The Future City? Mitigating the Technological Threat Cities Face in their Adoption of Smart Services and Infrastructure

Neems, A. J.[1] and Colarik, A. M.[2]

[1]Centre for Defence and Security Studies, Massey University, Wellington, New Zealand

[2]Centre for Defence and Security Studies, Massey University, Albany, New Zealand

Abstract - *This paper identifies technological weaknesses as the primary threat to cities adopting smart services and infrastructure. To mitigate this threat, a solution is proposed aimed at the convergence of the industries of smart cities and the Internet of Things. To achieve this, standardization for security mechanisms of all devices comprising a smart network, essentially the Internet of Things, could be adopted and regulated through an international governing body. Liability can then be placed upon the manufacturers of technological devices which do not adhere to these standards and lack adequate security. Although viable, numerous limitations are present and need to be overcome in order to implement the proposed solution.*

Keywords: City, IoT, Infrastructure, Standardization, Liability.

1 Introduction

As more than half of the world's population has moved towards urban living, cities around the world are required to counter the natural challenges of urbanization [1]. Increased population density places pressure on a city's services and infrastructure, such as transportation systems, waste management and power supplies. Integrating Smart Services and Infrastructure (SSI) into urban living around the world can assist in countering these urban challenges, and is transforming the way people live. Increasing efficiency and productivity of citizens, smart technology can also encourage sustainable, economical and environmentally friendly living. Smart public transport and real time traffic updates enable people to plan efficiently, whilst monitored waste management, power and water regulate the usage of natural resources and critical infrastructure. Despite all these benefits, the reliance of SSI upon technology creates new opportunities for malicious exploitation, ultimately compromising the safety of citizens.

Smart cities are advancing urban living through the collaboration of data and technology, creating an integrated and connected network of services and infrastructure. However, independent domains of a city possess the potential to adopt smart technology, regardless of its integration into the wider community. For example, smart public transport services can operate throughout a city irrespective of other domains adopting smart technology, such as electricity. The potential for SSI to operate independently from one another has resulted in the act of defining a smart city to be a contentious issue.

The diverse range of SSI possessing the potential to improve urban living has challenged both scholars and practitioners in their quest for a sole definition of a smart city [2]. The collaboration of numerous elements of smart living are recognized in the practical definition provided by the Institute of Electrical and Electronics Engineers (IEEE), and will be adopted throughout this paper. The IEEE believe a smart city "brings together technology, government, and society to enable the following characteristics: a smart economy, smart mobility, a smart environment, smart people, smart living and smart governance" [3]. As inclusive as this definition is, focusing on what comprises a smart city neglects the underlying components which can threaten public safety when exploited. Essentially, the defined smart city is created through the adoption and integration of SSI, such as smart transport or electricity grids, tailored around the identified characteristics. However, the transition into a smart city which consists of all these elements is realistically a staggered process of implementing smart technology throughout individual domains over a prolonged period of time. When reviewing the threat smart cities pose to public safety, it becomes critical to break the overarching smart city concept down into 'SSI,' providing an inclusive analysis of both complete smart cities and those cities slowly adopting SSI. This broader classification identifies the fact that public safety is jeopardized not necessarily once a city becomes smart, but through the individual domains of a city utilizing SSI.

Further, SSI are a product of the aggregation of technological devices. The phenomenon of the Internet of Things has enabled easy access to individual devices connecting to the internet, whilst collecting and disseminating data. These devices have the potential to form an integrated network of communication throughout a city, and are essential in both formulating the architecture of SSI, and enabling citizens to interact and utilize these services. The capabilities of individual devices are what enable SSI to function, and when they exist throughout numerous domains, a smart city is created. As beneficial as SSI can be for the operation of a city, the adoption of this complex system involves inherent challenges requiring solutions.

Part two of this paper will discuss these challenges, identifying technological weaknesses as the primary threat causing vulnerabilities throughout SSI. Part three builds upon this, outlining viable solutions to mitigate the threat these weaknesses pose. Two integrated solutions are proposed: the standardization for security mechanisms of all devices comprising a smart network and the establishment of liability upon the manufactures whom do not comply with these standards. Limitations to the adoption of these solutions will then be discussed in part four, followed by our conclusions

2 Challenges Inherent with the Adoption of Smart Technology

As with any large scale urban initiative, cities will face inherent challenges in their adoption of SSI. These challenges can be categorized under three headings: people, management and technology. Each category has numerous elements comprising it which can prevail at every stage of a city's adoption of SSI, from planning to operation.

2.1 People

As all services and infrastructure are designed for the express use of people, people possess the opportunity to make or break these benefits provided to them. When viewing smart technology, a foundational security threat to the safe operation of services and infrastructure are the actions of people, regardless of intent or motivation. In a new field of research, cyber-psychologists are depicting the reasoning behind criminal activity in the cyber world, identifying the exploitation of technology as a force multiplier for further, more life threatening attacks [5].

2.2 Management

Effective management is crucial for the success of any public initiative, from a community led project to a national policy [6]. The implementation of SSI throughout a city requires thorough planning to operate in a reliable, efficient and resilient manner. Without effective planning of an integrated network, smart technology can lay dormant and vulnerable to malicious exploitation. Further, local and central governance are crucial to ensure the best possible resources are used, enough funding is provided, and perspectives from both the public and private sectors are heard. Governance of a city's infrastructure, whether smart or not, needs to be timely and thorough, ensuring infrastructure is secure and updated, and services are managed by adequate staffing. If there are any deficiencies in these areas, services and infrastructure can become disrupted and unreliable, wasting resources and potentially establishing new threats to citizens.

The role of the active citizen is also critical for the resilience of SSI. Citizens need to be aware of the available services, educated in how to securely interact and utilize them, and engage with both the services and management of the services, providing feedback and contributing to future initiatives. If awareness, education and engagement are poor, SSI are not utilized in an efficient manner, unintentional security threats to the network can occur, and the services may not meet public needs (i.e. further reinforcing a lack of engagement).

2.3 Technology

The reliance of SSI upon technology and the network of the Internet of Things creates a multitude of challenges which could threaten the stability of the city, and the safety of its people. The technological devices comprising SSI need to be secure and resilient, with thorough measures to achieve these integrated into the architecture of each individual device within, or those connecting to, the network. Poor encryption, authentication and security patching mechanisms can make an individual device, and thus the whole smart network, easily exploited and vulnerable to malicious attack. A significant virus, malware, Trojan, or Disrupted Denial of Service (DDoS) attack has the potential to infiltrate or disrupt a smart network if adequate barriers are not in place. Further, if access is granted to a malicious user through any of these means, there exists potential for data to be stolen or services and infrastructure to either be disrupted or control to be seized, placing an immense threat on the city [7].

These three challenges – people, management, and technology – are inherent with the adoption of SSI, requiring solutions to mitigate the impact they have upon the resilience of a city and the safety of its people. The creation of a smart city ecosystem has been proposed by scholars, focusing on the integration and collaboration of all components of smart cities, from integrated public and private management to interconnected services city wide [8][9]. A smart city ecosystem should certainly be the aim for all prospective smart cities. However, inadequate technology is arguably the foundational issue causing vulnerability for any smart service or infrastructure, and could further undermine the success of any alternative initiative. Seeking a solution for these technological inadequacies should therefore be a priority for the industries of both the smart city and the Internet of Things.

3 A Viable Solution?

SSI, and ultimately smart cities, are a product of the aggregation of individual devices all connected to the same network. These devices, and their aggregated form, possess the ability to drastically change the way society functions. Despite the benefits of an inter-connected civilization, the devices driving this transition are inherently prone to security threats, often the product of weaknesses within the architecture of the device. A security breach of an individual device can have immense consequences, from data theft to the seizure of control, depending on the device. With the aggregation of these devices in a network, the security threat itself multiplies and consequences drastically proliferate. As cities around the world begin their transition into a smart city, these weaknesses inherent within technological devices need to be mitigated. The convergence of the smart city industry with the Internet of Things is a viable solution, which might be achieved through two proposals. The first is the adoption of standardization for security mechanisms of all devices comprising a smart city network, essentially the Internet of Things, regulated through an international governing body of smart city technology. The second is the establishment of liability upon the manufacturers of technological devices, essentially those of the Internet of Things, which lack adequate security mechanisms within their architecture.

3.1 The Adoption of Standardization, regulated through an International Governing Body

Drawing from the achievements of the International Electro-Technical Commission (IEC), formulated to provide agreed upon standards across the electrical industry during the adoption of electricity in homes, the smart city industry requires an international governing body to implement technological standardization. Such a governing body should be inclusive across the wider industry, particularly inclusive of the Internet of Things, requiring expert members representative of all domains – the manufacturers, technology experts, private and public sectors, city planners, and local and national governance to a identify a small sample. This forum enables experts to collaborate their knowledge, perspectives and ideas surrounding the current and future states of the industry, whilst managing and mitigating current and future challenges.

This potential governing body would be required to place a large emphasis on the technological challenges which are facing cities adopting SSI. Establishing standardization and performing conformity assessments across both domains of smart city technology and the devices of the Internet of Things, would ensure all manufactured devices adhere to the same quality standards. Standardization is viewed as the voluntary adoption of technical specifications throughout an industry, developed throughout the cooperation of the industry experts, consumers, public authorities and any further interested parties [10]. The applicability of any device to these standards can be measured by a conformity assessment, ensuring the product corresponds to its requirements [11]. Establishing standards and conformity assessments for the smart city industry would facilitate the adoption of secure, resilient and reliant SSI throughout the world.

However, standards cannot be implemented at the aggregated level of a smart city without reference to the individual device. Here it becomes imperative to analyze the problem from a bottom-up perspective, identifying and mitigating the weaknesses of any individual device which contributes or connects to the smart network. Devices of the Internet of Things then become further issues requiring attention, regardless of their connection to smart services or infrastructure. In order to integrate and form a collaborated industry, the Internet of Things is required to fall under the standardization of the smart city industry. Effective interoperability could result from the convergence of the two industries. Although this may be occurring naturally, it would not harm either entity to function as an official and coherent unit. Whether this comes under a pre-established body, such as the IEC, or stands independent from any other forms of standardization, would need to be determined by industry experts, with both options harnessing benefits and weaknesses.

3.1.1 Current Initiatives

The production of agreed standardization for smart cities is currently underway by the IEC. In their White Paper, “Orchestrating infrastructure for sustainable Smart Cities,” the IEC call for “wider collaboration between international standardization bodies that will ultimately lead to more integrated, efficient, cheaper and environmentally friendly solutions” [9]. With a focus on the broader construction and functioning of smart cities, The White Paper provides a thorough argument for why the smart city industry requires international standardization in general, and the benefits of adopting these. Coming from the international body focused on providing standardization, the IEC’s White Paper can be used to support the concept of establishing technological standards across both the smart city and Internet of Things domains.

Further, the IEEE is currently collaborating with industry stakeholders to create standardization for the Internet of Things. By creating an architectural framework for the industry, the standard “IEEE P2413,” aims to reduce fragmentation across domains and encourage the growth of the Internet of Things market [12]. This project is a result of the Internet of Things “Ecosystem Study,” in which stake holders around the world provided their perspectives on three principal areas – market, technology and standards [13]. However, whether standardization for technological specifications and security mechanisms to address the identified technological weaknesses will be incorporated in P2413, is yet to be disclosed [13] [14]. In parallel to the IEEE, one of the leading private corporations of the Internet of Things industry, International Business Machines (IBM), has recently invested $200 million (USD) to lead the Internet of Things market [15]. IBM are focusing on collaborative innovation of all stake holders throughout the industry, placing immense emphasis on integrating adequate security mechanisms into the architecture of individual devices [16].

These initiatives, undertaken by key stake holders of both the smart city and the Internet of Things industries, represent the developing necessity to converge the industries, and create a unified market of interoperability and collaboration. Standardization across the Internet of Things, combined with standardization across the smart city industry, will advance the quality, safety, and resilience of cities adopting smart technology around the world. What these standards in particular should encompass is beyond the scope of this paper, but to directly counter the threat technological weaknesses have upon SSI, they should focus on robust and resilient security measures built into the architecture of every device interacting with the smart network.

3.2 Establish Liability upon the Manufacturers of Devices

In order to ensure the standardization of secure technological devices is adhered to, liability would need to be established upon the manufacturing companies whom fail to produce devices of the recognized quality. To do so, it becomes essential to make the standardization of security mechanisms within the architecture of devices mandatory through the creation of legal frameworks, regardless of whether this occurs at a local, national or international level. This issue is currently contentious throughout product liability law discussions, particularly focused on the rise of innovative technology. Experts predict that product liability law will develop over time based on the precedents of case law, and evolve to reflect the advancements of the technology industry [17] [18].

Further, establishing liability upon devices of the Internet of Things ultimately sees the convergence of the smart city industry and the Internet of Things, further highlighting their intrinsic relationship. If liability is placed upon the manufacturers of the devices, supposedly the vendors of the Internet of Things, an incentive to design and produce secure and reliable products would be provided. However, placing the responsibility upon manufacturing companies could drive them further from participating in the city governance space. This approach is predicated on the notion that mitigating liability increases commitment and cooperation. The quality of individual devices comprising the network would predictably rise, the partnerships between public and private sectors are likely to strengthen, and the adoption of SSI throughout cities should become a more secure and reliable initiative.

4 Limitations for Implementing the Proposed Solutions

When seeking to counter the technological weaknesses inherent in the technological development of SSI, numerous limitations can arise. Although the formation of an international governing body for smart cities, which could administer standardization and conformity assessments, and the establishment of liability upon manufacturers, would mitigate the occurrences of inadequate, unreliable and insecure technology, implementing these initiatives is likely to be a challenging process. These challenges may delay the process of adopting these initiatives.

4.1 The Governing Body

An initial challenge for formulating an international governing body reflects common challenges faced by any developing international body. A lack of consensus, representation across nations, cooperation, and an agreed scope of influence will all restrict the formation of a cohesive smart city governing body. These challenges, often faced by supra-national bodies, are easily overcome with thorough discussion and compromise.

4.2 Standardization

Once this governing body is established, adopting agreed upon standards and conformity assessments will require further discussion and compromise. This is likely to be a lengthy process, requiring the perspectives from every domain of the smart city industry. Further, the convergence of the smart city industry with the Internet of Things increases this task substantially, broadening the amount of contrasting perspectives and interests to be considered. An issue likely to arise is whether these adopted standards and conformity assessments are applicable to every device of the Internet of Things, or just those comprising and connecting to a smart network. Drawing the line between these domains will be a controversial task as any device interacting with a smart network can be exploited. However, standardization for mechanisms across all devices possessing the ability to connect to the internet would mitigate any further technological threats outside of the realm of SSI.

4.3 Adoption

Once potential standards and conformity assessments are agreed upon, adoption of these may not necessarily be welcomed across all representative nations. If smart city standardization is paralleled to those of the IEC, the adoption of these regulations would be a voluntary act, one which may contradict the aim of collaboration across the industry. Thus, whether to make the agreement and implementation of standardization and conformity assessments mandatory for all cities utilizing SSI would be another contentious issue for discussion. As SSI are designed for a specific city's requirements, implementing international standards that encompass every individual city and do not restrict any required initiatives is a significant task. However, allocating the governance of standardizing technology to an international body and the planning, implementation and management of any potential smart city to the local body would counter this problem.

4.4 Who is Liable

The challenges of creating standardization across the technological industry are directly related to those which may arise when establishing liability upon the manufacturing companies. Current discussions surrounding the liability of technology focus on who exactly should be liable for the fault of a device if it causes harm. The three parties involved in any situation regarding new technology – the potential attackers, manufacturers and users – all hold their own case for liability. Obviously, the direct blame can fall upon the attacker. However, the problem of attribution throughout the cyber world often shields attackers from responsibility and any possible repercussions [19]. With this reality, the focus must shift to defensive mechanisms. Implementing security into devices then becomes a task for the manufacturing companies. Under product liability law, manufacturers of any product can be deemed liable if a person is caused harm from their product [17] [18]. Damages can be sought for negligence, design or manufacturing defects, failure to warn and numerous others. However, manufactures also have their own legal protections and can shift liability onto the users, and any actions which may have caused harm by their own fault – such as failure to administer updates, respond to recall instructions, or irresponsible usage [20]. Therefore, placing liability upon the manufacturers of devices if a security fault arises is an initiative which will face numerous legal challenges but can be overcome through the adoption of standardization for security mechanisms throughout devices comprising the Internet of Things, and ultimately smart cities.

4.5 Product Liability and Innovation

Establishing product liability for technological devices, such as the Internet of Things and those used for smart services or infrastructure, is further complicated through the intersection of product liability and innovation. As technological innovations occur so quickly, establishing legal ramifications for any fault bears the consequence of restricting innovative design and creation, the very concept which has provided all the benefits of technology. Creating strong ramifications for any fault of the manufacturer, often the innovator, can restrict the adoption of new technology into society. In the current social climate, technological advances gain popularity at a fast pace, with the device itself often experimental and requiring further advancement. Placing liability on these manufacturers, particularly small companies, can discourage them to create new products and think innovatively. However, innovation itself can provide a legal protection for manufactures who may be liable. With the rapid speed of innovative technology, it becomes difficult to perceive any security threat which may arise, providing the argument that such an event was unforeseeable at the manufacturing and design stage.

5 Conclusions

As the adoption of smart services and infrastructure increases around the world, weaknesses within the security architecture of devices require mitigation to reduce opportunity for exploitation. Viewing the rise of smart technology across the globe through a security lens, this paper has identified some inadequacies in incorporating security mechanisms. These may in turn become the primary weakness of the technologies used in smart cities.

We have proposed that the convergence of the smart city industry with the Internet of Things may give rise to viable solutions to mitigate the risk technological weaknesses pose to the safety of citizens. This could be achieved through two combined initiatives: the adoption of standardization for security mechanisms of all devices comprising a smart city network, essentially the Internet of Things, regulated through an international governing body of smart city technology; and the establishment of liability upon the manufacturers of technological devices, essentially those of the Internet of Things, which lack adequate security mechanisms within their architecture. Despite the benefits these solutions may provide, significant limitations for their implementation exist. These initiatives are offered in the hope that the cooperation of all stakeholders involved in the adoption of smart services and infrastructure will enable these limitations to be overcome.

6 References

[1] United Nations (2014). World Urbanization Prospects: The 2014 Revision, Highlights. Department of Economic and Social Affairs. *Population Division, United Nations*. Retrieved from https://esa.un.org/unpd/wup/publications/files/wup2014-highlights.Pdf

[2] Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology*, *22*(1), 3-21.

[3] IEE Smart Cities. *About Smart Cities.* Retrieved from http://smartcities.ieee.org/about.html

[4] Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L., & O'Carroll, E. (2015). A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online. *Contemporary Social Science*, 1-19.

[5] Piazza, J., & Bering, J. M. (2009). Evolutionary cyber-psychology: Applying an evolutionary framework to Internet behavior. *Computers in Human Behavior*, *25*(6), 1258-1269.

[6] Torrington D., & Weightman, J. *Effective Management:*

People and Organisation. New Jersey: Prentice Hall Inc.: 1994.

[7] Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J., & Shen, X. (2017). Security and Privacy in Smart City Applications: Challenges and Solutions. *IEEE Communications Magazine,* 112-129.

[8] Clarke, R. Y. (2013). Smart cities and the internet of everything: The foundation for delivering next-generation citizen services. *Alexandria, VA, Tech. Rep*.;

[9] International Electrotechnical Commission. (2014). Orchestrating Infrastructure for Sustainable Smart Cities. *Published in Geneva, Switzerland.*

[10] Guillemin, P., Berens, F., Carugi, M., Arndt, M., Ladid, L., Percivall, G., & Thubert, P. (2013). Internet of Things Standardisation—Status, Requirements, Initiatives and Organisations. *River Publishers Series in Communications*, 259.

[11] International Electrotechnical Commission. *Conformity Assessment.* Retrieved from http://www.iec.ch/conformity/?ref=menu

[12] IEEE. *Internet of Things*. Retrieved from http://standards.ieee.org/innovate/iot/

[13] IEEE Standards Association. *Internet of Things (IoT) Ecosystem Study: Executive Summary*. Retrieved from http://standards.ieee.org/innovate/iot/iot_ecosystem_exec_summary.pdf

[14] IEEE Standards Association. *P2413 - Standard for an Architectural Framework for the Internet of Things (IoT).* Retrieved from http://standards.ieee.org/develop/project/2413.html

[15] IBM. *IBM Invests to Lead Global Internet of Things Market - Shows Accelerated Client Adoption.* Retrieved from https://www-03.ibm.com/press/us/en/pressrelease/50672.wss

[16] IBM Analytics (2015). *IBM Point of View: Internet of Things Security, White Paper.* Retrieved from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=RAW14382USEN

[17] Cohen, R. A. (2015). Self-Driving Technology and Autonomous Vehicles: A Whole New World for Potential Product Liability Discussion. *Defense Counsel Journal*, *82*(3), 328.

[18] O'Brien, M. (2015). *The Internet of Things: The Inevitable Collision with Product Liability.* Retrieved from http://www.productliabilityadvocate.com/2015/07/the-internet-of-things-and-the-inevitable-collision-with-products-liability-part-2-one-step-closer/

[19] Bartholomew, B. & Guerrero-Saade, J. A. (2016). Wave Your False Flags! Deception Tactics Muddying Attribution in Targeted Attacks. *Virus Bulletin Conference.*

[20] Villasenor, J. (2014). Products liability and driverless cars: Issues and guiding principles for legislation. *Brookings Institute.* Retrieved from https://www.brookings.edu/wpcontent/uploads/2016/06/Products_Liability_and_Driverless_Cars.pdf