After the pandemic: securing smart cities

Kevin Curran

Kevin Curran, Ulster University

Covid-19 has forced us all to rethink the way we live, work and socialise, with technology proving how vital it has become to cities and how have they responded to the pandemic. Indeed, innovations such as the Internet of Things (IoT), 5G and location-based services have been used to help minimise the risk of transmission, maintain social distancing measures and ensure the continuation of vital services.

According to Capgemini's 'Fast-forward to the future: defining and winning the post-Covid new normal' 2020 report, the pandemic has "cemented technology's role at the heart of transformation, driving new ways of interaction, sharing, engaging, and decision making".[1] Undoubtedly, these technologies will play a major role in the UK's 'Build Back Better' recovery strategy as local councils and political leaders are now taking "inclusive measures to pair economic revival with environmental sustainability, urban mobility and energy efficiency".[2]

"Smart city technologies, when deployed correctly, can be implemented at scale, allowing growing populations to be serviced more far more easily"

Governments around the world will now be looking to deploy new technologies and innovations at scale within a city's ecosystem as society begins to return to 'normal', whatever that may be. This includes a mixture of residential, industrial, commercial, retail and public sector bodies alongside greenways, parks and the public realm.

Ultimately, governments are aiming to transform the delivery of public services through a citizen-centric approach, resulting in greater efficiencies and more responsive services that can drive inclusive growth. For example, the City of London Corporation is currently reviewing its long-term strategy and planning policies – not only to account for flexible working practices but also push for the adoption of new smart city technology and renewable energy networks, including making 5G and broadband readily available for business across the centre of London.[3]

What is a 'smart city'?

A 'smart city' fundamentally relies on IoT to deliver all vital public services. These include addressing problems with clean water, air pollution, traffic and landfill waste. Sensor-enabled devices can help monitor the environmental impact of cities and collect details about sewers, air quality and garbage. Smart city technologies, when deployed correctly, can be implemented at scale, allowing growing populations to be serviced more far more easily.

While a true smart city is designed from the ground up, many cities are now integrating technologies that operate over IoT to improve public services. Some argue that the future growth of the planet's population can only be sustained through scalable smart city technology. One area, of course, is traffic management, which can be improved using smart traffic lights, road-implanted sensors and even communications with future 'smart-cars'.

Sensor-enabled IoT devices deployed in smart cities can also help to monitor the environmental impact of cities, collecting details about sewers, air quality, rubbish and energy consumption. Connected technologies can also be used to increase awareness and visibility into individual energy and resource use. IoT-enabled thermostats can make transparent decisions to turn heating on, based on fluctuating energy costs. Moreover, smart IoT water management sensors, in combination with data analytics programmes, can provide consumers with increased visibility into the amount of water they use. Devices such as smart meters that increase visibility into usage have been proven to save money, as well as conserve natural resources.

However, one must remember that smart eco cities are basically cities that fundamentally attempt to integrate technology to achieve efficiencies in a multitude of domains. Other examples of integrating technology into cities are smart lighting, which only turns on in conjunction with nearby traffic or pedestrians; rubbish bins that alert when they need to be emptied; water sprinklers that autonomously test the soil conditions and turn on watering as required; and smart meters which remove the need for humans to check.

Increased connectivity

In the future, we will also require smart cars to become more integrated with national intelligent transport infrastructures to ensure that vehicles can operate safely and efficiently. Satellite navigation and traffic signal control systems will ensure that vehicles know when to stop, slow down and speed up as well as identify hazards in good time. This communication will result in better traffic management and significantly reduce the number of accidents. Ultimately, the roads beneath us will communicate with smart cars, most likely through indestructible sensors embedded within the road.

In fact, with smart technology, it is now possible to access live data, allowing real-time reporting of a structure's condition, enabling managers to remotely monitor and predict routine and emergency maintenance. A key sensor can be worth a thousand visits by an inspection engineer, as it can alert to different patterns of frequency

and life. For instance, consider basic city-level infrastructure in a location that is regularly affected by extreme weather.

When it comes to bridges, crucial road links and mainland connections, upkeep needs to be carefully monitored in order to keep a city running smoothly and safely. Wireless IoT bridge sensors can keep track of all aspects of a bridge's health, collecting data in areas such as vibration, pressure, humidity and temperature. This data can be used to predict early signs of damage and deterioration, as well as monitor overall traffic volume.

Not without risks

However, increased connectivity between vehicles and wider national infrastructure is not without its risks. Modern vehicles have evolved to contain a complex network of as many as 100 independent computers, or electronic control units (ECUs). ECUs perform a variety of functions such as measuring the oxygen present in exhaust fumes and adjusting the fuel or oxygen mixture, improving efficiency and reducing pollutants. Gradually these ECUs have become integrated into nearly every aspect of a vehicle's functioning, including steering, cruise control, air bag deployment and braking.

As electronics and related code become more integrated into modern vehicles, we are reaching a point where they will require similar protection to that of smartphones, tablets and traditional computers. There is a real worry about hackers controlling vehicles in different scenarios, from downloading rogue apps, to disabling the vehicle's ignition or potentially overriding braking systems. The universal controller area network (CAN) bus on vehicles makes such breaches possible. Important aspects such as the speed control, steering and brakes are all located on a separate vehicle network, but there is still interconnectivity between both vehicle network backbones so that a breach in one can cause havoc in the other. It is still proving to be a rather difficult system to breach, but as more and more exploits get shared on the Internet, there is much cause for concern. As vehicles become more integrated into wider networks, there could be serious consequences.

Critical services exposed

Smart cities are inevitable but the introduction of advanced technologies into the fabric of a city comes with varying risks. Relying on a central technological hub to control an infrastructure can allow hackers to target a city more easily than ever before and a smart city is only as secure as its weakest part – and, increasingly, we are finding that this is an IoT device. Any part of a smart city infrastructure could be compromised – for instance, the street light system could potentially be targeted in a denial-of-service attack, leading to widespread blackouts.

Training of those who install IoT devices – such as gas engineers and plumbers – was outlined in an earlier UK Government report on the Internet of Things, which focuses on security by design.[4] In this, leaders have proposed for the first time in the UK that providers should have to undergo mandatory cyber security training to prevent smart devices from being exploited by criminals or state-sponsored attackers. This can be done by having security professionals work more closely with industry bodies to embed IoT training as standard.

Ransomware attacks

Ransomware presents a continuous challenge and attacks are growing more sophisticated by the day. In fact, recently it has led to serious disruptions to vital services – as we saw earlier this year, with the ransomware attack by the group DarkSide, on the fuel pipeline carrying 50% of fuel in North America. Consider how an attack would affect our wider traffic or energy infrastructure. If other IoT innovations are further integrated, there will be an endless number of endpoints which nefarious actors can use to their advantage – and a single loophole could be catastrophic.

Ryuk ransomware is possibly the best example, due to its widespread popularity. It is a very sophisticated ransomware threat that has been targeting hospitals, government institutions, businesses and other organisations for the past five years. The group behind the malware is known for using manual hacking techniques and open-source tools to move laterally through private networks and gain administrative access to as many systems as possible before initiating the file encryption.

Some attackers have adopted a 'radio silence' technique, through a sophisticated monitoring of system processes, where malware knows when to stay silent or lie dormant. There are in fact some really impressive 'stealth mode' techniques adopted by malware to evade detection. Techniques include frequently checking AV results and changing versions and builds on all infected servers when any traces of detection appear, in addition to monitoring memory consumption to prevent common server administration utilities from detecting the ransomware processes.

Adept measures

It is essential to deploy connected devices with sufficient security policies such as firewalls and intrusion detection and prevention systems. It's also important to ensure there is confidentiality of customers' data with encryption, strong passwords and certificate-based authentication across all devices. Device management agents can highlight failed access attempts and attempted denial-of-service attacks. To ensure the city is as safe as possible, all non-IoT devices must also be patched and kept malware free.

As indicated in earlier government reports, in order to prevent smart devices from being exploited by criminals or state-sponsored attackers, security professionals should work closely with industry bodies to embed IoT training as standard for engineers who install any connected devices. In fact, in the future, these engineers will have to understand the inherent risks of any given IoT device if they are planning on applying it to a wider public network.

City planners will also need to consider the public's own cyber security awareness. In a recent survey conducted by the World Economic Forum (WEF), safety and security, and privacy and trust likely pose the greatest levels of risk, especially in the consumer IoT domain.[5]

Users are often unaware of the responsibility IoT manufacturers and service providers bear in order to mitigate privacy

risks, and the regulations that they have to meet with, with regard to how personal data is collected. However, users often lack the awareness and experience needed to properly manage their own exposure to IoT security risks. If more and more devices are added to city infrastructures and linked to vital public networks, including consumer IoT products, the public needs to have an understanding of the risks involved, and how we all have a part to play to mitigate any potential threats or unnecessary risks.

Plentiful risks

While the benefits of smart cities and further connectivity are plain to see – from more-efficient distribution of resources, improved road traffic management and safety, and reducing our carbon footprint, the cyber security risks are plentiful.

Industry and governments are working hard to respond to potential privacy threats: however, the road ahead will be challenging. Mapping a secure online or digital environment of this magnitude, with a multitude of endpoints will be tricky, and no project of this size has ever been completed before. Hackers and other nefarious actors will test its limits.

About the author

Kevin Curran is a professor of cyber security at Ulster University and an IEEE senior member. As executive co-director of the Legal Innovation Centre and group leader for the Cyber Security and Web Technologies Research Group, he has made significant contributions to advancing the knowledge of computer networking and systems, evidenced by more than 800 published works. Regarded as one of the top cyber security experts within the UK, he regularly comments on the latest technological developments and cyberthreats, including the Internet of Things (IoT) and smart devices, crypto-currency, phishing-attacks and ransomware.

References

1. 'Fast Forward to the Future'. CapGemini. Accessed Nov 2021. www.capgemini.com/gb-en/research/fast-forward-to-the-future/.
2. 'Smart City Index 2020'. IMD. Accessed Nov 2021. www.imd.org/globalassets/wcc/docs/smart_city/smartcityindex_2020.pdf.
3. 'City of London sets out five year post-pandemic recovery plan'. Financial Times (payw-all). Accessed Nov 2021. www.ft.com/content/91c887fc-29ef-472f-8e3f-22cb7d21573a.
4. 'The Internet of Things: making the most of the Second Digital Revolution'. UK Government Office for Science. Accessed Nov 2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf.
5. 'State of the Connected World'. World Economic Forum, Dec 2020. Accessed Nov 2021. www3.weforum.org/docs/WEF_The_State_of_the_Connected_World_2020.pdf.

Smart plugs invite cyber criminals into the home


Richard Hughes

Richard Hughes, A&O IT Group

The Internet of Things (IoT) is one of the fastest-growing technology markets and has steadily picked up steam in recent years as technology improves and price points drop, with the global IoT market forecast to reach revenues of $1.1tr by 2024.[1] Fields including manufacturing, healthcare and transport have benefited hugely from the ability to create linked networks of smart devices, facilitating a growing level of operational automation and visibility.

The consumer IoT market has also grown rapidly and saw a further boost during the pandemic. Research commissioned by the UK Government found that almost half of consumers had bought at least one connected device over the course of the pandemic, including smart watches, TVs and cameras.[2] However, while the flourishing market means more choice and competitive prices for enterprises and consumers alike, it has also contributed to the large number of devices that skip out on security in favour of low costs.

The market has long been overflowing with devices that lack basic security capabilities such as data encryption, or designs that make it difficult for users to carry out standard activity such as changing default passwords or applying updates. As a result, multiple regions are seeking to introduce legislation that will improve the security of connected devices, with the UK's Department for Digital, Culture, Media & Sport recently announcing plans for laws that will ban weak default passwords and make it mandatory for smart device manufacturers to alert users when they will cease to receive security updates.[3]

In the meantime, however, consumers must be aware of the potential risks of any new connected device they introduce into their network, particularly lower-cost items.

An innocuous threat

To highlight the threat posed by poorly secured IoT devices, we decided to investigate the smart plug – a widely available item that can be cheaply purchased to grant some IoT capabilities to non-smart devices. The plugs can be remotely controlled to provide a simple way of switching ordinary devices on and off.