**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | 9 July 2020 | **Name:** | Anupama J S |
| **Course:** | Cisco certification:IOT | **USN:** | 4AL16EC005 |
| **Topic:** | 1. Everything can be Automated 2. Everything Needs to be Secured | **Semester & Section:** | 8th sem “A”section |
| **Github Repository:** | AnupamaJS |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| **C:\Users\User\Pictures\Screenshots\Screenshot (272).png**  **C:\Users\User\Pictures\1 (2).png**  The Internet of Things (IoT) has become a ubiquitous term to describe the tens of billions of devices that have sensing or actuation capabilities, and are connected to each other via the Internet. The IoT includes everything from wearable fitness bands and smart home appliances to factory control devices, medical devices and even automobiles.  Security has not been a high priority for these devices until now. It is now time to establish The Internet of Secure Things.  There has been a lot of discussion regarding the 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 many of these systems – thought to be safe – are still vulnerable. For instance, even though Industrial Automation 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. On top of that, insider threats, whether malicious or accidental, make up 70% of cyber-attacks, and they usually originate inside that perimeter.  It is necessary to secure the Things themselves.  **Security Challenges for the Internet of Things**  The Internet of Things is comprised of a wildly diverse range of device types- from small to large, from simple to complex – from consumer gadgets to sophisticated systems found in DoD, 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.  These industrial operational assets are commonly fixed function devices designed specifically to perform a specialized task.  Many of them use a specialized operating system such as VxWorks, MQX or INTEGRITY, or a stripped down version of Linux. 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   How are ML, AI, and IBN Linked?  Intent-based networking harnesses the power of automation, AI, and ML to control the function of a network to accomplish a specific purpose, or intent. Intent-based networking allows the IT team to specify, in plain language, exactly what they want the network to accomplish and the network makes it happen. The network is able to translate the intent into policies and then use automation to deploy the appropriate configurations required across the network. The intent-based network uses AI and ML to ensure that any services that are deployed meet the required service level. If they do not meet the service level, the intent-based network can make alerts and provide suggestions for improvement. In some cases, the intent-based network can automatically reconfigure the network to comply with the service levels. The intent-based networking model shown in the figure consists of three key elements:  • Assurance - The assurance element is end-to-end verification of network-wide behavior. It predicts the results of any changes, tracks compliance with the original intent, and makes recommendations or adjustments when there is a misalignment between the intent and the outcome. This stage relies heavily on AI and ML. Systems are part of a closed-loop that continually monitors performance and security of the network, and reconfigures the network to ensure compliance.  • Translation - The translation element is the ability to apply business intent to network configuration. The intent is what you wish to accomplish, not how it is accomplished. This intent is specified in plain language and used by the system to create policies across the system. For example, an intent might be to segment guest traffic from corporate traffic, or to enable access for remote users.  • Activation - The activation element occurs after the intent has been specified and the policies created. This is when individual devices are provisioned to match the intent-based policies. This can be an automated or semi-automated mode that allows the network team to verify configuration before the devices are deployed. An intent-based network creates an agile, responsive network that scales easily and adapts to meet business requirements. It makes efficient use of highly-skilled resources and allows man and machine to work together to optimize the customer experience. Additionally, intent-based networking provides a more secure digital experience by automating time consuming or complicated processes. This makes deploying security policies much easier |

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |