NIELIT, Gorakhpur

Course Name: A-level (1st Sem.) **Subject: IoT**

Topic: Security in IoT **Date: 12.05.2020**

What is the Need to Secure the Internet of Things?

The Internet of Things (IoT) has become a widely used term to describe the billions of physical devices connected to each other via internet and have sensing or actuation capabilities . Presence of IoT is found everywhere in our day to day life like fitness bands, smart home appliances which can be controlled from anywhere in the world, Medical devices for disabled and old persons, automobile sector is also using it and Smart City development etc., So from here it can be seen that every sector is touched somehow to IoT . Security of these devices is now come under high priority. It's time to go not only for Internet of Things but for Internet of *Secure* Things.

Every day we heard about hacking of devices and systems to obtain information and data. However, just as critical are cyber-attacks against the devices themselves - attacks which take over control of the device and cause them to operate in dangerous and insecure ways.

Unfortunately these systems – thought to be safe – are still vulnerable to cyber threat . Industrial Automation, Smart city and Critical Infrastructure devices are usually installed inside the secure perimeter of an enterprise network, that perimeter is porous and can be easily penetrated or disabled.

It is necessary to secure the Things themselves.

Security Challenges

The Internet of Things is consisting of a diverse range of physical device types- from small to large, from simple to complex – from consumer gadgets to sophisticated systems, utility and industrial/manufacturing systems.

Now part of the expanding web connected network – Internet of Things, embedded devices are very different from standard PCs or other consumer devices. Automation in industrial sector is design to perform fixed task or specialized task.   Installing new software on the system in the field either requires a specialized upgrade process or is simply not supported. In most cases, these devices are optimized to minimize processing cycles and memory usage and do not have extra processing resources available to support traditional security mechanisms.

As a result, standard PC security solutions won't solve the challenges of embedded devices. In fact, given the specialized nature of embedded systems, PC security solutions won't even run on most embedded devices.

Use of multiple layers of protection is the driving principle for enterprise security. It includes firewalls, authentication/encryption, security protocols and intrusion detection/intrusion prevention systems. These are well established and proven security principles. Despite this, firewalls are virtually absent in embedded systems, instead relying on simple password authentication and security protocols. This is based on assumptions that embedded devices are not attractive targets to hackers, embedded devices are not vulnerable to attacks, or authentication and encryption provide adequate protection for embedded devices. These assumptions are no longer valid; the number and sophistication of attacks against embedded devices continues to rise and greater security measures are needed.

For over 25 years, cybersecurity has been a critical focus for large enterprises, whereas it has only recently become a focus for most engineers building embedded computing devices. “Experience is the best teacher, but the tuition is high”, or so goes the saying. Rather than learn all the lessons by experience, embedded engineers can take a page from the enterprise security playbook.

What are the challenges for implementing the Internet of Secure Things and assuring security of embedded devices? The specialized nature of these devices presents the following challenges:

1. Critical functionality: In addition to devices, systems and appliances in a home, embedded devices also are found controlling the world’s transportation infrastructure, the utility grids, communication systems and many other capabilities relied upon by modern society.Interruption of these capabilities by a cyber-attack could have catastrophic consequences.

2. Replication: Once designed and built, embedded devices are mass produced. There may be thousands to millions of identical devices. If a hacker is able to build a successful attack against one of these devices, the attack can be replicated across all devices.

3. Security assumptions: Many embedded engineers have long assumed that embedded devices are not targets for hackers.These assumptions are based on outdated assumptions including the belief in security by obscurity. As a result, security is often not considered a critical priority for embedded designs. Today’s embedded design projects are often including security for the first time and do not have experience and previous security projects to build upon.

4. Not easily patched: Most embedded devices are not easily upgraded.Once they are deployed, they will run the software that was installed at the factory. Any remote software update capability needs to be designed into the device to allow security updates. The specialized operating systems used to build embedded devices may not have automated capabilities that allow easy updates of the device firmware to ensure security capabilities are frequently updated. The device itself may not have the IO or required storage that allows for updating to fight off security attacks.

5. Long life cycle: The life cycle for embedded devices is typically much longer than for PCs or consumer devices.Devices may be in the field for 15 or even 20 years.Building a device today that will stand up to the ever evolving security requirements of the next two decades is a tremendous challenge.

6. Proprietary/industry specific protocols: Embedded devices often use specialized protocols that are not recognized and protected by enterprise security tools.Enterprise firewalls and intrusion detection system are designed to protect against enterprise specific threats, not attacks against industrial protocols.

7. Deployed outside of enterprise security perimeter: Many embedded devices are mobile or are deployed in the field.As a result, these devices may be directly connected to the Internet with none of the protections found in a corporate environment.