The Dangers of **Smart City Hacking**

IBM

Part 1. Executive Overview

The adoption of smart city technology by cities across the globe is transforming the way municipalities manage common services and critical infrastructure. With as many as hundreds of thousands of connected systems embedded throughout a city's critical infrastructure, city managers and urban planners have found they can remotely and efficiently improve the daily lives of their citizens, or alert citizens to emergency situations in real-time.

But the same innovations that make smart city technology attractive to cities – such as their connectivity and ease of management – also make them attractive targets to attackers.

By taking advantage of readily available tools for identifying exposed devices, and the relatively immature security in smart city technology, attackers can take control of these systems. They can potentially cause citizens to panic, put workers in danger, and send law-enforcement officers on wild-goose chases.

City leaders and citizens alike are trained to trust these systems and their alerts. If control is placed in the wrong hands, attackers can abuse that trust, to devastating consequences.

Snapshots

- **In early 2018, IBM X-Force Red and Threatcare discovered 17 zero-day vulnerabilities in smart city sensors and controls used in cities around the world.** Left unpatched, these vulnerabilities could allow hackers to gain access to sensors and manipulate data.
- **It's important to keep in mind that even a simple false sensor alert, generated by malicious hacking or otherwise, can trigger mass panic.** As an example, the January 2018 false ballistic missile alert in Hawaii – a simple employee error, not a hacking incident – generated text messages to citizens: "BALLISTIC MISSILE THREAT INBOUND TO HAWAII. SEEK IMMEDIATE SHELTER. THIS IS NOT A DRILL." Frightened people fled to shelter, inundated emergency services phone lines, and overloaded cell-phone networks with calls to family and friends.
- **An actor who is determined to incite mass chaos could create far greater impact with minimal effort if security for sensors and controls is not strengthened.**

Part 2. How Smart Cities are Growing

Smart city technology is becoming ubiquitous as cities deploy a rapidly growing array of internet-connected sensors to monitor and control factors, such as traffic, environmental variables, the electrical grid and more to help manage infrastructure and improve public safety. These Internet of Things (IoT) enabled devices have become cost-effective and easy to deploy and manage, allowing cities to connect typically siloed devices to the internet for remote administration. The devices, in turn, help cities save time and money because they alleviate the response process by removing the need to deploy personnel to check a widespread network of devices that may or may not need immediate attention.

Worldwide spending on technologies that enable smart cities is projected to reach **$80 billion in 2018** and will grow to **$135 billion by 2021**, according to IDC's *Worldwide Semiannual Smart Cities Spending Guide*.[1]

- The United States is expected to be the **largest** market, with China close behind.
- Latin America and Canada will see the **fastest** growth in spending.

Smart city projects around the world

Cities are using sensors and controls for everything from traffic monitoring to smart-building monitoring.

- **New York City**
  More than 600 sensor cameras gather traffic data for the city's Department of Transportation, primarily for signal timing and emergency management. The data collected by the cameras also sheds light on average vehicle speeds and bicycle usage.

- **Las Vegas "Innovation District"**
  Of the city's 10,000 sensors, about 1,000 are in a section of the city that hosts tests to gather data about traffic flow, pedestrian use of crosswalks, and detection of potential threats like packages left in public areas, in order to alleviate congestion.

- **Singapore**
  The city-state's "Smart Nation Sensor Platform" is testing the connection of hundreds of thousands of sensors to monitor street light energy usage, gauge transport network performance, and capture and analyze video from street cameras.

- **Barcelona**
  The city's Barcelona Lighting Masterplan uses smart city technology to improve the efficiency of lampposts; when the streets are empty, lights automatically dim to conserve energy. The lampposts also have sensors that collect air quality data.

**These smart city project examples were not part of the current research.*

1 "Investments in Technologies Enabling Smart Cities Initiatives Are Forecast to Reach $80 Billion in 2018, According to a new IDC Spending Guide," IDC, February 20, 2018: https://www.idc.com/getdoc.jsp?containerId=prUS43576718.

Part 3. How IBM X-Force Red Uncovered Smart City Vulnerabilities

In early 2018, as part of an ethical hacking project, IBM X-Force Red and Threatcare discovered 17 zero-day vulnerabilities in smart city sensor and control devices currently deployed across the globe by various municipalities.

The team conducted the research to learn more about real-world possibilities for the hacking of smart city technology, assess if "supervillain-level" attacks on smart cities were possible, and to determine whether testing methods such as those employed in every day application security review and penetration testing work could be used to find such vulnerabilities.

As the combined X-Force Red and Threatcare team uncovered vulnerabilities, they followed standard disclosure practices by reaching out to device manufacturers and appropriate city agencies.

The 17 vulnerabilities fell into various categories, but several were recurring:

> Public default passwords

The devices could be placed into operation without requiring the user to create a secure password. Default passwords such as "admin" allows even the most novice hackers to easily gain access to these devices.

> Authentication bypass

These flaws allow attackers to skip a login page and call up an internal administrative menu page that shouldn't be accessible to them, allowing an outsider the same control as a legitimate administrator would have.

> SQL injection

A long time entry on the OWASP Top Ten, a list of the most common application security mistakes, SQL injection involves sending data that looks like part of the communication between the application and the database, confusing the database into performing actions it shouldn't, such as disclosing usernames and passwords.

**At no point were citizens put in danger by the discovery of the vulnerabilities, nor was any private data exposed. IBM ensures that all vulnerabilities are disclosed to the affected vendors before publicly announcing the results of its projects.*

It's painfully easy to find out the locations of smart city devices, their purpose, and the minimal security safeguards they are shipped with. Here's one path our research team used to discover these systems

1. **Search Shodan or Censys**, two search engines for IoT and connected devices, for the specific locations and IP addresses of devices.
2. **Match the search data to published vendor information** to determine what the device is used for, such as air-quality monitoring.
3. **Search for vendor support information** (such as installation guides) that outline password protection, troubleshooting and other security features.

Attackers who can track down and research smart-city controls and sensors may have little trouble exploiting vulnerabilities and getting past minimal security barriers. Every single device examined by **X-Force Red** and **Threatcare** was still using the default passwords that they came with in the box, which are easily found online. To make matters worse, all of them also have authentication bypass issues.

Part 4. Attack Paths

Here are the paths attackers might take to attack each of the devices studied as a part of the research when the default passwords and keys have been changed:

Libelium Meshlium

Exploiting the Meshlium involves sending a shell injection payload to one of a series of endpoints that do not check authentication and which feed user input into shell commands in an unsanitized way. This allows any shell command to be executed as the "www-data" user, which controls the web server. This user is also given passwordless sudo access, meaning that it can execute any command as root, a user with complete control over the entire system. Attackers can now take a variety of actions, including attacking other systems accessible by the Meshlium, inserting fake sensor data to disrupt systems that rely upon correct sensor data, or selectively removing sensor data to prevent important events from being detected.

Battelle V2I Hub

In V2I Hub v2.5.1, which has been deprecated along with the rest of v2.x in response to our discoveries, there is a hard-coded administrator account which cannot be removed without modifying the code. While it's unlikely this will be changed in any real-world deployment, if it is, there is still an API. This API requires a key, and if the default has been changed, it's possible to request the API key directly through the web server, without authentication. In one of the API endpoints, there is a SQL injection flaw, which can be used to retrieve credentials for the rest of the application. In V2I Hub v3.0, there is a SQL injection flaw in the login process, which allows attackers to retrieve credentials from the database directly, without authentication.

Echelon i.LON 100 / i.LON SmartServer and Echelon i.LON 600

The Web and FTP passwords for the i.LON device family are default values out of the box, and don't need to be changed, but when they ARE changed, they must be changed individually. Changing the Web password doesn't change the FTP password, and vice versa. If both passwords have been changed from their default values, however, the API for the i.LON 100 / i.LON SmartServer does not require authentication with the default configuration. This API, in older versions, allows the username and password for the FTP server to be retrieved. In newer versions, the FTP credentials cannot be retrieved from the device, but they can be changed through the API.

Once authenticated to the FTP server, an attacker can replace the files on the device to change the way it functions, which could be used to gain persistent access to the device, add a new Web user to access the functionality provided by the Web server, and sabotage the device.

The i.LON 600 has a secure default authentication configuration, but the i.LON family suffers from an authentication bypass bug. When a Web request is made, the path requested (e.g. /dir/file.txt for http://example.com/dir/file.txt) is compared character by character against the paths in the configuration file to see if the i.LON should ask for a username and password. However, if a single slash in a requested path is replaced with two or more slashes, this will prevent the i.LON from matching against the configured paths. Once the path is requested at the operating system level, the extra slashes will be removed, and the file will be served normally.

There's an additional challenge to exploiting the i.LON 600, though. Even with an authentication bypass, the i.LON 600 runs in a restricted mode by default which prevents most changes from being made. In order to put it in the open mode that allows all settings to be changed, a person must physically be present at the device to push a button while it boots. While this prevents an attacker from altering the FTP credentials to be able to replace the binaries on the device, it does not prevent them from changing the IP address of the device, locking legitimate users out of the device until they reset the device while pushing a button on the device itself with a paper clip.

Part 5. The Security Challenge

At a high level, smart city technologies present, and sometimes further complicate, many of the security challenges that local government and ICS networks have been facing in the last decade. These challenges often have to do with the fact that the devices/assets are often attached to legacy equipment on legacy operating systems or have been connected to the internet without a full security audit of the risks.

The world witnessed how easy and dangerous it is for attackers to take control of our ICS networks, in global news stories of the last several years – most notably the **2015 Ukranian power grid shutdown** and the New York State dam that was **hacked by Iran in 2016.** Further, legacy technology issues have been brought to question in situations like the 2017 WannaCry attack, when Microsoft took note of out-of-service software running on ICS and other sensitive devices that customers had deployed that became critical to develop patches for – completely contrary to their past traditional protocols.

If smart city device manufacturers and the agencies deploying them do not learn from these recent examples and work harder to secure them today, they will be faced with episodes of mass confusion and potentially chaos when they're compromised in the future. The discoveries by the **IBM Security** and **Threatcare** team paint a frightening picture of the possibilities.

How "supervillain" attackers can cause chaos

The vulnerabilities discovered in this project could not only allow "supervillain" hackers to break into individual sensors and monitors, but to trigger false alerts that could terrify residents, cause city leaders to divert resources to nonexistent problems, or block warnings about real dangers.

Many of these scenarios have been key moments in major movie plots – but the truth is, it's incredibly easy to do and is a very real threat today. **Here are some possible outcomes of successful smart city technology hacks that could very well be enacted by taking advantage of the specific vulnerabilities the team discovered:**

> **Disasters, real and fake**

By causing water level gauges, radiation detectors, wind speed sensors, and other disaster detection and alarm systems to report incorrect data, an attacker could potentially cause an evacuation as a distraction, or as a means to soften a target as a precursor to a kinetic attack. Alternatively, if these systems are relied upon to detect disaster as it approaches, and the systems report that everything is normal, a city could suffer far worse damage as a result of the delayed response, a scenario most dangerous when it comes to threats humans are bad at detecting, such as radiation.

> **Manipulation of law-enforcement response**

This is a favored scenario for action movies: Chances are high that the bad guys hack into traffic control and vehicle systems to reroute vehicles to their benefit or prevent good guys from getting to the scene. (In the movie "Fate of the Furious," the villain takes control of "zombie cars" and forces them to smash into each other at key traffic intersections, blocking the escape path of a government official.) While this scenario may seem far-fetched, hackers could accomplish simultaneous traffic tie-ups on key city blocks by taking control of traffic control infrastructure – enough to create gridlock and delay law-enforcement teams from accessing the real scene of a crime.

> **Agricultural crop manipulation**

Smart farming has becoming commonplace as farmers use sensors to measure humidity, rainfall, and temperature to efficiently irrigate crops and determine optimal harvest times. Manipulation of this sensor data could result in irreversible crop damage, targeting a specific farm or an entire region – which from a global perspective, could cut off food to populations, dictate new market realities, or even spread disease.

ICS attack strategies could be adopted by smart city attackers

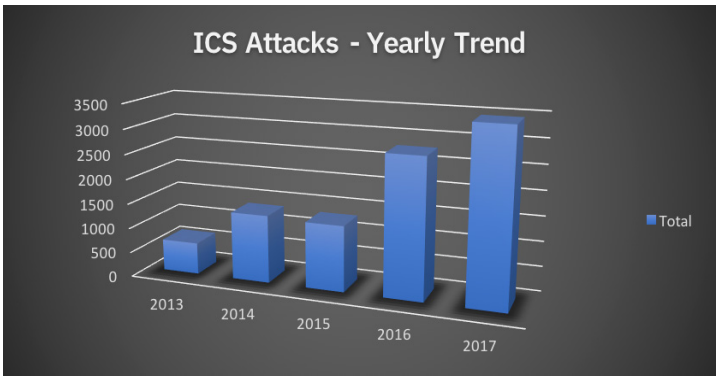
Industrial control systems (ICS) have long been favored targets for hackers. Malware that is designed to infect ICS technology is evolving rapidly, becoming more capable of inflicting damage on critical systems that run power plants and utilities. It's highly likely that attackers will use the same tools and strategies on smart city sensors and controls that they've used on ICS.

Figure 1. Top ICS attack signatures

Data from IBM intrusion prevention systems shows the prevalence of ICS attacks. As seen in Figure 1, password brute-force and buffer overflow attacks are the most prevalent type of ICS attack signatures in 2018 to date.

Figure 2. Attacks on the rise

As seen in Figure 2, ICS attacks show a steady rise since 2013. As attackers realize they can use similar attacks to exploit vulnerabilities against smart city technology, we can expect to chart a growing number of attacks on these networks.



Part 6. What's the solution to the smart city hacking threat?

There's no easy way to patch a city, and this maps back to the fact that when it comes to device security, the responsibility is twofold: while it's the manufacturer's job to make sure that their products are built securely, it's the user's responsibility to make sure they are practicing good security hygiene. Further, there's a shared responsibility between the manufacturer and the user: with the former issuing software updates for security issues, and the latter actually applying those updates.

Even with that said, with the hundreds of thousands of connected devices deployed over many square miles – and from many vendors – city IT leaders can't easily patch or automatically update their sensor networks. Because of these factors, vulnerabilities can go undiscovered for a long time, allowing hackers a foot in the door.

As smart cities grow, city leaders and smart city vendors need to prioritize security by re-examining the vendors' security protocols, building proper frameworks for these systems, and developing standard best practices for patching security flaws. Devices' default configurations are often weak enough to allow attackers to access the sensors by finding the default credentials or hard-coded API keys. On the provider side, vendors should add network port restrictions and stronger password controls to ensure that the devices are accessible only by authorized users. In addition, vendors and city leaders should run frequent security tests and IP scans on devices and networks to provide additional protection against unauthorized access and manipulation.

Guidelines for city security personnel to secure smart cities

> Implement IP address restrictions for who can connect to the smart city devices, especially if networks rely on the public internet.

> Leverage basic application scanning tools that can help identify vulnerabilities.

> Use strong network security rules to prevent access to sensitive systems, as well as safer password practices.

> Disable unnecessary remote administration features and ports.

> Take advantage of security incident and event management tools to scan network activity and identify suspicious internet traffic.

> Hire ethical hackers to test systems, such as IBM X-Force Red. These teams are trained to "think like a hacker" and find flaws in systems before the bad guys do.

What steps will you take to protect your smart city from the bad guys?

About IBM X-Force Red

IBM X-Force Red, an autonomous group within IBM Security, is an elite squad of consultants who specialize in security testing almost anything in the world — from networks and applications to planes, trains and automobiles, and everything in between. X-Force Red team members are enthusiastic colleagues in the vulnerability research community and are available to help your organization in all aspects of offensive security.

For more information: http://ibm.biz/smartcities

To learn more about the IBM Security portfolio, please contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

To learn more about IBM X-Force Red, visit:
https://www.ibm.com/security/services/offensive-security-services

Follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog