Reviewer: Security Issues in IoT

Lesson 5

Security Issues in IoT

The Reality of IoT Vulnerabilities: Insecurity by Design

IoT security is based on a ***cybersecurity strategy*** to protect ***IoT devices*** and the ***vulnerable networks*** they connect to from ***cyber attacks***.

- ***Weak Credentials***: ***Default passwords***, ***hardcoded credentials***, and ***unencrypted telemetry*** are industry standard, enabling trivial ***unauthorized access***.
- ***Supply Chain Risk***: ***Complex, opaque supply chains*** introduce ***firmware and component risks*** that are nearly impossible to detect or remediate at scale.
- ***Patching Gaps***: Many devices lack ***secure update mechanisms***. Billions of vulnerabilities remain unpatched across device ***lifecycles*** spanning years.

IoT Security Risks

The following represent the core risks within the IoT ecosystem:

- ***Insecure Default Settings***
- ***Lack of Device Management***
- ***Insecure Network Services***
- ***Insecure Data Transfer***
- ***Lack of Secure Updates***
- ***Use of Insecure Components***

What is Internet Security?

IoT security is the practice that keeps your ***IoT systems safe***.

- ***IoT security tools*** protect from ***threats and breaches***.
- ***IoT security tools*** identify and monitor risks and can help ***fix vulnerabilities***.
- ***IoT security*** ensures the ***availability, integrity, and confidentiality*** of your IoT solution.

System Communication Components (C&C Architecture):

- ***Botmaster***
- ***C&C Server*** (Command and Control)
- ***Bot*** (Multiple instances)
- ***Command and Response*** (Bidirectional communication)

Application of IoT Security

Businesses use a wide range of ***IoT devices***, including:

- ***Smart security cameras***
- ***Trackers*** for vehicles, ships, and goods
- ***Sensors*** that capture data about ***industrial machinery***

Vulnerable IoT Devices

Attackers are evolving faster than defenses. New techniques now enable ***persistence, automation, and evasion*** at unprecedented scale.

Weak Guessable Password

Weak guessable passwords: Most of IoT devices come with ***pre-set credentials*** (username and Passwords) that are provided by the ***manufacturer***.

Unsecured Network Connection

One of the ***core features*** of IoT devices involves ***networking capabilities*** that allow ***endpoints*** to [communicate] amongst themselves over a ***secure internet connection***.

Example Device Label (Router): Model: CPF903; SSID: 4G-CPE_0336; ***WIFI KEY: 1234567890***; WEBGUI: 192.168.199.1; ADMIN: admin.

Note on Public Wi-Fi: There are significant ***Security Dangers of Public Wi-Fi***. ***5G network slice misconfigurations*** now allow ***side-channel snooping*** between ***industrial IoT tenants***, creating new ***lateral movement paths*** for attackers.

Vulnerabilities of IoT

- ***Improper data transfer and storage***: Even the most robust IoT equipment can be exploited if users ***fail to encrypt data*** within their ***IT ecosystems***. ***Sensitive information*** can be stolen at the point of ***collection***, while it is in ***transit*** or during ***processing***.
- ***Inefficient update mechanism***: To prevent IoT devices from being compromised, companies must be able to send ***real-time updates*** to each ***endpoint*** as soon as they are made available.

Common IoT Device Vulnerabilities to Watch Out For

1. ***Insecure components***: ***Outdated components*** or components that contain ***vulnerabilities***.
2. ***Unnecessary open ports***: ***Unused open ports*** in some devices can allow hackers to exploit ***vulnerable services***.
3. ***Insufficient logging mechanisms***: ***Lack of logging mechanism*** in devices makes it difficult to detect ***malicious activities***.
4. ***Inadequate privacy protection and encryption***: ***Poor data management*** capabilities and ***lack of encryption*** on shared data.
5. ***Lack of automatic patch management***: Devices lack ***automated patch mechanisms*** and checks that can prevent ***malicious modification of patches***.
6. ***Hardcoded passwords***: ***Passwords cannot be changed***.

Defending the IoT Ecosystem: Best Practices & Policy Priorities

Security is not solved by any single control. ***Defense*** requires ***layered, comprehensive strategies*** across ***design, deployment, and governance***:

1. ***Inventory & Segmentation***: Know every device on your network. ***Isolate IoT zones*** with ***micro-segmentation*** to limit ***breach radius*** and ***contain attacks***.
2. ***Security by Design***: Mandate ***secure development lifecycles***, ***code signing***, ***cryptographic hardening***, and ***automated over-the-air update mechanisms***.
3. ***Identity & Access***: Deploy ***passwordless multi-factor authentication***, ***machine identity management***, and ***zero standing privilege models***.
4. ***Policy & Regulation***: Support ***IoT security labeling standards***, ***supply chain transparency mandates***, and ***international security cooperation frameworks***.

The Human and Organizational Challenge

Technical controls alone are insufficient. Organizations face persistent challenges in ***asset management***, ***monitoring***, and ***resilience***:

- ***Lifecycle Mismatch***: Devices operate ***5-10 years***; manufacturer support ends in ***2-3 years***. ***Unpatched devices persist indefinitely***.
- ***Procurement Risk***: ***Complex buying processes*** and ***asset management*** often represent the ***weakest security links*** in organizations.
- ***Continuous Defense***: ***Monitoring***, ***penetration testing***, and ***offensive security exercises*** are now mandatory for ***IoT resilience***.