RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: HTA-T10

Hacking Smart Cities

Cesar Cerrudo

CTO, IOActive Labs
IOActive
@cesarcer

What happens when…?

How would you feel?

Are Cyber Threats real?

What is a Smart City?

- Many different definitions, but here's a simple one:

A city that uses technology to automate and improve city services, making citizens life better

- More than a $1 trillion potential market by 2020

How is a City “Smart”?

- Traffic control
- Parking
- Street lighting
- Public transportation
- Energy, Water and Waste management

How is a City “Smart”? (cont.)

- Security
- City management systems
- M2M
- Sensors (weather, pollution, seismic, smell, flood, sound, etc.)
- Open data (could be real time)
- Mobile apps

Problems

- New technologies (system, devices, etc.) are being deployed without any security testing
  - Ease-of-use and quick deployment vs security
  - Plagued by vulnerabilities (vendors are clueless about security)
- Almost everything is wireless
  - Custom protocol and encryption-related issues (even in RF transceiver chips)
- Lack of city CERTs means weak coordination and communication on security incidents

Problems (cont.)

- Huge and unknown attack surface
  - Complexity, interdependency, chain reaction
- Patch deployment and systems updates
  - How to test on non-production system?
  - How to keep up patching up to date?
  - If patch isn't available for a vulnerability, stop the service?
  - Patch delays by vendors and patches difficult to apply
- Legacy systems (vulnerable) communicate with new systems
  - Lack of standards

Problems (cont.)

Problems (cont.)

- Simple bugs can cause big problems and have big impact
  - May 2012 California: Placer County Courthouse system accidentally summoned 1,200 people to jury duty on the same morning causing traffic jam
  - November 2013 Bay Area Rapid Transit (BART): major software glitch, service was shut down by a technical problem involving track switching, it affected 19 trains with about 500 to 1,000 passengers on board
  - August 2003 Northeast: blackout, primary cause was a software bug in the alarm system at a control room of the FirstEnergy Corporation, 55 million people affected

Problems (cont.)

- Government bureaucracy and shortage of skilled people
- No response plan to react to possible cyber attacks on city services, systems, infrastructure, etc.
- Many possible ways to abuse and attack services
  - Smart City DoS
- Devices and systems difficult to get for research community

Attacks

- Last year proven attacks on traffic control systems
  - University of Michigan – Econolite – 100,000 intersections in US and Canada
  - Myself – Sensys Networks – 200,000 sensors worldwide
  - Demo…
- Street lighting
  - Wireless encryption problems
  - Could black out big city area, island, etc.

Attacks (cont.)

Attacks (cont.)

- City management systems
  - Manipulate information
  - Send workers to dig a hole to wrong place (gas, water pipes)

On June 7, 2010, a 36-inch gas pipeline explosion and fire in Johnson County, Texas, was caused by workers installing poles for electrical lines. One worker was killed, and six were injured. Confusion over the location and status of the construction work led to the pipeline not being marked beforehand

Attacks (cont.)

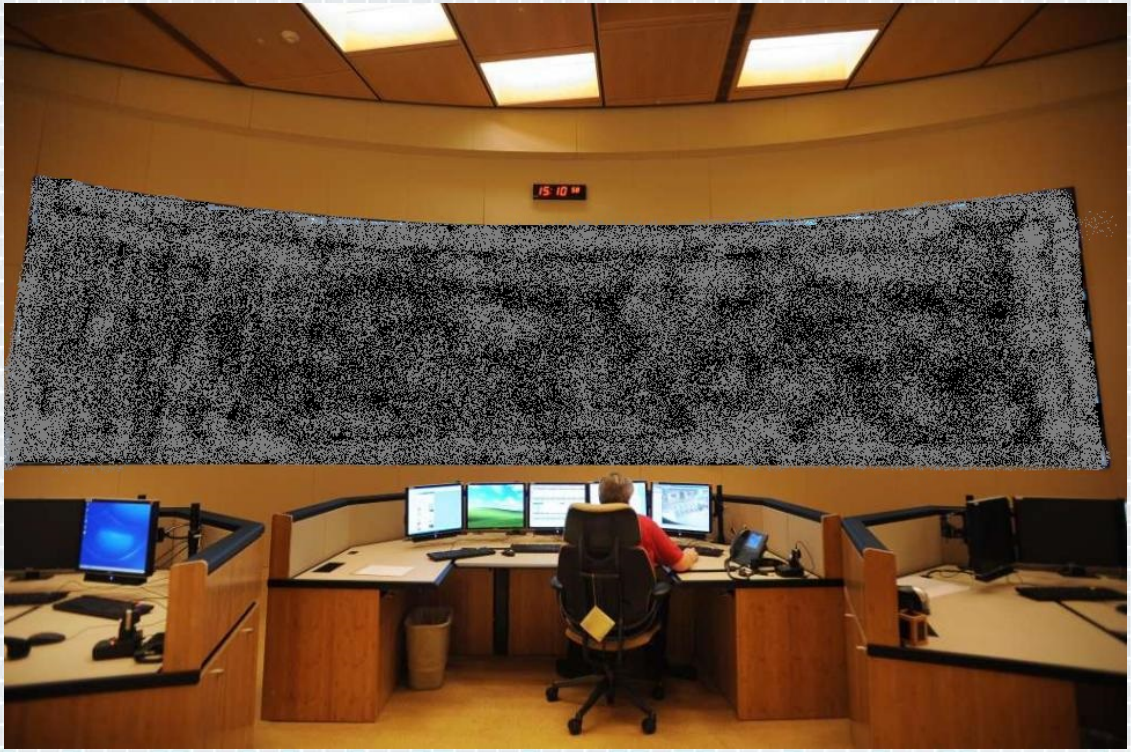
- Sensors
  - Fake seismic detection, fake flood detection, fake *, etc.
- Public data (sometimes real time) available to attackers
  - Easily find vendors and implemented solutions
  - Schedule attacks, attack triggers, coordination, etc.
- Mobile apps
  - Attack apps, apps developers, data feeds
- Smart City servers and cloud infrastructure
  - Beware of Smarty City SaaS
  - DDoS attacks can take services off line (Smart City DoS)

Attacks (cont.)

- Smart grid related attacks
  - Attacks on end points (smart meters, devices, etc.)
- Public transportation information systems
  - Influencing behavior by displaying wrong information, overcrowding, etc.
- Attack impact can increase if people get panic
  - Promote attacks on social media
- Traffic cameras and surveillance
  - Hundreds of same brand, no remote restart, vulnerabilities, etc.
  - DoS attacks make Smart Cities blind

Attacks (cont.)

Attacks (cont.)



Threats and skilled attackers

- New war scenarios (cyberwar) make cities technologies an important and interesting target
- Nation states have the knowledge and skills to easily attack cities and cause significant damage
- Cyber terrorism could be just around the corner. People with university degrees are joining extremist groups
- Cybercriminals are well organized and have plenty of resources. Their attack techniques and malware continuously evolve
- Hacktivists groups are known for launching cyber attacks campaigns on companies, organizations, groups of people, governments, and so on

Solutions and applications

- Do not implement systems and devices without security testing
  - Simple checklist for encryption, authentication, authorization, and software updates will make big difference
- Ask vendors to provide all security documentation and timely response
  - SLA include patching vulnerabilities on time and 24/7 response in case of incidents
- Fix security issues as soon as they are discovered. A city can continuously be under attack if issues are not fixed as soon as possible
- Create City CERT that can handle incidents, vulnerability reporting and patching, coordination, information sharing, etc.

Solutions and applications

- Regularly run pen tests in all city systems and networks
- Implement fail safe and manual overrides on all city systems
- Implement and make known secondary services/procedures in case of cyber attacks
  - Define a formal communication channel
- Restrict access to public data
  - Request registration, track and monitor access/usage
- Prepare for the worst, threat model everything

Conclusions

- Smart Cities current attack surface is huge and wide open to attacks
- It's only a matter of time until attacks on city services and infrastructure become common
- Smart Cities related technologies should be properly audited to make certain that they are secure before use
- Actions must be taken now to make cities more secure and protect against cyber attacks
- Smart Cities become Dumb Cities when the data that feeds them is blindly trusted and easily manipulated

QA

- Thanks!

Contact:

Cesar Cerrudo

ccerrudo@ioactive.com

@cesarcer

www.ioactive.com

References

- Smart Cities – Anthony M. Townsend
- https://www.google.com/search?q=smart+cities
- http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf