**DAILY ASSESSMENT FORMAT**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date:** | **09-07-2020** | **Name:** | **Karthik J** |
| **Course:** | Cisco- Introduction to IoT | **USN:** | **4AL16EC030** |
| **Topic:** | Chapter 5 | **Semester & Section:** | **8TH A** |
| **GitHub Repository:** | Karthik-J |  |  |

|  |
| --- |
| **FORENOON SESSION DETAILS** |
| 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   **Cyber warfare and the motivated hacker**  The level of security required for an embedded device varies dramatically depending upon the function of the device.  Rather than asking if the device is secure, the OEMs should be asking if the device is secure enough.  A military communication satellite or nuclear power plant control system clearly needs a very different level of security than a water softener equipped with Internet connections for remote diagnostics and automated reordering of salt.  If there is one lesson to be learned from well publicized cyber-attacks like StuxNet, it is that hacking is not just the domain of bored teenagers, hacking drones or even the small groups of motivated hackers.  When the stakes are high enough, Cyber-attacks are multi-phased, multi-year efforts carried out by large, well-funded teams of hackers or even by nation states.  We are no longer just talking about protecting a device from malformed IP packets or DoS packet floods.  Hacking organizations invest significant resources in gathering information on the device or devices they wish to attack.  They hack corporate networks to steal design information.  If possible, they physically obtain target devices they wish to hack and attempt to reverse engineer the device and use it to test possible attacks.  It’s likely that they have attempted to obtain design information on networks and devices using other methods of espionage including attempts to hire engineers involved in designing the devices they wish to hack.  Any OEM building a device that would be a prime target for terrorists or cyber warfare should consider how to protect the device from attack from a group led by a member of their own engineering team, or from someone with detailed knowledge of the inner workings of the RTOS, or other vendor solutions included in your product.  **Security requirements for the Internet of Secure Things**  A security solution for embedded devices must ensure the device firmware has not been tampered with, it must secure the data stored by the device, secure communication and it must protect the device from cyber-attacks. This can only be achieved by including security in the early stages of design.  **Report**-  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   **Cyber warfare and the motivated hacker**  The level of security required for an embedded device varies dramatically depending upon the function of the device.  Rather than asking if the device is secure, the OEMs should be asking if the device is secure enough.  A military communication satellite or nuclear power plant control system clearly needs a very different level of security than a water softener equipped with Internet connections for remote diagnostics and automated reordering of salt.  If there is one lesson to be learned from well publicized cyber-attacks like StuxNet, it is that hacking is not just the domain of bored teenagers, hacking drones or even the small groups of motivated hackers.  When the stakes are high enough, Cyber-attacks are multi-phased, multi-year efforts carried out by large, well-funded teams of hackers or even by nation states.  We are no longer just talking about protecting a device from malformed IP packets or DoS packet floods.  Hacking organizations invest significant resources in gathering information on the device or devices they wish to attack.  They hack corporate networks to steal design information.  If possible, they physically obtain target devices they wish to hack and attempt to reverse engineer the device and use it to test possible attacks.  It’s likely that they have attempted to obtain design information on networks and devices using other methods of espionage including attempts to hire engineers involved in designing the devices they wish to hack.  Any OEM building a device that would be a prime target for terrorists or cyber warfare should consider how to protect the device from attack from a group led by a member of their own engineering team, or from someone with detailed knowledge of the inner workings of the RTOS, or other vendor solutions included in your product.  **Security requirements for the Internet of Secure Things**  A security solution for embedded devices must ensure the device firmware has not been tampered with, it must secure the data stored by the device, secure communication and it must protect the device from cyber-attacks. This can only be achieved by including security in the early stages of design.  There is no one one-size fits all security solution for embedded devices.  Security requirements must take into consideration the cost of a security failure (economic, environmental, social, etc.), the risk of attack, available attack vectors, and the cost of implementing a security solution.  **Making a secure thing**  Building protection into the device itself provides a critical security layer - the devices are no longer depending on the corporate firewall as their sole layer of security.  In addition, the security can be customized to the needs of the device.  Security must be considered early in the design of a new device or system.  Support for secure boot or device tamper detection requires specific hardware capabilities, so this capability must be considered prior to that decision.  Since many embedded devices are deployed outside of the standard enterprise security perimeter, it is critical that security be included in the device itself.  **Summary**  Many of today’s modern embedded devices and systems are complex connected devices charged with performing critical functions.  Including security in these devices is a critical design task.  Security features must be considered early in the design process to ensure the device is protected from the advanced cyber-threats they will be facing now as well as attacks that will be created in the future.  These are the steps to make your things secure and help create the Internet of Secure Things. |