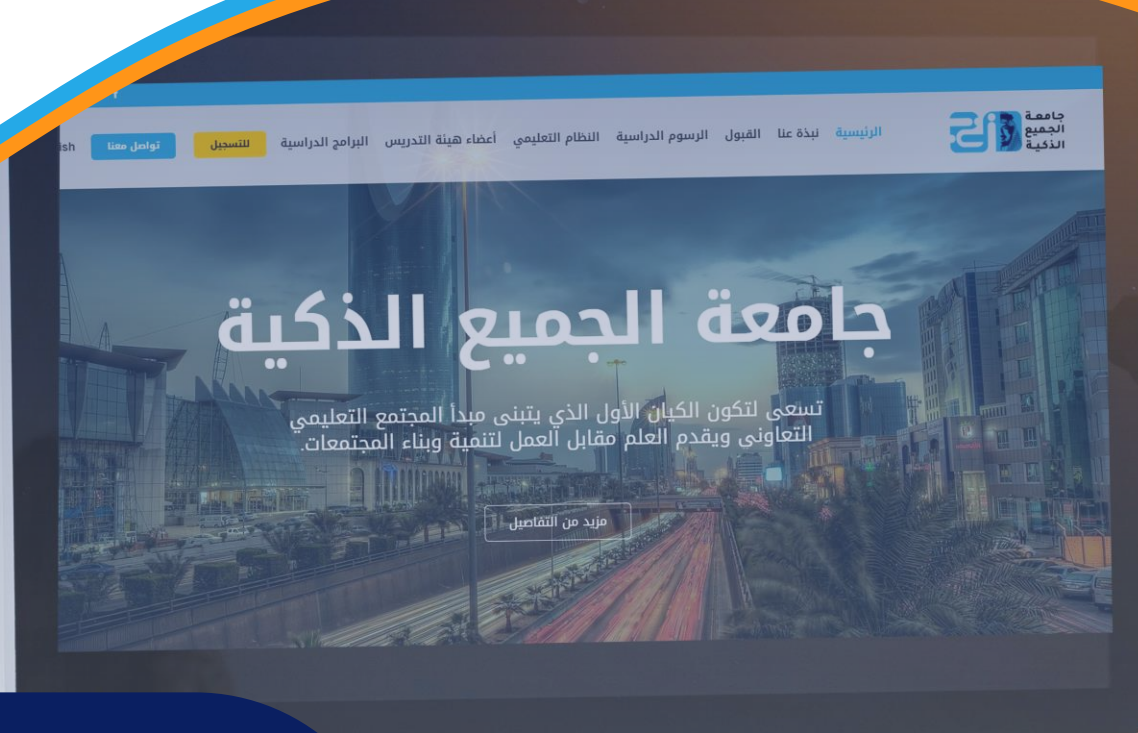




جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY



IoT Security
Prepared by Dr. Abdelrhman Ahmed
Lecture 6

Mobile Network of IoT Security

Advancements in connectivity bring new possibilities. It is essential to prepare for cyber threats that stem from utilizing connected mission-critical applications in a borderless internet of things (IoT) network environment. New technological evolutions to IoT and advanced mobile networks like 5G will push mission-critical network-security management for enterprises to new levels. As we transition to the new reality, the ideal cybersecurity solution balances harmonized networks with emerging mobile technology.



A **mobile network** is a communications network that spans over a large area, wirelessly connecting many sites. Many people believe that when you say "mobile network" you are referring to a wireless network. In actuality, a mobile network and a wireless network are two different types of networks. A mobile network is a communications network that is spread out over an immense land area around the world and connected wirelessly by transceivers at fixed locations that are known as cell sites or base stations. **Transceivers** communicate wirelessly based on the old principle of radio signals. **Radio signals** are electromagnetic radiation that includes light and infrared waves. These signals are considered to be transverse waves in that they have a frequency and a wavelength. **Wavelengths** are measured in the distance between the peaks of sequential waves, and the frequency is the number of cycles per second. To calculate the speed of a transverse wave, you multiply the wavelength and the frequency.



While a mobile network and a wireless network perform similar functions, they are completely different networks.

- A mobile network commonly is described as a physical device that can be taken anywhere. It is composed of a battery to provide power and must have some type of mobile network connectivity in order for the device to operate in order to send and receive data without having to attach the device to a hardware base.
- A wireless network does not indicate a physical device. Wireless means having access to a wireless network such as a local area network (LAN), wide area network (WAN), or a 4G/3G cellular network. You take what used to connect through a router and cable and make that connection wireless. These types of networks still require some type of physical hardware within close proximity to have a physical connection to a power supply and a router or network node in order to communicate.

- A wireless network provides a fixed or portable endpoint to gain access to a distributed network. A mobile network, on the other hand, provides access to distributed networks, through a portable device that allows you to travel anywhere, as long as there is sufficient coverage.



1. Risky entry points:-

- SIM cards can be lost or stolen, allowing attackers to access a customer's private mobile network
- Employees may violate company policy by installing a company-issued SIM card on a risky device

2. Lack of device and security visibility:-

- Traditional IT security products do not know which cellular user equipment (UE) is at risk because they are unfamiliar with International Mobile Equipment Identity (IMEI) or International Mobile Subscriber Identity (IMSI), which are used in communications technology (CT) networks
- CT solutions are generally bad at identifying threats

3. Hard to manage security policies:-

- The IP address of a UE in a private mobile network change occasionally, thus, security management can no longer be based on IP addresses.

4. Critical assets need to be protected:-

- Edge computing application servers, such as facial recognition, mixed reality (MR), and automatic optical inspection (AOI) on your multi-access edge computing (MEC) system, are generally closed systems. This makes it hard to install any existing security products on them, thus, they can be vulnerable to threats
- UEs in a private mobile network may have difficulty maintaining the most up-to-date patches, therefore making them vulnerable to threats.

5. Quick response needed:-

- Some advanced IT security products may know which UE is risky, but security operators can still have difficulty with quickly responding to and preventing the UE from accessing its CT network. This is because UEs access to its CT network is managed by CT system, and it takes time for a security operator to respond to the threat between IT and CT networks

6. Lack of expertise in CT and IT integration:-

- Interconnection between CT and IT can be a challenge when managing private mobile network security across these two heterogeneous platforms.

Mobile Device Security refers to the measures designed to protect sensitive information stored on and transmitted by IoT devices. At the root of mobile device security is the goal of keeping unauthorized users from accessing the enterprise network.



- Regulatory compliance
- Security policy enforcement
- Support of “bring your own device” (BYOD)
- Remote control of device updates
- Application control
- Automated device registration
- Data backup

Above all, mobile device security protects an enterprise from unknown or malicious outsiders being able to access sensitive company data.

Securing mobile devices requires a multi-layered approach and investment in enterprise solutions. While there are key elements to mobile device security, each organization needs to find what best fits its network.

here are some mobile IoT device security best practices:

1. Password protection:-

One of the most basic ways to prevent unauthorized access to a mobile IoT device is to create a strong password, and yet weak passwords are still a persistent problem that contributes to the majority of data hacks. Another common security problem is workers using the same password for their mobile IoT devices, email, and every work-related account. It is critical that employees create strong, unique passwords (of at least eight characters) and create different passwords for different accounts.

2. Establish, share, and enforce clear policies and processes:-

Mobile device rules are only as effective as a company's ability to properly communicate those policies to employees. Mobile IoT device security should include clear rules about:

- What devices/sensors can be used
- Allowed OS levels
- What the company can and cannot access on a personal phone
- Whether IT can remote wipe a device
- Password requirements and frequency for updating passwords

3. Leverage biometrics:-

Instead of relying on traditional methods of mobile access security, such as passwords, some companies are looking to biometrics as a safer alternative. Biometric authentication is when a computer uses measurable biological characteristics, such as face, fingerprint, voice, or iris recognition for identification and access. Multiple biometric authentication methods are now available on smartphones and are easy for workers to set up and use.

4. Avoid public Wi-Fi:-

A mobile IoT device is only as secure as the network through which it transmits data. Companies need to educate employees about the dangers of using public Wi-Fi networks, which are vulnerable to attacks from hackers who can easily breach a device, access the network, and steal data. The best defense is to encourage smart user behavior and prohibit the use of open Wi-Fi networks, no matter the convenience.



5. Beware of apps:-

Malicious apps are some of the fastest growing threats to mobile devices. When an employee unknowingly downloads one, either for work or personal reasons, it provides unauthorized access to the company's network and data. To combat this rising threat, companies have two options: instruct employees about the dangers of downloading unapproved apps, or ban employees from downloading certain apps on their phones altogether.

6. Mobile IoT device encryption:-

Most mobile devices are bundled with a built-in encryption feature. Users need to locate this feature on their device and enter a password to encrypt their device. With this method, data is converted into a code that can only be accessed by authorized users. This is important in case of theft, and it prevents unauthorized access.

- **Enterprise Mobile Management platform:** In addition to setting up internal device policies that protect against unauthorized access, it's equally important to have an Enterprise Mobile Management (EMM) platform that enables IT to gather real-time insights to catch potential threats.
- **Email security:** Email is the most popular way for hackers to spread ransomware and other malware. To combat such attacks, it's critical for businesses to be armed with advanced email security that can detect, block, and address threats faster; prevent any data loss; and protect important information in transit with end-to-end encryption.

- **Endpoint protection:** This approach protects enterprise networks that are remotely accessed by mobile devices. Endpoint security protects companies by ensuring that portable devices follow security standards and by quickly alerting security teams of detected threats before they can do damage. Endpoint protection also allows IT administrators to monitor operation functions and data backup strategies.
- **VPN:** A virtual private network, or VPN, extends a private network across a public network. This enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. VPNs' encryption technology allows remote users and branch offices to securely access corporate applications and resources.

Chapter 06

Systems-Based approach to secure cellular IoT

Over the next decade, 5G networks will support billions of Internet of Things (IoT) devices. They will be the engine for societal transformation through use cases that benefit the public and private sectors, such as Industry 4.0, smart critical infrastructure, connected cars, and enhanced public safety. While great benefits will be realized, IoT also introduces new security risks due to the number of devices, impact of an attack, and lack of appropriate security controls. IoT solutions have unique security considerations because the devices are data-centric rather than human-centric.



The attack surface is across the entire system, including the individual device profile, scale of devices, network interfaces, IoT application, IoT platform, and shared resources in the cloud. A strong IoT security posture has to take zero trust and defense-in-depth approaches by placing security controls across the system at multiple layers, protecting the end-to-end system and data to minimize risk.

The United States National Institute for Standards and Technology (NIST) and other government agencies around the globe have contributed security guidelines and best practices for manufacturers and users. While device security is a critical component of an IoT security posture, it alone cannot ensure a secure IoT solution. The devices should be secure-by-design, but the reality is that market forces pushing for low-cost devices will often require security controls that are implemented across the end-to-end system. IoT devices are not all the same and must be treated individually. As a result, risk management must be appropriate for the use case.

Many IoT devices connect to applications across the network using cellular IoT or Wi-Fi access technologies. Since 3GPP purposely architected each generation of mobile technology to be more secure than the previous one, 5G is considered to have the highest level of security. 5G provides the global coverage, quality of service, scalability, security, mobility, and flexibility to handle the different requirements for a comprehensive range of use cases. Devices may have Wi-Fi connectivity through an IoT gateway with 3GPP cellular access. The gateway can support both Wi-Fi 6, to securely provide local area device connectivity, and 5G, to securely provide wide area connectivity to applications in the private data center or public cloud. From a security perspective, the IoT gateway is both an asset and a control. As an asset, it must be secured to provide only authenticated access on the management plane and to protect itself from malware infection. It is important to make sure the gateway is properly configured so there are no unused open ports or use of default or weak passwords.

The gateway provides security controls for the IoT system through the following capabilities:

- Block anomalous behavior from a device.
- Block non-permitted unsolicited traffic destined for the device.
- Detect and block devices participating in a botnet, based upon indicators of compromise (IoC) that are identified by real-time threat intelligence and/or anomaly detection.
- Detect and block lateral propagation of malware between devices at Layer 2 and across VLANs.
- Detect and block devices from accessing known malicious websites and IP addresses.
- Detect and block malware from passing through the WAN to devices.
- Rate-limit traffic to a device to prevent targeted DDoS attacks.

- Network separation and segmentation isolate infections and attacks so that impact is minimized and contained. 5G network slicing provides isolated logical networks to enable services with diverse requirements on the same 5G network.
- Dynamic resource management enables each slice to meet QoS and SLA requirements, but network slices also provide inherent security advantages, since end-to-end isolation ensures resources dedicated to one slice cannot be consumed by another and traffic cannot be intercepted or spoofed by another slice.

- Cloud-native technologies and network automation allow customization of each network slice to meet use case and customer requirements. Each slice can be architected to provide tailored security controls for an individual customer and use case.
- Implementation of physically separated slices can provide further network segmentation, and private networks using directly licensed 5G spectrum provide further isolation and tailoring of security controls.

A strong IoT security posture uses zero trust principles and an end-to-end defense-in-depth approach to place security controls across the IoT System that minimize risk. It is recommended that a secure IoT system includes the following security controls:

- Use secure IoT devices, but do not assume trust. These devices should comply with NIST, or other national or industry guidelines, and have a recognized IoT security certification. Devices should be checked to ensure secure configuration is used in production.
- Use 5G. It is designed to provide secure IoT use cases by enabling many of the security controls needed for IoT security.

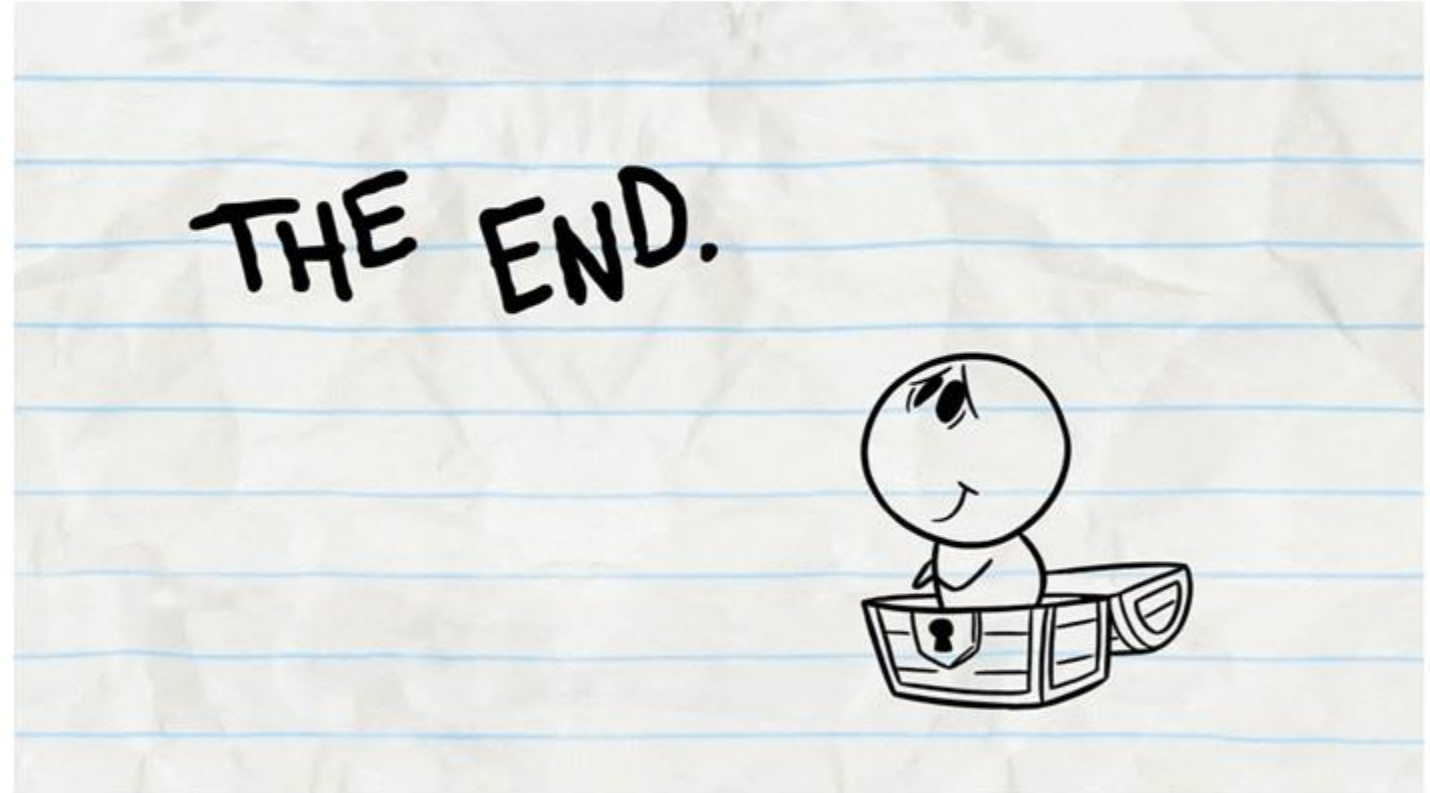
- Assume zero trust. IoT solutions should be part of a zero trust architecture (ZTA). Identify authorization boundaries and use strong authentication on every solution component and interface. DTLS 1.2, TLS 1.2, or TLS 1.3 should be used for mutual authentication and protection of data in transit.
- Use network-based security controls on the user plane that provide additional protection against internal attacks from connected devices and external attacks from the public internet. The network can protect the IoT device when it is a target of an attack, such as botnet infection. If a device has been infected to target the network or system resources, such as acting as a C&C botnet or sourcing a DDoS attack, the network can protect itself, applications, and the IoT platform. Network-based security controls also provide protection from external attacks that target network availability, such as DDoS attacks.

- Use an IoT gateway for Wi-Fi 6-capable IoT devices to access the 5G network. The gateway can provide security controls closer to the devices, but it is also an asset that must be protected.
- Use network slicing to provide isolation and tailored security controls. Private networks provide further isolation and tailoring.
- Use cloud security best practices and tools to protect applications and data in the cloud.
- Use a security management solution for enhanced visibility into the threat landscape as well as for security policy configuration and continuous compliance monitoring.



The End

Please feel free to contact me anytime if you have any questions



جامعة الزكية
EVERYONE'S SMART UNIVERSITY