JOURNAL REPORTS: TECHNOLOGY

How Hackers Could Break Into the Smart City

The more connected a city is, the more it may be vulnerable to cyberattacks. Here are some of the potential weak spots.

By James Rundle
Sept. 17, 2019 11:18 pm ET

Smart cities are coming. And you can be sure that hackers won't be very far behind.

We've already gotten a glimpse of that future, as cities across the globe start to use technology to connect their services and residents in ways that were science fiction just a few years ago. They are using sensors to collect data—about public utilities, traffic, garbage collecting, road conditions and much more—and then using that data to deliver services to more people and more efficiently.

RELATED

- Debate: Should Cities Ever Pay Ransom to Hackers?

But this rush to become a smart city has a major drawback: The more connected a city is, the more vulnerable it is to cyberattacks. Hackers have, in recent years, effectively held cities hostage through ransomware, sometimes crippling critical systems for months at a time. The damage can cost millions to repair, as Baltimore and Atlanta have discovered.

And this is just the beginning. As cities add connectivity to their streetlights, power grids, dams, transit lines and other services, they are adding more targets that have the potential to be hacked. What's more, as additional information on residents is collected, officials worry the resulting reams of data could attract nation-states or terrorists who could incorporate the data into physical and cyberwarfare campaigns.

JOURNAL REPORT

- Read more at WSJ.com/CybersecurityReport

MORE IN CYBERSECURITY

- The Greatest Hacking Movies Ever
- Getting People to Use Strong Passwords
- Make Your Phone More Private

"The reality of the situation, and the risk we have to manage, is that we're introducing new opportunities for malicious hackers to exploit devices that have previously required physical access. We're lowering the barriers to entry," says Dave Weinstein, former chief technology officer of the state of New Jersey and now chief security officer at the security firm Claroty Ltd.

What are the most vulnerable places in a smart city? And what are the threats hackers pose to them?

Here's a look at a handful of what cybersecurity experts say could be the most worrisome areas.

Sensors, data and privacy

Sensors are the building blocks of smart-city initiatives. Cities place them on traffic lights, garbage cans, street lamps and buildings to collect mountains of data—such as the level of pollution in the air, vehicle movements and the population of certain areas at different times of day.

These sensors transmit data back to collection stations, which can use the information to, say, identify and reduce sources of pollution, manage traffic flows and arrange garbage pickups.

Pretty smart stuff. Unfortunately, though, the technology itself is often not nearly as smart, and could be an open door for determined attackers, potentially allowing them to get into other city systems as well as hijack the data itself.

The potential for harm is pretty much endless. Hackers could, for instance, either create erroneous data or obscure real information about the integrity of bridges, divert emergency services to nonexistent floods, or corrupt information about air quality, instigating false alarms.

Charles Henderson, global head of International Business Machines Corp. 's offensive cybersecurity unit, X-Force Red, says his team has probed the weaknesses of urban technology.

In one case, they found 17 major vulnerabilities in a sensor that had been deployed in their client's city. That was just from examining the software that runs the sensors, without having one of the sensors physically in their possession. "We just downloaded the [software] from the [manufacturer's website] and started plowing through it, finding vulnerabilities," he says. "That's not good."

Then there is the data that these sensors are collecting. This data may be the biggest target for hackers looking to compromise smart-city systems. The amount of data that will be collected on

a city's residents, even just through traffic and pedestrian sensors, is enormous, says Michael Sherwood, director of innovation and technology for the city of Las Vegas. That leads to privacy concerns about personal information being tracked, which could be used to identify individuals and their locations. Hackers have shown an appetite for such information in the past, such as the 2015 breach of the U.S. Office of Personnel Management, which exposed the records of more than 20 million people.

PHOTO: PETER OUMANSKI

Energy and water-supply systems

Smart technologies allow for more efficient distribution of power and water in urban areas, particularly in regions that have a high daytime population, such as central business districts. Coupled with monitoring technologies, smart grids can divert power to areas of high demand, or lessen the supply in areas that don't need it while others do. Smart grids also allow power companies to know more precisely how much electricity a household uses over a given period.

Yet, malicious software could disable power plants, for instance, as was seen during the spread of the NotPetya malware in 2017 that struck Ukraine, before spreading throughout the world. More than 225,000 people were left without power.

The ubiquity of smart meters also means that the possible points of entry into the network number in the thousands.

An attacker who manages to compromise power systems would have free rein to cause havoc, such as diverting power away from a hospital, depriving fire departments of a local water supply during a blaze by diverting water from hydrants, or triggering a citywide blackout, warns research from the Securing Smart Cities initiative, which acts as a forum for experts from government, security firms and technology companies to research cybersecurity issues associated with smart-city development.

At a household level, compromised smart meters could start fires by overloading circuits, distort billing and, perhaps most ominously, allow access to other internet-connected devices within a house.

What's more, once a utility's system is attacked, it's hard to just turn it off and look for the problem.

When a city establishes internet-connected technology and comes to depend on it—such as hospitals that depend on smart grids—the city has to figure out a way to deal with an attack while keeping services running. That makes it crucial to plan for attacks ahead of time. "If you don't cover security from the very beginning, then it becomes very difficult to protect it," says Cesar Cerrudo, the founder of Securing Smart Cities.

Autonomous vehicles

Autonomous vehicles have the potential to transform the efficiency of public transport and other services. Plans drawn up for the proposed smart-city development in Toronto, for instance, by Alphabet Inc. 's Sidewalk Labs include a provision for driverless vehicles to deliver mail to homes after receiving it in a central depot.

But autonomous vehicles rely on a host of technologies that are susceptible to attack. That could mean everything from causing traffic nightmares to using cars as weapons. Terrorists have shown how manned vehicles can drive into busy streets, causing mass casualties.

That becomes even easier, and exponentially more dangerous, if a single hacker can take control of multiple driverless cars. Hackers could also could reroute vehicles carrying people targeted for abduction.

Specialists at hacker conferences have repeatedly demonstrated how the onboard systems of such vehicles can be compromised. In addition, they have shown how easily the AI technology that runs these vehicles can be fooled.

"You can strategically place little bits of tape on a stop sign that tricks an autonomous vehicle into misclassifying what it sees," says Darren Shou, vice president of strategy and research at security firm Symantec Corp. "Now it's not a stop sign, but a 45-miles-per-hour sign, and as a result, the car drives right through."

Waste management

Cities have long recognized the potential for smart technology to help alleviate waste-management issues. Garbage-collection sites that can transmit information about their capacity levels can save money by avoiding unnecessary pickups, improve living conditions, and check the spread of vermin and prevent public-health crises.

New York, for instance, has deployed hundreds of smart garbage bins from Bigbelly Inc. across the city; it also has converted a number of these into public Wi-Fi hot spots.

Again, though, the disruption of waste-management services can have severe repercussions, particularly if the connected technology includes the sewer system.

Hackers, for instance, could create public-health disasters by rerouting sewage disposal, or by overloading sections of the system.

One cautionary tale comes from Maroochy Shire, Australia, where a disgruntled ex-employee of the local council hacked into its sewage-management system dozens of times over two months in 2000.

More than 264,000 gallons of raw sewage was released into parks and rivers as a result, causing massive environmental damage.

Traffic-control systems

In addition to relieving the pressure of rush-hour traffic, cities see the potential benefits that smarter traffic-control systems can bring to first responders and law-enforcement activities. Traffic lights can be adjusted at a moment's notice, making it easier for city vehicles to get to an emergency.

But again, what the system gives, it can also take away.

Compromised traffic lights, in the wrong hands, could result in enormous fatalities. Imagine, for a second, a hacker who turns all traffic lights in the city green at the same time.

In 2018, researchers from the University of Michigan were able to mislead a system being tested by the U.S. Transportation Department by hacking into the data that passed between the system and the vehicle that was equipped to receive it, without touching the network at all. They were able to change traffic-light timing and switch all signals to red, which could create gridlock scenarios.

Prevention and remediation

So what can cities do to at least try to minimize the potential damage?

In addition to basic cyber hygiene, which includes encrypting data that is being sent over networks, cities also can make sure everything isn't on the same network.

Kevin Martin, program manager for Smart City PDX, Portland, Ore.'s urban-technology initiative, says its sensors are deliberately kept separate from the city's wider networks as much as possible, to prevent the sensors from being used as a point of attack.

Portland also anonymizes its data and destroys video footage it collects immediately after it is analyzed.

In New York, officials have set up a testing laboratory for Internet of Things devices and have run full examinations of more than a dozen devices to date, looking at both performance and

vulnerabilities. Geoff Brown, head of New York City Cyber Command and the city's chief information-security officer, says they aim to double the lab's capacity over the next two years.

"I think that the city has done technology, for years and years, exceptionally well," Mr. Brown says. "My organization's job is to keep New Yorkers safe, and I think that they shouldn't expect anything less than that as we embrace the future."

Mr. Rundle is a reporter on The Wall Street Journal's Pro Cybersecurity desk. He can be reached at james.rundle@wsj.com.
