SA  
课堂作业报告

得分：

|  |  |
| --- | --- |
| 内容 | 探讨软件系统的安全属性 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 角色 | 小组成员 | QQ号 | 联系电话 | 得分 |
| 组长 | 陈德霖 |  |  |  |
| 文档管理员 | 陈溢嘉 | 1561308699 | 17796321047 |  |
| 其它组员 | 江隽轩 | 2642888754 | 15918790372 |  |
| 陈柏霖 |  |  |  |
| 钱靖 |  |  |  |

1. **Write a set of concrete scenarios for security for an automatic teller machine. How would you modify your design for the automatic teller machine to satisfy these scenarios?**

**Scenarios for ATM Security**

1. **Physical Theft**: Criminals may attempt to steal cash from the ATM or the machine itself through ram raids or burglary.
2. **Logical Attacks**: Cybercriminals could install malware to compromise the system and steal financial data or manipulate transactions.
3. **Skimming**: Fraudsters attach devices to the ATM to capture card information and PINs.
4. **Vandalism**: ATMs may be targeted for vandalism, causing damage to the physical components and disrupting service.
5. **Social Engineering**: Attackers may deceive users or staff to gain access to sensitive information or insert malicious devices.

**Design Modifications for ATM Security**

1. **Physical Security Enhancements**:

**Bolt ATMs to the floor** and use reinforced materials to resist ram raids and burglaries.

Install **high-security locks** on all accessible parts and **tamper-evident seals** on critical components to detect unauthorized access .

1. **Logical Security Measures**:

Implement **intrusion detection systems** and **firewalls** to prevent unauthorized network access.

Regularly update the **ATM software** to protect against known vulnerabilities and ensure the use of **encrypted communication channels** for all transactions .

1. **Anti-Skimming Devices**:

Equip ATMs with **anti-skimming technology** such as sensors that detect foreign objects attached to card slots or cameras monitoring the PIN pad area.

Use **integrated card readers** that are less susceptible to skimming devices and ensure that any additions to the ATM, such as privacy shields, do not facilitate skimming .

1. **Vandalism Protection**:

Use **durability and vandal-resistant materials** for the ATM exterior and screens.

Install **security cameras** with **motion detection** capabilities to deter vandalism and provide evidence in case of an incident .

1. **Social Engineering Defenses**:

Train staff to recognize and respond to social engineering attempts.

Educate users about security practices when using ATMs, such as covering their PIN entry and being vigilant for any unusual ATM behavior or appearance .

1. **Regular Audits and Inspections**:

Perform **regular physical inspections** of ATMs to identify any signs of tampering or unauthorized modifications.

Conduct **security audits** to ensure compliance with industry standards and to identify potential weaknesses in the system .

1. **User Interface Security**:

Ensure that the **ATM user interface** cannot be manipulated to display false prompts or to log keystrokes.

Use **PCI PTS-approved EPPs** (Encrypting PIN Pads) for PIN entry to protect against PIN theft .

1. **Network Security**:

Secure all **communication interfaces** within the ATM and ensure that they do not accept unauthorized connection requests.

Implement **network isolation** techniques and use **intrusion detection/mitigation tools** to protect against network-based attacks .

1. **Software and Firmware Security**:

Ensure that the **ATM software is hardened** and configured to run with the least necessary privileges.

Implement **secure software update mechanisms** that verify the integrity and authenticity of the updates .

1. **Life Cycle Management**:

Manage the entire life cycle of the ATM, from manufacturing to decommissioning, with a focus on security at every stage.

Ensure that **decommissioned ATMs** are properly sanitized to remove all sensitive data

1. **One of the most sophisticated attacks on record was carried out by a virus known as Stuxnet. Stuxnet first appeared in 2009 but became widely known in 2011 when it was revealed that it had apparently severely damaged or incapacitated the high-speed centrifuges involved in Iran's uranium enrichment program. Read about Stuxnet and see if you can devise a defense strategy against it based on the tactics in this chapter.**
   1. **Resist Attacks**: Stuxnet exploited zero-day vulnerabilities in Windows. Regularly update and patch all systems, especially those running critical infrastructure, to protect against unknown vulnerabilities.
   2. **Encrypt Data**: Since Stuxnet targeted industrial systems, ensure that all programmable logic controller (PLC) configurations and operational data are encrypted to prevent unauthorized changes.
   3. **Attack System Detection**: Implement robust monitoring tools that can detect anomalies in industrial control systems, as Stuxnet manipulated physical processes.
   4. **Maintain Audit Trail**: Maintain detailed logs of all system activities, especially changes to PLC configurations, to trace back any unauthorized modifications.
   5. **Limit Exposure**: Stuxnet spread via infected USB drives. Restrict the use of USB drives and other removable media in industrial environments.
   6. **Recover from Attacks**: Have a disaster recovery plan that includes regular backups of critical systems and data, ensuring that you can restore operations quickly after an attack.
   7. **React to Attacks**: Develop an incident response plan that includes steps to isolate affected systems to prevent the spread of the virus.
   8. **Revoke Access**: Stuxnet exploited legitimate credentials. Implement strong authentication mechanisms and promptly revoke access for any compromised credentials.
   9. **Lock Computer**: Implement automatic system lockdown after a period of inactivity to prevent unauthorized access.
   10. **Detect Intrusion**: Use intrusion detection systems (IDS) that are capable of monitoring for the specific types of behavior exhibited by Stuxnet, such as unauthorized PLC modifications.
   11. **Change Default Settings**: Stuxnet exploited default settings. Change default passwords and configurations on all systems, especially industrial control systems.
   12. **Separate Entities**: Stuxnet moved laterally within networks. Segment networks to limit the spread of malware and ensure that critical systems are isolated.
   13. **Identify Actors**: Use identity and access management systems to track and control access to critical systems.
   14. **Authorize Actors**: Ensure that only authorized personnel have access to change system configurations or operational parameters.
   15. **Inform Actors**: Educate personnel on the risks associated with malware like Stuxnet and the importance of following security protocols.
   16. **Binding Time**: Since Stuxnet was a late-bound attack, ensure that there are mechanisms in place to validate and control the behavior of all system components, especially those loaded at runtime.
   17. **Choice of Technology**: Choose security technologies that are designed to protect against advanced persistent threats (APTs) and are capable of detecting and responding to complex attacks like Stuxnet.
2. **Some say that inserting security awareness into the software development life cycle is at least as important as designing software with security countermeasures. What are some examples of software development processes that can lead to more-secure systems?**

Integrating security awareness into the software development life cycle (SDLC) is crucial for creating more secure systems. Here are some key processes that can lead to enhanced security:

1. **Security Planning**: This involves identifying and documenting security requirements at the outset, considering features like access controls and data protection .
2. **Security Training**: Ensuring that all team members, including developers, testers, and operations staff, are trained in secure coding practices and are aware of the latest security threats and mitigation strategies .
3. **Threat Modeling**: This process involves identifying potential threats to a software system and designing mitigations to address those threats .
4. **Code Reviews**: Regular code reviews can help identify and fix security vulnerabilities before they are exploited .
5. **Static and Dynamic Analysis**: Using tools to automatically detect security vulnerabilities in code during development .
6. **Penetration Testing**: Simulating attacks on the system to identify vulnerabilities that can be exploited .
7. **Secure Deployment**: Ensuring that servers and environments are securely configured and that access controls are in place during deployment .
8. **Maintenance and Monitoring**: Regularly updating and patching software, monitoring for security events, and having incident response procedures in place .
9. **Security and usability are often seen to be at odds with each other. Security often imposes procedures and processes that seem like needless overhead to the casual user. But some say that security and usability go (or should go) hand in hand and argue that making the system easy to use securely is the best way to promote security to the user. Discuss.**
10. **List some examples of critical resources for security that might become exhausted.**
11. **List an example of a mapping of architectural elements that has strong security implications. Hint: think of where data is stored.**
12. **Which of the tactics in our list will protect against an insider threat? Can you think of any that should be added?**
13. **In the United States, Facebook can account for more than 5 percent of all Internet traffic in a given week. How would you recognize a denial-of-service attack on Facebook.com?**

Signs of a denial-of-service attack on Facebook.com might include:

1. **Unusually slow network performance:** If the site loads slowly or not at all, it could indicate an attack.
2. **Inability to access the website:** Widespread reports of users being unable to access Facebook might suggest a DoS attack.
3. **Sudden surge in network traffic:** A sharp increase in traffic could be a result of attackers sending a flood of requests.
4. **Flood of error messages:** Frequent error messages such as "service unavailable" or "server error" might indicate that the server cannot handle the requests.
5. **Drastic increase in spam emails:** A sudden influx of spam or malicious requests could be part of the attack.
6. **Monitoring for network anomalies:** Keeping an eye on network traffic for unusual patterns, such as a sudden increase in traffic or unusual packets, is crucial.
7. **Security measures:** Having security measures like firewalls and intrusion detection systems in place can help identify and mitigate potential attacks.

If there is suspicion of a DoS attack on Facebook.com, it would be advisable to contact the internet service provider and use security tools to analyze traffic and block malicious packets.

1. **The public disclosure of vulnerabilities in production systems is a matter of controversy. Discuss why this is so and the pros and cons of public disclosure of vulnerabilities.**

The public disclosure of vulnerabilities in production systems is indeed a contentious issue. There are several reasons why this is so, and it's important to consider both the pros and cons of such disclosure.

**Pros of Public Disclosure:**

1. **Raising Awareness:** Public disclosure can alert a wide audience to the existence of a vulnerability, which can lead to increased vigilance and a quicker response from the affected organizations
2. **Pressure for Quick Fixes:** When vulnerabilities are made public, there is often public pressure on companies to address the issue promptly, which can lead to faster remediation.
3. **Transparency and Trust:** Organizations that are transparent about their security issues can build trust with their users and the public, demonstrating a commitment to security.

**Cons of Public Disclosure:**

1. **Risk of Exploitation:** Public disclosure can provide would-be attackers with detailed information on how to exploit a vulnerability, potentially before a fix is widely available.
2. **Damage to Reputation:** Companies may be reluctant to disclose vulnerabilities publicly due to the potential damage to their reputation and the trust of their customers.
3. **Legal and Economic Challenges:** There can be legal barriers and a lack of cooperation among stakeholders, as well as limited market incentives for security researchers to participate in coordinated vulnerability disclosure.

**Responsible Disclosure as a Middle Ground:**

A middle ground that is often advocated is responsible or coordinated disclosure. In this model, vulnerabilities are reported privately to the organization first. The details are then disclosed publicly once a patch is available, sometimes with a delay to allow for widespread patching. This approach aims to balance the need for quick fixes with the desire to minimize risk to users.

In conclusion, the decision to publicly disclose vulnerabilities should be made carefully, weighing the potential benefits of increased awareness and pressure for fixes against the risks of exploitation and reputational damage. Responsible disclosure policies can help navigate this complex issue.