# Unit 5: Hardware and System Security

## 1. Meltdown Attack

What is Meltdown?

Meltdown is a critical vulnerability in modern CPUs that allows malicious programs to access privileged memory, including sensitive data like passwords and encryption keys. It exploits a flaw in speculative execution, a performance optimization technique used by processors. Discovered in 2018, Meltdown affects Intel processors, some ARM-based chips, and other architectures, making it a significant threat to global cybersecurity.

How it Works:

The CPU speculatively executes instructions that access memory unauthorizedly. Even if these instructions are discarded, the side effects (like changes in the CPU cache) are observable. Attackers use these side effects to infer the contents of protected memory.

Applications:

Data theft from protected kernel memory.

Mitigations:

Kernel Page-Table Isolation (KPTI), microcode updates, and software patches.

## 2. Spectre Attack

What is Spectre?

Spectre is a class of vulnerabilities that trick a CPU into executing instructions speculatively on incorrect assumptions, leading to unauthorized access to sensitive information. Named after 'speculative execution,' Spectre exploits vulnerabilities in the branch prediction mechanism of CPUs. First revealed in 2018, Spectre affects almost all modern processors from Intel, AMD, and ARM.

How it Works:

Attackers craft malicious code that manipulates the CPU's branch predictor. This speculative execution leads to unauthorized memory access. Side-channel techniques, like cache-timing analysis, are then used to infer sensitive data.

Applications:

Gaining access to data across virtual machines or within the same application.

Mitigations:

Software fixes, like Retpoline, and architectural changes in new processors.

## 3. Authentication and Passwords

What is Authentication?

Authentication is the process of verifying the identity of a user, system, or device to ensure secure access to resources. Common authentication methods include passwords (knowledge-based), tokens (possession-based), and biometrics (inherent-based). Multi-factor authentication (MFA) combines these methods for enhanced security.

How it Works:

Passwords are hashed and stored securely. During login, the provided password is hashed and compared to the stored hash. MFA adds layers, like OTPs or biometric scans, to verify identity further.

Applications:

Used in systems ranging from personal devices to enterprise networks.

Mitigations:

Regular password updates, strong password policies, and use of password managers.

## 4. Access Control Concepts

What is Access Control?

Access control determines who can access a resource and what actions they can perform. Two main types:

- Discretionary Access Control (DAC): Users control resource permissions.

- Mandatory Access Control (MAC): Policies strictly define permissions.

Role-Based Access Control (RBAC) is widely used in organizations, assigning permissions based on user roles.

## 5. Access Control List (ACL)

What is an ACL?

An ACL is a list of permissions attached to an object, specifying which users or groups can access it and what operations they can perform. Examples include file systems and network firewalls.

How it Works:

The ACL contains entries defining access levels for users/groups. The system evaluates these entries when access is requested.

Applications:

Restricting access to sensitive files or controlling network traffic.

## 6. Capability

What is a Capability?

A capability is a token that grants access rights to a resource. Unlike ACLs, capabilities are distributed and act as keys.

How it Works:

Capabilities are securely issued by the system. When access is requested, the capability is validated, ensuring permission adherence.

Applications:

Used in distributed systems, API authentication, and secure delegation of rights.

## 8. Threats of Hardware Trojans and Supply Chain Security

What are Hardware Trojans?

Hardware Trojans are malicious modifications to a hardware design, often introduced during manufacturing.

How They Work:

Trojans activate under specific conditions to compromise functionality, leak data, or create backdoors.

What is Supply Chain Security?

Ensuring the integrity of components throughout their lifecycle, from design to deployment.

How it Works:

Audits, secure transport, and tamper-proof measures are employed to safeguard the supply chain.

Applications:

Critical infrastructure, consumer electronics, and IoT devices.

## 9. Side-Channel Analysis-Based Threats and Attacks

What are Side-Channel Attacks?

Side-channel attacks exploit physical characteristics of systems (e.g., timing, power consumption) to extract sensitive data.

How They Work:

Example: Observing power usage during cryptographic operations to infer keys.

Applications:

Attacking smart cards, secure processors, and IoT devices.

Mitigations:

Design hardware with noise and randomization to prevent leakage.

## 10. Issues in Critical Infrastructure and SCADA Security

What is SCADA?

* SCADA (Supervisory Control and Data Acquisition) is a combination of software and hardware components that work together to monitor and control industrial processes. It is commonly used in power generation, water treatment, manufacturing, and other large-scale industrial applications.
* SCADA systems provide high-level supervision and data acquisition, enabling operators to monitor the status of devices and processes, detect anomalies, and make informed decisions.
* SCADA consists of components like Programmable Logic Controllers (PLCs), Remote Terminal Units (RTUs), and Human-Machine Interfaces (HMIs), each playing a key role in the system's functionality.

How it Works:

* Real-time operation: Controls physical processes requiring immediate attention.
* Geographic distribution: Often spans large areas, making security management challenging.
* Legacy systems: Many are based on outdated technology, not designed with modern security.
* Limited resources: Often constrained by processing power and memory.

**Security Threats:**

* Cyberattacks: Malware, ransomware, and phishing can target SCADA systems, leading to data corruption, system shutdowns, or theft of sensitive information.
* Unauthorized Access: Attackers gaining unauthorized access can manipulate or disrupt SCADA processes, potentially affecting operations and safety.
* Data Breaches: SCADA systems often store critical data. If compromised, it can lead to exposure of sensitive or proprietary information.
* Physical Attacks: Physical sabotage or vandalism can disrupt the functioning of SCADA infrastructure, such as damage to servers or communication equipment.
* Insider Threats: Employees or contractors with malicious intent or lack of awareness can cause security breaches or unintended disruptions to the system.

**Mitigations:**

* Implement perimeter protection measures like firewalls, intrusion detection systems, and VPNs.
* Use interior security practices, including access control, host-based protections, and network segmentation.
* Regularly audit and test SCADA systems for vulnerabilities.
* Ensure robust monitoring and incident management systems are in place.
* Secure remote devices like RTUs and PLCs by limiting access and employing encrypted communication protocols.