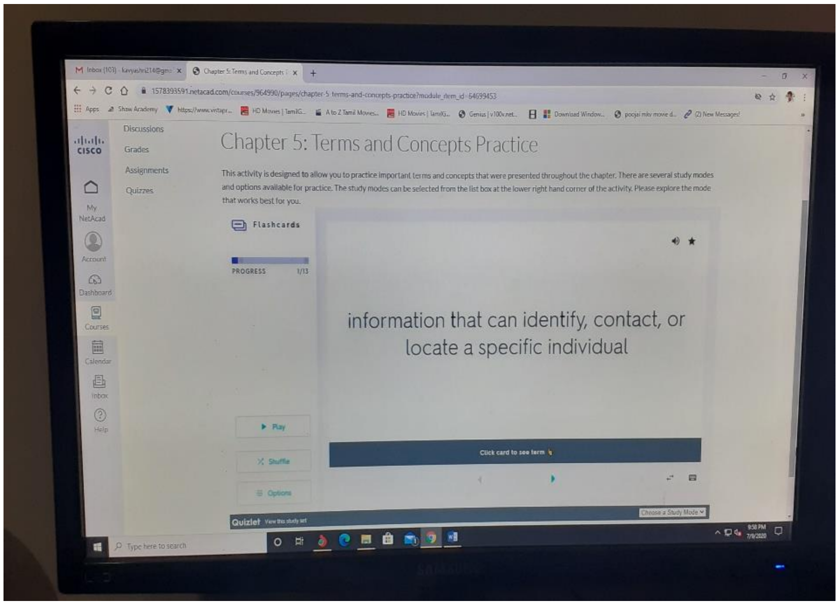
DAILY ASSESSMENT

Date:	**9-7-2020**	**Name:**	**Kavyashree m**
Course:	**Cisco**	**USN:**	**4al15ec036**
Topic:	**Everything needs to be secured**	**Semester & Section:**	**8th A**
Github Repository:	**kavya**		

FORENOON SESSION DETAILS



Chapter 5: Terms and Concepts Practice

This activity is designed to allow you to practice important terms and concepts that were presented throughout the chapter. There are several study modes and options available for practice. The study modes can be selected from the list box at the lower right hand corner of the activity. Please explore the mode that works best for you.

information that can identify, contact, or locate a specific individual

What is Really Needed to Secure the Internet of Things?

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.

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.

Internet of Things security management

The sheer volume of Internet of Things devices makes their security a high priority and is crucial for the future wellbeing of the internet ecosystem.

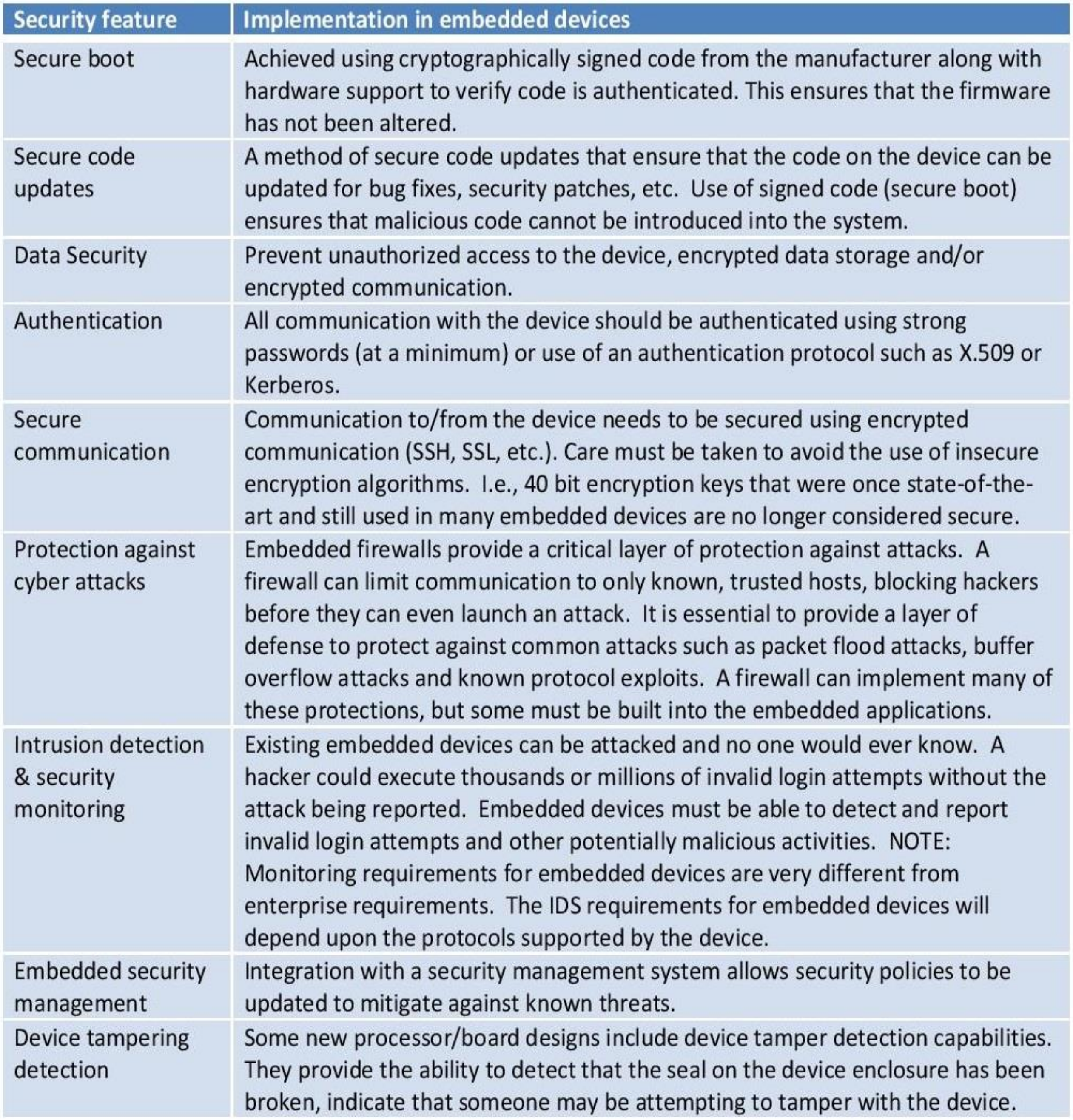
For device users, this means abiding by basic security best practices, such as changing default security passwords and blocking unnecessary remote access (e.g., when not required for a device’s functionality).

Vendors and device manufacturers, on the other hand, should take a broader approach and invest heavily in securing IoT management tools. Steps that should be taken include:

1. Proactively notifying users about devices running outdated software/OS versions.

2. Enforcing smart password management (e.g., mandatory default password changes).
3. Disabling remote access to a device, unless it’s necessary for core functions.
4. Introducing a strict access control policy for APIs.
5. Protecting C&C centers from compromise attempts and DDoS attacks.

Features that need to be considered are:



Security feature	Implementation in embedded devices
Secure boot	Achieved using cryptographically signed code from the manufacturer along with hardware support to verify code is authenticated. This ensures that the firmware has not been altered.
Secure code updates	A method of secure code updates that ensure that the code on the device can be updated for bug fixes, security patches, etc. Use of signed code (secure boot) ensures that malicious code cannot be introduced into the system.
Data Security	Prevent unauthorized access to the device, encrypted data storage and/or encrypted communication.
Authentication	All communication with the device should be authenticated using strong passwords (at a minimum) or use of an authentication protocol such as X.509 or Kerberos.
Secure communication	Communication to/from the device needs to be secured using encrypted communication (SSH, SSL, etc.). Care must be taken to avoid the use of insecure encryption algorithms. I.e., 40 bit encryption keys that were once state-of-the-art and still used in many embedded devices are no longer considered secure.
Protection against cyber attacks	Embedded firewalls provide a critical layer of protection against attacks. A firewall can limit communication to only known, trusted hosts, blocking hackers before they can even launch an attack. It is essential to provide a layer of defense to protect against common attacks such as packet flood attacks, buffer overflow attacks and known protocol exploits. A firewall can implement many of these protections, but some must be built into the embedded applications.
Intrusion detection & security monitoring	Existing embedded devices can be attacked and no one would ever know. A hacker could execute thousands or millions of invalid login attempts without the attack being reported. Embedded devices must be able to detect and report invalid login attempts and other potentially malicious activities. NOTE: Monitoring requirements for embedded devices are very different from enterprise requirements. The IDS requirements for embedded devices will depend upon the protocols supported by the device.
Embedded security management	Integration with a security management system allows security policies to be updated to mitigate against known threats.
Device tampering detection	Some new processor/board designs include device tamper detection capabilities. They provide the ability to detect that the seal on the device enclosure has been broken, indicate that someone may be attempting to tamper with the device.

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.