European Commission

TRIMIS
TRANSPORT RESEARCH AND INNOVATION MONITORING AND INFORMATION SYSTEM

D I G E S T

Issue 3
April 2018

Subscribe to Free Bi-monthly Research Alerts

Source: Li, Z. and Liao, Q. (2018)
Economic solutions to improve cybersecurity of government and smart cities via vulnerability markets.
DoI: 10.1016/j.giq.2017.10.006
Available Here.

The contents and views included in the TRIMIS research digest do not necessarily reflect the position of the European Commission.

Read more about TRIMIS at:
https://trimis.ec.europa.eu

Improving the cybersecurity of smart cities

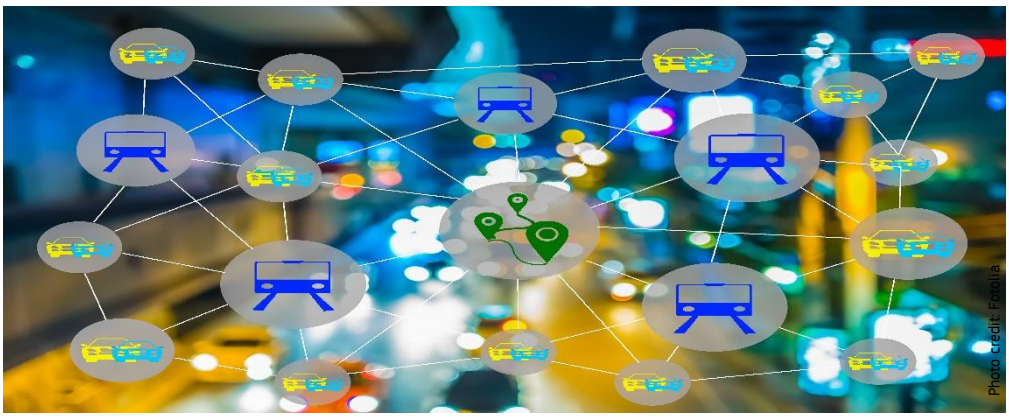


Photo credit: Fotolia

Smart city technologies are changing the lifestyle of people but also creating huge opportunities for cyber attacks. The potential vulnerabilities of smart city products and imminent attack of smart city infrastructure and services will have significant consequences and substantial economic losses. A study examines the economic solutions to improve cyber security of smart cities.

Cities are getting smarter and 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 brings together various information and communication technologies and solutions.

However, the rapid growth of smart cities poses enormous safety and security challenges. One specific concern is the safety of smart city products. The potential vulnerabilities of smart city devices and systems are due to inherent vulnerabilities of these products and the lack of incentives in the design and implementation of security features. As smart city infrastructure outpaces cybersecurity solutions, smart software devices, and systems are vulnerable to intrusions and malicious cyber attacks. Cybersecurity protects availability, integrity and ability, as well as confidentiality requires to support smart environments.

Smart city technologies involve data collection and sharing, machine to machine communications, Internet of Things (IoT), and city management systems. The smart city and smart mobility relies on wireless and mobile technologies for providing services. Wireless networks set the communication infrastructure required for smart objects, people and sensors, and allow real time monitoring and coordination. 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 many have access to other local area networks. Attackers have the potential to interfere and disrupt connected services.

Continued/...

TRIMIS
TRANSPORT RESEARCH AND INNOVATION MONITORING AND INFORMATION SYSTEM
DIGEST

TRIMIS

The Transport and Research and Innovation Monitoring and Information System (TRIMIS) supports the implementation and monitoring of the Strategic Transport Research and Innovation Agenda (STRIA) and its seven roadmaps.

TRIMIS is an open-access information system to map and analyse technology trends, research and innovation capacities, as well as monitor progress in all transport sectors.

TRIMIS is developed and managed by the Joint Research Centre on behalf of the European Commission.

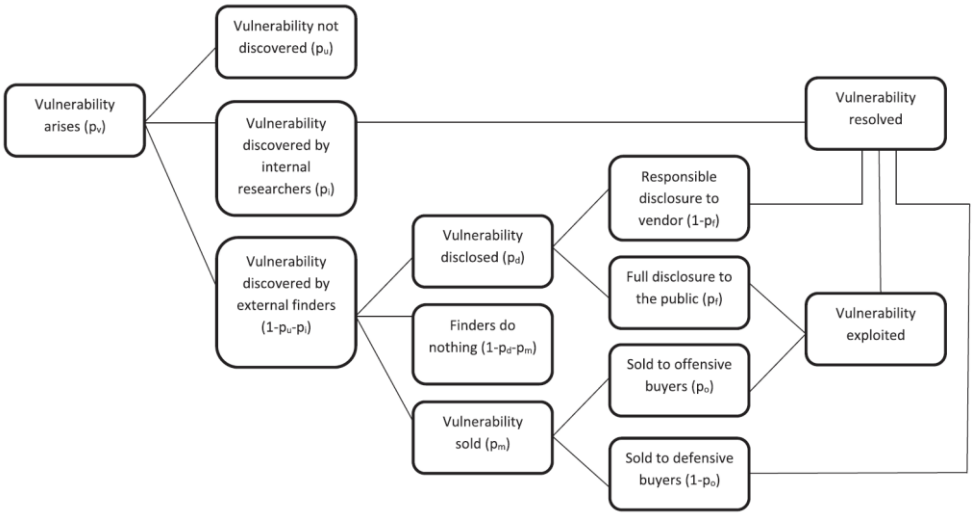
Contact:
European Commission
Joint Research Centre, Ispra, Italy
Email: *EU-TRIMIS@ec.europa.eu*

Improving the cybersecurity of smart cities

While smart cities have not yet become major targets of cyber attacks, threats are becoming real, both technically and intentionally. Large-scale attacks are not a matter of *if* but *when*. Disincentives are common in software development resulting in overall negligence of cybersecurity in smart city products.

Smart technologies are tested for functionality, resistance to weather conditions, etc. but not for cybersecurity. Some vulnerabilities found in smart products are due to a systematic lack of security consciousness.

The discovery and disclosures of vulnerabilities are processes that are significantly impacted by economics. To seek economic solutions to improve cybersecurity of smart cities, it is necessary to understand economic incentives of various smart city stakeholders A lifecycle of vulnerability can be outlined (see Figure below).



Phases during the life cycle of vulnerability and the casual relationship of events

The study provides a theoretical framework of incentive structures that policymakers may consider in security policy design. It explored working economic solutions to make smart cities securer. By modelling the life cycle of vulnerabilities the study identified key factors determining the probability of cyber attacks.

Based on the analysis of probability and incentives, it proposed two alternative economic solutions that government could use to address cybersecurity challenges facing smart cities. These are the creation of incentive mechanisms for vendors to invest in security and the usage of a vulnerability market for defensive buyers. It also requires a shared financial burden between the government and the vendor.

These solutions can be integrated into policy instruments in defending smart cities against cyber attacks.