

Securing IoT Network

Lecture 5

IoT Security

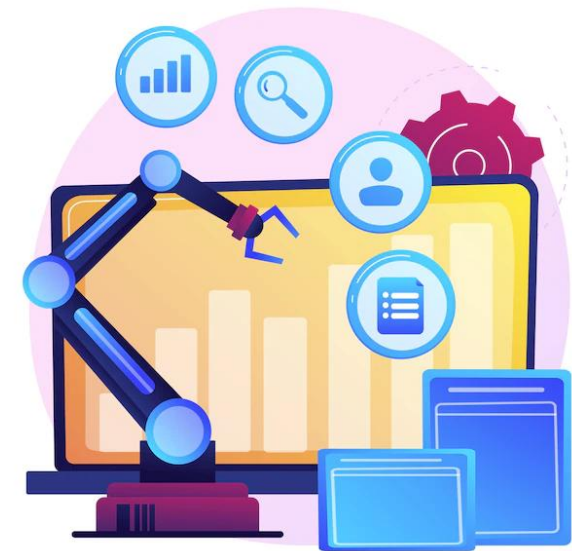
Prepared by
Dr. Abdelrhman Ahmed

Operational Technology (OT)

Over 24 billion active internet of things (IoT) and operational technology (OT) devices exist today, with billions more projected to exist by 2030.

We can get information in real-time, and stay in touch with each other. They're essential. Companies love smart IoT devices because they make it possible to stay connected to consumers and gather information.

This form of IoT, though, is referred to as **operational technology (OT)**.



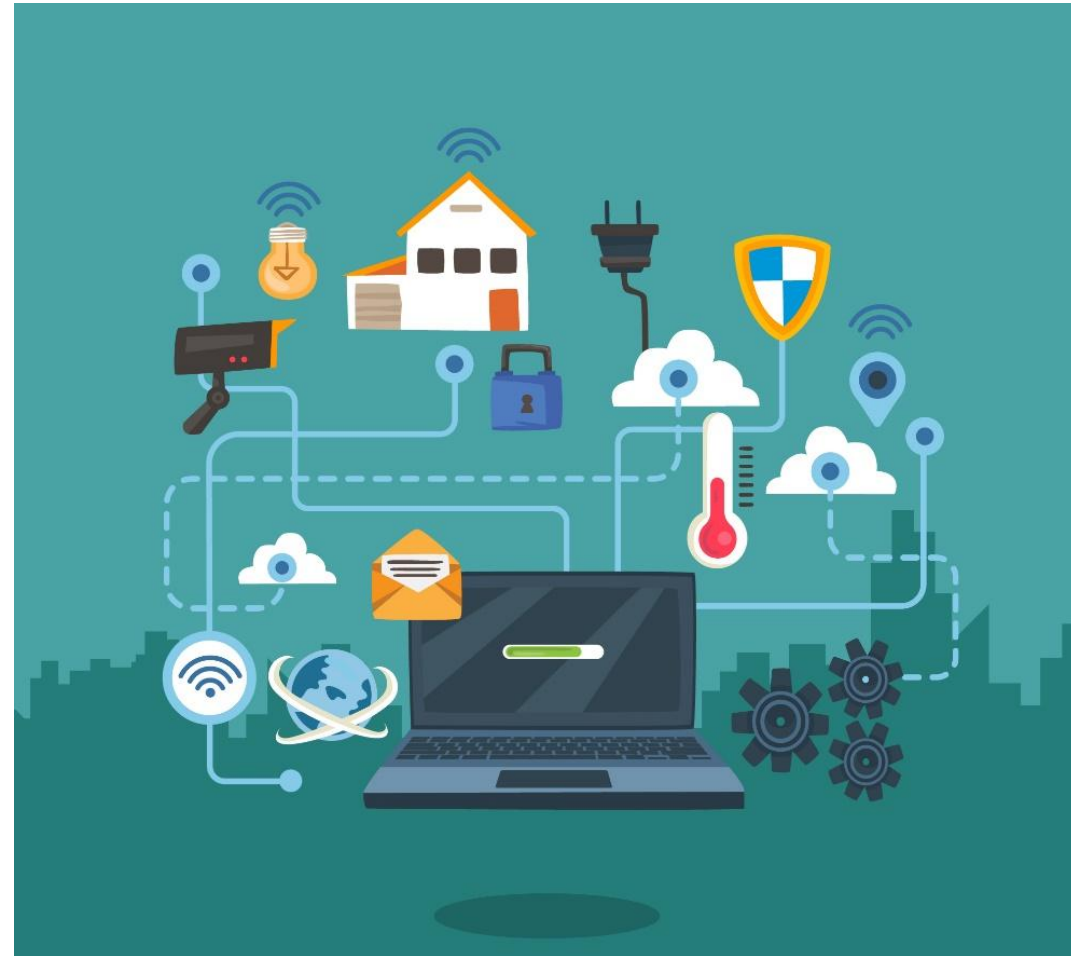
Industrial Control System (ICS)

A term associated with OT is **industrial control system (ICS)**. Industrial control systems include devices and networking capability that allows robots, wind turbines and container ships to operate efficiently. If an IoT device is used to control a physical system, such as an element in the power grid or a device on the factory floor, it is said to be an OT device.



IoT & ICS Network Attacks

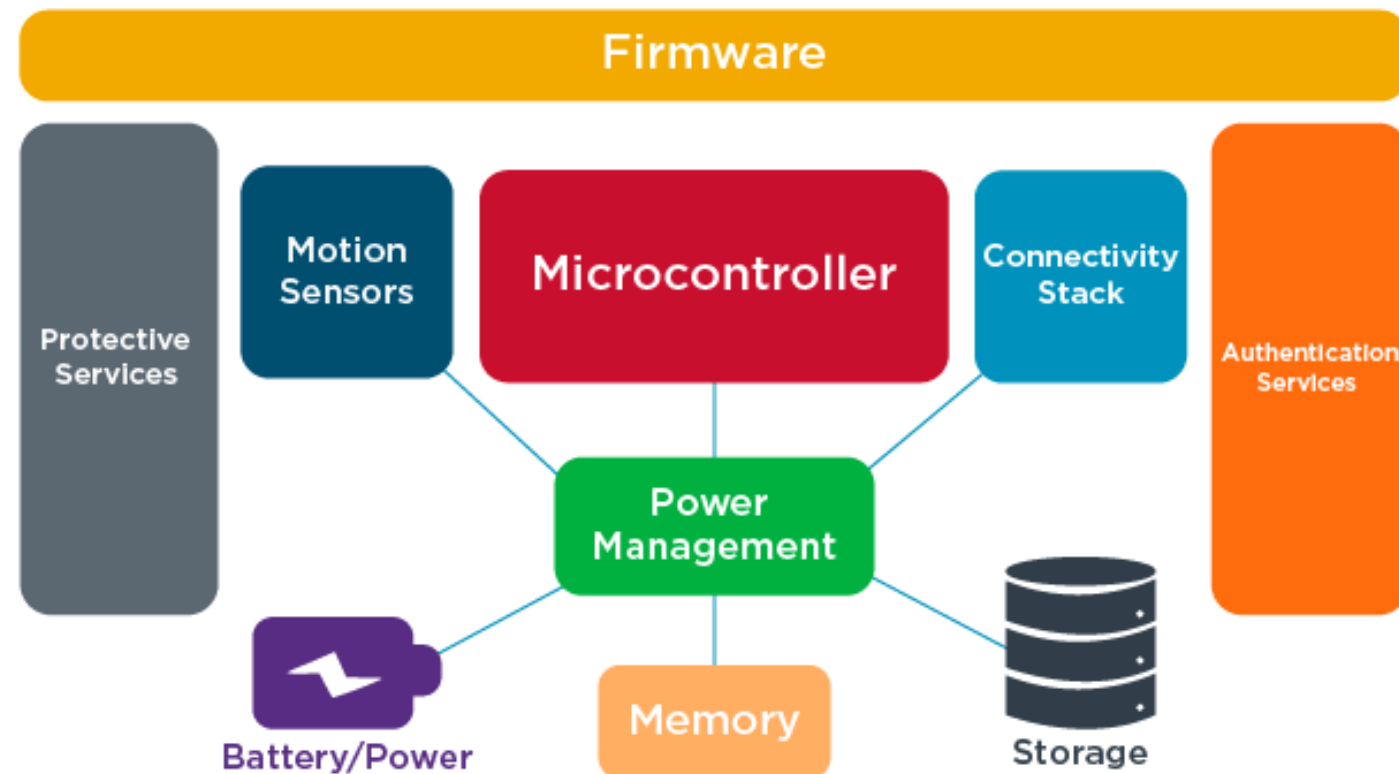
The major issue with IoT and ICS devices is that they make it possible for an individual or company to conduct new and different cyberattacks. Hackers will find malicious ways to interfere with the operations of a company, city, or even country. Cybersecurity professionals often refer to this fact by saying that **IoT increases the attack surface that hackers can exploit.**



Chapter
05

Elements Of Typical IoT Device

IoT and ICS devices are considered endpoints. In other words, they are devices at the end of a communications chain that starts with a person or robotics device and end in cloud platforms and data centers. IoT and ICS devices don't just appear out of thin air. They are designed, developed, and managed, just like any other computer.



Elements Of Typical IoT Device

Firmware: Read-only memory embedded in the device that provides low-level control of the hardware. It can be updated, but usually not programmed. Communicates between each of the elements in the device as well as other networked devices.

Protective services: A portion of the device's firmware or operating system that provides security functionality, including the ability to isolate processes so that they can't be used to defeat security, and encryption.

Motion sensors: The combined hardware and software used to track how the device is moved. Can include detection of simple movement (e.g., moving the device back and forth, or up and down), or satellite connectivity (e.g., Global Positioning System or GLONASS).

Elements Of Typical IoT Device

Microcontroller: The processor used to run the software and provide the “brains” of the unit.

Connectivity stack: Responsible for providing network connectivity. Networking capabilities can include Bluetooth, mobile (e.g., 3G, 4G, 5G), Zigbee, LoRA, SigFox or WiFi.

Authentication services: When included, provides the ability for the IoT device to verify and validate users, network traffic or processes.

Elements Of Typical IoT Device

Power management: If the device requires significant use of power, functionality that manages power usage, as well as the charging of the device.

Battery/power: The physical capability to store power, as well as receive power from a remote source.

Memory: The working “muscle” of the IoT device, in that it provides the ability to store working data, machine code, and information that is then addressed by the processor.

Elements Of Typical IoT Device

Storage: Provides the ability to capture and keep data for relatively long periods of time. Such information can include storing the location(s) the IoT device wearer/operator took the device, information about other devices that have connected with it, and information entered by the user. Such information can be added actively (e.g., by the user programming the IoT/OT device on purpose), or passively (e.g., by the device capturing the motions and actions of the wearer/user).

It doesn't matter if that device is a webcam, the smartwatch, or the Raspberry pi device your local water utility company developed to control devices for your community water supply, the elements remain the same.

IoT Ecosystem

Element	Description
Software developers	The people who develop the software that runs IoT devices.
Hardware Engineers	The people who create the hardware devices, including processors and microcontrollers.
Network Connectivity	Service providers, local LANS and mobile networks (including 4G and 5G), are responsible for transporting data and keeping us connected.
Platforms	These can include cloud-based services that gather and process the terabytes, petabytes and exabytes of data IoT devices generate.

IoT Ecosystem

Element	Description
Data Analysts and scientists	People who crunch the data from IoT devices and turn it into useful, actionable information.
IT workers and managers	Responsible for maintaining the IoT infrastructure, including managing end points as well as IoT network traffic all along the device's lifecycle.
Cybersecurity workers	Individuals responsible for applying IoT security controls, managing cyberthreats and enabling data protection schemes.
AI & ML	Services often tied to IoT/ICS data to help automate the operation of devices, the collection of data and the processing of data into information.

Insecure IoT Devices' Conditions

IoT devices that are not properly developed or secured can result in the conditions found in

Condition	Description
Service disruption	Manipulating an IoT device or devices to make an essential service (e.g., a power generating dam, the water system, a database) completely unavailable.
Data theft	Gaining improper access to personally identifiable information (PII), such as names, user accounts, social security, national health ID numbers, telephone numbers and residence addresses. Increasingly, organizations and individuals alike are concerned about the use – and misuse – of personal information.
Data or service manipulation	Where the attacker can make arbitrary changes to the settings of a device, which can cause loss of life, loss of service, damage to the device itself or damage to other devices.

Securing IoT Network

With increased internet-based convenience comes an increased risk of becoming the target of **cyberpunks**. These hackers can steal and misuse your personal information and banking details and even take control of those smart cameras or microphones to spy on you.

In other words, if you own smart devices such as smart speakers, TVs, thermostats, fridges, and security cameras, your privacy and security could be at stake. Because, in essence, these are multiple entry points with **rickety security** that could leave you prone to attacks.

So, if you're investing dough in setting up an IoT device, you must also invest some time and energy in securing it.

Chapter
05

Securing IoT Network

“You can purchase the most expensive IoT devices from top companies and yet, at the end of the day, your smart device’s security is in your hands.”

So, take the time to do your research before committing to any device. Check if it’s still receiving updates from the manufacturer or if it has vulnerabilities reported by users. Yes, it takes time and money, but it’s always better to be safe than sorry.



Securing IoT Network

7 ways to Secure your IoT device :

1. **Set up Your Router Correctly:** by changing the router's default name, setting the password to something unique, and using the highest level of encryption which currently is WPA2 (WPA3 is just around the corner). If your router only supports the WPA or WEP protocols, maybe it's time for an upgrade.

Typically, routers are primary IoT targets for hackers. Thus, a secure router translates to a substantially more secure IoT device.



Securing IoT Network

7 ways to Secure your IoT device :

2. **Use Super Strong Passwords:** Apart from your Wi-Fi router's password, there are other areas where you need to ensure you have a super-strong password. For instance, your IoT devices require you to create an account and sign in to use them. The devices usually have associated mobile apps where those login credentials are needed. Now, it is important to create unique credentials for every IoT device's account and app. This is so that if the password of one device gets compromised, others still remain intact.



Securing IoT Network

7 ways to Secure your IoT device :

3. Create a Separate Wi-Fi Network for IoT Devices: Many modern routers provide you the ability to set up a guest (or secondary) network. By creating a separate network dedicated to your IoT devices, you can safeguard your main network against IoT threats. This means relatives, friends, and guests can log into a network that isn't related to your IoT devices. So, your local IoT device network is only accessible to you (and your family).

As putting IoT devices on a different network keeps them detached, if hackers do manage to get through, they can't access any of your more important devices, such as your laptop or smartphone.

Securing IoT Network

7 ways to Secure your IoT device :

4. Disable Features You Don't Use: Many IoT devices give you the ability to control them from anywhere on the planet. But if you only use them on your home's Wi-Fi connection, disable remote access. Likewise, smart speakers have Bluetooth connectivity in addition to Wi-Fi. Don't use it? Turn it off. Smart TVs come with voice control, but this feature often goes unused even in voice-controlled households where smart assistants such as Google Assistant, Siri, or Alexa rule the roost. It may sound paranoid but an active mic, if hacked, can also be used to pry on your conversations. Thus, disabling features is all about blocking as many of those multiple entry points as possible.

Securing IoT Network

7 ways to Secure your IoT device :

5. Keep Your Devices Up-To-Date: Updates to your Wi-Fi router's firmware may not happen automatically. These updates often include essential security patches that can greatly enhance your network's security. So, see to it that you do a manual check every few months and if you find any pending firmware updates, install them right away. In the same vein, many IoT devices (and their apps) don't update automatically but prompt you to do so whenever available. Again, don't procrastinate — update straight away.

Securing IoT Network

7 ways to Secure your IoT device :

6. **Enable Multi-Factor Authentication:** If you've ever used net banking, you know what **multi-factor authentication** is. Multi, typically two, -factor authentication (2FA) is an added layer of security beyond a **mere password**. With two-factor authentication, every time someone tries to log in to your IoT device, they have to provide additional proof of identity. This proof can come in the form of a **one-time pin (OTP)** or a **verification code sent to your phone or email address** that confirms that the person logging in is indeed you. Most smart devices have the multi-factor authentication feature by **default**, but there are some devices that don't. In that case, you can enable 2FA by using third-party apps such as Google Authenticator. Even if your IoT device has two-factor authentication with its associated mobile app, having an extra layer of security via a trusted third-party service can give you further peace of mind.

Securing IoT Network

7 ways to Secure your IoT device :

7. **Employ a Next-Generation Firewall (NGFW):** While your router has a built-in firewall, it may not prove to be sufficient. Because a traditional firewall lacks important security features like an **intrusion prevention system (IPS), malware protection, content filtering, SSL/SSH interception, QoS management, and virtual private network (VPN).**

A next-generation firewall (NGFW) is an integrated network platform that combines a traditional firewall with other security functionalities such as the ones just mentioned. An NGFW has all the capabilities of a traditional firewall as well, making it powerful in detecting and protecting against cyberattacks. Next-generation firewalls are a fairly expensive investment, but the level of security boost for your smart iot device makes it a worthy investment. After all, if you can afford the devices, you can surely spend a little extra to secure them. By doing so, you're securing your privacy.



Thank You