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