An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks

Cesar Cerrudo
(@cesarcer)
Chief Technology Officer, IOActive Labs

Abstract

Cities around the world are becoming increasingly smart, which creates huge attack surfaces for potential cyber attacks.

In this paper, IOActive Labs CTO Cesar Cerrudo provides an overview of current cyber security problems affecting cities as well real threats and possible cyber attacks that could have a huge impact on cities.

Cities must take defensive steps now, and Cesar offers recommendations to help them get started.

IOActive
Hardware | Software | Wetware
SECURITY SERVICES

Contents

Introduction

The idea for researching current cyber security-related issues in cities originated during my previous research, hacking traffic control systems. As my knowledge grew regarding our connected infrastructure, I became increasingly concerned about the current security posture of the world's infrastructure. After an in-depth analysis and weighing the security challenges of new technology adoption in cities, I felt compelled to write this report.

The goal of this paper is to generate consciousness about current cyber security issues in cities in order to kick-start discussions and actions to improve their security.

During my 15 years in offensive cyber security, I have found and reported hundreds of security vulnerabilities to CERTs (Computer Emergency Response Teams) and to most major software vendors. I have created innovative offensive cyber security techniques, employing different technologies for various security areas.

My experience gives me a unique view of a cyber attacker's perspective when targeting a city. It allows me to better assess current and future possible cyber threats and attack impacts.

It is important for decision makers, technology vendors, and the general public to understand and take action on the content of this report.

Smarter Cities

Cities have been incorporating new technologies for several years, but lately the rate of technology adoption has increased and cities around the world are becoming smarter. Newer technologies along with faster and easier connectivity allow cities to optimize resources, save money, and at the same time provide better services to its citizens.

Depending on the amount of new technology, some cities are smarter than others, but most cities around the world have implemented at least some technology. Others have implemented much more.

Maybe the city where you live is not described as smart, but it likely still uses some level of technology. Instead of being filled with smart, highly-integrated systems, it may just use a few simple technologies.

US cities like New York, San Francisco, Los Angeles, Washington DC, Seattle, and Miami are becoming smarter by the day, a trend seen around the world. We also can see this in Europe, in London, Barcelona, Amsterdam, Paris, Stockholm, and Berlin; in Asia-Pacific, in Singapore, Seoul, Tokyo, Sydney, Melbourne, and Hong Kong; in the Middle East, in Abu Dhabi, Dubai, Saudi Arabia, and Qatar, and in the South American cities of Rio de Janeiro and Santiago.

The increasing intelligence of cities is a global, accelerating, and unstoppable phenomenon.

Smart Cities Defined

If you search for a definition of the term smart city, you will find many definitions. For this discussion, I'm using the following:

> "A city that uses technology to automate and improve city services, making citizens' lives better."

In the truly smart city of the future, everything will be connected and automated. While this is not yet a reality, many cities are committing big budgets to get smarter. For instance:

- Saudi Arabia is investing US $70 billion into smarter cities[1]
- In Dubai, 1000 government services will go smart in few years[2]
- Barcelona is already ranked as the world's smartest city[3]
- In South Africa, a $7.4 billion smart city project just started[4]

According to some estimates, by 2020 the potential market for smart cities could be more than $1 trillion.[5] More conservative estimates place it at hundreds of billions of dollars, but regardless we can agree that vendors are seeing a great opportunity with smart cities and the buzz around it is growing.

How Does a City Become "Smarter"? What Technologies Are Used?

Main city services become smarter by deploying new technologies like:

- **Smart traffic control:** Traffic lights and signals that adapt based on volume and current traffic conditions. Current traffic is detected and that real-time information is used to coordinate and improve traffic flow, on streets, highways, ramps, and so on.[6]
- **Smart parking:** Citizens can use a parking application to find available parking slots, review pricing including pricing changes based on time of day, availability, location, etc.[7]

---

1 http://www.cisco.com/web/about/ac79/docs/success/Saudi_Arabian_General_Investment_Authority_SAGIA_Engagement_Snapshot.pdf

2 http://www.uaeinteract.com/docs/Smart_Dubai_strategic_plan_launched/60399.htm

3 http://smartcitiescouncil.com/article/juniper-ranks-barcelona-worlds-smartest-city-find-out-why

4 http://www.africapropertynews.com/southern-africa/3071-construction-begins-on-south-africa-7-4bn-smart-city.html

5 http://ww2.frost.com/news/press-releases/frost-sullivan-global-smart-cities-market-reach-us156-trillion-2020

6 http://en.wikipedia.org/wiki/Intelligent_transportation_system

7 http://en.wikipedia.org/wiki/SFpark

- **Smart street lighting:** Managed centrally, street lights can adapt to weather conditions, report problems, or be automated by time of day. Street lights can even turn off and on based on the detection of moving cars and people. [8, 9]
- **Smart public transportation:** Real-time data about schedules (bus, train, and subways), arrivals, and delays is provided to inform citizens. Contactless payments allow citizens to easily pay, even using a smart phone.
- **Smart energy management:** A smart grid can deliver energy based on needs. Smart meters can talk to the smart grid to schedule energy supplies at a specific time for lower cost. The smart grid can even turn off your home's water heater during peak hours when electricity is more costly. Smart buildings use the same kind of techniques to conserve energy and buy electricity when rates are low.[10]
- **Smart water management:** Smart pipes measure water quality, detect leaks, distribute water, detect problems, and so on.[11] Similar techniques are used for gas and oil pipelines.
- **Smart waste management:** Sensors in waste containers detect the volume of garbage, smell, and so on. Garbage collection can be better planned, skipping empty containers or making an early stop at a container that smells.
- **Security:** Traffic and surveillance cameras, gunshot detection sensors, and other security devices provide real-time information on what is happening and where. People-counting technology such as tracking of mobile phones or communication (such as WiFi or Bluetooth) is used to determine the number of people in a given area like a street, park, or building.[12, 13]

Those technologies are backed up by others:

- **City management systems:** These systems help to automate different city administration tasks.
- **M2M (Machine to Machine):** In order to make a city smarter, you need devices (machines) talking to each other, machine to machine, making decisions automatically.
- **Sensors:** Used for everything, sensors (often wireless) continuously feed smart city systems with data. Sensors are a core part of a smarter city.
    - **Weather:** Sensors detect weather conditions and send out alerts.

[8] http://en.wikipedia.org/wiki/Intelligent_street_lighting
[9] http://www.silverspringnet.com/article/us-investor-owned-utilities-choose-silver-spring-for-networked-street-lights
[10] http://en.wikipedia.org/wiki/Smart_grid
[11] http://www.itu.int/en/ITU-T/focusgroups/ssc/Documents/Approved_Deliverables/TR-SWM-cities.docx
[12] http://en.wikipedia.org/wiki/Gunfire_locator
[13] http://en.wikipedia.org/wiki/People_counter

    - **Pollution level:** Sensors detect and inform pollution levels in different parts of a city.
    - **Seismic:** Bridges and underground sensors detect damage to tunnels and infrastructure caused by earthquakes, aging, or other infrastructure problems.
    - **Smell:** For garbage, natural gas, and a variety of other situations, smell sensors detect trouble.
    - **Flood:** Sensors detect flood conditions.
    - **Sound:** Sound sensors can detect gunshots, alarms, activity, and so on.
- **Open Data:** Data is shared (sometimes real-time data) by governments so that people can develop applications, for instance the Transport for London open data project.[14]
- **Mobile applications:** In a smart city ecosystem, we could say mobile apps foster interaction of citizens with the city. Citizens retrieve information from city systems, sensors, and so on via mobile apps and make decisions based on information.

Living in a Smarter City

Let's say someone wakes up on a regular working day, takes a look at his smart phone or tablet, and starts to look at different mobile apps to choose the best alternative to go to work. He checks schedules and delays for trains, buses, and subways. He also checks for temperature, pollution level, and weather conditions. (This could be something simple like packing an umbrella or a jacket, or avoid going out because of pollution level.)

Sensors everywhere are feeding city systems and these are sending the data to mobile apps. Let's say that the person chooses to go by car since there was a delay in public transportation and/or it's a rainy day. On the way to work, he checks a mobile app for the best route to avoid traffic and checks another app to select parking based on availability and pricing. Traffic flow is good because of smart traffic control systems that adjust traffic lights based on current traffic conditions. Because of rainy weather, smart street lighting will leave street lights on until there is more daylight. If rain causes floods, flood detection sensors will immediately alert city management and citizens too. City management closely monitors the entire city with the help of surveillance and traffic cameras. The rain causes public transport delays, and information on delays and problems is pushed out so people can choose transport alternatives.

Let me stop there, since I think you get the picture. Smart technology is significantly changing life in metropolitan areas.

[14] http://www.tfl.gov.uk/info-for/open-data-users/our-feeds?intcmp=3671

Cyber Security Problems

Every new technology and innovation brings new challenges and problems. In this report, I'm focusing on cyber security-related problems that currently affect or will affect cities in general around the world, whether considered smart or not. These problems would impact the city government, residents, and the businesses and other organizations that conduct business there.

Keeping in mind the new technologies and life in a smarter city, let's consider what could happen if one or more technology-reliant services don't work. What would commuting look like with non-functioning traffic control systems, no street lights, and no public transportation? How would citizens respond to an inadequate supply of electricity or water, dark streets, and no cameras? What if garbage collection is interrupted in summertime and stinks up the streets? I guess it would be unpleasant and probably cause a lot of chaos in any city.

That scenario might not be as unlikely as you think. Any number of cyber security problems could trigger it.

- Lack of Cyber Security Testing
- Poor or Nonexistent Security
- Encryption Issues
- Lack of Computer Emergency Response Teams
- Large and Complex Attack Surfaces
- Patch Deployment Issues
- Insecure Legacy Systems
- Simple Bugs with Huge Impact
- Public Sector Issues
- Lack of Cyber Attack Emergency Plans
- Susceptibility to Denial of Service
- Technology Vendors Who Impede Security Research

Lack of Cyber Security Testing

Sadly cities are implementing new technologies without first testing cyber security. In fact, this is happening in most countries. I have proven this with my latest research. I learned that about 200,000 vulnerable traffic control sensors were installed in important cities

around the world such as Washington DC, New York, Seattle, San Francisco, London, Lyon, and Melbourne.[15]

In our research at IOActive Labs, we constantly find very vulnerable technology being used across different industries. This same technology also is used for critical infrastructure without any security testing. Although cities usually rigorously test devices and systems for functionality, resistance to weather conditions, and so on, there is often little or no cyber security testing at all, which is concerning to say the least.

Poor or Nonexistent Security

Vendors claim to have obscure, nonexistent security features, with no documentation, which is only described in a sales pitch. At IOActive Labs, we continue to see vendors with little or no experience in implementing security features; they lack skilled security people and don't properly invest in improving security. For instance, many vendors don't object to giving full privileged access to a device or system to anyone who is on a local network, because they think of the internal network as safe. However, if an attacker accesses the network, he can easily fully compromise available devices and systems. It may sound incredible but exceptionally poor security practices are common on industrial systems and devices on the Internet of Things (IoT)[16]. These practices are being propagated into city technology.

Encryption Issues

Most new devices are wireless (such as traffic and surveillance cameras, smart meters, street lights, traffic lights, smart pipes, sensors, and so on), which makes them easy to implement but also easier to hack if communication is not properly encrypted.

Wired communication requires physical access which generally makes it more difficult to hack, but some systems that rely on wired communication are more exposed and easier to access such as Power-line Communication (PLC) technologies.[17] An attacker simply connects to electric power to get access to the network. Some smart grid and street lighting solutions use this technology.

Many vendors implement custom wireless and wired communication protocols with either very poor security or no security. Even when encryption is implemented at wireless and wired communications, very few vendors properly implement encryption.

Some vendors implement outdated and weak encryption algorithms, while others implement known good standard encryption but still have weak encryption key management. Most common encryption problems are related to poor key generation,

[15] http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html
[16] http://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/
[17] http://en.wikipedia.org/wiki/Power-line_communication

fixed keys, shared keys, leaked keys, and so on.[18] Once an encryption key is compromised, attackers get full access to communications.

Sometimes encryption options are available to secure communications but cities simply don't turn them on. This is something common that usually happens because people without security knowledge deploy the systems or because of the complexity to implement it.

When either wireless or wired communications security is poor, an attacker can easily intercept and hijack communications and take control of devices and networks. We see this all the time; most such communications are insecure.

Lack of City Computer Emergency Response Teams

Another important issue is the lack of specific CERTs[19] for cities and states.

Existing CERTs already have problems with coordination and communication. For instance, for the latest important research at IOActive Labs, we provided detailed information to CERTs but we still received calls and emails from the military, federal agencies, and others asking for this information. We don't know why the military and federal agencies do not receive such important information on time. This is common.

Large and Complex Attack Surfaces

There is a huge and unknown attack surface on smarter cities. With so much complexity and interdependency, it is difficult to know what and how everything is exposed. Therefore, simple problems could cause a big impact due to interdependency and chain reactions.[20] This is what makes threat modeling so important. We will see an example of this later.

Has anyone seen a threat model for a city? Maybe these exist, but I haven't seen one. Some larger software and services vendors have issued general documents about cyber security in cities but nothing very specific.

Patch Deployment Issues

Patch deployment and system updates face many security problems. Because of complexity, patches are difficult and costly to test on non-production systems, since some production systems are costly to reproduce. It is increasingly common for cities to use vulnerable devices and systems because vendors are either slow to release patches or patches are not available.

---

[18] http://www.networkworld.com/article/2168513/security/oil--gas-field-sensors-vulnerable-to-attack-via-radio-waves.html

[19] http://en.wikipedia.org/wiki/Computer_emergency_response_team

[20] http://www.amazon.com/Smart-Cities-Civic-Hackers-Utopia/dp/0393082873

For vulnerabilities discovered in my previous research, the vendor took a year to release a patch, and we still don't know if it really fixed the vulnerabilities. Even if it worked, devices are still vulnerable if the patch wasn't applied worldwide.

Insecure Legacy Systems

New technology is being integrated with old technology that may be vulnerable. Some old technologies that lack standards can require a piece of technology in the middle to communicate between old and new systems and to translate protocols. Some systems won't run on newer, more secure operating systems; therefore, vulnerable and older operating systems are used. This adds complexity, increases the attack surface, and makes for slow adoption of new technologies.

I was quite surprised when I saw a CNN story[21] on the Burj Khalifa smart building, the world's tallest and smarter building. Main building systems are run on the Windows XP operating system, which is old, outdated, not supported[22] and less secure than new operating systems. This makes Burj Khalifa an easy target for possible cyber attacks.

Simple Bugs with Huge Impact

When you have a city that is running hundreds of systems and devices for critical services, a simple software bug can have huge impact. Let's consider some real examples to better illustrate this:

May 3, 2012

A tie-up on Interstate 80 was caused by a computer glitch. The Placer County court accidentally summoned 1,200 people to jury duty on the same morning. Taking their duty seriously, residents tried to be on time at 8:00 a.m. and were in a line of traffic with other would-be jurors, causing the traffic jam.[23, 24]

Nov 22, 2013

San Francisco Bay Area Rapid Transit (BART) was shut down. Due to a major software glitch earlier in the morning, service was shut down by a technical problem involving track switching, which began shortly after midnight and affected 19 trains with about 500 to 1,000 passengers on board. Passengers were trapped on trains in the late evening and early morning hours.[25]

[21] http://outfront.blogs.cnn.com/2014/06/19/city-of-tomorrow-a-tour-of-the-worlds-tallest-tower
[22] http://windows.microsoft.com/en-us/windows/end-support-help
[23] http://www.npr.org/2012/05/03/151919620/computer-glitch-summons-too-many-jurors
[24] http://www.amazon.com/Smart-Cities-Civic-Hackers-Utopia/dp/0393082873
[25] http://www.bizjournals.com/sanfrancisco/blog/2013/11/bart-system-shut-down-by-software.html

August 14, 2003

A blackout affected an estimated 10 million people in Ontario and 45 million people in eight US states.[26] The blackout's primary cause was a software bug in the alarm system at a control room of the FirstEnergy Corporation, located remotely in Ohio. A lack of alarms left operators unaware of the need to redistribute power after overloaded transmission lines hit unpruned foliage. This triggered a software bug known as a race condition in the control software.

The race condition existed in General Electric Energy's Unix-based XA/21 energy management system. Once triggered, the bug stalled FirstEnergy's control room alarm system for over an hour. System operators were unaware of the malfunction; the failure deprived them of both audio and visual alerts for important changes in system state. What would have been a manageable local blackout cascaded into widespread distress across the electric grid.

Some information about the blackout impact:

- 508 generating units at 265 power plants were shut down
- Water systems in several cities lost pressure
- At least 10 deaths were reported
- New York City had 3,000 fires calls
- The New York City 311 information hotline received over 75,000 calls
- Mobile networks overloaded and were disrupted
- Hundreds of flights were cancelled
- New York State was responsible for billions of dollars in costs

These simple software bugs had a big impact, and there are many more examples. Imagine what could happen if an attacker could trigger bugs like these at will.

Public Sector Issues

Another problem with city cyber security is government bureaucracy. When dealing with security issues, there is no time to lose. On top of time pressures, cities have a shortage of workers with security skills. Cities have inadequate budgets, training, and resources to help workers develop skills, and this can make the problem worse.

Lack of Cyber Attack Emergency Plans

Cities should be required to seriously consider how to best prepare against possible cyber attacks. Cities need to develop an emergency plan that provides steps to follow during a

[26] http://en.wikipedia.org/wiki/Northeast_blackout_of_2003

cyber attack and educate people on how to react while under attack. Fast and effective reaction can be key to preventing bigger problems including city chaos.

Susceptibility to Denial of Service

With so many services dependent on technology in a city, attackers have many methods to abuse them and cause Denial of Service (DoS). The cause of DoS could be something simple; for instance, a DoS attack could interrupt of an Internet-facing server that feeds data to a couple of systems; this would have a big impact on regular city services and activities.

Technology Vendors Impede Security Research

Finally, the security research community is anxious to test more technologies used by cities, but these devices and systems are difficult to acquire. They are expensive, and they are only sold to governments or to specific companies or people. This makes life easier for some vendors since they can continue to release unsecured products without accountability from researchers.

The public needs to see to believe. Cities are not spurred to action by discussions about suspected vulnerable products and threats on cities. Without clearly seeing or directly experiencing problem, the public doesn't generally care. People need to see me and other ethical researchers hacking traffic lights, smart grids, and so on in order to understand that the threat is real, and not just theoretical.

Cyber Attacks on Cities

All technologies used by cities plus all the associated cyber security problems that were previously described open the door for several possible cyber attacks. Each new city technology or system creates a new opportunity for cyber attackers.

Let's discuss in depth some of the key technologies and systems that together make up the smart city's complex attack surface:

- Traffic Control Systems
- Smart Street Lighting
- City Management Systems
- Sensors
- Public Data
- Mobile Applications
- Cloud and SaaS Solutions
- Smart Grid
- Public Transportation

- Cameras
- Social Media
- Location-based Services

Traffic Control Systems

Last year, a research team from University of Michigan and I independently proved that traffic control systems could be easily hacked.[27, 28] The University of Michigan research found that some Econolite devices were used without any encryption for communication between traffic control systems and traffic lights, traffic controllers, and so on, allowing an attacker to directly change traffic lights. 100,000 intersections in the US and Canada could be affected.

In my research I found that Sensys Networks devices didn't have any encryption, any authentication, or any security at all. It was possible to feed traffic control systems with fake data making them accept incorrect options when setting configuration and timing on traffic lights, ramp meters, traffic signals, and so on. It was possible to fully compromise the sensors and even to create a firmware update worm. 200,000 vulnerable sensors deployed worldwide were affected.

We still don't know if these vulnerabilities were patched. If they were, we don't know how the patch addressed the vulnerability and whether the patches actually were applied. Cities can't easily detect if someone did something malicious like updating firmware with backdoors. I had an interesting discussion with someone from the US Department of Transportation (US DOT), who wasn't really worried about these vulnerabilities since he said "we have worse things to worry about." I couldn't fight that argument but it shocked me to know that US cities are vulnerable to worse attacks on traffic control systems that the one I discovered.

Smart Street Lighting

Wireless street lighting systems are being deployed in many cities around the world.[29] Most systems use wireless communications and have the encryption related problems previously described. Attacks on smart street lighting systems are not complex and can have big impact by causing street blackouts in large areas. For example, there exists a scenario where a street blackout could affect an entire island in the US Virgin Islands where a wireless street lighting system was implemented.[30]

[27] https://www.usenix.org/system/files/conference/woot14/woot14-ghena.pdf
[28] http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html
[29] http://explore.citytouch.com/references
[30] http://www.digi.com/learningcenter/stories/digi-wirelessly-enables-cimcon-street-light-management-system

I have tried to get my hands on the specific devices used in the US Virgin Islands, resulting in about a dozen calls and emails with the vendor, who promised to send me a quote for the devices but did not send it. Why is it to hard to acquire such equipment? Why the vendor wouldn't sell it to IOActive?

There are also wired solutions using Power-line Communication (PLC) technologies that also could have the encryption problems that were already mentioned.

City Management Systems

Every city has hundreds of systems to manage different services and tasks. Hacking these systems would give an attacker a lot of options to cause harm. Just as simple software bugs can create significant harm, manipulating simple information could also have a seemingly oversized security effect.

Imagine if an attacker can intentionally trigger those bugs and with some planning, get an even bigger impact. For instance, an attacker could manipulate map information and work orders to send city or contractor workers to dig a hole over gas or water pipes or communication cables, with the intention to damage those facilities. After all, this has already happened in the past by mistake several times.

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 eight were injured. Due to confusion about the location and status of the construction work, the pipeline was not marked beforehand.[31]

Sensors

Smart city systems rely heavily on sensor data to make decisions and take action. Most sensors use wireless technologies that are affected by the types of security problems already mentioned. Attacks that involve compromising sensors and sending fake data can directly affect systems since decisions and actions will be based on fake data. This could have great impact depending on how the affected systems use the data and interact with other systems.

Attackers could even fake an earthquake, tunnel, or bridge breakage, flood, gun shooting, and so on, raising alarms and causing general panic. An attacker could launch a nuisance attack by faking data from smell or rubbish level sensors in empty garbage containers, to make garbage collectors waste time and resources.

Keep in mind that many systems and services from cities rely on sensors, including smart waste and water management, smart parking, traffic control, and public transport. Hacking wireless sensors is an easy way to remotely launch cyber attacks over a city's critical infrastructure.

[31] http://www.wfaa.com/story/news/2014/08/09/13587360

Public Data

Public data (open data) is available to attackers, sometimes in real time. This data can help them determine the best timing for attacks, schedule attacks, create attack triggers, coordinate attacks, and so on. Attackers don't need to act blindly; they can act precisely, relying on real data. For instance, attackers can identify exactly when a bus or train is arriving. They can see when traffic is heaviest, when more people are gathering at a location, and so on.

Also, information about the technologies in use in cities is often available since governments have public lists of technology providers and contracts.[32] Sometimes vendors will highlight case studies for cities that have been deployed.[33]

All of this gives attackers a lot of detailed information to work with.

Mobile Applications

Mobile applications are affected by common security vulnerabilities which could allow attackers to perform a variety of attacks, from simple Man in The Middle (MiTM)[34] attacks to more complex attacks. Attackers could also target mobile application development companies or just target the data that feeds the applications. Mobile applications are an important target since cities' citizens will make decisions and act based on information from those apps. Hacking mobile apps has direct impact on citizens' behavior. For instance, if the public transport app is showing a delay on a bus, a citizen could choose to travel to work by car; if the same decision is taken by hundreds of people in high density area, the result is a traffic jam, which we can think of as a city DoS.

Cloud and SaaS Solutions

City servers and cloud infrastructure are exposed to common Distributed Denial of Services (DDoS) attacks. Severs and cloud infrastructure are cheaper targets for cybercriminals or cyber terrorists. Also, when in use, Software as a Service (SaaS) could allow attackers to hack a single service provider and then launch attacks against many cities at same time. Cities should consider the security implications of SaaS solutions as well as their functionality.

Smart Grid

Energy is the life line of a city; without energy there is no smart city. Last year, researchers Alberto Garcia Illera and Javier Vazquez Vidal at Black Hat Europe

[32] http://wwe2.osc.state.ny.us/transparency/contracts/contractsearch.cfm
[33] http://wstc.wa.gov/Meetings/AgendasMinutes/agendas/2011/March22-23/documents/032211_BP10_IntelligentTransportationSystems.pdf
[34] http://en.wikipedia.org/wiki/Man-in-the-middle_attack

demonstrated it was possible to black out big city areas by manipulating smart meters[35] exploiting encryption problems in Power-line Communication (PLC) technologies. This is not new; years ago Mike Davis of IOActive created the first proof-of-concept worm for the smart grid.[36]

Attacks on a smart grid could be devastating, causing millions of dollars in losses and even loss of life.

Public Transportation

Citizens use public transportation information systems daily to know what time some transport is scheduled to arrive or depart, whether to expect delays, etc. By just by displaying incorrect information by manipulating public transportation information systems, it's possible to influence people's behavior to cause delays, overcrowding, and so on. For instance, by faking a delay in a subway line, attackers can influence people to move to another line, overcrowding it.

Also an attacker could target payment systems. If payment systems don't work, people might ride for free or thousands of people could jam customer service counters and hotlines with complaints.

Cameras

Cameras are becoming more widely used in most cities around the world. Traffic and surveillance cameras are the eyes of the city and by attacking them, attackers can make cities blind. Our research has shown that DoS attacks on these devices are not difficult and that these attacks are very effective. It is not always possible to remotely restart cameras. In addition, DoS attacks can be made persistent by modifying firmware or exploiting vulnerabilities.

Usually cities deploy hundreds of cameras of the same brand and model. This makes attacks easier since any vulnerability will affect all cameras in the city.

Some of these cameras are wireless and suffer from the problems already described for wireless communications such as no encryption, weak encryption, and so on.

Recently Kaspersky Labs researcher, Vasilis Hiuorios, found that police surveillance cameras were vulnerable and easy to hack.[37]

Social Media

Social media can be used as an amplification platform for attacks. We saw this in recent high-profile company hacks. For instance, attackers can increase the impact of an attack

[35] https://www.blackhat.com/eu-14/briefings.html#lights-off-the-darkness-of-the-smart-meters
[36] http://www.blackhat.com/presentations/bh-usa-09/MDAVIS/BHUSA09-Davis-AMI-SLIDES.pdf
[37] http://blog.kaspersky.com/internet-of-crappy-things/

by causing panic in a population. If just one simple attack is real, then a bigger attack can be promoted. Even if promoted attack never happens, it will scare people. Every day that such a problem persists, it will grow and incite increasingly angry citizens. Attackers know this and can play with social media perceptions at will.

Location-based Services

Many services are location-based, which means GPS spoofing and other attacks are possible. People get real-time location information, and if the location is wrong, then people will make decisions based on incorrect information. The nature of the impact depends on the extent to which a city relies on the services affected.

Threats and Skilled Attackers

New war scenarios make cities technologies an important and interesting target. Cyber war attacks will target city services and infrastructure.[38]

Cyber terrorism could be just around the corner. Terrorism is evolving. People with university degrees are joining extremist groups.[39] They are skilled and can use new technologies to launch terrorist attacks.

Nation states are already targeting companies and governments around the world for espionage, cyber attacks, and so on.[40] Nation states have the knowledge and skills to easily attack cities and cause significant damage.

Billions of dollars a year are lost worldwide because of cybercrime.[41] Cybercriminals are well organized and have plenty of resources. Their attack techniques and malware continuously evolve. City technology is vulnerable because almost everything in a city is or will soon be running software inside. For instance, cybercriminals could find a good business opportunity: Charging cities a ransom to regain control of compromised systems and infrastructure. Their message could be: "Do you want the smart grid back? Then pay us $100 million in bitcoins."

Hacktivists groups are known for launching cyber attacks campaigns on companies, organizations, groups of people, governments, and so on. These attacks could target city technologies too as part of a cyber attack campaign on a country or specific geographic area.

[38] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia
[39] http://www.liverpoolecho.co.uk/news/liverpool-news/revealed-liverpool-john-moores-university-8858428
[40] http://www.darkreading.com/attacks-breaches/nation-state-cyber-espionage-targeted-attacks-becoming-global-norm/d/d-id/1319025
[41] https://www.europol.europa.eu/sites/default/files/publications/europol_iocta_web.pdf

Recommendations

The following are just basic, general recommendations to reduce problems. Much work is needed, but cities can get started using these steps that can make a big difference in the current situation:

- Create a simple checklist-type cyber security review. Check for proper encryption, authentication, and authorization and make sure the systems can be easily updated.
- Ask all vendors to provide all security documentation. Make sure Service Level Agreements include on-time patching of vulnerabilities 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. For instance, if a traffic control system is hacked and not quickly fixed, it will continue being hacked over and over again and turn the city into chaos.
- Create specific city CERTs that can deal with cyber security incidents, vulnerability reporting and patching, coordination, information sharing, and so on.
- Implement and make known to city workers secondary services/procedures in case of cyber attacks, and define formal communication channels.
- Implement fail safe and manual overrides on all system services. Don't depend solely on the smart technology.
- Restrict access in some way to public data. Request registration and approval for using it, and track and monitor access and usage.
- Regularly run penetration tests on all city systems and networks.
- Finally, prepare for the worst and create a threat model for everything.

Conclusion

The current attack surface for cities is huge and wide open to attack. This is a real and immediate danger. The more technology a city uses, the more vulnerable to cyber attacks it is, so the smartest cities have the highest risks.

It's only a matter of time until attacks on city services and infrastructure happen. It could be at any moment.

Actions must be taken now to make cities more secure and protect against cyber attacks.

It's extremely important: Technologies used by cities must be properly security audited to make certain that they are secure before they are implemented. To fail to do so is reckless.

When we see that the data that feeds smart city systems is blindly trusted and can be easily manipulated, that the systems can be easily hacked, and there are security problems everywhere, that is when smart cities become Dumb Cities.

About Cesar Cerrudo

Cesar Cerrudo is Chief Technology Officer for IOActive Labs, where he leads the team in producing ongoing, cutting-edge research in areas including Industrial Control Systems/SCADA, smart cities, the Internet of Things, and software and mobile device security. Cesar is a world-renowned security researcher and specialist in application security.

Throughout his career, Cesar is credited with discovering and helping to eliminate dozens of vulnerabilities in leading applications including Microsoft SQL Server, Oracle database server, IBM DB2, Microsoft Windows, Yahoo! Messenger, and Twitter, to name a few. He has a record of finding more than 50 vulnerabilities in Microsoft products including 20 in Microsoft Windows operating systems. Based on his unique research, Cesar has authored white papers on database and application security as well as attacks and exploitation techniques. He has presented at a variety of company events and conferences around the world including Microsoft, Black Hat, Bellua, CanSecWest, EuSecWest, WebSec, HITB, Microsoft BlueHat, EkoParty, FRHACK, H2HC, Infiltrate, 8.8, Hackito Ergo Sum, NcN, Segurinfo, and DEF CON.

Cesar collaborates with and is regularly quoted in print and online publications. His research has been covered by Wired, Bloomberg Businessweek, TIME, The Guardian, CNN, NBC, BBC, Fox News, and so on.

About IOActive

IOActive is a comprehensive, high-end information security services firm with a long and established pedigree in delivering elite security services to its customers. Our world-renowned consulting and research teams deliver a portfolio of specialist security services ranging from penetration testing and application code assessment to chip reverse engineering. Global 500 companies across every industry continue to trust IOActive with their most critical and sensitive security issues. Founded in 1998, IOActive is headquartered in Seattle, US, with global operations through the Americas, EMEA and Asia Pac regions. Visit www.ioactive.com for more information. Read the IOActive Labs Research Blog: http://blog.ioactive.com. Follow IOActive on Twitter: http://twitter.com/ioactive.

Keywords

Hacking, security, smart cities, cyber cities, cities, cyber terrorism, cyber attacks, cyberwar, cyber criminal

