Software Security

Social Engineering and Human Factors in Software Security

Dr. Zeyad Safaa Younus Saffawi

Social Engineering

- Social Engineering is a type of **cyber attack** that **targets human behavior rather than software vulnerabilities**.
- Instead of **hacking** into **systems** using **technical tools**, attackers **manipulate human behavior** to **gain access** to **sensitive information** or **systems**.
- Attackers often **take advantage** of:
  - Human trust
  - Lack of security awareness
  - Curiosity or fear
  - human mistakes, not software vulnerabilities.

- **Example:**
  An **attacker** sends an **email pretending** to be from the **IT department** asking the **user to reset their password**.

Why are Human Factors Matter important in the field of Security?

- Even the most secure systems can fail if **users make mistakes**.
- **Human factors** in **security** include:
  - **Poor password practices**
  - **Sharing sensitive information**
  - **Falling for phishing emails**
  - **Ignoring security warnings**
- **Example:**
  A **user receives an email saying**:
  "Your account will be suspended. Click here to verify your password."
  - If the **user clicks the link and enters the password**, the **attacker gains access**.
  - Therefore, **people are often the weakest link in cybersecurity.**

Common Social Engineering Attacks

- Some of the most **common social engineering attacks** include:

  1. **Phishing**: **Fraudulent emails** or **messages** that **trick users** into **revealing passwords or personal data**.

  2. **Impersonation**: An **attacker pretends to be someone trusted** (IT staff, manager, bank employee) to **obtain information**.

  3. **Baiting**: Offering **something attractive** (free software, USB drive) to **trick users into installing malware**.

  4. **Tracking**: An **attacker physically follows** an **authorized person** to **enter a restricted area**.

Impact of Social Engineering Attacks

- Social engineering attacks can cause **serious damage** to organizations:

  - **Data breaches**
  - **Financial loss**
  - **Identity theft**
  - **Unauthorized system access**
  - **Reputation damage**

Preventing Social Engineering Attacks

- **Organizations** can **reduce social engineering risks** by applying **security practices** such as:

  - **Security Awareness Training**
    - Educate employees about phishing and scams.
  - **Strong Authentication**
    - Use **Multi-Factor Authentication (MFA)**.
  - **Email Security Filters**
    - Detect suspicious emails.
  - **Access Control**
    - Apply the **Principle of Least Privilege**.
  - **Verification Procedures**
    - Always verify sensitive requests before responding.

References

- Helfrich, J. N. (2019). *Security for software engineers*. CRC Press.