of the potential solutions and the recommendations for the future work to secure the smart city from a cyber security perspective.

REFERENCES

AGT, CISCO(2014, May) Retrieved April 23, 2016 http://www.cisco.com/c/dam/en_us/solutions/industries/docs/agt-cisco-city_safety-aag.pdf

Brasuell, James. (2015, June 22). *PlanetizenI.* Retrieved March 5, 2016 from http://www.planetizen.com/node/78847

Cerrudo, Cesar (2015, April 20). Hacking Smart Cities. *RSA Conference 2015*, pages 2 – 18 Cerrudo, Cesar, Hasbini, Amin, Russel, Brian (NDA) (2015). Cyber Security Guidelines for Smart

City Technology Adoption. *Securing Smart Cities, Cloud security Alliance. Pages 1- 17*

Edwards, Lilian (2015, December). Privacy, Security and Data Protection in Smart Cities: a critical EU Law Perspective. CREATe Working paper. Pages 1 – 39

Yangqing and Zuo, Jun (2015). Research on Security Construction of Smart City. *International journal of smart home*, vol.9, No. 8 pages 197 – 204

Smart grid cyber security strategy and requirements. (2009) [Online].Available: www.nist.gov Adel

S. Elmaghraby and Michael M. Losavio (July 2014), Cyber security challenges in Smart Cities: Safety, security and privacy, *Journal of Advanced Research* Volume 5, Issue 4, Pages 491–497

M. Naphade, G. Banavar, C. Harrison, J. Paraszczak and R. Morris, (2011). "Smarter cities and their innovation challenges", *Computer (Long. Beach. Calif).*, vol. 44, no. 6, Pages. 32-39

M. Sen A. Dutt S. Agarwal and A. Nath (2013). "Issues of privacy and security in the role of software in smart cities", *2013 International Conference on Communication Systems and Network Technologies*. Pages. 518-523.

S.A. Kumar, T. Vealey, and H. Srivastava, (2016). "Security in Internet of Things: Challenges, Solutions and Future Directions", *2016 49th Hawaii International Conference on System Sciences (HICSS)*. Pages 5772-5781.