Control Risks

SMART CITIES AND CYBER THREATS

Nicolas Reys, Consultant, Cyber Security Services

Control Risks' Cyber Security Services provide threat intelligence, protection and response in the face of a continually evolving cyber threat landscape.

- Smart cities will provide businesses with unprecedented economic opportunities. However, cyber threat actors will be presented with an unprecedented attack surface in smart cities because of the significant increase in the number of interconnected devices.
- Securing these cities needs to be a joint project involving the local administrations and the private sector organisations with an immediate stake in the continuation of the city's stable function.
- Ensuring that these cities are cyber secure will require the identification and prioritisation of critical assets, behaviour based security – establishing a benchmark of normal operation of critical assets and continuously ensuring that all parts of the city adhere to said benchmark, rapid component replacement in the event of compromise or failure and the secure segmentation of critical private assets from the city network.

Faced with rapid urbanisation, city planners are turning to technology to solve a wide range of problems associated with modern cities. Smart cities are the outcome of this deepening integration of technology with new or existing urban landscapes. They are set to change how we experience and what we come to expect from the cities around us. In practical terms, these transformative effects will arise from the combination of three pieces of technology: inexpensive logic controllers, millions of sensors connected to devices dispersed across a city and a network that connects all of these nodes together and enables real-time communication.

Such connectivity will enable a better and more efficient provision of urban services. Amsterdam, Barcelona, Santa Cruz and Stockholm have begun the process of incorporating elements of a "smart grid" – or a network of interconnected sensors within the city – across many of their urban domains such as energy provisions, transport systems and telecommunications infrastructure. The inhabitants of these cities have already begun to feel the benefits. However, increased connectivity carries with it potentially severe cyber security risks that have yet to be fully revealed and, in many cases, mitigated.

HOW SMART IS SMART?

The concept of smart cities relies on three fundamental ideas:

1. Physical infrastructure can be used more efficiently as data analytics and artificial intelligence progress.
2. Engagement of the urban population with the city administration can be achieved through e-participation – or the carrying out of civic duties through the internet.
3. As technology continues to progress, computer systems will learn and adapt to challenges autonomously.

The benefits of and opportunities presented by smart cities - for both citizens and businesses - are broad-ranging. With proper implementation, smart cities will provide tremendous economic, social and cultural advantages for their inhabitants. For instance, a city's electricity infrastructure could be significantly improved with the introduction of technologies such as 'smart meters' – electric or gas meters that provide real-time data, via an internet connection, to the consumer and the electricity company regarding each user's consumption. This allows better management of electricity supplies by tailoring them to the live demand, thereby reducing overall cost as well as the impact and incidence of power outages.

Indeed, smart cities are dependent on machine-to-machine (M2M) interactions and decision-making. This is, in part, a product of the sheer number of inputs and the frequency and speed with which associated calculations need to be completed. In the case of the energy grid, it would be impossible for a human operator to process all the data necessary to make decisions at the speed required by the system. However, while M2M decision-making (M2MD) is an unavoidable and beneficial feature of smart cities, it is also one of the greatest risks.

NEW CITY, NEW RISK

M2MD is a highly promising means of ensuring efficient automation across smart cities. However, given the absence of human operators, the risk of a cascading error is significant. A cascading error refers to the potential for a small, unchecked mistake to spread through a system and become a systemic risk. For instance, if a minor computing error caused a smart electricity reader to transmit inaccurate data readings to its control centre for a period of time this could lead to an automated, and mistaken, assessment that a particular private organisation's premises required an increased amount of electricity. This would necessitate rerouting some of the existing energy supply to this facility which, in turn, could culminate in increased costs for the affected business, as well as for the city, and a reduced pool of electricity for other companies and citizens. Although minimal at this scale, the consequences of such errors when they affect a larger area – an entire block or an industrial zone for example – could be far more substantial.

SMART CITIES AND CYBER THREATS

Beyond the potential for human or computer error, smart cities will provide cyber threat actors with a large attack surface to target and potentially exploit and incorporate into broader campaigns:

Cybercriminals

As we have described above, smart cities will be composed of thousands – if not millions – of interconnected devices. Such a structure is a boon to criminal actors able to create or purchase and subsequently deploy self-propagating malware, variants of which have been known to proliferate across multiple connected networks. These 'worms' could be used to acquire easily commoditised information such as healthcare information, social security numbers and banking credentials, or even to take control of a significant number of systems.

Were attackers able to successfully hijack these systems they could then be used for extremely powerful distributed denial of service (DDoS) attacks or to hold an entire city for ransom in extortion attacks. Ransomware variants could be designed to encrypt and cripple an entire city's grid, with ransom demands likely to be considerable in such a scenario. These tactics could be highly profitable for cybercriminals and represent a natural evolution of trends that we have observed in the current cybercriminal community. Incident response will become increasingly difficult in the case of city-wide compromise. Private sector organisations and municipal authorities will share ownership of systems and the responsibility for their security. Beyond adding legal and financial costs for the private sector, this will create the need for highly complex pre-planned incident response schemes involving multiple parties.

Cyber activists

As cyber activist groups grow increasingly capable and in some cases, more radical, smart cities will provide them with an attack surface enabling a broad range of attacks from those akin to nuisances such as defacements of a city's billboards, to the more extreme targeting of a smart city's energy grid with the aim of physical destruction.

In addition, many cyber activist groups are supporting physical protesters by launching cyber attacks. This practice in a smart city environment could allow cyber activists to take a leading role in coercing governments and private sector organisations in meeting their demands.

The potential destructiveness of a cyber attack on smart cities is such that even the threat of compromise of the city's system is likely to be treated by governments and businesses as an existential one. When threat actors such as cyber activists, who arguably lack the self-control of other groups, have the possibility of causing serious physical damages, the security of smart cities becomes essential to the cities' survival.

Nation states

As the underlying network of smart cities will encompass most aspects of life within the city, if that network were to be compromised by an attacker, it would grant them unfettered access to a target individual or organisation. For instance, state-owned competitors could compromise a smart city's infrastructure to gather intelligence on a large number of rival private sector firms. This information could include movements of their executives within the city, private and commercial communications grabbed from the ubiquitous presence of 'free Wi-Fi hotspots' managed by the city, and many more. Moreover, organisations operating within the city are likely to have their networks overlap to some extent with the city's own network, or at the very least, have frequent data transfers from their networks to that of the city. This would enable highly advanced threat actors such as nation states to exploit weaknesses within a city's infrastructure to reach a target organisation and compromise the confidentiality of its network.

Beyond traditional espionage operations, the large-scale destruction or disruption of physical infrastructure via computer systems could become a technical reality with the advent of smart cities. The interconnectedness of systems within smart cities will lead to the

reliance of components on the availability of the entire system to function properly. As such, an advanced cyber attack seeking to destroy parts of the system could have catastrophic cascading effects onto the wider network. This would enable a determined nation state actor to cause large-scale physical destruction throughout an entire city.

Although indirect, a belligerent nation state actor could abruptly interrupt the traffic light system of an entire city to cause significant damages and potentially the loss of human lives. Similar scenarios are conceivable for the interruption of energy supplies or water networks. Whilst such events will become more plausible with the increase in smart cities, the actual likelihood of them being undertaken is low because of the possibility that such an attack would provide a potentially justifiable basis – legally and ethically – for military retaliation, something which the perpetrator would presumably appreciate.

SECURING THE IMPLEMENTATION OF SMART CITIES FOR THE PRIVATE SECTOR

Although the exact form that smart cities will eventually take remains uncertain, organisations and city planners can take a number of precautions to ensure a smoother implementation process and, ultimately, more secure infrastructure.

Prioritise the security of critical assets:

Contemporary networks are already impossible to protect in their entirety, a problem which will apply equally to smart cities. Some components of the system will have to be made more secure than others. Public and private sector organisations will need to work together to identify the city's critical assets and oversee the institution of appropriate security measures.

Behaviour based security:

Auditing millions of separate devices for signs of malware is simply not feasible. A more workable approach would be to evaluate the behaviour of smart city components and systems against an established baseline of normal functionality or network behaviour. Any significant deviation from the norm – above a determined threshold – would trigger an investigation into the possible presence of malware on the subcomponents.

Rapid component replacement:

Given the potential for component failure or attacks compromising these components, an automated replacement system will enhance the security of the whole system. Although difficult to apply to critical components without full redundancy, such measures would be suitable for low-level, relatively isolated components.

Segment critical assets of private organisations from the city's network:

Paramount to the security of organisations in the smart city environment is the segmentation of their critical assets from the city's network. Although costly and potentially reducing the effectiveness of the organisations, this policy will enable organisations to contain and mitigate any threat actors exploiting vulnerabilities in the smart city network to reach their assets.

For more information or to schedule a discussion with our experts, please contact us at:

enquiries@controlrisks.com