B.Tech, 6^{th} Sem., Computer Networking: Security(CLASS NOTE)

Dr. Laxmidhar Biswal

May 15, 2025

Compare and contrast various types of security controls

1 Chapter 07
  - Introduction
- Application Vulnerabilities
- Operating System (OS)-Based Vulnerabilities
- Web-Based Vulnerabilities
- Hardware Vulnerabilities
- Cryptographic Vulnerabilities
- Misconfiguration Vulnerabilities

Introduction/Motivation

Explain various types of vulnerabilities

Objectives of this chapter

In this chapter, our objective to learn about different types of cybersecurity weaknesses—like those found in apps, operating systems, websites, hardware, and cloud systems. We also understand the risks of using outside suppliers and mobile devices at work. This overview will help you see why companies use these security steps and prepare you well for related exam questions.

Explain various types of vulnerabilities

Application Vulnerabilities

- Memory injection

  For Example: Code Red worm that affected Microsoft IIS web servers in 2001.

- Buffer overflow

  Example: Slammer worm, also known as the SQL Slammer. In January 2003.

- Race conditions

- Malicious update

  Example: CC Cleaner.

Explain various types of vulnerabilities

Operating System (OS)-Based Vulnerabilities

- Occur when attackers exploit flaws in the operating system (OS) that controls hardware and software resources.
- Vulnerabilities may arise from bugs in the OS's code, design, or configuration.
- Threat actors use these flaws to:
  - Gain unauthorized access
  - Disrupt operations
  - Steal sensitive data
- Example: BlueKeep (CVE-2019-0708)
  - Affected unpatched Microsoft Windows systems
  - Enabled remote code execution
  - Compromised over 1 million devices

OS vulnerabilities pose both risks and opportunities—while defenders aim to secure systems, attackers look for hidden

Explain various types of vulnerabilities

Web-Based Vulnerabilities

- Major Web-Based Threats – Structured Query Language Injection (SQLI) and Cross-Site Scripting (XSS).
- Web vulnerabilities act as entry points for cyber attackers.
- SQL Injection (SQLI): Exploits faulty inputs to manipulate databases.
- Cross-Site Scripting (XSS): Injects malicious scripts into websites.
- Both threats can severely compromise digital security and user experience.

Explain various types of vulnerabilities

SQLI

- SQLI is a cyberattack targeting input vulnerabilities in websites or applications.
- Attackers inject malicious SQL code into input fields (e.g., login forms, search boxes).
- The malicious code alters the SQL queries in the backend.

SQLI works as follows:

- Input Fields: Web applications often use user inputs from forms or URL parameters to build SQL queries.
- Malicious Input: Attackers inject specially crafted input containing SQL code (e.g., ' OR '1'='1).
- Query Manipulation: If inputs aren't properly sanitized or validated, the SQL code gets executed as part of the database query.

Explain various types of vulnerabilities

SQLI

- Data Exposure & Control
  - Attackers can: Extract confidential data
  - Alter or delete records
  - Gain admin-level access to the database

Example (Login Form) of SQL Injection

SELECT * FROM users WHERE username = ’alice’ AND password = ’password123’;

Injected Input: ’ OR ’1’=’1

If the application doesn’t sanitize this input, the resulting query becomes:

SELECT * FROM users WHERE username = ” OR ’1’=’1’ AND password = ”;

Explain various types of vulnerabilities

SQLI Mitigation

- Stored Procedure:
  - A stored procedure is a set of SQL statements saved in the database that encapsulates a sequence of SQL statements.
  - Used for tasks like data manipulation, queries, or transactions.
  - Can be called from applications or other database objects.
  - Helps improve performance and security (reduces SQL injection risks).
- Input Validation
  - Always validate and sanitize user inputs.
  - Use parameterized queries or prepared statements — they prevent injection by treating input as data, not code.

Explain various types of vulnerabilities

SQLI Mitigation

- A serious web vulnerability where malicious code is injected into websites.
- The injected code runs in the victim's browser, not the attacker's.
  Can cause:
  - Theft of user data
  - Session hijacking
  - Website defacement
  - Often involves:
  - $< script >$ ... $< /script >$tags
    JavaScript (.js) files

Explain various types of vulnerabilities

SQLI Mitigation

- A malicious user posts the following comment:
  html
  $< script >$
  alert('XSS Attack!');
  $< /script >$

Hardware Vulnerabilities

Hardware vulnerabilities can be mitigated through proactive measures, including rigorous testing (e.g., fuzz testing, vulnerability assessments) during design and manufacturing. Regular firmware updates are crucial to address security flaws, and collaboration between manufacturers and security experts strengthens defenses.

Explain various types of vulnerabilities

Types of Hardware Vulnerabilities

- Firmware Vulnerabilities:
  - Flaws in firmware can compromise system functionality.
  - Risks: outdated firmware, weak security, poor encryption.
  - Mitigation: Regular updates and best security practices.
- End-of-Life (EOL) Systems:
  - No support or updates after product life cycle ends (e.g., Windows XP).
  - Risk: Increased vulnerability due to lack of patches.
- Legacy System Vulnerabilities
  - Older systems still in use with outdated security features.
  - Risk: Exploitation due to no vendor support or updates.

Explain various types of vulnerabilities

Cryptographic Vulnerabilities

Cryptographic vulnerabilities—especially those related to certificates and encryption—demand careful analysis. These flaws pose significant security risks. This section outlines the key vulnerabilities, highlights potential threats, and provides strategies to strengthen cryptographic defenses.

- Certificate authority (CA) compromise:
  - Attackers forge digital certificates.
  - Leads to interception of encrypted data.
- Key Compromise:
  - Due to theft, weak generation, or poor management.
  - Allows unauthorized decryption or data access.
- Flawed Implementation:
  - Errors in coding encryption algorithms or key handling.
  - Opens paths for exploitation despite strong algorithms.

Explain various types of vulnerabilities

Cryptographic Vulnerabilities

- Outdated Algorithms:
  - Old cryptographic methods become vulnerable.
  - Breakable with modern computing power.
- Side-Channel Attacks:
  - Leaks through power, timing, or radiation.
  - Used to infer encryption keys
- Backdoor Exploitation:
  - Hidden access (intentional or accidental).
  - Completely bypasses encryption security.
- Weak Random Number Generation:
  - Predictable keys due to poor randomness.
  - Weakens entire encryption system.

Explain various types of vulnerabilities

Cryptographic Vulnerabilities

- Certificate Revocation Failures (CRLs & OCSP):
    - CRL = List of revoked certificates (slow).
    - OCSP = Real-time revocation check (faster).
    - Both are crucial for trust and preventing misuse.
- Poor Key Management:
    - Requires secure generation, storage (e.g., HSM), rotation.
    - Mishandling leads to breaches.
- SSL Stripping:
    - HTTPS → HTTP downgrade.
    - Captures login/data during unsecured sessions.
- SSL/TLS Downgrade Attacks:
    - Forces browser to use weaker encryption.
    - Example: POODLE Attack (exploits SSL 3.0 via MITM).

Explain various types of vulnerabilities

Misconfiguration Vulnerabilities

In today's highly interconnected world of devices (firewalls, routers, servers, computers, etc.), misconfigurations in IT systems pose serious security risks. These can result from human error, complex setups, or rushed deployments, and can lead to data breaches, financial loss, and reputation damage. This section examines these vulnerabilities and stresses the importance of secure configuration.

Explain various types of vulnerabilities

Misconfiguration Vulnerabilities

- Network Devices (Routers, Switches, Access Points):
  - Default Settings: Must be changed immediately after purchase to prevent misuse.
  - Open Ports & Weak Access Control: Exposes the system to DDoS and man-in-the-middle (MITM) attacks.
  - Unpatched Firmware: Leaves devices vulnerable to known exploits.
  - Misconfigured ACLs (Access Control Lists): May unintentionally allow unauthorized access to critical network zones.

Explain various types of vulnerabilities

Misconfiguration Vulnerabilities

- Firewalls:
  - Unauthorized Access: Poor port management can let attackers breach the network.
  - Malware Entry: Open or unnecessary ports can serve as gateways for viruses and malware.
  - Regulatory Violations: Misconfigurations can lead to non-compliance in regulated industries (e.g., healthcare, finance).

Explain various types of vulnerabilities

Misconfiguration Vulnerabilities

- Firewalls:
  - Overly Permissive/Restrictive Rules:
    - Permissive: Easier for attackers to bypass.
    - Restrictive: May block valid traffic and disrupt services.
  - Default Credentials: Using default usernames/passwords creates major security risks.
  - Unpatched Software: Outdated firmware/software makes devices easy targets.
  - Excessive Privileges: Over-privileged accounts increase the risk of unauthorized access.
-

References

https://www.ebooks.com/en-ag/book/210192090/comptia-security-sy0-601-certification-guide/ian-neil/

Question

??

The End