Smart Cities: An Inspection of Cybersecurity Vulnerabilities and Prevention

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Matthew T. Moore

Spring 2020

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Sean M. Ferguson, Department of Engineering and Society

Smart Cities: An Inspection of Cybersecurity Vulnerabilities and Prevention

A 2016 survey of chief information officers of cities and counties reported around 25% of local US governments were facing attempted cyber-attacks every hour (Pandey, Golden, Peasley, & Kelkar, 2019). These types of attacks are on the rise as cities become more connected with an increase of 38% of global security incidents between 2014 and 2015 (Norwich University, 2016). Smart cities are a great example of how the implementation of modern technology into services such as transportation or public security can increase efficiency, safety, and well-being of the city and its citizens. The integration of IoT devices, such as sensors and cameras, into cities and homes are just one of the advancements that helps develop these cities. With the blending of technology and infrastructure, there is an abundance of user data that is now collected and stored by companies and governments. As these cities grow "smarter," the amount of data collected and the danger of cyber-attacks rise. Through the actor network theory framework, this research explored the vulnerability of smart cities to cyber-attacks, as well as how organizations, governments, and cities are working to produce cyber security policies through smart governance and programs to teach people smart practices to prevent these cyber-attacks.

Vulnerabilities in Smart Cities

Infrastructure in these smart cities is changing with the integration of systems for monitoring and automation of services. The number of IoT devices is expected to increase from 8.4 billion this year to almost 20 billion by 2020. (Pandey, Golden, Peasley, & Kelkar, 2019) This will enhance interconnectivity and efficiency of services; however, the risk of cyber-attacks will rise. These types of attacks have momentous impacts on data or financial loss and even city infrastructure and services such as power and utility, transportation, or health care. In March of 2018, the city of Atlanta was targeted with ransomware on their city's connected systems. Ransomware is a type of malicious software that blocks access to a computer system until a ransom is paid, in this case the attackers requested a $50,000 payment in bitcoin. The malware disrupted programs dealing with law enforcement and court systems and citizens found themselves unable to do basic city-based tasks like paying parking tickets or utility bills. In June 2018, almost 2 months after the attack, still more than a third of the 424 software programs used by the city were still offline or partially disabled. This attack cost the city $2 million in emergency procurement, as well as an additional $9.5 million added to the original $35 million budget allocated for the Atlanta Information Management. This is just one example from the past year of the damage these cyber-attacks can really have on a city. These types of attacks are not domestic, but happen every day all around the world, targeting large corporations, government entities, and your everyday citizen.

Despite these dangers, the research into the vulnerabilities of smart cities is relatively new. There are many weaknesses found within these cities and their infrastructure but for the purpose of this research they can be broken into three critical sections for smart cities worldwide. The first being how a city's infrastructure can be compromised through its computer control systems like in the attack in Atlanta. The implementation of industrial control systems (ICS) into modern city infrastructure has allowed the control of these systems to be done remotely through the internet. Recently there has been a push towards open standards for ICS devices instead of proprietary. As a result, hackers will be able to find a large amount of detailed knowledge on how these devices work and find vulnerabilities in them from the public domain (Joo & Tan, 2018). If these ICS devices become overtaken by hackers, they can control the entire infrastructure. For example, in 2015 Russian hackers took down Ukraine's power grid by subverting the ICS that controlled the power grid leaving 230,000 without power for hours. This power grid was connected to the banking sector along with critical city services like water treatment, transportation, telecommunications, and hospitals. Ukrainian officials were luckily able to limit the severity of the attack by switching back to manual control (Joo & Tan, 2018). The outcome of such an attack would likely be much worse in a smart city due to the interconnectivity of these infrastructures and often these ICS controlled infrastructures do not have a manual backup feature. This an example of how a collapse of one system has the potential to result in a domino effect shutting down multiple systems and services.

The second crucial vulnerability stems from smart cities being susceptible to attacks through poorly protected edge devices with limited computing power, firewall protection, or anti-virus protection. Research shows that many IoT devices such as sensors, cameras, or smart-meters in these smart cities are both digitally and physically vulnerable. Digitally, in the sense that the devices lack security measures such as anti-virus protection or firewalls. This leaves them vulnerable to cyber-attacks. Physical vulnerability refers to the possibility of tampering or the installation of modifications. The root of this vulnerability is the necessitation for these devices to be left in the wide open (Joo & Tan, 2018). Things like smart gas or electricity meters, surveillance cameras, and smart parking meters are examples of such devices that are susceptible to these types of attacks. Once these types of devices are subverted, they can be used by hackers to create a botnet to launch a distributed denial-of-service (DDoS) attack on other systems in the same network. A botnet is a group of malware infected devices which is controlled by the hacker while a DDoS attack in its simplest form is a disruption of normal traffic of a specific server, service, or network by overwhelming the target with internet traffic. These inadequately secured IoT devices are prime targets for such an attack because of their lack of security, but also the inability to patch security updates once off the assembly line because of their basic designs (Joo & Tan, 2018). These risks are compounded by the fact that many of these devices are mass produced. Once a successful cyber-attack is engaged on one of these devices, it can be replicated on the entire product line.

Finally, the third crucial vulnerability comes from something that people who do not even live in smart cities use every day, that being of course the extensive use of wireless communications. Wireless communication encompasses everything from Wi-Fi to 4G, Bluetooth, and Near Field Communication (Joo & Tan, 2018). The benefits of wireless communication to a smart city are clear; they can expand their network as well as add more electronic devices with no increase in physical IT resources and possibly the biggest benefit being mobility. This allows people to use of digital devices wherever they can connect wirelessly. However, this wireless mode of communication exposes devices to what are called man-in-the-middle (MitM) attacks. Wireless communications, unlike hardwired communications (ethernet), involves the passing of information or data through the air between endpoints making this data much more susceptible to being intercepted by an unauthorized party. The simple way MitM attacks work are that if a third party with a special interception device is situated between the two endpoint devices that are communicating to each other, this third party can capture this data that is flowing between the endpoints. They can do this by interfering with legitimate networks or creating fake networks that they control. These types of attacks so far have been contained mostly to homes and businesses, but that is likely to change now with this new surge of smart cities. With the rise in the use of smart sensors in these cities which typically broadcast their data through the air not through secure networks or channels, but openly to other in range devices these types of attacks can find their way into disrupting city infrastructure. For example, the use of smart CCTV cameras could be easily be the target of a MitM attack where a hacker would feed false security footage to law enforcement to impede the police's surveillance or investigation (Joo & Tan, 2018). The most effective countering to these types of attacks are strong encryption and authentication protocols, but with many smart sensors opting for minimalist designs they rarely, if ever, have any strong digital security features.

Steps Towards Safer Smart Cities

Government/Policy

These problems with cyber security are not going away anytime soon. With the mixing of the physical and digital worlds these types of attacks will only become more prevalent in everyday life. Regardless of this there has been little regulations or policy on the manufacturing of these IoT devices that can be so vulnerable. The main actors involved are the consumers or citizens within these cities along with governments and companies that oversee the production of such devices as well as ensure the safety and protection of their data. First, we will look into what kind of government agencies here in the US and abroad are addressing these challenges. While many formal policies have not passed through US Congress on IoT security (or cybersecurity in general), the US federal agencies are still very much involved in support of the IoT by providing direction on standards of development and interoperability.

The FTC published guidance on how to build security into IoT devices for businesses and the Department of Defense published "*Strategic Principles for Securing the Internet of Things*," which discussed security issues of IoT devices as well as provided principles for responsible cybersecurity practices (Chatfield & Reddick, 2019). In late 2015 the Cybersecurity Information Sharing Act (CISA), formerly known as the Cyber Intelligence Sharing and Protection Act, was passed into law. CISA can be used to force private companies, even massive companies like Apple, Google, or Microsoft, to share data with the government. (Stoddart, 2016). A year later in 2016 President Obama issued the Cybersecurity National Action Plan (CNAP) to strengthen cybersecurity. This plan had multiple initiatives involving cybersecurity including but not limited to the establishment of the Commission on Enhancing National Cybersecurity, a $3.1 billion Information Technology Modernization Fund (as well as over $19 billion in the budget to address cybersecurity deficiencies), and a new National Cybersecurity Awareness Campaign (Kent, 2016).

This sort of minimalist approach to IoT policy making was seen in the UK as well, but as of late there has been a push towards real government regulations of IoT devices. While no official policy has been passed on IoT devices directly, they fall under the scope of other laws that are being changed or updated. For example, in 2016 the EU passed the General Data Protection Regulation (GDPR) which went into effect in the UK in May of 2018, unaffected by their decision to leave the EU. The GDPR introduced the two principles of "data protection by design" and "data protection by default" meaning that products must have data integrity defenses built in from the earliest stages of development (Tanczer, Brass, Elsden, Carr, & Blackstock 2019). This regulation also applies to any entity in the world that offer goods to the EU or monitor the behavior of EU citizens (Black, et al., 2019). It also enacts hefty fines to those in violation of the GDPR. Certain violations of these provisions may subject the data controller to administrative fines of up to 10 million or up to 2% of the total worldwide annual turnover of the previous financial year, whichever is higher. For much more serious violations these fines can be doubled, so 20 million or 4% of total worldwide annual turnover of the previous financial year (Black, et al., 2019). These types of repercussions will help ensure manufacturers will follow these protocols as they are at risk of high penalties if they do not. Similar to in the US, the U.K also established a National Cyber Security Plan in 2011. This strategy was built on by the United Kingdoms Office of Cyber Security and Information Assurance (OCSIA) who were provided a £650 million budget through 2015 (Stoddart, 2016). The four main objectives in this strategy are for the UK to fight cyber-crime and become a very secure place to do business in cyberspace, be more resilient to cyberattacks to protect UK interests, help share an open cyberspace that the UK public can use safely and freely, and to have crosscutting knowledge, skills, and capability to build upon the UK cybersecurity objectives (Stoddart, 2016). This National Cyber Security plan is still ongoing, with an increase in funding of £1.9 billion earmarked for cybersecurity from 2016-2020 (Stoddart, 2016). Many of these bills, policies, or government divisions are relatively new, so seeing the results of these changes over a small period of time is unfeasible. While the results may not be instantaneous, this is a step in the right direction as national governments are addressing that the problem of cyberattacks will not be going away anytime soon, needs constant attention, and a more preventative approach to stopping them.

Commercial/Business

Moving on to the commercial or business side of this problem, organizations are working together with network providers, government agencies, and industrial associates to provide response to computer security incidents, research and analysis of such incidents involving ICS devices. Ultimately these efforts will help disseminate this information to better inform the public. One such organization is the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) who is working on proactive security measures in Japan. These measures include providing guidelines and best practices for ICS security, security assessments of important Windows systems, and security assessments of ICS personnel (Abe, Fujimoto, Horata, Uchida, & Mitsunaga, 2016). JPCERT/CC also provides a middle-man connecting these entities that use the ICS devices to the cyber security industry to improve security measures and promote proactive approaches. These efforts are determined to prevent attacks from happening before they even begin.

Another company here in the US, IBM, is also doing a similar campaign to help local government officials become more educated and prepared for if or when they have to deal with a cyberattack. These cyberattack simulations are only a part of the series of free trainings specified for municipal workers that IBM Security is hosting. The simulations are designed to feel real, using the real types of attacks and malwares that have been used on governments across the US. These simulations are held at IBM's Cyber Range which was opened in November 2016. Since its opening thousands of people working at banks, hospitals, retailers, and government agencies have gone through these trainings. IBM is offering these trainings for free because "Cities need to be looking at the root of the problem rather than dealing with threats such as ransomware as one-off situations" says Vice President of X-Force Threat Intelligence at IBM Security Wendi Whitmore said in a statement announcing the trainings (Bond, 2019). Ms. Whitmore then went on to say that "preventative steps to strengthen cybersecurity in cities now, can help them prepare for, and protect against, issues in the future." And that they (the governments), "need to place an importance on them and develop response plans, similar to how they handle state of emergencies." (Bond, 2019). This type of outreach and involvement straight to consumers and workers that are subject to these types of attacks is a great way of getting out ahead of the problem. If employees are well trained in the proper way to handle ransomware and cyberattacks, they can act hastily and effectively to limit damage of such an attack.

Conclusion

It is clear that cyber-attacks can affect enormous amounts of people, cause extensive damages, cost millions of dollars, and can happen at home or abroad. As we progress towards smarter technology and tighter regulations on the development of this technology, these attacks will become more sophisticated to defeat security measures. There is no clear solution to this problem, as it is a dynamic landscape that evolves constantly. The implementation of more secure systems into smart city infrastructure as well as smart governing policies or principles on the development of IoT devices and data protection are steps in the right direction. This can be seen in the passing of things like the GDPR in the EU which requires strict manufacturing oversight to the creation of IoT devices as well as the issuing of the CNAP here in the US which gave massive funding to research into cybersecurity vulnerabilities and government agencies in the world of cybersecurity. Smart city infrastructure is also continually upgrading their security whether it be though new technologies to better encrypt or protect data, or through companies like IBM and JPCERT/CC which increase the safety of these systems by educating and preparing the people who actually use the systems. Communication between industries and governments in which these cyber-attacks are prevalent and the actual cyber security industry is key to future prevention of these constantly changing security threats. This sharing of knowledge between entities will promote smarter cybersecurity practices in the future as well as introduce a symbiotic relationship between the two industries. This relationship can be between an individual consumer and a company, an individual and their government, companies working together with governments or other companies, and governments working together to learn what is working and what is not. As these attacks become smarter it will be crucial for governing agencies to adapt and react to the rapidly changing world of cyber security that is ever changing.

Citations

Chatfield, A. T., & Reddick, C. G. (2019). A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quarterly*, *36*(2), 346–357. doi: 10.1016/j.giq.2018.09.007

Joo, Y.-M., & Tan, T.-B. (2018). Smart Cities: A New Age of Digital Insecurity. *Survival*, *60*(2), 91–106. doi: 10.1080/00396338.2018.1448577

Tanczer, L. M., Brass, I., Elsden, M., Carr, M., & Blackstock, J. (2019). The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. In R. Ellis & V. Mohan (Eds.), Rewired: Cybersecurity Governance (pp. 37–56). Hoboken, New Jersey: Wiley

The Rise of Cyber Threats. (2016). Retrieved November 7, 2019, from https://online.norwich.edu/academic-programs/masters/diplomacy/resources/infographics/the-rise-of-cyber-threats.

Hatmaker, T. (2018, June 7). The damage from Atlanta's huge cyberattack is even worse than the city first thought. Retrieved November 6, 2019, from https://techcrunch.com/2018/06/06/atlanta-cyberattack-atlanta-information-management/.

Kent, J. (2016, May 20). Cybersecurity National Action Plan. Retrieved February 11, 2020, from https://www.hsdl.org/c/cybersecurity-national-action-plan/

Abe, S., Fujimoto, M., Horata, S., Uchida, Y., & Mitsunaga, T. (2016). Security threats of Internet-reachable ICS. *2016 55th Annual Conference of the Society of Instrument and Control Engineers of Japan (SICE).* doi: 10.1109/sice.2016.7749239

Pandey, P., Golden, D., Peasley, S., & Kelkar, M. (2019, April 11). Making smart cities cybersecure. Retrieved November 6, 2019, from https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html#endnote-sup-3.

Black, K. D., Alam, C. B., Bucher, S. M., Giannetti, A. J., Godfrey, L. D., & Wear, J. D. (2019). Recent Developments in Cybersecurity and Data Privacy. Tort Trial & Insurance Practice Law Journal, 54(2), 403–433.

Bond, M. (2019, September 23). After ransomware attacks on cities, IBM offers free cybersecurity training for local officials. Retrieved February 9, 2020, from https://www.inquirer.com/news/ransomware-cyberattack-government-ibm-security-cyber-range-training-municipal-20190923.html

Stoddart, K. (2016). Live Free or Die Hard: U.S.-UK Cybersecurity Policies. Political Science Quarterly, 131(4), 803–842. doi: 10.1002/polq.12535