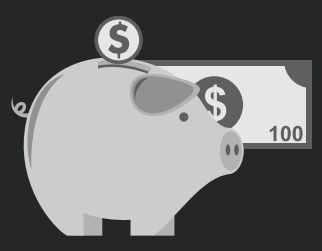
IOActive | Smart Cities Cyber Security Worries

SMART CITY TECHNOLOGIES

According to some estimates, by 2020 the potential market for smart cities could be more than

ONE trillion dollars



SMART TRAFFIC CONTROL
No encrypted communications allows attackers to manipulate traffic lights.

SMART PARKING
Inform available parking in advance

SMART STREET LIGHTING
Attackers can compromise all street lights in a city and turn them on and off at wil

SMART PUBLIC TRANSPORTATION
Real time data about schedules and mobile payments

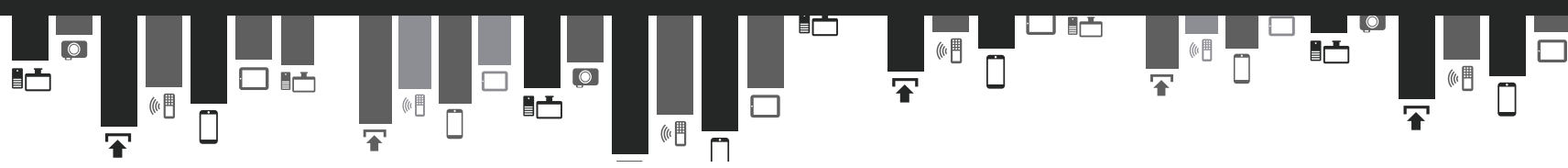
SMART ENERGY MANAGEMENT
Smart grid delivers energy based on needs

SMART WATER MANAGEMENT
Smart pipes for water quality measurement and leak detection

SMART WASTE MANAGEMENT
Sensors detect volume of garbage and smell in containers

SECURITY
Traffic and surveillance cameras, gunshot detection sensors

CYBER SECURITY PROBLEMS



1 LACK OF CYBER SECURITY TESTING
Most cities around the world are implementing new technologies without first testing cyber security.

2 POOR OR NONEXISTENT SECURITY
No basic security practices present on city technology development.

3 ENCRYPTION ISSUES
Most technologies are wireless which are easier to hack if communication is not properly encrypted.

4 LACK OF COMPUTER EMERGENCY RESPONSE TEAMS
Cities don't have Computer Emergency Response Teams to help coordinate security incidents response.

5 LARGE AND COMPLEX ATTACK SURFACE
With so much complexity and interdependency, it is difficult to know what and how everything is exposed.

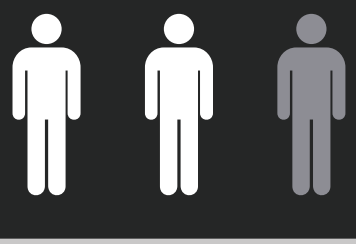
6 PATCH DEPLOYMENT ISSUES
It is common for cities to use vulnerable technology because vendors are slow to release security patches or patches are not applied.

7 INSECURE LEGACY SYSTEMS
Vulnerable and older systems are used, this adds complexity and increases the attack surface.

8 PUBLIC SECTOR ISSUES
Cities have inadequate budgets, training, and resources and on top of that there is bureaucracy.

9 LACK OF CYBER ATTACK EMERGENCY PLANS
Cities are not prepared against possible cyber attacks.

10 SUSCEPTIBILITY TO DENIAL OF SERVICE
With so many city services dependent on technology, attackers have many methods to abuse them and cause Denial of Service (DoS)



According to the United Nations, two-thirds of the world's population will live in urban areas by 2050, leading many—from engineers to political leaders—to concentrate on developing smart-city initiatives.

Smart Cities Cyber Security Worries

CYBER ATTACKS AND THREATS

SMART TRAFFIC CONTROL

Devices were found without encrypting communications allowing attackers to change traffic lights.

SMART STREET LIGHTING

Malicious hackers can compromise all street lights in a city and turn them on and on at will.

SMART GRID

It is possible to black out big city areas by manipulating smart meters exploiting cyber security problems.

CITY MANAGEMENT SYSTEMS

Atlanta city systems were hacked and data encrypted by ransomware, authorities were asked to pay a ransom to get data back.

SMART PUBLIC TRANSPORTATION

Cyber attacks can display incorrect information on public transportation systems, it's possible to influence people's behavior to cause delays and overcrowding.

SENSORS

Smart sensors can be hacked to send fake data to systems affecting decision making. Attackers could fake earthquakes, tunnel or bridge breakage, flood, etc, raising alarms and causing general panic.

CAMERAS

Traffic and surveillance cameras are the eyes of the city and by hacking them, attackers can make cities blind.

PUBLIC DATA

This data can help attackers to determine the best timing for attacks, schedule attacks, create attack triggers, coordinate attacks, and so on.

SOCIAL MEDIA

It can be used as an amplification platform for attacks. For instance, attackers can increase the impact of an attack by causing panic in a population by promoting attacks.

MOBILE APLICATIONS

Hacking mobile apps has direct impact on citizens' behavior since they take decisions based on what mobile applications show.

LOCATION BASED SERVICES

GPS spoofing and other attacks are possible. Systems get real-time location information, and if the location is wrong, then decisions will be based on incorrect information.

CLOUD & SAAS SOLUTIONS

City servers and cloud infrastructure are exposed to common Distributed Denial of Services (DDoS) attacks that render services inoperable.

Smart Cities Cyber Security Worries

TOP SMART CITIES AND POSSIBLE CYBER ATTACK TARGETS

BARCELONA

- Smart street lighting
- Smart sensors network
- Smart irrigation system
- Shared bike systems
- WiFi public network
- Smart parking (apparkB)
- Smart Waste management

DUBAI

- Smart government services
- Smart energy and water
- Smart Dubai Platform
- Smart parking
- Smart traffic
- Smart transportation
- Smart cameras and security surveillance
- Smart street lighting

LONDON

- Traffic sensors
- Surveillance cameras
- Smart street lighting
- Smart parking
- Open data (London Datastore)
- London Underground railway system
- Transport for London Oyster systems

NEW YORK

- Surveillance cameras
- Traffic detection systems
- Communications network (LinkNYC)
- Gunshot detection sensors
- Smart street lighting
- Smart public transportation
- Smart waste management (BigBelly)
- GPS based systems (Traffic Signal Priority)
- Wireless Water Meters

RIO DE JANEIRO

- Surveillance Cameras
- Flood detection and rain gauge sensors
- Rio Operations Center (COR)
- Open Data (data.rio)
- Smart street lighting
- GPS based systems
- Weather control system
- Traffic signal control system

SAN FRANCISCO

- Traffic sensors
- Municipal Railway system
- Smart traffic systems
- Public transportation systems
- Smart parking
- Smart street lighting
- Gunshot detection sensors

SYDNEY

- Smart traffic
- Smart video surveillance (Rail Network)
- Smart parking (CellOPark)
- Smart public transportation (Opal system)
- Smart Sensing Network
- Smart Waste management

SINGAPORE

- HetNet
- Nationwide Sensor Network
- Intelligent Transport Systems
- Parking Guidance System
- Expressway Monitoring
- Advisory System
- Contactless Payment for public transport
- Digital Government services

Smart Cities Cyber Security Worries

SMART CITIES UNDER ATTACK

December 23, 2015

UKRAINE

Power grid: Attackers compromised three energy distribution companies systems, affecting 30 substations and leaving 230,000 people without electricity.

March, 2016

UNDISCLOSED CITY

Water treatment plant: Attackers changed the levels of chemicals used to treat water, and the data of 2.5 million utility customers was compromised.

November 4, 2016

SWEDEN

Air traffic Control systems: Attack affected several airports, preventing air traffic controllers from seeing aircraft on their screens. This resulted in the cancellation of multiple domestic and international flights and affected thousands of people.

November 25, 2016

SAN FRANCISCO

Municipal Railway:
Systems were infected by ransomware, attackers demanded 100 Bitcoins ($70,000 at that time).

April 7, 2017

DALLAS

Emergency alarms:
Attackers activated 156 emergency sirens at 11:40 p.m., waking up and frightening a lot of people until 1:20 a.m. when the alarms were turned off.

The incident resulted in 4,400 calls to 911.

October 11, 2017

SWEDEN

Transport Administration systems: A distributed-denial-of-service (DDoS) attack affected systems that monitor trains. It also affected the federal agency email system, website and road traffic maps. Train traffic and other services had to be managed manually, using backup processes. Some trains stopped and had delays that affected thousands of passengers.

November 18, 2017

SACRAMENTO

Regional Transit systems: A ransomware attack deleted 30 million files, and the attackers demanded $7,000 in Bitcoin.

March 22, 2018

ATLANTA

Municipal systems: Attackers used ransomware to infect city systems. They demanded $51,000 in digital currency and caused outages across various important city systems.

IOActive®

SECURING SMART CITIES

Source:

https://ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf
https://www.forbes.com/sites/forbestechcouncil/2018/04/18/cities-are-facing-a-deluge-of-cyberattacks-and-the-worst-is-yet-to-come/
https://securingsmartcities.org/