CHAPTER 5

SMARTER CITIES DEMAND SMARTER SECURITY

Adel S. Elmaghraby and Michael Losavio

INTRODUCTION[1]

Smart cities and the Internet of Things (IoT) inextricably weave networked computation into the lives of billions. They thus become woven into the political life of the city. Yet there seems a blithe indifference to the security implications for the daily, mundane affairs of people. We examine how things might go wrong, how things might be righted, and the questions of accountability needed in this human system of computation. A smarter perspective on what affects security in this new information paradigm is needed.

Concerns about increased urbanization are a driving force for exploration of smarter approaches to efficient management of urban areas, leading to many smart city initiatives. With the evolution of smart cities, novel concerns related to safety, security, and privacy emerge.[2]

According to Ivan Berger:

> Some 4 billion people live in cities now, and more than 6 billion—at least two thirds of the world's population—will live in urban areas by 2050, according to the United Nations [UN]. To deal with the challenges that brings, cities will need sophisticated technologies to monitor, analyze, and quickly respond to traffic tie-ups, citizen complaints, and lots more. And they must do so in the face of budgetary constraints and other obstacles.[3]

Lee, Hancock, and Hu have provided a framework to analyze the lessons learned from smart cities such as Seoul and San Francisco.[4] In their study, they concluded that eight stylized factors are the basis of a smart city. An adapted version of these findings can be represented by only the following five factors:

1. Intelligent data collection through sensors and multiple sources;
2. Open data initiatives to engage citizens in innovation and data usage;
3. Creation of a diversified development and service sources;
4. Accelerated adoption of technology through public initiatives and incentives; and,
5. An overarching strategy needed to assure the integration and growth of a smart city.

CONVENIENCE, SECURITY, AND PRIVACY

New lifestyles may demand convenience in many aspects of daily life. No one is willing to tolerate limited access to services or demanding physical access to business or government offices when the service can be delivered over the Internet. This places increased demands on such offices to open up their systems to the users. Convenient access to such services is in many ways the reason for the increased vulnerability of data leading to security and privacy challenges. Figure 5-1 shows that smart cities are mainly focused on providing convenience and are founded on security and privacy.

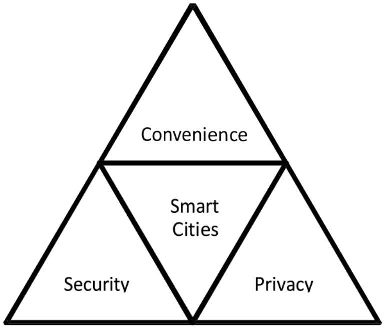

Figure 5-1. Convenience, Security, and Privacy.

CONNECTED INFRASTRUCTURE

Technological advances in the office, home, transportation, and service industries are the foundations of a smart city. Cesar Cerrudo has studied issues such as hacking traffic controls and other vulnerabilities.[5] He identified a list of technologies that help cities become smarter, and the technologies that are required on the back-end to support them.

In an earlier work,[6] the present authors identified the components of smart cities as a whole domain comprised of sets and relations.

The sets are mainly: the Persons (P), the Servers (S), and the Things (T) that are elements of the IoT. Essentially, we have:

$$\mathrm{P} = \{p_1, p_2, \ldots, p_L\}$$
$$\mathrm{S} = \{s_1, s_2, \ldots, s_M\}$$
$$\mathrm{T} = \{t_1, t_2, \ldots, t_N\}$$

Where $\mathrm{M} < \mathrm{L} \ll \mathrm{NM} < \mathrm{L} \ll \mathrm{N}$ since the number of servers and trusted entities are by far much less than the number of persons and clearly much less than the devices comprising the IoT, which is the backbone of smart cities. In addition, traditionally, the focus of attacks has been on servers; therefore, most security efforts have focused on securing servers. With the explosion of interaction between people and devices, the trend started to shift toward that communication link. However, with the next steps already in place, we project that the interaction among things is the next frontier of security and privacy.

A SMART SECURITY REGIME

How bad can it be? We have argued that an effective information security regime must begin to incorporate lessons learned for public security in the noncyber realm. The U.S. Director of National Intelligence has promoted the idea that "Changing the Game" is the only way to re-revitalize an effective information security regime for our information infrastructure. Yet changing how we approach security, as with every change of paradigm, has been difficult. Cybersecurity reports have detailed the vulnerabilities in home, consumer, and small business systems that in turn, may serve as attack platforms against other systems. However, little has been done in this domain except by operating system designers who incrementally add protections without full involvement of the users at risk. This becomes a huge mash-up with the smart city and the IoT. The integration of computational elements into all aspects of life requires examination of information security as public security. It requires engagement at all levels of the information polity, from high-level designers to the user on the street and in their homes.

For the smart city, this is directly connected to the protection of the governmental infrastructure using computational technologies to enhance service and efficiency. Compromise of those systems, so fundamental to daily life, could crash the social ecology that the smart city seeks to support. With the IoT, this moves into direct and immediate personal security for individuals within the computational social ecology. Each personal device can represent an opportunity for enhanced well-being and a vector for attack.

Attacking the Smart City.

Cerrudo detailed the diversity of interconnected applications within the smart city, and a sampling of the vulnerabilities to those systems reads like a traditional list of information security issues:

- Lack of Cybersecurity Testing
- Poor or Nonexistent Security (implementation)
- Encryption Issues (poor or nonexistent implementation of)
- Lack of Computer Emergency Response Teams (CERTS)
- Large and Complex Attack Surfaces (a target rich environment)
- Patch Deployment Issues
- Insecure Legacy Systems
- Simple Bugs with Huge Impact
- Public Sector Issues
- Lack of Cyberattack Emergency Plans
- Susceptibility to Denial of Service (DoS)
- Technology Vendors Who Impede Security Research (in order to protect their proprietary market position)[7]

All of these represent standard issues for information security and corporate governance: lack of knowledge, money, and foresight.

Cerrudo also details various “wide-open” city-cyber infrastructure security failures with examples of potential damage from intentional compromise. He then notes the proof of concept exercise compromising the traffic control systems due to a lack of communication encryption. This could potentially affect 100,000 intersections in the United States and Canada.[8] Critically, he notes that there is no way to assure remedies for such vulnerabilities. He notes this is not simply a matter related to criminality, but one that opens a target rich environment for war fighting over the wire.

A core concern is the nature of political accountability, which often acts in a post hoc, retrospective manner after a failure of government. Public accolades and positive press coverage come with the deployment of new smart technologies for the city. However, who will be held accountable for the failure of those systems? Moreover, particularly with the lagging nature of political accountability, were only those who are currently in office held responsible for failures that may have predated their tenure, how will the expenditure of monies to security systems be viewed by the taxed public?

Attacking the Citizens of the Smart City.

The ubiquitous deployment of interconnected computable systems will, as with the smart city, offer expanded conveniences and efficiencies for personal life. Yet, each such system can offer a personal vector to attack an individual.

One historical example of this phenomenon deals with online and electronic payment systems, which have become the focus of theft activities by criminals. As the use of these systems has exploded, so has exploitation. The technical information security-based response to the problem of static credit card encoding information being duplicated and forged was the new Europay, Mastercard, and Visa (EMV) chips for credit cards that dynamically assigned transaction information that, once used, could not be reused for further transactions. This has drastically reduced counterfeit credit card fraud in Europe. While this same benefit may be expected for in-store credit card use in the United States, it will also produce a shift toward online transactions (which will not have the same level of security) and check counterfeiting. It may also increase the impetus for credit card theft and the commensurate personal risk this may entail.

We posit that this will begin to be seen across domains involving devices throughout people's lives. Health, transportation, social engagement, entertainment, and work: all of these domains may be instrumented and exploited.

Attacking the Smart Citizens of the Smart City.

This is a consequence of the interactive nature of the smart systems we hope to introduce into our lives. Think of the mischief. Think of the misery. Therefore, as in other aspects of our lives, **people** need to be prepared for their own guardian roles in the safe deployment of these technologies throughout our world. The understanding of interaction among various elements of information exchange is mandatory. In Figure 5-2, some of the nodes involved in such information exchange are highlighted.

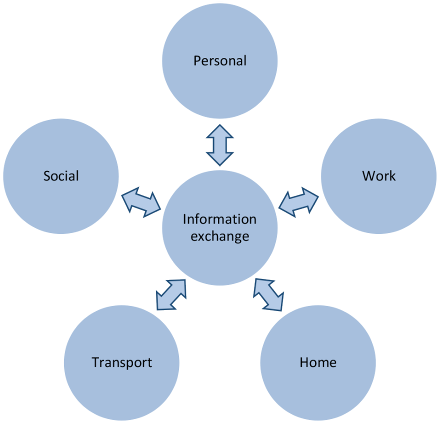

Figure 5-2. Exchange Nodes of Activities and Services.

We look at these vulnerabilities and map them to standard crimes that, in the past, required a physical presence and risk for the perpetrator.

1. Murder, Aggravated Assault.

Causing the death or physical injury of another, absent justification, is a crime in all systems of criminal law. Simple elements are the act that causes death or injury, the intent to commit that act, and the resulting death or injury. The highest penalty is for a death that was intended and accomplished.

One of the first proof of concepts relating to the use of instrumented and interconnected devices was that of the hacked operating system for a personal insulin pump via its Bluetooth port. Demonstrated by Jay Radcliffe at the 2013 Black Hat conference, one commentator observed that the more disturbing aspects of this were the significant lack of both security controls and incentives for manufacturers to properly secure their systems.[9]

More recently, security researchers Charlie Miller and Chris Valasek demonstrated the control takeover of a 2014 Jeep Cherokee, shutting off the engine, disabling the brakes, and turning the steering wheel.[10] Given the number of deaths caused by defective floor mat/accelerator combinations and effective ignition switches causing some airbags to fail during crashes, the murder and mayhem that would follow from this kind of attack could be significant.

The motives for such actions are the same as with any other crimes of violence. Jealousy, envy, and hatred, all of which play a role in criminal conduct, can now be enhanced through the use of these new technological tools.

2. *Assault, Stalking, Harassment, Sexual Assault, Invasion of Privacy.*

Stalking and harassment were given new extensions with the development of information technologies and the Internet. Facebook page harassment, use of systems to track people, and text messages or emails with vile content have all been used in this context.

However, the intensive penetration of our lives by more technology creates even more opportunities. Invasive monitoring of webcams unbeknownst to a homeowner, or the placement of hidden webcams can radically change the dimensions of voyeurism. The ability to capture extensive video and then to publish it online around the world deeply expands the damage done by such conduct.

At the other end of the spectrum are new opportunities for malicious mischief and vandalism, simply inflicting misery on others because it can be done. Much of this kind of malicious behavior, representing some of the earliest illegal behavior with the dawn of the Internet, can now find its way into all manner of small torments. The kitchen, for example, offers a host of opportunities. The Internet toaster can now always burn the toast. The Internet refrigerator can defrost or spoil a week's worth of food. The Internet stove can be manipulated to ruin breakfast, lunch, and dinner. Security and practices are needed to prevent this.

3. Burglary, Theft.

Lastly, we have to consider the way that the physical security systems of our families, homes, transportation, and businesses might be configured within this interconnected environment. Should we rely on these electronic security systems, which seem to offer so much? If so, we may also face a common vulnerability base that may allow physical injury in all spaces and the theft of the things within them. Indeed, used with the monitoring systems themselves, it may inform the criminals both of the goods available and the location of the people who might otherwise complicate a theft and deter its execution, or themselves become targets of physical attack.

Fighting the Attacks: Application of Criminological Theory.

We look at these vulnerabilities to give body to the problems faced by these new and amazing systems that do not consider security as a primary function simply because that is not the designers' forte. These new systems are meant to do something good, and the exploitation of them by bad people is an afterthought. Given the expanse of these vulnerabilities, and how it may allow for an expansion of those vulnerabilities to affect our own physical safety, we need to integrate security and security practices now, as we have done with the traditional aspects of our lives.

It is valuable to look at the application of modern criminological theory in this technical space. These theories help identify potential perpetrators. However, they can also help identify vulnerabilities in the human factor and ways in which systems may be best configured to reduce exploitation. Whether it is general strain theory, social control theory, routine activities theory, or other theoretical models that define the space for criminal conduct and public security, these models should be examined and mapped into the conduct that will be beneficial in both the smart city and the IoT, and identify potential risk from those that will harm others.

Routine Activity Theory posits the benefits of both a suitable guardian and the hardening of an available target. These can be strengthened by practices shifted to the private and public realms, just as the IoT/smart cities paradigm shifts to these realms. Strain Theory examines elements that both heighten the risk of deviant behavior (particularly insiders), as well as the risk of victimization (either individually or as a member of an organization opening a door to an attacker). Social Control Theory examines related and complementary factors that, again, can have an impact both on deviant attacks and the heightened risk of victimization. Displacement theory addresses how the "hardening" of one class of potential targets/victims may simply lead to victimization of other targets, a special concern for the target-rich environment of technologically advanced polities like the smart city.

These and other aspects of criminology may take these information security issues and map them to programs that have successfully reduced crime and victimization in the traditional world. They may serve as models for enhanced security within the smart city and the IoT in private life. These do presuppose a general security regime in place on core systems, itself questionable in some political environments.

Possible Responses: Initiatives that Reflect New Practices.

New possibilities for effective responses in public/information security can be seen in two initiatives by a global nongovernmental organization (NGO) that focuses on worldwide economic prosperity and security. These examples, initiatives of the World Economic Forum (WEF), demonstrate both the imaginative possibilities for new and effective systems of security as well as critical importance of this for the economic health of the world's economies. Conversely, failure of such an information security regime has the potential for economic damage and concurrent misery for the targeted populations.

Cyber-Hygiene.

People build wealth, but in the cyber realm, individuals are vulnerabilities for the total system. Smart cities will depend on smart systems, and smart systems will depend on informed formulation, responsive management, and efficient implementation. This applies to public safety systems, education systems, and, increasingly, information and communication technology (ICT) systems. In fact, the "smarter" cities get, the more ICT systems, through the Internet, will insert themselves into other systems. As the IoT becomes more ubiquitous, the safety of not only ICT systems, but also every system that has any kind of connectedness to the web will be in doubt. These are the fears of every large organization, from governments to corporations. Many of these organizations have decided the best way to protect themselves proactively is to institute cyber-hygiene regimes by creating and implementing Critical Controls.

Cyber-hygiene can be most clearly explained by analogizing it to another critical system for cities: public health. While the public becomes glued to television (TV) coverage of outbreaks of frightening diseases like the plague or Ebola, a vastly larger number are killed every year by more outbreaks of mundane diseases like malaria or influenza. Straightforward solutions that are now thought of as simple, such as washing hands or covering the mouth when coughing, can prevent the spread of these diseases and eliminate a huge amount of risk, allowing resources to be focused on larger, more complex threats. Cyber-hygiene works in much the same way—preventative measures can be can be taken to mitigate the thousands of everyday low-level attacks that cause the vast majority of security issues so that resources can be focused on larger, more dangerous threats. These measures are known as critical controls, a set of actions that are the most important things to do first when trying to reduce vulnerability and ensure sound cyber-defense. This is especially important in the era of the IoT, where everything from cars to insulin pumps to lightbulbs are fitted with microchips and connected to the web. Technological advances have outpaced their ability to be secured, and with ever-increasing hyper-connectedness, there are more fronts than ever before on which to attack. More complicated linkages between endpoints and central databases have led to attacks in areas previously thought safe, or at the very least, unnecessary to closely guard. The 2015 hacking of a Jeep Cherokee proved that linkages in the IoT could be its downfall when hackers entered the car's computer through its entertainment system and then gained control of steering and braking functions. This is why a cyber-hygiene system is so critical to ensure well-run, cyber-secure smart cities.

Several organizations, including the SANS Technology Institute and the Council on Cyber Security, have created their own set of Critical Security Controls. The challenge, though, is the implementation of popular security measures across populations and groups, not just by expert organizations.

Cyber Resilience.

Another initiative that reflects this is the cyber resilience effort of the WEF, which, again, is concerned with global economic policy that recognizes the critical nature of cybersecurity in that economy. It argues for the need for an integrated approach.[11] This recognizes the reality of information security: it will never be perfectly secure, no more than banks or levees, and recovery planning and execution are essential.

The WEF recommendations in this space are for the private sector, public sector, their collaborative intersection, and the academy. They include, even at this late date, true awareness, best practices implementation, criminal justice engagement, trans-jurisdictional collaboration, and continued research on incentive factors. As detailed in its policy statements, they cover:

- **For the private sector:**
  - Join the Partnering for Cyber Resilience initiative; commit to the Principles
  - Develop a pervasive culture of cyber awareness and resilience
  - Commit to responsibility and accountability for developing the organization's level of cyber resilience
  - Promote the spread of best practices throughout supply chain
  - Engage in policy debate, and where possible, align under common core principles and commitments as a first step towards harmonizing policy needs
- **For the public sector:**
  - Work towards a flexible, but harmonized criminal justice capabilities framework
  - Engage private sector and adjacent policy domain experts to identify potential unintended consequences of policy development in advance
  - Ensure individual protections and foreign jurisdiction counterparts to share lessons learned and improve harmonization
  - For public agencies: join the Partnering for Cyber Resilience initiative; commit to the Principles (of Cyber Resilience)
- **For the private and public sectors together:**
  - Commit to develop robust and sustainable public-private partnerships for a resilient cyber environment, based on clear and

    mutually agreed assignment of roles and responsibilities and the principle of accountability
  - Explore the need for the development of a cyber-risk market
- **For academia:**
  - Promote the concept of economics of cybersecurity to non-specialist fields
  - Advance research on information sharing and the link between cyber resilience and national competitiveness[12]

WEF and other public organizations and NGOs promote the development of guidelines for policy and criminal justice communities. They promote their implementation as part of a total security and safety regime for the cyber environment.

THE FUTURE ISSUE

We submit that, first and foremost, there is one salient issue for the implementation of smart security in the smart city. Moreover, that issue is political accountability. All the stresses associated with the implementation of information security in a business are present in the political life of the city. However, the metrics of success, and the accountability for failure, is much more diffuse. If the traffic system fails and the city is paralyzed, who will be called to account? Elected leaders are in for their terms, so there will not be any immediate sanction (absent an impending election). Bureaucrats who may be responsible will only be held to account if it serves a political purpose, from political leaders who may or may not understand enough about these issues even to know whom to hold accountable. Even political leaders concerned about the future must balance expenditure for potential risk management against current demands. This all seems to shift the political will to act off to future political leaders and future generations.

This future issue is, in fact, a massively complex one, particularly given the unique American system of federalism and the practices in some states for the development of responsibility to local entities. In one recent infrastructure failure, a U.S. city switched municipal water supply only to find it was now poisoning its citizens with metallic lead in the water; yet, no political leader has been held to account beyond offering apologies (with some bureaucrats resigning their positions).[13] Jurisdictional control of factors within the city may lie with multiple political entities at various levels, including federal, state, local, and local special-purpose entities. Some of these have been intentionally designed to insulate them from popular political will, such as public utilities given appointed boards and even limited taxing power. All may be shielded, to a greater or lesser degree, by sovereign immunity from liability for even significant wrongdoing. Therefore, when traffic systems fail under a cyberattack and people die, there may only be that diffuse, downstream political accountability to demand change.

Without the political will to protect the people of the smart city, there is not going to be any safety.

CONCLUSION

The smart city absolutely demands smarter security, even as we struggle to define what that means. The lack of a coherent approach toward the identification and remediation of attacks on nodes of security will only mean growth in open targets. The leadership of private organizations and NGOs, the academy, and core governmental agencies, is vital to build the foundations for protection. This must be embraced by all the entities and organs of the city. This requires a strong political effort to implement and maintain a safe and secure smart city—every smart city—before things go very, very wrong, and people—men, women, and children—are hurt by the evil of others who exploit the wonders the city can offer.

ENDNOTES - CHAPTER 5

1. The author thanks Joseph D. Losavio for his assistance in research, writing, and developing the original concept paper of this chapter and China Tom Miéville for his insistence that we look at the city in a different way. An earlier version of this chapter appeared as the paper Adel S. Elmaghraby and Michael Losavio, "Smarter Cities Demand Smarter Security," Presented at The City University of New York (CUNY), City College, Cyber Infrastructure Protection (CIP) Conference in New York on October 15, 2015.

2. Adel S. Elmaghraby and Michael M. Losavio, "Cyber security challenges in Smart Cities: Safety, security and privacy," *Journal of Advanced Research*, Vol. 5, Iss. 4, July 2014, pp. 491-497, available from *dx.doi.org/10.1016/j.jare.2014.02.006*.

3. Ivan Berger, "IEEE's First Smart City Conference to Meet in Mexico's First Smart City: Guadalajara gathering to cover data collection, analytics, and privacy," the institute: The IEEE news source, August 7, 2015, available from *theinstitute.ieee.org/*.

4. Jung Hoon Lee, Marguerite Gong Hancock, and Mei-Chih Hu, "Towards an effective framework for building smart cities: Lessons from Seoul and San Francisco," *Technological Forecasting and Social Change*, Vol. 89, November 2014, pp. 80-99, available from *dx.doi.org/10.1016/j.techfore.2013.08.033*.

[5] Cesar Cerrudo, "Brief: Keeping Smart Cities Smart: Preempting Emerging Cyber Attacks in U.S. Cities," Institute for Critical Infrastructure Technology, June 25, 2015.

[6] Elmaghraby and Losavio, "Cyber security challenges in Smart Cities," pp. 491-497.

[7] Cesar Cerrudo, "An Emerging US (and World) Threat: Cities Wide Open To Cyber Attacks," *White Paper*, Securing Smart Cities, May 2015, p. 8, available from *securingsmartcities.org/wp-content/uploads/2015/05/CitiesWideOpenToCyberAttacks.pdf*, accessed September 8, 2015.

[8] Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure," 8th USENIX Workshop on Offensive Technologies (WOOT '14), San Diego, CA, 2014, available from *https://www.usenix.org/conference/woot14/workshop-program/presentation/ghena*, accessed September 13, 2015; Cesar Cerrudo, "Hacking US (and UK, Australia, France, etc.) Traffic Control Systems," April 30, 2014, IOActive blog, available from *blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html*, accessed September 13, 2015.

[9] Eric Basu, "Hacking Insulin Pumps And Other Medical Devices From Black Hat," *Forbes*, August 3, 2013.

[10] Craig Timberg, "Hacks on the highway: Automakers rush to add wireless features, leaving our cars open to hackers," *The Washington Post*, July 22, 2015.

[11] World Economic Forum (WEF) and Deloitte, "Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience," Geneva, World Economic Forum, May 31, 2012, p. 7, available from *https://www.weforum.org/reports/risk-and-responsibility-hyperconnected-world-pathways-global-cyber-resilience/*.

[12] *Ibid.*, p. 7.

[13] Claire Groden, "How Michigan's Bureaucrats Created The Flint Water Crisis," *Fortune*, January 20, 2016, available from *fortune.com/flint-water-crisis/*, accessed January 27, 2016.