Threat of Cyber Attacks in Smart Cities

–Inderjeet Singh Barara,
Chief Cyber security Officer, Vara Technology, inderjit.barara@gmail.com

Smart cities are the outcome of integration of technologies with new or existing urban landscapes. There is going to be a paradigm shift of what we experience and what we come to expect from the cities around us. **"Smart Cities"** would bridge *cyber-physical technologies and infrastructure for improving the overall quality of life*. In times to come, smart cities will provide businesses efficiency and unprecedented economic opportunities. In effect, these transformations of today's cities into smart cities will be an amalgamation of two major technologies – millions of **Internet of Things (IoT) devices** dispersed across a city and **Network** that connects all of these nodes together and enables real-time communication. By year 2020, there will be more than ***50 Billion Internet-connected devices*** that will transform the way we live and work.

Cities are becoming smarter by deploying newer technologies, such as:

- Smart Traffic Control.
- Smart Parking Application.
- Smart Street Lights.
- Smart Surveillance Network:
- Smart Public Transportation.
- Smart Energy Management.
- Smart Water Management.
- Smart Waste Management.

Vulnerabilities of Smart Cities

Every new technology also brings new Risks and Vulnerabilities and so is Internet of Things. Risks and vulnerabilities of Internet of Things (IoT) Devices would impact the city administration, residents, businesses and other organizations alike. Internet of Things (IoT) based Smart devices are the enabler for effectively converting the exiting city to be a smart city. These are extensively utilized in traffic and surveillance cameras, meters, street lights, traffic lights, smart pipes and sensors are easy to implement and at the same time are even easier to hack due to ***lack of stringent security measures and insecure encryption mechanisms***. This is a major point of concern as smart cities are implementing newer technologies at a very fast pace without testing them for cyber threats and its vulnerabilities.

As the cities become smarter, consider as to what could happen if one or more technology-reliant services fails to work.

- What would commuting look like with non-functioning traffic control systems, no streetlights, and no public transportation?
- How would citizens respond to an inadequate supply of electricity or water, or to dark streets, and no cameras?
- What if garbage collection is interrupted during the summer time and the smell of refuse stinks up the streets?

To anybody's guess that it would be unpleasant and probably cause a lot of chaos in any city. When prolonged, interruptions to sanitation services or other basic services, goes beyond unpleasant odours and inconvenience, it does not take long before these issues create major concerns.

In case, if a cyber-attack on smart cities causes an inadequate supply of electricity or water or tripping of complete electricity grid, dark streets, or/and no cameras and the hackers asking for Ransom to restore the services. ***Then how would citizens respond to it?***

Cyber Threats and vulnerabilities will be presented with an unprecedented attack surface in smart cities due to the significant increase in number of inter-connected IoT devices. *Smart IoT devices create huge potential for cyber-attacks due to numerous vulnerabilities, making smart cities more vulnerable than today's computers and smartphones. People residing in smart cities might face a panic attack when they are* ***made slaves of their "cyber masters/criminals for***

Ransom." This scenario might not be as unlikely as you think. Problems in cyber security could trigger anytime causing devastating effects.

Cyber Attacks on Smart Cities

Simple bugs can cause big problems and have big impact, Whether it's a water dam in Rye Brook or power grids, financial institutions, water systems or online networks, all these infrastructures are going to be at risk and would be under assault like never before, and we need to do more about it. Recently, a police department in Massachusetts paid $750 to get its files back after being hit by the ransomware. In February 2016, California's Hollywood Presbyterian Medical Center paid a ransom of about $17,000 in Bitcoins, one of at least six major health care systems victimized so far this year. In Mar 2016, the city of Plainfield, New Jersey, faced a demand for about $700 in Bitcoins to unfreeze their municipal servers.In addition, the recent attack of Wannacry and PetyaRansomwere. Technologies used by smart cities would pose a major cyber security threat and open the door for several possible cyber-attacks. Each Smart City creates a new opportunity for cyber attackers. Some of the key technologies and systems that together make up the smart city's complex attack surface are:

Traffic Control Systems. Traffic control systems could be easily hacked as some of the devices used are without any encryption for communication between traffic control systems and traffic lights, traffic controllers, and so on, allowing an attacker to directly change traffic lights.

- **Smart Street Lighting Systems**. Wireless street lighting systems are being deployed in many cities around the world use wireless communications and have the encryption related problems. Attacks on smart street lighting systems are not complex and can have big impact by causing street blackouts in large areas.
- **City Management Systems.** Every city has hundreds of systems to manage different services and tasks. Hacking these systems would give an attacker many options to cause harm. Just as simple software bugs can create significant harm, manipulating simple information could also have a seemingly oversized security effect.
- **Cloud and SaaS Solutions**. City servers and cloud infrastructure are exposed to DDoS attacks. Servers and cloud infrastructure are cheaper targets for cybercriminals or cyber terrorists.
- **Smart Power and Water Grid.** Attacks on a smart grid and water could be devastating, causing millions of dollars in losses and even loss of life.
- **Public Transportation**. Just by displaying incorrect information by manipulating public transportation information systems, it's possible to influence people's behaviour to cause delays, overcrowding, and so on
- **Surveillance Cameras**. Traffic and surveillance cameras are the eyes of any city and by attacking them, attackers can make the city blind. DDoS attacks on these have long-term damaging effects.
- **Location-based Services**. Location-based Services which extensively use GPS, spoofing and other attacks are possible. People get real-time location information, and if the location is wrong, in that case people will make decisions based on incorrect information. The nature of the impact depends on the extent to which a city relies on the services affected.

Challenges in Implementation of Cyber Security

Cyber war scenarios make cities technologies an important and interesting target. Cyber-attacks will target city services and infrastructure. Cyber-threats are expanding in every way from attack frequency to scale, sophistication and impact severity. Present day Virus and Malware with Machine Learning and Artificial Intelligence is also on the rise. There are large number of challenges in ensuring cyber security while implementing smart cities such as:

- Lack of Cyber Security Testing
- Encryption Issues of IoT Devices and Network Components
- Lack of Computer Emergency Response Teams
- Patch Management Issues
- Insecure Legacy Systems
- Lack of Cyber Attack Emergency Plans
- Susceptibility to Denial of Service
- Proliferation of "Smart" Devices or The Internet of Things
- Lack of Security Life Cycle Management.

Securing Against Cyber Attacks

Ensuring that smart cities are cyber secure against cyber-attacks will require the identification and prioritization of critical infrastructure and assets, behavior based security. Establishing a benchmark of normal operations of all the critical infrastructures/ assets and continuously ensuring that all parts of the city adhere to said benchmark. Businesses operating public or private infrastructures that want to enhance cyber-security against Ransomware can started by:

- Adopt or create a Cybersecurity Framework.
- Explicit policies from selection of systems, procurement of systems, management of systems, and who accesses systems to the manner in which technology is disposed of securely once it has reached the end of its service life.
- Create a simple checklist-type cyber security review. Check for proper encryption, authentication, and authorization and make sure the systems can be easily updated
- Applying application white listing to prevent unauthorized applications from running
- Enabling a USB lockdown on all SCADA environments to stop malware from physically entering the environment
- Proactively monitor networks for unusual traffic, access logs, or requests that could indicate an attack in progress.
- Create specific city CERTs that can deal with cyber security incidents, vulnerability reporting and patching, coordination, information sharing, and so on.
- Regularly run penetration tests on all city systems and networks.

Current attack surface for smart cities is unimaginably vast open to attack. This is a real and immediate danger. The more technology a city uses, more vulnerable it would be to cyberattacks. Therefore, the smartest cities have the highest risks. It is only a matter of time until attacks on city services and infrastructure happen. It may be ongoing or could happen at any moment in the future. Actions must be taken now to make cities more secure and protect against cyber-attacks. ■

Colonel Inderjeet Singh is the Chief Cyber Security Officer and Head of the Cyber Security Center of Excellence at Vara Technology. In this role he is instrumental in building the Cyber Security Business Unit for the Group. He is working on the disruptive technologies in the Cyber Security Space for securing IT networks, Smart cities and Critical Information Infrastructure.

He served in the Indian Defence Forces, is Alumnus of IIT Kharagpur and Symbiosis Institute of Management. He is an experienced Information Systems professional with experience of more than 27+ year across wide spectrum of areas spanning Information Security ,Risk Management, Cyber Security, Cyber Forensics, Cyber Warfare, Cyber Terrorism, Expertise in SOC and CERT, Internet of Things (IoT) including IoT Security, Blockchain and Cryptonomics, Machine Learning and Artificial Intelligence and Smart Cities.

He has held prestigious appointments while in Indian Army and has been CIO of E-Commerce Company. He has also served in United Nation Mission in Democratic Republic of Congo.

He is visionary for Start-Up Incubation, Entrepreneurship Development, Strategic Consulting and New Technology Evaluation for commercial viability. He is a Subject Matter Expert on latest innovative Technological domains and effectively managed mission critical projects

He has consistently delivered mission-critical results in the field of in Information Security Management, Cyber Security, Cyber Warfare and Cyber Risk Management.

He is a Council Member of CET (I) and fellow of IETE, IE, Member CSI and Executive Council Member Society for Data Science, Founder of Cyber Watch India, Member ISACA, IEE, ISOC, IoT4SCTF, CCICI, IETF, USI and many other professional bodies.

He has been consistently been awarded while in Army and was awarded “Magnificent CIO of the Year “Award in year 2016.