Software Security Testing Midterm Review

Brandon Thompson

October 8, 2019

1. CIA triad
   - Confidentiality
   - Integrity
   - Availability
2. Software assurance definition
   - Definition: The level of confidence that Software is free from vulnerabilities and functions in the intended manner.
3. 4 goals of software assurance
   - Trustworthy: Ensure no exploitable vulnerabilities or malicious logic exists in software.
   - Dependability: Ensure the software, when executed, functions as intended.
   - Survivability: Rugged and resilient
     - If compromised, damage will be minimum.
     - Will recover quickly to an acceptable capacity.
   - Conformance: Ensure Processes and products conform to requirements, standards, and procedures.
4. Computer security terminologies

   Adversary (threat agent) - An entity that attacks, or is a threat to, a system.

   Attack - An assault on system security that derives from an intelligent threat; a deliberate attempt to evade security services and violate security policy of a system.

   Countermeasure - An action, device, procedure, or technique that reduces a threat, vulnerability or attack.
   - By eliminating or preventing it (prevent)
   - By minimizing the harm it can cause (recover)
   - By discovering and reporting it so that corrective action can be taken (detect)

   Threat - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

   Vulnerability - Flaw or weakens in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy
   - Can be corrupted (loss of integrity)
   - Can become leaky (loss of confidentiality)
   - Can become unavailable (loss of availability)

   Risk - An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a harmful result.

- Low: limited adverse effect.
- Moderate: serious adverse effect.
- High: severe or catastrophic adverse effect.

Security Policy - A set of rules an practices that specify how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset) - Data; a service provided by the system, a system capability; an item of system equipment; a facility that houses system operations and equipment.

- Hardware
- Software
- Data
- Communication facilities and networks.

5. Types of General attacks

Active attack is a network exploit in which a hacker attempts to make changes to data on the target.

Passive attack is a network attack in which a system is monitored/scanned for open ports and vulnerabilities to gain information about the target.

Inside attack is a malicious attack performed on a network or computer system by a person with authorized system access.

Outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system.

6. Types of specific attacks

- Social Engineering Attacks

  Organization penetration is tricking people at work into giving access to company resources.

  Phishing creating a malicious web site and making it look like some other company's.

  Spam User clicks on email to read, email can install malware.

  Spoofing Change the "From" address in messages.

  Man in the middle unauthorized user requests or modifies messages between two parties.

- Attacks against software

  Cross-site scripting (XSS): embed JS functions into HTML data element, and redisplayed on the web page as hyperlink. Once clicked, users will be directed to other websites without knowing.

  Buffer overflows: While writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory location.

  SQL code injection: Attack on DB web server that allows SQL statements to come in the application undetected.

  Time/Logic bombs: execute malicious code based on certain time or event.

  Back door: Bypass the application's security mechanism and uses the application resources to view or steal information.

- Attacks against the supporting infrastructure

  Denial of service (DOS): Consume shared resources and compromise the ability of authorized users to access/use those resources.

  Virus: a program/code that replicates by being copied. A virus attaches itself to and becomes part of another program.

  Worm: A standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself.

  Trojan: Provide remote access to a system through a back door/open port.

Spyware: software installed on a machine that secretly gathers information about user activity.

Adware: a program that is unknowingly installed on the PC and produces ads while executing. Many adware come with spyware included.

- Physical attacks

7. How to ensure quality/security in the cube

   - Know the enemy
     - Know weak areas of the application and where attackers are most likely going to attack first.
     - Know who would want to attack your software and why.
     - Know what types of resources would be needed by attackers such as tools, privileges, and time slots.
     - Know how to build countermeasures.
   - Prevent social engineering
     - Verify callers
     - Only give information to identified people.
     - Share information on a need-to-know basis.
     - watch out for shoulder surfing.
   - Clean up the clutter
     - Do not keep sticky notes with passwords on them in or around your desk.
     - Delete old and unnecessary hard and soft documents.
   - Stay current
     - Keep informed of the latest software attacks.

8. Principles and concepts of secure software

   - Secure the weakest link
     - The weakest part of the system will most likely be attacked first.
   - Defense in depth
     - Multiple layers of different types of protection provide substantially better protection.
     - Goal is to limit access to certain features of the application.
   - Fail securely
     - What happens when the system goes down.
     - Address error-handling issues appropriately.
     - Degrade peacefully.
   - Least privilege
     - Give users the least amount of privilege required to perform the use case.
     - Applications that need access to other system resources; grant only what is needed.
   - Keep it simple
     - Keep security simple and keep the application simple.
     - Keep the design simple.
     - Keep the database and code as simple as possible.
   - Secrets are not kept
     - Binary code is not secure code.
     - Do not share passwords.
     - Do not place hard-coded values in code.
     - Place secrets in external resources e.g., DB.

  - Remove comments that reveal secrets.
- Complete mediation
  - Access to every object must be checked for authority.
- Separation of privilege
  - System should not grant permission based on single condition.
  - Company checks over $75,000 need to be signed by two officers.

9. Principles and concepts of quality software

   - Understandability
     - Variables given meaningful names.
     - Logic and loops coded an easy to follow way.
     - If a person does not understand the programming language, they should be able to follow the logic.
   - Flexibility and reusability
     - Can the code be modified easily without affecting a lot of other modules and programs?
     - Can the code be reused or other purposes?
     - Repeatedly used blocks of code should be made into subroutines.
   - Readability and capability
     - Is code so long that a person gets lost trying to follow the execution path?
     - Are inputs validated before use?
   - Maintainability and testability
   - Usability and reliability
     - Is there adequate online help?
     - Is a user manual provided?
     - Are meaningful error messages provided?
     - Will the software perform when needed?
     - Is exception handling provided?

10. Difference between authorization and authentication

    Authorization: Ensuring that the user has the appropriate role and privilege to view data.

    Authentication: Ensuring that the user is who he or she claims to be and that the data comes from the appropriate place.

11. Devise misuse cases

    (a)

12. Definition of assets

    Asset: Anything of value to the stakeholders.

13. ATM case study