STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

SSW 322: Software Engineering Design VI

Security Overview and User Authentication
2020 Spring

Prof. Lu Xiao
lxiao6@stevens.edu
Office Hour: Monday/Wednesday 2 to 4 pm
https://stevens.zoom.us/j/632866976
Software Engineering
School of Systems and Enterprises

Today's Topic – Security Overview

- What is security?---The CIA Triad
- Security Vulnerabilities
- Countermeasures
- Security Design principles

- Computer Security---Principles and Practice 4th Edition, William Stallings and Lawire Brown, ISBN-10 1-292-22061-9

What is Security?

- Computer Security: Measures and controls that ensure confidentiality, integrity, and availability (CIA triad) of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

CIA Triad

- Confidentiality
  - Data confidentiality: private or confidential information is not made available or disclosed to unauthorized users.
  - Privacy: individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
- Integrity
  - Data integrity: information and programs are changed only in a specified and authorized manner
  - System integrity: a system performs its intended functions in an unimpaired way.
- Availability: Assures that a system works promptly and service is not denied to authorized users.

CIA Triad- Examples

- Confidentiality:
  - Student grade information (FERPA) (High)
  - Directory information, such as student list and faculty list (low)
- Integrity:
  - A hospital patient's allergy information (high)
  - Users' registration on a recreation website (moderate)
  - Anonymous online poll (low)
- Availability:
  - A system that provides authentication for critical systems (high)
  - A public website for a university (moderate)
  - Online telephone directory lookup application (low)

Computer Security Terminology

- ***Adversary (threat agent):*** Individual, group, organization, or government that (has the intent to) conducts detrimental activities.
- ***Attack:*** Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.
- ***Countermeasure:*** any means taken to deal with security attack.
- ***Risk:*** A measure of 1) the adverse impacts and 2) the likelihood of occurrence.
- ***Security Policy:*** A set of criteria for the provision of security services.
- ***System Resource (Asset):*** hardware, software, data, and communication lines and networks.
- ***Threat:*** Any circumstance or event with the potential to adversely impact computer security
- ***Vulnerability:*** Weakens in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability

- The system can be **corrupted**, so it does the wrong thing or give wrong answers.
  - For example, stored data values may differ from what they should be because they have been improperly modified.
- The system could become **leaky**.
  - For example, someone who should not have access to some information obtain access through the network.
- The system can become **unavailable** or very slow.
  - That is, using the system or network becomes impossible or impractical.

Vulnerability

- The system can be **corrupted**, so it does the wrong thing or give wrong answers. **(Integrity)**
  - For example, stored data values may differ from what they should be because they have been improperly modified.
- The system could become **leaky**. **(Confidentiality)**
  - For example, someone who should not have access to some information obtain access through the network.
- The system can become **unavailable** or very slow. **(Availability)**
  - That is, using the system or network becomes impossible or impractical.

Attacks

- ***Active attack:*** An attempt to alter system resources or affect their operation
- ***Passive attack:*** An attempt to learn or make use of information from the system that does not affect system resources
- ***Inside attack:*** Initiated by an entity inside the security perimeter (an “insider”). The insider is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
- ***Outside attack:*** Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an “outsider”).

Attacks Cont.

1. ***Unauthorized disclosure*** is a threat to confidentiality.
   - ***Exposure***: this can be deliberate or accidental release of unauthorized knowledge of sensitive data.
   - ***Interception***: a common attack in the context of communications. E.g. a hacker can gain access to email traffic and other data transfer.
   - ***Inference***: an adversary gain information from observing the pattern of traffic on a network.
   - ***Intrusion***: an adversary gain unauthorized access to sensitive data by overcoming the system's access control protections.

Attacks Cont.

2. ***Deception*** is a threat to either system integrity or data integrity.

- ***Masquerade***: unauthorized user gain access to a system by posing as an authorized user.
- ***Falsification***: altering or replacing of valid data or the introduction of false data into a file or database.
- ***Repudiation***: a user either denies sending data, or a user denies receiving or possessing the data.

Attacks Cont.

3. ***Disruption***: a threat to availability or system integrity.

- ***Incapacitation***: this could occur as a result of physical destruction of or damage to system hardware.
- ***Corruption***: malicious software makes the system resources or services function in an unintended manner. Or a user could gain unauthorized access to a system or modify its function.
- ***Obstruction***: disabling communication links or altering communication control information. Or overloading the system by placing excess burden.

Attacks Cont.

4. ***Usurpation***: a threat to system integrity.

- ***Misappropriation***: this can include theft of service, such as distributed denial of service attack.
- ***Misuse***: malicious logic or a hacker gain unauthorized access to a system. Security functions can be disabled or thwarted.

Countermeasures

- FIPS 200 (*Minimum Security Requirements for Federal Information and Information Systems*) enumerates 17 security related areas about protecting the confidentiality, integrity, and availability of information systems.
- They combine technical and managerial approaches to achieve effective computer security.

Countermeasures

1. Access Control: Limit information system access to authorized users and to the types of transactions and functions that authorized users are permitted to exercise.
2. Awareness and Training: Ensure that managers and users are aware of the security risks; and ensure that personnel are adequately trained to carry out their information security-related duties and responsibilities.
3. Audit and Accountability: Create, protect, and retain information system audit records; ensure that individual users can be uniquely traced so they can be held accountable for their actions.
4. Certification, Accreditation, and Security Assessment: Periodically assess the security controls; develop and implement plans of action to correct deficiencies and reduce vulnerabilities; monitor information system security controls on an ongoing basis.

Countermeasures

5. Configuration Management: Establish and maintain baseline configuration and inventories of organizational information systems; establish and enforce security configuration settings.
6. Contingency Planning: Establish, maintain, and implement plans for emergency response, backup, operations, and postdisaster recovery.
7. Identification and Authentication: Identify information system users; and authenticate the identities of those users.
8. Incident Response: Establish an operational incident-handling capability; and tack, document, and report incidents.
9. Maintenance: Perform periodic and timely maintenance; provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Countermeasures

10. Media Protection: Protect information system media; limit access to authorized users; sanitize or destroy information system media before disposal or release for reuse.

11. Physical and Environmental Protection: Limit physical access to systems, equipment, and environments; protect the physical plant and support infrastructure; provide supporting utilities; protect information systems against environmental hazards; and provide appropriate environmental controls.

12. Planning: Develop, document, periodically update, and implement security plans.

13. Personnel Security: Ensure that individuals are trustworthy and meet established security criteria; ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; employ formal sanctions for personnel failing to comply with organization security policies and procedures.

Countermeasures

14. Risk Assessment: Periodically assess the risk to organizational operations.

15. Systems and Services Acquisition: Allocate sufficient resources to adequately protect information systems; employ system development life cycle processes that incorporate security considerations; employ software usage and installation restrictions; and ensure that third-party providers employ adequate security measures.

16. System and Communications Protections: Monitor, control, and protect organizational communications; employ architectural designs, software development techniques, and systems engineering principles

17. System and Information Integrity: Identify, report, and correct information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within organizational information systems; and monitor information system security alerts and advisories and take appropriate actions in response.

Fundamental Security Design Principles

1. Economy of mechanism
2. Fail-safe defaults
3. Complete mediation
4. Open design
5. Separation of privilege
6. Least privilege
7. Least common mechanism
8. Psychological acceptability
9. Isolation
10. Encapsulation
11. Modularity
12. Layering
13. Least astonishment

1. Economy of mechanism

- The design of security measures in both hardware and software should be as simple and small as possible.
- Relatively simple and small design is easier to test and verify thoroughly.
- The more complex the security mechanism is, the more likely it is to possess exploitable flaws.
- In practice, it is perhaps the most difficult principle to honor. There is a constant demand for new features in both hardware and software, complicating the security design task.

2. Fail-safe defaults

- Access decision should be based on permission rather than exclusion. That is, the default situation is lack of access, and the protection scheme identified condition under which access is permitted.
- A design or implementation mistake in a mechanism that gives permission tends to fail by refusing permission---a safe situation that can be quickly detected.
- On the contrary, a design or implementation mistake in a mechanism that excludes access tends to fail by allowing access---a failure that may long go unnoticed in normal use.

3. Complete mediation

- Every access must be checked against the access control mechanism. Systems should not rely on access decisions retrieved from a cache.
- In a system designed to operate continuously, this principle requires that access decisions are remembered for future use, careful consideration be given to how changes in authority are propagated into such local memories.
- File access system appear to provide an example of a system that complies with this principle. However, once a user has opened a file, no check is made to see of permissions change.

4. Open design

- The design of a security mechanism should be open rather than secret.
  - For example, although encryption keys must be secret, encryption algorithms should be open to public scrutiny. The algorithms can then be reviewed by many experts, and users can therefore have high confidence in them.

5. Separation of privilege

- Multiple privilege attributes are required to achieve access to restricted resource.
  - For example, multifactor user authentication, which require the use of multiple techniques, such as a password and a text pin code, to authorize a user.
  - This applies to any technique in which a program is divided into parts that are limited to the specific privilege task.

6. Least privilege

- Every process and user of the system should operate using the least set of privileges necessary to perform the task.
- In a system with multiple user roles, each role is assigned only those permissions needed to perform its functions.
- There is a temporal aspect to this principle. For example, system programs or administrators who have special privilege should have those privileges only when necessary; when they are doing ordinary activities, the privileges should be withdrawn.

7. Least common mechanism

- The design should minimize the functions shared by different users, providing mutual security.
- This principle helps reduce the number of unintended communication paths and reduce the amount of hardware and software on which all users depend, thus making it easier to verify if there are any undesirable security implications.

8. Psychological acceptability

- The security mechanism should not interfere the work of users, and at the same time meet the needs of those who authorize access.
- If security mechanism hinders the usability or accessibility of resources, users may opt to turn off those mechanisms.
- Where possible, security mechanisms should be transparent to the users or introduce minimal obstruction.
- Moreover, security procedures must reflect the user's mental model of protection.

9. Isolation

- This principle applies in three contexts:
  1. Public access systems should be isolated from critical resources to prevent disclosure or tampering. This could be the format of physical or logical isolation.
  2. The processes and files of individual users should be isolated from one another except where it is explicitly desired.
  3. Security mechanisms should be isolated in the sense of preventing access to those mechanisms.

10. Encapsulation

- This can be viewed as a specific form of isolation based on object-oriented functionality.
- Protection is provided by encapsulating a collection of procedures and data objects in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the protected subsystems.

11. Modularity

- It refers to the development of security functions as separate, protected modules
  - Provide common security functions and services, such as cryptographic functions, as common modules.
- And to the use of a modular architecture for mechanism design and implementation.
  - Each security mechanism can be upgraded without the requirement to modify the entire system.

12. Layering

- The use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems.
- A layering approach is often used to provide multiple barriers between an adversary and protected information or services. This technique is often referred to as ***defense in depth.***
- A common example for home users is the Norton Internet Security suite, which provides (among other capabilities): an antivirus application, a firewall application, an anti-spam application, parental controls, privacy controls

13. Least astonishment

- A program or user interface should always respond in the way that is least likely to astonish the user.
  - For example, the mechanism for authorization should be transparent enough to a user that the user has a good intuitive understanding of how the security goals map to the provided security mechanism.


thank you