# An Economic Alternative to Improve Cybersecurity of E-government and Smart Cities

Zhen Li
Department of Economics and Management
Albion College
Albion, Michigan, 49224 USA
zli@albion.edu

Qi Liao
Department of Computer Science
Central Michigan University
Mount Pleasant, Michigan, 48859 USA
liao1q@cmich.edu

## ABSTRACT

While the rapid progress in smart city technologies are changing cities and the lifestyle of the people, there are increasingly enormous challenges in terms of the safety and security of smart cities. The potential vulnerabilities of e-government products and imminent attacks on smart city infrastructure and services will have catastrophic consequences on the governments and can cause substantial economic and noneconomic losses, even chaos, to the cities and their residents. This paper aims to explore alternative economic solutions ranging from incentive mechanisms to market-based solutions to motivate smart city product vendors, governments, and vulnerability researchers and finders to improve the cybersecurity of smart cities.

## CCS Concepts

**•Security and privacy → Vulnerability management; Economics of security and privacy; •Applied computing → E-government; •Theory of computation → Algorithmic game theory and mechanism design;**

## Keywords

Security and Privacy; Economics; Smart cities; E-government; Vulnerability; Game Theory

## 1. INTRODUCTION

Smart cities and e-government are spreading around the world. Communities, from small towns to metropolitan areas, are turning to the latest information and communication technologies to connect government agencies and citizens to deal with urban problems such as traffic congestion, public service shortcomings, and energy shortages, thus to improve the efficiency and effectiveness of public services. While technologies are changing cities and the lifestyle of the people, the rapid growth in smart cities and e-government is also posing enormous challenges in terms of the safety and security of smart cities, in particular cybersecurity.

Cybersecurity is about defending cyber systems against intrusion and other malicious attacks. It used to be seen as a purely technical problem. Nevertheless, as humans are players in the cybersecurity game, economic and other nontechnical factors also matter. In case of smart cities and e-government, city governments decide on what e-services to deliver to citizens, which further determines what information and communication technologies are demanded for, software developers and vendors supply the technologies, vulnerability finders explore software holes, and cyber attackers exploit vulnerabilities to hack. It is important to study the incentives and interdependence of various stakeholders' decision making, thus to design corresponding mechanisms to reduce the chance of cyber attacks on smart cities and e-government. This paper aims to propose alternative economic solutions to enhance the cybersecurity situation of smart cities and e-government by analyzing incentives, especially economic incentives, of the players' actions and interactions. Our research is motivated by the potential vulnerabilities of smart city devices and systems resulting from the inherent vulnerable characteristics of these products as well as the lack of incentives in the design and implementation of these products to improve the security level of the products.

The main contributions of the paper are as follows. First, we formally model the life cycle of vulnerability of smart city products by considering the relationship between product vendors, governments, internal vs. external vulnerability finders, and offensive vs. defensive vulnerability buyers. Second, the model is analyzed in a four-party game theoretical framework. Third, two alternative economic solutions are proposed based on economic incentives to reduce the chance of cyber attacks on smart cities and e-government. The first is carrot-and-stick-like strategies, i.e., the government either rewards vendors for security investment by paying a security premium for their products or holds vendors accountable for product vulnerabilities and punishes vendors financially for vulnerability exploitation. The second solution we propose is to encourage vendors and governments to participate in the vulnerability market and compete with malicious attackers to purchase vulnerabilities for defensive purpose.

The rest of the paper is organized as follows. Section 2 reviews the concept of smart cities and discusses their potential vulnerability to cyber attacks. An introduction to market for zero-day vulnerabilities is also included. Section 3 uses a life cycle model of vulnerability to show the relationship between smart city software vendors, smart cities,

*dg.o '16, June 08 - 10, 2016, Shanghai, China*

ISBN 978-1-4503-4339-8/16/06...$15.00

DOI: http://dx.doi.org/10.1145/2912160.2912170

external vulnerability finders, and vulnerability exploiters, and to identify key factors that determine the chance of cyber attacks on smart cities. Dual disincentives in smart city product development and implementation processes are also discussed. Section 4 proposes economic methods that can be used to improve security situation of smart city systems, including introducing financial incentive mechanisms to motivate vendors to enhance product security and to use the vulnerability market to purchase vulnerabilities by defensive buyers. Section 5 discusses related works, and finally, Section 6 concludes our work.

# 2. BACKGROUND

In this section, we first review the concept of smart cities and their key characteristics, and explore the vulnerability of smart cities to cyber attacks. We also review the concept and structure of the vulnerability market.

## 2.1 Building Smart Cities

The United Nations projected that by 2050 about 64% of the developing world and 86% of the developed world will be urbanized, adding to demands for reliable city services [1]. Conventional difficulties in urban life such as traffic congestion, waste-disposal problems, and high energy consumption are exacerbated by the increasing population density and demands of urban environments. Smart city planning is essential in managing the problems as the world's urban areas swell.

Smart initiatives are generally delivered by a range of different information-and-communication-technology-based services connected to either a web device or smart phone apps. Although cities may be at different stages of building the smart community, most cities around the world have adopted at least some technology. The growing intelligence of cities is an increasing phenomenon. [25] provided a framework to study how smart cities are being implemented. It pointed to eight "stylized facts" that underlie the facilitation of an effective smart city, including

- movement towards more interactive services engaging citizens,
- open data movement facilitates,
- diversified service development,
- accelerated adoption of technology,
- new value-added smart city services supported by advanced intelligent technology,
- smart city services combined with robust incentive systems empower engagement,
- multiple device & network accessibility,
- centralized leadership implementing a comprehensive strategy to boost smart initiatives.

Cities provide a variety of services to urban citizens. Incorporating technologies to services apparently improves the quality and efficiency of the services. Some commonly adopted technologies include smart traffic lights, smart parking, smart energy management, smart public transportation, and smart waste and water management. While smart technologies are changing the lifestyle in cities, they also make cities potential objects of cyber attacks.

## 2.2 Smart Cities are Vulnerable to Cyber Attacks

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. Nevertheless, as hardware systems that were only physically accessible are now replaced by systems remotely accessible and software controlled, remote attacks become a possibility. Second, a smart city ecosystem is a widely interconnected network, much bigger than any regular system of a private organization such as a private business. It potentially involves every individual in the city range. With such complexity and interconnection, it is hard to know the level of exposure and what is exposed. Attackers have many potential ways to interfere with the services.

Smart city devices and systems could be easily hacked. [18] found that some Econolite devices are used without any encryption for communication between traffic control systems and traffic lights, traffic controllers, etc. An adversary can control traffic infrastructure to cause disruption, degrade safety, or gain an unfair advantage. Major security weaknesses have been revealed in smart power meters [22] that could allow an attacker to order a power blackout or perform electricity usage fraud over the power line communications network.

A single bug could have drastic impact on a city running critical services on a large number of devices and systems. There have been real world examples of huge impacts software bugs could have on city services and activities, such as the shut down of San Francisco Bay Area Rapid Transit on Nov 22, 2013 [12]. Considering passengers trapped in trains, the loss is significant to the city and people involved. Just like software bugs can do big harm, vulnerabilities exploited by hackers would have similar consequences. Attacks on smart grids, public transportation, and so on could result in dramatic financial and other losses, even loss of life, to cities. In a successful attack, the loss to the victim (the city and its citizens) and the gain to the hacker can be highly asymmetric, with the loss largely exceeding the gain.

While smart cities have not yet become major targets of cyber attacks, threats are becoming real, both technically and intentionally, and large-scale attacks are not a matter of *if* but *when*. On one hand, exploitation of mobile devices are overblown (though the overall number of exploited security vulnerabilities across all mobile platforms so far is negligible) [11], and will continue to be growth areas [2]. The vulnerability discovery and exploitation focus has turned to new areas in computing like the IoT and SCADA (Supervisory Control and Data Acquisition, systems used to control different types of processes within large infrastructures such as industrial power plants). There is a recent influx in remote code execution vulnerabilities in SCADA products [6]. On the other hand, new war scenarios in the world are making smart cities attractive targets to cyber terrorists. The black market for vulnerabilities in recent years is dominated by more disciplined, organized, and structured groups that often identify specific targets [2]. Nations also state that they are already targeting governments for espionage, cyber attacks, and so on. The potential vulnerability of smart cities and e-government to cyber attacks is problematic.

Considering the significant losses cyber attacks may impose on smart cities, one may assume that governments prioritize cybersecurity when building smart cities. Nevertheless in reality, cities are implementing new technologies without first testing cybersecurity. It has been found that cities usually rigorously test devices and systems for functionality, but there is often little or no cybersecurity testing at all [12]. The governments' lack of concern of cybersecurity could turn cyber threat on smart city ecosystem from a theoretical hypothesis to unfortunate reality. In fact, disincentives are common in software development. Smart city technologies are subject to dual disincentives, as discussed in 3.3, resulting in overall negligence of cybersecurity of the products. For instance, vulnerabilities found in [18] are not a fault of any one device or design choice, but rather a systematic lack of security consciousness.

## 2.3 The Market for Vulnerabilities

Vulnerabilities are holes in computer system that can be exploited to infiltrate malware, spyware or allow unwanted access to user information. Just like other commodities, software vulnerabilities may be traded in the market place [29]. The vulnerability market consists of three categories: the white market, in which vulnerabilities are sold to software vendors or other companies that work with the vendors to rectify security flaws; the black market, where vulnerabilities are sold to criminal organizations; and the intermediate gray market [37].

The white market is regulated where the transactions are properly documented and disclosed. Vulnerability reward programs are a major part of the white market. There are third-party security organizations such as iDefense's Vulnerability Contributor Program (VCP) and HP Tipping Point's Zero Day Initiative (ZDI) that buy vulnerabilities and sell to software vendors. The black market is not regulated by any laws, and market transactions are not recorded. It has no tempt to safeguard the society, and allows any buyer such as cyber criminals and terrorists to buy vulnerabilities. The price paid is said to be five to ten times higher than other vulnerability markets [3].

On the gray market, vulnerability and exploit brokers like Vupen and ReVuln buy and sell vulnerabilities, provide a link between a vulnerability finder and a buyer, and gain revenue from charging commission of the selling price. They may sell vulnerabilities to the vendor or some government organization, depending on who is willing to pay more. They advertise that they sell knowledge of vulnerabilities for cyber espionage and in some cases for cyberweapons. ReVuln actually specializes in finding remote vulnerabilities in industrial control systems that can be used to access - or disrupt - water treatment facilities, oil and gas pipelines and power plants. Recent reports suggest that government agencies in several countries have become major players in the gray market [32, 19, 20]. Generally, buyers on the gray market are legitimate buyers but they intend to use the vulnerabilities to exploit [29]. Transactions on the gray market can be termed legitimate or improper, depending on the point of view.

# 3. MODELING SMART CITY VULNERABILITY

The discovery and disclosure of vulnerabilities are processes that are significantly impacted by the economics involved [5]. To seek for economic solutions to improve cybersecurity of smart cities, we need to study economic incentives of various stakeholders in the smart city vulnerability game. In this section, we first introduce a life cycle model of vulnerability that illustrates the relationship between major vulnerability-related events, which leads to further discussion of incentives. We then analyze how incentive mechanisms and the vulnerability market can be used to reduce the chance of cyber attacks on smart cities in Section 4.

## 3.1 The Life Cycle of Vulnerability

The life cycle of a vulnerability can be divided into phases between distinct events [16]. Figure 1 is a life cycle model tailored to smart city vulnerabilities. Four major phases are included:

- Vulnerability arises: a smart city product with potential vulnerability is released.
- Vulnerability discovered: the vulnerability may be discovered by internal researchers or external vulnerability finders.
- Vulnerability exploited: the vulnerability is disclosed or sold to offensive buyers, resulting in exploitation activities.
- Vulnerability resolved: once the vendor is aware of the vulnerability, it will be able to assess the risk and to resolve the vulnerability. This will occur if the vulnerability is found by internal researchers, if the external vulnerability finder discloses to the vendor, if the vulnerability is purchased by defensive buyers, or if the identified exploitation provides vulnerability information to the vendor.

In the parentheses of Figure 1 are the probabilities for each event to occur. For example, $p_v$ is the probability that a security vulnerability arises in a smart city product.

Internal researchers refer to those vulnerability researchers affiliated with an organization who will follow proper disclosure policies and procedures to release the vulnerability information to the vendor. External vulnerability finders are freelance researchers who are free to dispose their vulnerability findings. A large percentage of vulnerabilities are found by external finders [3].

After a vulnerability is discovered by external vulnerability finders, they have several options [16]:

- Do nothing.
- Provide full disclosure of vulnerability information to all affected parties, including potential attackers.
- Privately disclose the finding to the product vendor or to a vulnerability program coordinator before disclosing detailed information to the public.
- Sell the information.

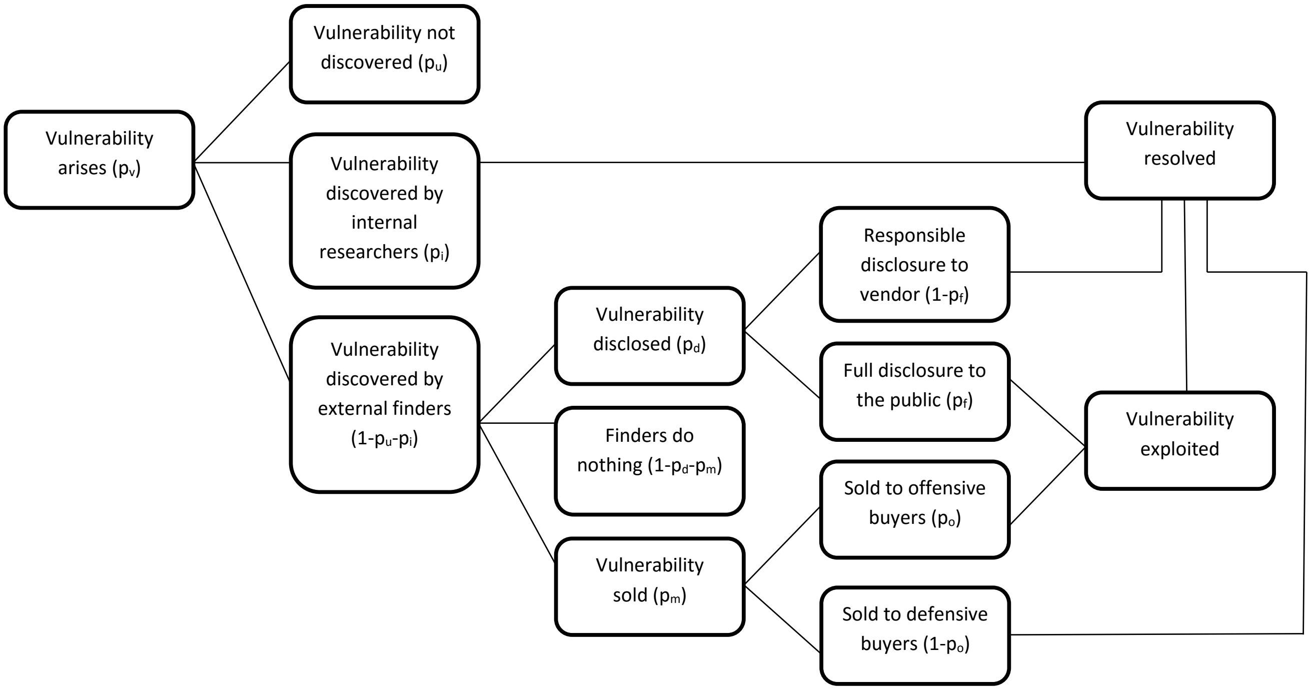
Vulnerability arises (pv)
Vulnerability not discovered (pu)
Vulnerability discovered by internal researchers (pi)
Vulnerability discovered by external finders (1-pu-pi)
Vulnerability disclosed (pd)
Finders do nothing (1-pd-pm)
Vulnerability sold (pm)
Responsible disclosure to vendor (1-pf)
Full disclosure to the public (pf)
Sold to offensive buyers (po)
Sold to defensive buyers (1-po)
Vulnerability resolved
Vulnerability exploited

**Figure 1: Phases during the life cycle of vulnerability and the causal relationship of events.**

The individuals who find vulnerabilities and those who exploit them are assumed to be two separate groups as attackers largely do not find vulnerabilities independently [35]. Finding vulnerabilities is not an illegal activity, whereas exploiting vulnerabilities generally is. External vulnerability finders represent a critical sources of security risk, should they choose to sell the vulnerability to malicious vulnerability exploiters.

Money and reputation are often the top two concerns for vulnerability finders when they consider the disposal of their findings. Finders may seek to preserve the right to their claim of findings. For example, a higher vulnerability discovery rate is observed during the mid-year months for Microsoft products, which can be explained by the coinciding date of a major conference in which security experts present their vulnerability findings [23]. Reputation and credit is an advantage a finder may choose the vendor over a black market buyer. For those who desire recognition more than money, they may choose to disclose vulnerabilities. The option is between reporting the finding to the vendor or posting the information publicly. Both are for free so which type of disclosure a finder would choose is more of ethical concerns. But full disclosure is problematic. The majority of vulnerabilities are exploited shortly after they are made publicly known [11], hence the probability of exploitation after full disclosure is high. For simplicity, we assume that full disclosure will for sure lead to vulnerability exploitation so that in Figure 1, exploitation occurs in case of full disclosure or in case of vulnerability sold to offensive buyers. The total probability of vulnerability exploitation is given by

$$p_v \times (1 - p_u - p_i) \times \{p_d \times p_f + p_m \times p_o\} \tag{1}$$

The chance of cyber attack on smart cities can be reduced if one or more of the following happens, i.e., 1. $p_v$ decreases, 2. $p_u$ increases, 3. $p_i$ increases, 4. $p_d$ decreases, 5. $p_f$ decreases, 6. $p_m$ decreases, 7. $p_o$ decreases.

Before the vulnerability market matured, it was not unusual for finders to pass the vulnerability to the vendor. It has been found that more finders have turned to vulnerability markets to sell the findings [6, 26, 32]. For example, a study [3] surveyed some top vulnerability finders, many of whom acknowledge the significance of the gray and black markets in vulnerabilities. In the life cycle model, this is translated to a rather low value of $p_d$ and high value of $p_m$. It is thus reasonable to argue that external vulnerability finders are largely money driven nowadays, hence $p_d \to 0$ and $p_m \to 1$. Equation (1) is simplified to

$$p_v \times (1 - p_u - p_i) \times p_o \tag{2}$$

## 3.2 Game Theoretical Analysis

In our game setup, we consider four economic agents involved in the life cycle of a smart city vulnerability: the software vendor that produces and sells the smart city product, the external vulnerability finder who discovers vulnerabilities in the product, the city that is the user of the product and the victim of vulnerability exploitation, and the malicious attacker who exploits the vulnerability to hack the product. By studying the interactions among these players, we consider how the vendor and city's choices affect the way the finder chooses the disposal of the vulnerability and the expected payoff of the attacker.

Of the four parties in the game, the finder is on the supply side of the vulnerability market, and the other three are all on the demand side. The finder has the power to choose to whom to sell, while the demand side is highly competitive. If the finder sold for price difference only, the vulnerability would be sold to the buyer who is willing to pay the most.

In an ideal situation, the finder shall seek no reward and submit the vulnerability to a responsible disclosure mechanism. This would be the case for those finders for whom getting recognition is sufficient compensation. Nevertheless, this is not enough for many finders since vulnerabilities can have significant economic values. We assume the finder is money driven who desires immediate economic payoffs. Although the fame received from responsible disclosure may eventually translate into economic opportunities, it is not as attractive as present financial gains, i.e., $p_d = 0$. This is equivalent to a single stage game setting which eliminates also the finder's incentive to hold onto the discovery in seek of higher expected returns in future stages. Thus, the money-driven finder will choose to sell the vulnerability for sure, i.e., $p_m = 1$. That is, the probability of vulnerability exploitation is as given in Equation (2).

The expected payoff from vulnerability exploitation to the attacker is

$$\{p_v \times (1 - p_u - p_i) \times p_o\} \times V \tag{3}$$

Given the value of exploitation to the attacker (denoted by $V$), the expected payoff to the attacker decreases as the exploitation probability decreases. To effectively defend smart cities against cyber attacks, economic solutions have to focus on reducing this probability because $V$ is largely composed of noneconomic (e.g., political, military) factors in case of hacking smart cities.

The probability of vulnerability exploitation of a smart city product depends on four probabilities: the probability for vulnerability to arise in a smart city product ($p_v$), the probability the vulnerability is not discovered ($p_u$), the probability the vulnerability is discovered by internal researchers ($p_i$), and the probability the vulnerability is sold to offensive buyers ($p_o$). Of the four, $p_v$ and $p_u$ depend on inherent quality of the product, directly related to vendor's investment in security during product development process. $p_i$ depends on vendor's followup investment in security researchers after a product is released. They are all at the direct control of the vendor related to the vendor's security investment strategy in product design and maintenance. The last probability $p_o$ is a control variable for the vulnerability finder, but it can be affected by the vendor and the city's decision regarding their willingness to pay for vulnerability: the more are defensive buyers willing to pay, the more likely for the finder to sell to defensive buyers, thus less likely to sell to offensive buyers. In other words, $p_o$ depends on the vulnerability reward programs of the vendor, whether they exist and how the rewards are designed. It depends also on the way defensive buyers participate in the vulnerability market.

Economic mechanisms can be developed to motivate the vendor to increase investment in security and to encourage market participation by defensive buyers.

## 3.3 The Exploration of Incentives

### 3.3.1 Functionality vs. Security

Smart software vendors provide technological products to governments to support smart city services. The quality of a product involves two major aspects, its functionality to provide reliable services and its resistance to cyber attacks. It is not unusual for vendors to place functionality over security. One possible reason is inherent to software development nature. [21] defined two types of vulnerabilities, functional vulnerability (from the weaknesses in software products' functionality such as data processing or time and state management) and management vulnerability (from the improper management of the codes or the security features). It was found that most vulnerabilities are functional in early stages of product development, management functionalities then start to appear, and eventually become the mainstream. It is therefore reasonable to assume that the vulnerability market starts with a focus on functional vulnerabilities before it transfers from functional to management vulnerabilities. It follows that functionality may be the prior concern than security in early stages of new product development. But as the dominant type of vulnerabilities transfers from the functional to the management, vendors are supposed to enhance the security features of their products such as permissions, privileges, and access control.

### 3.3.2 City Managers' Disincentives

Politicians' goal can be political success rather than social welfare. They are often criticized as making myopic decisions such as the accumulation of government debt [14] and under-investment in areas with long-term returns like basic research and environmental protection [27]. Economists have long been intrigued by the idea that elections may induce a short-term bias [31]. In our setting, city managers' myopia arises from the desire to improve performance of current term while neglecting the potential costs of future outcomes in order to win reelection. Normally, politicians receiving the largest number of votes win elections. Building smart cities can affect the votes in two opposite ways. On one hand, smart city products improve the quality of life that benefits citizens, which will gain votes. On the other hand, exploitation of smart city vulnerabilities would harm citizens and lose votes, had exploitation occurred.

Compared to functionality of smart city products, city managers are lack of security consciousness. This is a combination of the nature of political accountability and the uncertain and contingent nature of vulnerability exploitation. Political accountability often acts in a post hoc, retrospective manner. Who would be held accountable for the failure of the smart city system when it happened under a different city administration from the one that adopted the system? With the lagging nature of political accountability, the metrics of success and the accountability for failure are diffuse. Elected officials are in for their terms of service. Considering the uncertainty of vulnerability exploitation of smart cities, government leaders serving only for certain terms may not be concerned with future security. Thus, city managers have strong incentives to build smart cities, which helps build service records during the present term and increases the chance of winning reelection, with little concerns of future cyber security.

### 3.3.3 Vendors' Disincentives

Vendors tend to be averse to making security investments against events that have never occurred, even if they might worry about them. Many firms are reactive in their investments, responding to actual vulnerabilities. They are not managing risk, but closing known vulnerabilities [13]. The city's lack of security conscientiousness further disincentives vendors to invest in security.

Consider the functionality and security features of a smart city product. Suppose the product would function well in absence of attacks. Microeconomic principle says that the price sellers may charge depends on buyers' willingness to pay, which further depends on the value of the product to buyers. Thus, what price the vendor can charge the city depends on the city's valuation of the product. If the city has no concern over security, the city would place no value of security on the product so that the price of the product would merely depend on its functionality. Since the vendor would receive no financial gains from investing in security, the optimal strategy would be to waste no money on security.

Similarly, the vendor would also lack incentives to purchase vulnerabilities from the market. When a system is compromised, the vendor is normally not held financially liable for users' losses. Lack of legal liability protects the vendors from incurring significant costs in the event of a vulnerability exploitation [36]. The missing obligation of the vendor means that the risk of being attacked is taken by the city and its citizens, not by the vendor. The vendor hence may be lack of incentives to buy vulnerabilities. Different from vulnerabilities that threat vendors directly, vendors have limited incentives to dedicate resources to purchase vulnerabilities found in their smart city technologies as the attack will not cause much direct financial loss to the vendor other than burdens to patch. Actually, it has been found that vendor liability for patching costs can be more effective than vendor liability for damages [9].

# 4. ECONOMIC SOLUTIONS TO ENHANCE SMART CITY CYBERSECURITY

In this section, we will discuss two economic methods that can be used to reduce the chance of smart city cyber attacks: to introduce incentive mechanisms to motivate vendors to improve product security (to lower $p_v$, and raise $p_u$ and $p_i$), and to take advantage of the vulnerability market to acquire vulnerabilities from external finders (to lower $p_o$).

## 4.1 Correcting Vendor's Disincentives

Consider functionality and security of a smart city product. Let $P$ be the price of the product. If the city values both functionality and security, then the price of the product depends on both of the product features, i.e., $P = P(f, s)$, where $f$ measures the level of functionality, and $s$ measures the level of security. The cost structure of the vendor depends on its investment in functionality and security of the product, denoted by $C = C(f, s)$. The total cost is increasing in the level of functionality and security of the product.

If the vendor does not gain from increased security (by selling products at a higher price), or does not suffer from a product failure (facing no financial punishment), the profit-maximizing strategy for the vendor is to minimize expenditure on security (i.e., $s = 0$). Vendor's profit from supplying smart city products to the city is $\pi = P(f) - C(f)$.

When security does not appear in the profit function of the vendor, to maximize profit, the vendor chooses the optimal level of functionality $f^*$ that satisfies $P'(f) = C'(f)$. The maximum profit gained by the vendor is

$$\pi^*_{s=0} = P(f^*) - C(f^*) \tag{4}$$

To correct for the lack of security concern by the vendor, either value of security has to be attached to the price of the product or the vendor must be held financially responsible for loss from product failure. The former requires the government to be willing to pay not only for functionality of a product, but also its security. The latter requires some punishment mechanism to force the vendor be at stake when an attack occurs.

### 4.1.1 Rewarding Vendor for Security Enhancement

One way to provide financial incentives for the vendor to invest in security is to reward the vendor for improved security by offering a higher price for its smart city product. When security enters both the revenue and the cost side of the vendor's choice, the profit function becomes $\pi = P(f, s) - C(f, s)$. The vendor now has two decision variables, functionality and security. The vendor chooses the optimal strategy $\{f^*, s^*\}$ that satisfies $P_f(f, s) = C_f(f, s)$ and $P_s(f, s) = C_s(f, s)$. The optimal profit accordingly is

$$\pi^*_{s=s^*} = P(f^*, s^*) - C(f^*, s^*) \tag{5}$$

If functionality and security of the product are independent, then the level of optimal functionality shall be the same in Equations (4) and (5), and the profit-maximizing level of security chosen by the vendor satisfies $P'(s) = C'(s)$. Given the cost structure of the vendor, it is the security premium (the increase in product price due to enhanced security) the city is willing to pay that determines the product's security level. As the security premium increases, security of the product increases. As long as $\pi^*_{s=s^*} > \pi^*_{s=0}$, the vendor would choose to invest in security to reach the optimal security level $s^* > 0$.

A couple of prerequisites for this solution to work:

- The city needs to test for security (not merely functionality) of the product to determine its security level.
- The pricing function needs to be linked to security.

The challenge of this approach lies in the difficulty of measuring security [33], thus it may not be easy to effectively place a premium on more secure software. Nevertheless, what is actually required on the city side is to signal vendors that they will be rewarded for security. Once this becomes a general practice, the supply-and-demand forces in the market for smart city products will set the equilibrium security premium function for calculating total security premium at various levels of security. The city can induce the desirable level of security from the vendor by adjusting the total security premium payment. The more is the city willing to pay, the more secure the product will be.

### 4.1.2 Punishing Vendor For Vulnerability Exploitation

No product is perfectly secure. There is always a chance for the product to be hacked even if $C(s) = \infty$. Suppose the product is hacked in the $t^{th}$ year from its release that causes a loss of $M_t$, the present value of the loss is $\frac{M_t}{(1+i)^t}$, where $i$ is the discount rate, such as applicable market interest rate, used to convert a future loss to the present (the selling date of the product), and $\frac{1}{(1+i)^t}$ is the discount factor. The expected loss of exploitation valued in today's dollar (denoted by $L$) is the weighted average of present values of the exploitation losses occurring during the lifespan of the product ($n$ years). The weights are the discount factors. That is,

$$L(s, M) = \sum_{t=0}^{n} \{p_v \times (1 - p_u - p_i) \times p_o\} \times \frac{M_t}{(1+i)^t} \quad (6)$$

where $\{p_v \times (1-p_u-p_i) \times p_o\} \times \frac{M_t}{(1+i)^t}$ is the present value of the expected loss of exploitation occurring $t$ years from today. For simplicity, the probability of attack is held constant over time.

The expected loss depends on the probability of vulnerability exploitation and the actual loss occurred. It is decreasing in exploitation probability and increasing in the size of loss, i.e., $L_s(s, M) < 0$ and $L_M(s, M) > 0$. If the loss to the city were to be covered by the vendor, this would be contingent cost to the vendor in addition to its existing cost of production.

At presence of the contingent financial punishment, the objective function of the vendor becomes

$$\pi = P(f) - C(f, s) - L(s, M) \quad (7)$$

The $M$ component of the contingent cost function is assumed exogenous to the vendor. What the vendor controls is the level of security that affects the likelihood of vulnerability exploitation.

The profit-maximizing security level (denoted by $s^*_{contingent}$) solving the first-order condition of Equation (7) satisfies

$$C_s(f, s) + L_s(s, M) = 0 \quad (8)$$

The maximized profit can be positive and negative. Considering the significant damage cyber attacks may impose on the city, the maximized profit is highly likely to be negative. Since the vendor would not be willing to supply a product with negative expected payoff, the actual financial liability of the vendor cannot exceed $\pi^*_{s=0}$. The proposed punishment mechanism has more signaling effect to motivate the vendor to invest in security ex ante rather than to punish the vendor ex post.

Similar as in 4.1.1, the city has the power to induce desired level of security by choosing the financial liability of the vendor $(L(s, M))$ in the range of $[0, \pi^*_{s=0}]$. In response, the vendor will choose the optimal security level $s^*_{contingent}$ satisfying (8).

There can be variations of the financial punishment mechanism, such as to attach a termination date, equivalent to the term of warranty. Practice can be of different ways. What is essential is to have the vendor share vulnerability risks with the city without eliminating the vendor's incentive to supply the smart city product.

Indeed, such contingent financial punishment may motivate the vendor to create a bug bounty program. The vendor's willingness to pay to the vulnerability finder depends on the expected penalty. The vendor will be better off if the vulnerability reward paid to the finder is less than the expected penalty. The maximum possible reward the vendor is willing to pay is also capped by $\pi^*_{s=0}$.

## 4.2 The Use of Vulnerability Market

The vulnerability finder seeking to sell the vulnerability discovery may share it with responsible disclosure programs and get the reward, sell on the black market but facing potential criminal prosecution, or arrange a deal through an exploit broker. Ultimate buyers of the exploit information can be defensive or offensive. Defensive buyers intend to defend the product against cyber attack. They will use the purchased vulnerability information to patch the product and make it securer. Offensive buyers intend to use the vulnerability to exploit. In the context, we call the vendor and the city defensive buyers, and malicious attackers offensive buyers. To improve smart city cybersecurity, we propose active market participation by defensive buyers, especially by governments so that to reduce the chance vulnerability information is purchased by offensive buyers.

There are several reasons why it is better to sell vulnerabilities to vendors, including the decreased risk of getting ripped off, and the possibility of future job offers. Finders receive also recognition. Currently, there are only a few vulnerability reward programs, most of which were created a few years ago [3]. The programs deserve further development. Recent research has found such programs to be economically efficient, comparing favorably to the cost of hiring full-time security researchers to locate bugs internally [15].

Vendors' reward programs are a good option for finders to sell in an easy and legitimate way, but they do not offer anywhere near the prices offered in the underground market. When a government agency is a buyer, nevertheless, the money it can bring to the market may be unable for other buyers to match. A case study in [29] described the profitable alternatives for finders: instead of selling for a few thousand dollars to programs like the ZDI, they can sell to government agencies for more money.

The government can be highly competitive in the market. The government's willingness to pay for a vulnerability is capped by the actual loss to the city if the vulnerability is exploited $(M)$. As $\pi^*_{s=0} \ll M$ is normally the case, the city's economic interest in participating the vulnerability market largely exceeds the vendor. The government may pay much more to the finder compared to the vendor, thus largely increasing the chance for the vulnerability to fall in the hands of defensive buyers.

Governments around the world are already buying vulnerabilities on the market, normally for offensive purpose. We argue that government agencies with defensive purpose, such as smart city governments, shall also participate in the vulnerability market to compete with malicious buyers. Considering the features of smart city vulnerabilities: absence of direct monetary return to hackers and the inequality between the loss to the city and the gain to the hacker, having governments join the buying side of smart city vulnerabilities can be an effective way to prevent attacks on smart cities.

While the vulnerability market has developed, vulnerability commercialization remains a controversial issue. One controversy is about the buyers' intents. The issue could be less controversial if more vulnerabilities were purchased for defensive purpose.

## 4.3 Further Discussion

As discussed in previous sections, our proposed economic alternatives to improve smart city cybersecurity include creating financial mechanisms to motivate the vendor to invest in security, and to encourage the vendor and the government to actively participate in the vulnerability market. The key difference among the proposals is the split of financial responsibility between the city and the vendor. In cases of rewarding the vendor for improved security and having the city purchase the vulnerability, the city picks up the tab;

in cases of punishing the vendor for vulnerability exploitation and having the vendor pay for vulnerability purchased, it is the vendor that pays the bill. Nevertheless, economic theories tell us that essentially, the vendor (as the seller of the product) and the city (as the buyer of the product) will share the financial burden of vulnerability. In which way the burden is shared depends on market forces of supply of and demand for smart city products.

How to minimize the cost of participating in the vulnerability market? As vulnerability finders are seeking profitable alternatives, mechanisms need to be developed to make it more likely for finders to sell to defensive buyers and reduce trading with malicious buyers. In the vulnerability market, defensive buyers would face competition from offensive buyers. Sales in the three categories of the vulnerability market increase competition. For instance, the gray market has driven competition in the white market: white market prices typically vary from $\$500$ to $\$5,000$, while gray market prices may start at $\$20,000$ [26]. Although prices are typically higher in the gray and black markets, vulnerability finders that sell to the white market are getting the vulnerability fixed. In the game theoretical analysis, we consider only the financial factor in the finder's decision about the disposal of the vulnerability discovery. Yet, if other factors such as ethical and legal are taken into account, selling to defensive buyers will become more attractive. Moral, legal and other methods may be used in combination with economic tools. For instance, cities may request that security researchers accept lower compensation with the assurance that the vulnerability information will be used for benevolent purpose.

A formal test of the model's predictions and policy recommendations goes beyond the scope of this paper. It will be worthwhile to further develop the topic with empirical analysis based on real data.

## 5. RELATED WORK

Smart urban services depend on mobile communications. Researchers have found that mobile ecosystem carries potential vulnerabilities that may be exploited to undermine the system. The increasing potential benefit from the vulnerability exploitation in the mobile system has attracted significant attention from the black market [3]. While Android continuously increases its popularity in the mobile ecosystem, compared to other vulnerabilities, the vulnerabilities in the Android market are more exploitable with a substantially higher percentage of high risk vulnerabilities and worse impact of the vulnerability exploitation, possibly due to the fast growing number of apps [21]. A study of Android apps found substantial software reuse, and the quality of the apps and libraries reused determines the quality of Android apps [30].

Software vulnerabilities are inevitable. There has been active research around vulnerability disclosure. While disclosure is found to force vendors to release patches [8], it may also affect the volume of attacks [7]. Market-based mechanisms of vulnerability disclosure can be effective to restrict the diffusion of vulnerability exploitation, to reduce the risk of exploitation, and to decrease the volume of exploitation attempts [34].

Security is essential to the success of e-government because it determines users' incentive to use e-government services [4]. To protect smart cities against vulnerability exploitation, usual cybersecurity technologies and best practices are necessary to protect smart city devices and systems. Studying the life cycle of vulnerabilities can help vendors reduce potential vulnerabilities during the software development process [10]. Nevertheless, 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. Owing to the rapid increase of sophisticated cyber threats with potentially large destructive effects on smart cities, economic, political, and other non-technical incentives are increasingly perceived as the primary reasons for today's increased risk exposure, and non-technical approaches have been explored to manage security vulnerability issues. In [24], researchers proposed two systems that aim at improving cybersecurity education: the taxonomy serving as a collection of cybersecurity topics that provides links to relevant educational or research material; the personal cybersecurity assistant portal serving as a platform for users to discuss the security of web sites. The sources can be linked together, helping to strengthen the knowledge of government officials and citizens with regard to cybersecurity issues.

Economics-based solutions have also been analyzed. There have been empirical studies on vulnerability reward programs. [28] presented Google's experience with its vulnerability reward programs. [15] studied two vulnerability reward programs by competing browser vendors, Google Chrome and Mozilla Firefox. Both studies found that the reward programs are economically beneficial to vendors. 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 [17].

To the best of our knowledge, this paper is the first systematic study of the economics of the life cycle of vulnerability, and the guiding principles of the design of economic mechanisms to improve smart city cybersecurity.

## 6. CONCLUSION

Along with the fast growth and applications of smart city technologies is the increasing concerns on the cybersecurity of smart cities. What is essential to the success of smart city efforts is the reliability and security of smart city products. Compared to functionality of these products, their security quality is often neglected. Intuitively, any technological products would be more secure if they are produced with higher level of security, or found vulnerabilities are patched by vendors before the information is exploited by attackers. This paper reviewed key characteristics of smart city technologies and vulnerability exploits. By formally modeling the life cycle of vulnerabilities and the determining factors of cyber attacks, we discussed alternative economic mechanisms to make smart cities cyber securer based on the analysis of motives and the likelihood of vulnerability exploitation, including the motivation of software vendors, governments, and vulnerability finders. The proposed creation of financial incentives for vendors to invest in security and the usage of the vulnerability market to purchase vulnerabilities by defensive buyers can reduce the likelihood of malicious cyber attacks and increase cybersecurity of e-government and smart cities.

# 7. REFERENCES

[1] Open-air computers. *The Economist*, October 27 2012.

[2] L. Ablon, M. C. Libicki, and A. A. Golay. Markets for cybercrime tools and stolen data: Hackers' bazaar. *RAND Corporation research report*, 2014.

[3] A. M. Algarni and Y. K. Malaiya. Software vulnerability markets: Discoverers and buyers. *International Journal of Computer, Information Science and Engineering*, 8(3):71–81, 2014.

[4] Y. A. Alsultanny. Evaluating users intention to use e-government services. *International Journal of Emerging Trends & Technology in Computer Science*, 3(5):55–60, September-October 2014.

[5] R. Anderson and T. Moore. The economics of information security: A survey and open questions. *Science*, 314:610–613, 2006.

[6] S. Anthony. The first rule of zero-days is no one talks about zero-days (so we'll explain). *Ars Technica*, October 20 2015.

[7] A. Arora, A. Nandkumar, and R. Telang. Does information security attack frequency increase with vulnerability disclosure: An empircal analysis. *Information Systems Frontiers*, 8(5):350–362, 2006.

[8] A. Arora, R. Telang, and H. Xu. Optimal policy for software vulnerability disclosure. *Management Science*, 54(4):642–656, 2008.

[9] T. August and T. I. Tunca. Who should be responsible for software security? a comparative analysis of liability policies in network environments. *Management Science*, 57(5):934–959, 2011.

[10] L. Bilge and T. Dumitras. Before we knew it: an empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 833–844, Raleigh, NC, October 16-18 2012.

[11] J. Brumfield. Verizon 2015 data breach investigations report. April 13 2015.

[12] C. Cerrudo. An emerging US (and world) threat: Cities wide open to cyber attacks. *IOActive White Paper*, 2015.

[13] S. Dynes, E. Goetz, and M. Freeman. Cyber security: Are economic incentives adequate? *IFIP International Federation for Information Processing*, 253:15–27, 2008.

[14] M. Eslava. The political economy of fiscal deficits: A survey. *Journal of Economic Surveys*, 25(4):645–673, 2011.

[15] M. Finifter, D. Akhawe, and D. Wagner. An empirical study of vulnerability reward programs. In *Proceedings of the 22nd USENIX conference on Security*, pages 273–288, Washington, D.C., August 14-16 2013.

[16] S. Frei. The known unknowns: Empirical analyais of publicly unknown security vulnerabilities. *NSS Labs*, December 2013.

[17] S. Frei and F. Artes. International vulnerability purchase program: Why buying all vulnerabilities above black market prices is economically sound. *NSS Labs*, December 2013.

[18] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman. Green lights forever: Analyzing the security of traffic infrastructure. In *WOOT'14 Proceedings of the 8th USENIX conference on Offensive Technologies*, pages 7–7, San Diego, CA, August 19 2014.

[19] A. Greenberg. Meet the hackers who sell spies the tools to crack your PC (and get paid six-figure fees). *Forbes*, March 21 2012.

[20] A. Greenberg. Shopping for zero-days: A price list for hackers' secret software exploits. *Forbes*, March 23 2012.

[21] K. Huang, J. Zhang, W. Tan, and Z. Feng. An empirical analysis of contemporary android mobile vulnerability market. In *Proceedings of the 2015 IEEE International Conference on Mobile Services (MS)*, pages 182–189, New York, NY, June 27-July 2 2015.

[22] A. G. Illera and J. V. Vidal. Lights off! The darkness of the smart meters. *Black-hat Europe*, October 14-17 2014.

[23] H. Joh and Y. Malaiya. Seasonal variation in the vulnerability discovery process. In *Proceedings of ICST '09, International Conference on Software Testing Verification and Validation*, pages 191–200, Denver, CO, April 1-4 2009.

[24] D. Klaper and E. Hovy. A taxonomy and a knowledge portal for cybersecurity. In *Proceedings of the 15th Annual International Conference on Digital Government Research*, pages 79–85, 2014.

[25] J. H. Lee, M. G. Hancock, and M.-C. Hu. Towards an effective framework for building smart cities: Lessons from Seoul and San Francisco. *Technological Forecasting and Social Change*, 89:80–99, November 2014.

[26] R. Lemos. Private market growing for zero-day exploits and vulnerabilities. *TechTarget*, November 2012.

[27] R. M. Margolis and D. M. Kammen. Evidence of under-investment in energy R&D in the United States and the impact of federal policy. *Energy Policy*, 27:575–584, 1999.

[28] A. Mein and C. Evans. Dosh4Vulns: Google's vulnerability reward programs. March, 2011.

[29] C. Miller. The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales. In *Proceedings of the Sixth Workshop on the Economics of Information Security*, Pittsburgh, PA, June 2007.

[30] I. J. Mojica, B. Adams, M. Nagappan, S. Dienst, T. Berger, and A. E. Hassan. A large-scale empirical study on software reuse in mobile apps. *IEEE Software*, 31:78–86, 2014.

[31] W. D. Nordhaus. The political business cycle. *Review of Economic Studies*, 42(2):169–190, April 1975.

[32] N. Perlroth and D. E. Sanger. Nations buying as hackers sell flaws in computer code. *The New York Times*, July 13 2013.

[33] S. Pfleeger and R. Cunningham. Why measuring security is hard. *IEEE Security & Privacy*, 8(4):46–54, July/August 2010.

[34] S. Ransbotham, S. Mitra, and J. Ramsey. Are markets for vulnerabilities effective? *MIS Quarterly*, 36(1):43–64, March, 2012.

[35] M. J. Schwartz. So you want to be a zero day exploit millionaire? *InformationWeek*, November 10 2011.

[36] M. D. Scott. Tort liability for vendors of insecure

software: Has the time finally come? *Maryland Law Review*, 67(2):425–484, 2008.

[37] P. N. Stockton and M. Golabek-Goldman. Curbing the market for cyber weapons. *Yale Law & Policy Review*, 32:101–128, December 18 2013.