Cyber attack: How easy is it to take out a smart city? By SamWong

New Scientist No. 3033, 8 August 2015

How vulnerable is your city?

WHEN is a smart city not so smart? With cities worldwide racing to adopt technologies that automate services such as traffic control and street lighting, many aren't doing enough to protect against cyberattacks.

That's according to security researchers who have hacked into countless pieces of city infrastructure, from ATMs to power grids, looking for weaknesses.

One such researcher is Cesar Cerrudo of security consultancy IOActive Labs, based in Seattle. Inspired by how hackers switched traffic lights at will in Die Hard 4.0, Cerrudo decided to see if he could do the same to a smart traffic control system in use around the world. He found that the devices didn't use any encryption or authentication, and he could feed fake data to their sensors from a drone flying overhead.

Cerrudo was so alarmed by his discovery that he joined with others to set up the Securing Smart Cities initiative, which plans to bring together governments, security firms and technology companies.

"The idea is to generate resources so cities can incorporate technology but at the same time make sure that technology is safe and securely implemented," he says. "What I saw in my research is that most city governments, when they evaluate technology, just focus on functionality."

How bad could a cyberattack on a city be? Unlike companies, which have a unified leadership and policies, cities are fractured into public and private organisations, making them much harder to defend against cyberattacks.

Hackers can target multiple layers, from breaking into officials' email accounts to tapping wires underneath drain covers in the street, to targeting your home.

"The complexity is really off the scale," says Greg Conti, director of the US Army Cyber Institute at West Point, New York. His research suggests that cities vary widely in terms of how prepared they are for possible attacks.

Medium-sized cities of about a million people occupy a "sweet spot", he says, with smaller cities under-resourced and larger ones too complex to manage.

Cerrudo thinks the worst-case scenario would be if hackers took out the power grid. Although not caused by malign intent, he points to the blackout that affected the north-east US in August 2003 as an example. Caused by a software bug, it resulted in 10 million people without power, and 10 deaths from fires and accidents.

Another approach would be to black out areas of a city by manipulating smart power meters. Cerrudo imagines a situation in which hackers take out the smart grid and demand a ransom in return for restoring power.

Water supplies are also targets. Last year, a Chinese hacking group was caught infiltrating a water control system for a US municipality. Luckily it wasn't a real control system, only a "honeypot" set up to lure hackers, but it shows that people are actively looking to exploit weaknesses.

How can we make smart cities safer? What's needed is a holistic approach to cybersecurity, says Conti. He believes cities should look to large companies for lessons in cyberdefence, and that city leaders should appoint a chief information security officer with appropriate resources. Conti and colleagues Tom Cross and David Raymond will brief others working in information security on the challenges faced by smart cities at the Black Hat conference in Las Vegas this week.

Another problem is that many companies selling technology to cities are new to the software business. While established software companies have good security mechanisms in place, manufacturers of some recent internet-connected devices have been reluctant to let Cerrudo and others test their products.

“They are producing devices that aren’t secure because they don’t have this knowledge,” he says.

Cerrudo says cities need to develop plans for responding to cyberattacks, just as they have plans for earthquakes and other natural disasters.

He also believes citizens should get more involved: security researchers can highlight weaknesses, but he thinks citizens have a responsibility to learn about threats and demand action from their officials. “People should start complaining to the government and companies so they start taking care of this,” he says. “If no one says anything, nothing will change.”

For now, Cerrudo is confident that researchers are ahead of the bad guys. Conti is less sure.

“If you look at the low end where you’ve got individuals doing things with significant effects, what could larger, more capable organisations do?” he says.