Government Information Quarterly xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

# Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets

Zhen Li[a], Qi Liao[b,*]

[a] Department of Economics and Management, Albion College, USA
[b] Department of Computer Science, Central Michigan University, USA

ARTICLE INFO

*Keywords:*
Smart cities
E-government
Cybersecurity
Vulnerability
Economics
Game theory

ABSTRACT

Cities are becoming smarter and smarter. While the rapid progress in smart city technologies is changing cities and the lifestyle of the people, it creates also huge attack surfaces for potential cyber attacks. The potential vulnerabilities of smart city products and imminent attacks on smart city infrastructure and services will have significant consequences that can cause substantial economic and noneconomic losses, even chaos, to the cities and the people. In this paper we study alternative economic solutions ranging from incentive mechanisms to market-based solutions to motivate governments, smart product vendors, and vulnerability researchers and finders to improve the cybersecurity of smart cities and e-government. These solutions can be integrated into policy instruments in defending smart cities and e-governments against cyber attacks.

## 1. Introduction

Cities are getting smarter and smarter in recent years. Communities around the world, from small towns to big metropolitan areas, are turning to modern technologies to connect government agencies and citizens to deal with urban problems such as traffic congestion, public service shortcomings, and energy shortages. To ensure the efficiency and effectiveness of providing public services to people, the smart city concept requires bringing together various information and communications technologies and solutions. While technologies are changing cities and the lifestyle of the people, the rapid growth of smart cities and e-government is also posing enormous challenges in terms of the safety and security of the cities. One specific concern is the safety of smart city products themselves. The potential vulnerabilities of smart city devices and systems largely result from the inherent vulnerable characteristics of these products as well as the lack of incentives in the design and implementation of security features of these products. As smart city infrastructure development outpaces cybersecurity solutions, smart software, devices, and systems are vulnerable to intrusion and malicious cyber attacks.

In smart cities, cybersecurity plays the key role in protecting availability, integrity, stability, as well as the confidentiality required to support smart environments. Cybersecurity used to be seen as purely a technical problem. Researchers and practitioners largely depended on technologies for cybersecurity solutions. Nevertheless, humans are players in every cybersecurity attack-defense game. It is informative to study the motives of each interested party involved in the cybersecurity issue and design corresponding non-technical solutions to reduce cyber attacks. In the cybersecurity game of smart cities and e-government, there are at least four types of stakeholders involved: governments, smart solution providers, vulnerability finders, and cyber attackers. It is important to study the incentives and interdependence of various stakeholders' decision making. This paper focuses on feasible economic solutions to enhance the cybersecurity situation of smart cities and e-government by analyzing incentives, especially financial incentives, of the stakeholders' behaviors and interactions during the process of building and managing smart cities.

The main contributions of this study are twofold. First, we formally model the life cycle of smart city vulnerabilities by considering the role of government, smart product vendors, internal vs. external vulnerability finders, and offensive vs. defensive vulnerability buyers, as well as the likelihood of malicious cyber attacks on smart cities and e-government. The model is further analyzed in a four-party game theoretical framework. Second, two alternative economic solutions are proposed based on the modeling analysis of economic incentives. The first proposal is carrot-and-stick-like strategies, i.e., the government either rewards the product vendor for security investment by paying a security premium on smart city products or holds the vendor accountable for product vulnerabilities and punishes the vendor financially for vulnerability exploitation. The second proposal is to encourage smart product vendors and governments to participate actively in the vulnerability market and compete with malicious attackers to acquire

* Corresponding author at: Department of Computer Science, Central Michigan University, Mount Pleasant, Michigan 48859, USA.
*E-mail address:* liao1q@cmich.edu (Q. Liao).

http://dx.doi.org/10.1016/j.giq.2017.10.006
Received 18 October 2016; Received in revised form 9 October 2017; Accepted 12 October 2017

vulnerabilities for defensive purpose.

The rest of the paper is organized as follows. Section 2 discusses related work and how this study fits in the literature. Section 3 discusses potential vulnerability of smart cities to cyber attacks and how dual disincentives existing in product development and implementation may lead to lack of security in smart city products. Section 4 uses a life cycle model of vulnerability to study the relationship between government, smart product vendors, vulnerability finders, and vulnerability exploiters. It identifies key factors that determine the chance of cyber attacks on smart cities. Section 5 proposes two economic mechanisms to improve security situation of smart city systems. Policy instrument design, limitation of this study, and future research avenues are also discussed. Section 6 concludes the paper.

## 2. Related work

Interest in the concept of smart cities has been expanding in recent years since it was first studied in the 1990s (Cocchia, 2014). There exists a large literature on the implementation of smart city concept and the around-world practices of making cities smart (Sureshchandra, Bhavsar, & Pitroda, 2016). They address shortcomings, challenges and risks with smart city initiative, and give practical suggestions. It has been argued that smart city thinking and initiatives need to be reframed in several ways, including normative and conceptual thinking with regards to goals, cities and epistemology, and practical and political thinking with regards to management/governance, ethics and security, and stakeholders and working relationships (Kitchin, 2016).

Smart urban services depend on mobile communications. The increasing potential benefit from the vulnerability exploitation in the mobile system has attracted significant attention from the black market (Algarni & Malaiya, 2014). While Android continuously increases its popularity in the mobile ecosystem, compared to other vulnerabilities, the vulnerabilities in the Android market are more exploitable, possibly due to the fast growing number of apps (Huang, Zhang, Tan, & Feng, 2015). Android apps have been found to have substantial software reuse, and the quality of the apps and libraries reused determines the quality of the apps (Mojica et al., 2014).

Security is essential to the success of smart cities and e-government because it determines users' incentive to use government services (Alsultanny, 2014, September-October). The ability to measure the quality of a technology is a prerequisite to obtain a high quality service, but it is hard to evaluate the quality of the services e-governments provide to users in all the management, information, service, and technical domains (Sa, Rochac, & Cota, 2016). Governments' lack of ability to frame cybersecurity can lead to the failure of developing suitable security policies (de Bruijn & Janssen, 2017). Considering the way humans, government, and technology interact, security education is desirable to strengthen the knowledge of government officials and citizens with regard to cybersecurity issues (de Bruijn & Janssen, 2017; Klaper & Hovy, 2014). As cybersecurity specialists are found to overdramatize or over-simplify cybersecurity risks with management guru techniques, there is also a need for government to validate those statements (Quigley, Burns, & Stallard, 2015). A report outlined common risks that come with technologies adopted by local governments, and provided a *Best Practices and Resources Guide* local governments can use to achieve technology proficiency (Pfeiffer, 2015).

Usual cyber security technologies and best practices are necessary to protect smart city devices and systems. Studying the life cycle of vulnerabilities helps vendors reduce potential vulnerabilities during the software development process (Bilge & Dumitras, 2012), but technologies are only part of the solution. Technical advancements within software design and development have not prevented the release of insecure software and consequently the appearance of vulnerabilities and occurrence of exploitation. Depending on layers of walls difficult to breach to create security is outmoded for cybersecurity (Leuprecht, Skillicorn, & Tait, 2016). Economic, political, and other non-technical incentives are increasingly perceived as the primary reasons for today's increased risk exposure. Non-technical approaches need to be explored.

Software vulnerability disclosure is found to force vendors to release patches (Arora, Telang, & Xu, 2008). It may also affect the volume of attacks (Arora, Nandkumar, & Telang, 2006). Economics-based mechanisms of vulnerability disclosure, such as vulnerability reward program, can be effective to restrict the diffusion of vulnerability exploitation (Ransbotham, Mitra, & Ramsey, 2012, March). Study of Google's experience with its vulnerability reward programs (Mein & Evans, 2011, March) and a comparative research on two vulnerability reward programs by competing browser vendors, Google Chrome and Mozilla Firefox (Finifter, Akhawe, & Wagner, 2013) found reward programs economically beneficial to vendors. The government may create legal protections for cybersecurity research and enhance financial incentives to limit the supply of software vulnerabilities to attackers (Herr, 2017). It has been proposed to create an international vulnerability purchase program in which the major software vendors would be induced to purchase all of the available and known vulnerabilities at prices well above the black market prices (Frei & Artes, 2013, December).

There has been rising attention paid to cybersecurity of smart cities and e-government. Issues studied include the protection of citizen's privacy and personal data (Belanche-Gracia, Casalo-Arinob, & Perez-Rueda, 2015; Wu, 2014), security of e-government websites (Zhao & Zhao, 2010), and security of governmental use of cloud computing (Paquette, Jaeger, & Wilson, 2010). Economic mechanisms were proposed to improve smart city cybersecurity (Li & Liao, 2016). As consumers of smart city technology and policy maker, the government's potential to create economic incentives with policy making has not been fully addressed in the context of smart cities and e-government. This study extends existing work and further discusses economic solutions that can be disengaged into working policy instruments in defending smart cities and e-government against cyber attacks.

## 3. Security implications of smart cities

In this section, we discuss the potential vulnerability of smart cities to cyber attacks and the existing lack of security consciousness in the design and adoption of smart city products.

### 3.1. Cyber attack threat on smart cities

Smart city technologies are backed up by data collection and sharing, machine to machine communications, Internet of Things (IoT), and city management systems. Conventional cybersecurity issues apply to smart city technologies as well. Smart cities may be even more vulnerable to cyber attacks.

First, smart cities rely on wireless and mobile technologies for providing services. Wireless networking sets the communication infrastructure required for connecting smart objects, people, and sensors together, and allows for new capacities such as real-time monitoring and coordinating. For instance, many cities use wireless technology for their security cameras and infrastructure, rather than the hard-wired setups common in the past. This shift from wired to wireless networks makes things more cost and time effective for cities, but compared to hardware systems that were only physically accessible, remote attacks become possible on systems software controlled and remotely accessible.

Second, the information technology infrastructure of smart cities is different from other entities. A smart city ecosystem is a widely interconnected network, much bigger than any regular system of a private organization such as a business. It features complex interdependence between agencies and infrastructure, all working together to keep cities as a whole functioning properly. For example, smart payment terminals are commonly used at train stations, parking garages, etc. that process user information. They are connected to each other, run 24/7, and may