Smarter Cities Demand Smarter Security

Adel S. Elmaghraby and Michael Losavio
University of Louisville, KY, USA

ABSTRACT - Smart Cites and the Internet of Things 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. Essentially a smarter perspective on what affects security in a new paradigm is needed.

INTRODUCTION

Concerns about increased urbanization are real and they seem to be the driving force for exploration of smarter approaches to efficient management of urban areas and leading to many smart city initiatives. With the evolution of smart cities concerns related to safety, security and privacy have emerged. [1]

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. 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."* [2]

Lee, Hancock, and Hu [3] have provided a framework to analyze the lessons learned from smart cities such as Seoul and San Francisco. In their study, they concluded that eight stylized facts 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. Creating a diversified development and service sources
4. Accelerated adoption of technology through public initiatives and incentives
5. An overarching strategy to assure integration and growth

CONVENIENCE, SECURITY, AND PRIVACY

It is easy to note that new lifestyles are demanding convenience in every aspect 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 s to such services is in many ways the reason for the increased vulnerability of data leading to security and privacy challenges. Figure 1 shows that smart cities are mainly providing convenience and are founded on security and privacy.

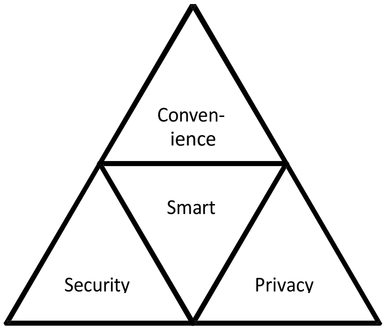

Figure 1 - Convenience, Security and Privacy

CONNECTED INFRASTRUCTURE

Technology Advances in the office, home, transportation and services are the foundations of a smart city. Cesar Cerrudo [4] has been researching issues such as hacking traffic controls and other vulnerabilities – he identifies a list of technologies that helps cities become smarter and the technologies that are required as back-end to support them.

In earlier work [1] we identified the smart cities components as a whole domain as some sets and relations as follows:

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

$P = \{p_{1,} p_2, \ldots , p_{L\}}$

$S = \{s_1, s_2, \ldots , s_3\}$

$T = \{t_{1,} t_2, \ldots , t_L\}$

Where M<L<<N since the number of servers and trusted entities is by far much less than the number of persons and clearly much less than the devices comprising the Internet of Things (IoT) which is the backbone of the smart cities. Also, traditionally the focus of attacks has been on servers and most security efforts has focused on securing servers. With the explosion of interaction between humans/persons and devices the trend started to shift towards that communication link. However,

with the next steps already in-place, we project that the interactions 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 non-cyber realm. The director of national intelligence for the United States has promoted the idea that "Changing the Game" is the only way to re-revitalize an effective information security regime for our information infrastructure.

For fifteen years various cyber security reports have also detailed the vulnerabilities in home, consumer and small business systems that may, in turn, serve as attack platforms against other systems.

This becomes a huge mash-up with the Smart City and the Internet of Things. The integration of computational elements into all aspects of life *requires* examination of information security as public security.

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 will crash the social ecology.

With the Internet of Things, 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 has also detailed the diversity of interconnected applications within the Smart City and a sampling of the vulnerabilities to those systems which reads like a traditional list of information security issues:

- The Failure or Absence of Adequate Cyber Security Testing
- Poor or Nonexistent Security Implementations
- Poor or Nonexistent Encryption Implementations
- Absence of an Attack Response Plan
- A Target Rich Environment (Large and Complex Attack Surfaces)
- Patch Deployment Issues
- Insecure Legacy Systems
- Simple Bugs with Huge Impact
- Public Sector Issues
- Susceptibility to Denial of Service
- Technology Vendors Who Impede Security Research in order to protect their proprietary market position. [5]

All of these represent standard issues for information security and corporate governance: lack of knowledge, lack of money, lack of 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 lack of communication encryption; this could potentially impact 100,000 intersections in the United States and Canada. [6] Critically, he notes that there is no way to assure that such vulnerabilities are remedied. He notes this is not simply a matter related to criminality, but one which 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. But who will be held accountable for the failure of those systems? And particularly with the lagging nature of political accountability, were only those who are currently in office will be held responsible for failures which 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 that 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 an exploitation. The technical information security-based response to the problem of static credit card encoding information being duplicated and forged will be the new EMV chips for credit cards, which dynamically assign transaction information which, once used, cannot 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 towards 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. So, 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 2 some of the nodes involved in such information exchange are highlighted.

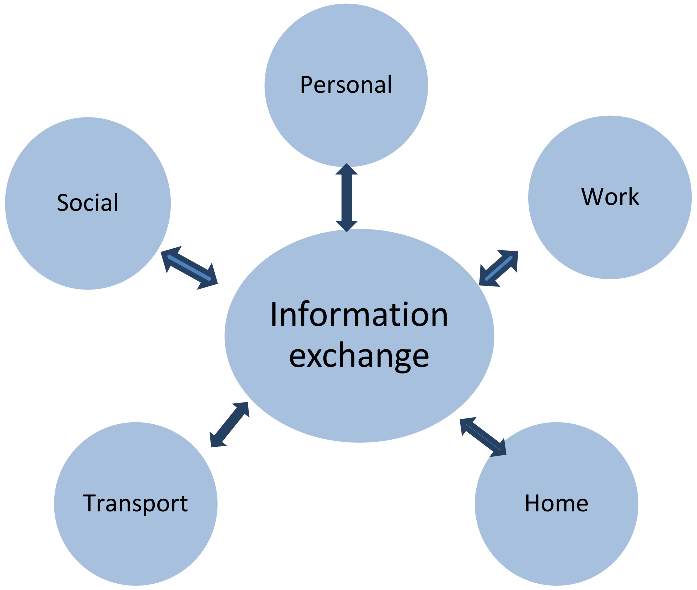

Figure 2- Exchange Nodes of Activities and Services

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 J 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. [7]

More recently, security researchers Charlie Miller and Chris Valasek demonstrated the control takeover a 2014 Jeep Cherokee, shutting off the engine, disabling the brakes and turning the

steering wheel. [8] Given the number of deaths caused by defective floormat/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 are the same with any other crimes of violence. Jealousy, envy, hatred, all of these that play a role in criminal conduct can look to use these new 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, text messages and emails with vile content have all been used in this context.

But the intensive penetration of our lives by more technology creates even more opportunities. Invasive monitoring of Web-Cams unbeknownst to a homeowner, or the placement of hidden Web-Cams 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 and 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 homes and cars and businesses might be configured interconnected environment. Should we rely on these electronic security systems, which seem to offer so much, then we also may face a common vulnerability base that may allow physical injury and all of the spaces and the theft of the things within the. Indeed, used with the monitoring systems themselves, it may inform the criminals both of the goods available and location of the people who might otherwise complicate a theft.

Fighting the Attacks: Application of Criminological Theory

We look at these vulnerabilities to give body to the problems faced by new and amazing systems that simply do not consider security as a primary function simply because that’s not the designers’ forte. In 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 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 into this technical space. These theories help identify potential perpetrators. But 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 both be beneficial in the Smart City in the Internet of Things and bring potential risk from those that will harm others.

Routine Activity Theory posits the benefits of both a suitable guardian and hardening of available target. These can be strengthened by practices shifted to the private and public realms, just as the Internet of Things/Smart Cities paradigm shifts to these realms. Strain Theory examines elements which both heighten the risk of deviant behavior, particularly insiders, as well as heightening 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 which, again, can have an impact both on deviant attacks and heightened risk of victimization.

The extent to which these have been mapped to programs that have successfully reduced crime and victimization in the traditional world may serve as models for enhanced security within the Smart City and the Internet of Things 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 for public/information security can be seen in two initiatives by a global nongovernmental organization that focuses on worldwide economic prosperity and security. These examples, initiatives of the World Economic Forum, 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 this 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 are "vulnerabilities" for the total system. Smart Cities will depend in 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 systems. In fact, the “smarter” cities get, the more ICT systems, through the internet, will insert itself into other systems. As the Internet of Things becomes more ubiquitous, safety of, not only ICT systems, but every system that has any kind of connectedness to the web will be in doubt. These are fears that every large organization, from governments to corporations, have. Many of those organization 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 coverage of outbreaks of frightening diseases like the plague or Ebola, a vastly larger number are killed every year by more mundane outbreaks of malaria or the influenza. Straightforward solutions, 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 focus 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 Internet of Things, 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 on which to attack. Ever 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 Chrysler Jeep Cherokee proved that linkages in the internet of things could be its downfall as hackers entered the cars computer through tis 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 SANS and the Council on Cyber Security have created their own set of Critical Security Controls. The challenge is this popular security implementation across populations and groups, not just by expert organizations.

Cyber Resilience

Another initiative that reflects this is the Cyber Resilience effort of the World Economic Forum, which, again, is concerned with global economic policy that recognizes the critical nature of cyber security in that economy. It argues for the need for an integrated approach. [9] This recognizes the reality of information security: it will never be perfectly secure, no more than banks or levees, and recovery planning and execution is essential.

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

- 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 cyber security to non-specialist fields – Advance research on information sharing and the link between cyber resilience and national competitiveness. *Id*., p 6

WEF, as do other public and NGO groups, promote development of guidelines for policy and criminal justice communities and their implementation to bring them into this process as part of a total security and safety regime for cyber.

THE FUTURE ISSUE

We submit that, first and foremost, there is one salient issue for the implementation of Smart Security in the Smart City. And that issue is political accountability for what happens. All the stresses associated with the implementation of information security in a business are present in the political life of the city. But 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 to even 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. 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, to a greater or lesser degree, be shielded by sovereign immunity from liability for even significant wrongdoing. So when traffic systems fail under a cyber-attack 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 towards the identification and remediation of nodes of attack nodes of security will only mean growth in open targets. The leadership of private and nongovernmental organizations, the academy and core governmental agencies is a 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.

ACKNOWLEDGEMENTS

We wish to thank Joseph D. Losavio for his assistance in research, writing and developing this concept paper and China Tom Miéville for his insistence we look at the City in a different way.

REFERENCES

[1] Adel S. Elmaghraby, Michael M. Losavio, "Cyber Security Challenges in Smart Cities: Safety, Security and Privacy," Journal of Advanced Research, Volume 5, Issue 4, July 2014, Pages 491-497, ISSN 2090-1232, http://dx.doi.org/10.1016/j.jare.2014.02.006.

[2] 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. August 7, 2015. (http://theinstitute.ieee.org/benefits/conferences/ieees-first-smart-city-conference-to-meet- in-mexicos-first-smart-city)

[3] Jung Hoon Lee, Marguerite Gong Hancock, Mei-Chih Hu. Towards an effective framework for building smart cities: Lessons from Seoul and San Francisco, Technological Forecasting and Social Change, Volume 89, November 2014, Pages 80-99, ISSN 0040-1625, http://dx.doi.org/10.1016/j.techfore.2013.08.033.

[4] Cesar Cerrudo, "Keeping Smart Cities Smart: Preempting Emerging Cyber-attacks in U.S. Cities," Institute for Critical Infrastructure Technology.

[5] Cerrudo Cesar, "Cities Wide Open To Cyber Attacks" http://securingsmartcities.org/wp-content/uploads/2015/05/CitiesWideOpenToCyberAttacks.pdf, accessed 9/8/2015 parental cyber security monitor

[6] Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure" https://www.usenix.org/system/files/conference/woot14/woot14-ghena.pdf, accessed September 13, 2015; Cesar Cerrudo, "Hacking US (and UK, Australia, France, etc.) Traffic Control Systems" April 30, 2014 http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html, accessed September 13, 2015

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

[8] Craig Timberg, "hacks on the highway: automakers rush to add wireless features, leaving our cars open to hackers," Washington Post, July 22, 2015

[9] World Economic Forum, “Risk and Responsibility in a Hyperconnected World: Pathways to Global Cyber Resilience,” 2012, http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf , accessed 9/9/2015.