Security

Idaho State University | Computer Science

Isaac Griffith

CS 3321
Department of Computer Science
Idaho State University

ROAR

Topics Covered

- Security and dependability
- Security and organizations
- Security requirements

Idaho State University
Computer Science

Security engineering

- Tools, techniques and methods to support the development and maintenance of systems that can resist malicious attacks that are intended to damage a computer-based system or its data.
- A sub-field of the broader field of computer security.

ROAR

Security dimensions

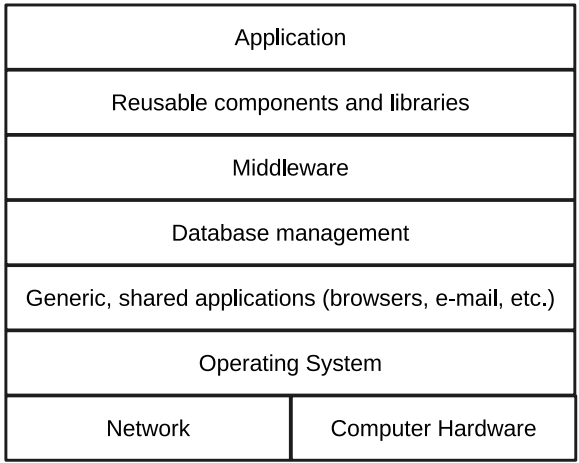
- **Confidentiality**
  - Information in a system may be disclosed or made accessible to people or programs that are not authorized to have access to that information.
- **Integrity**
  - Information in a system may be damaged or corrupted making it unusual or unreliable.
- **Availability**
  - Access to a system or its data that is normally available may not be possible.

Security levels

- Infrastructure security, which is concerned with maintaining the security of all systems and networks that provide an infrastructure and a set of shared services to the organization.
- Application security, which is concerned with the security of individual application systems or related groups of systems.
- Operational security, which is concerned with the secure operation and use of the organization's systems.

Idaho State University
Computer Science

System layers and security



ROAR

Application/infrastructure security

- Application security is a software engineering problem where the system is designed to resist attacks.
- Infrastructure security is a systems management problem where the infrastructure is configured to resist attacks.
- The focus of this chapter is application security rather than infrastructure security.

Idaho State University
Computer Science

System security management

- User and permission management
  - Adding and removing users from the system and setting up appropriate permissions for users
- Software deployment and maintenance
  - Installing application software and middleware and configuring these systems so that vulnerabilities are avoided.
- Attack monitoring, detection and recovery
  - Monitoring the system for unauthorized access, design strategies for resisting attacks and develop backup and recovery strategies.

ROAR

Operational Security

- Primarily a human and social issue
- Concerned with ensuring the people do not take actions that may compromise system security
  - E.g. Tell others passwords, leave computers logged on
- Users sometimes take insecure actions to make it easier for them to do their jobs
- There is therefore a trade-off between system security and system effectiveness.

Security and dependability

Security

- The security of a system is a system property that reflects the system's ability to protect itself from accidental or deliberate external attack.
- Security is essential as most systems are networked so that external access to the system through the Internet is possible.
- Security is an essential pre-requisite for availability, reliability and safety.

Fundamental security

- If a system is a networked system and is insecure then statements about its reliability and its safety are unreliable.
- These statements depend on the executing system and the developed system being the same. However, intrusion can change the executing system and/or its data.
- Therefore, the reliability and safety assurance is no longer valid.

Security terminology

- **Asset** - Something of value which has to be protected. The asset may be the software system itself or data used by that system.
- **Attack** - An exploitation of a system's vulnerability. Generally, this is from outside the system and is a deliberate attempt to cause some damage.
- **Control** - A protective measure that reduces a system's vulnerability. Encryption is an example of a control that reduces a vulnerability of a weak access control system
- **Exposure** - Possible loss or harm to a computing system. This can be loss or damage to data, or can be a loss of time and effort if recovery is necessary after a security breach.
- **Threat** - Circumstances that have potential to cause loss or harm. You can think of these as a system vulnerability that is subjected to an attack.
- **Vulnerability** - A weakness in a computer-based system that may be exploited to cause loss or harm.

Examples of security terminology (Mentcare)

- **Asset** - The records of each patient that is receiving or has received treatment.
- **Exposure** - Potential financial loss from future patients who do not seek treatment because they do not trust the clinic to maintain their data. Financial loss from legal action by the sports star. Loss of reputation.
- **Vulnerability** - A weak password system which makes it easy for users to set guessable passwords. User ids that are the same as names.
- **Attack** - An impersonation of an authorized user.
- **Threat** - An unauthorized user will gain access to the system by guessing the credentials (login name and password) of an authorized user.
- **Control** - A password checking system that disallows user passwords that are proper names or words that are normally included in a dictionary.

Threat types

- Interception threats that allow an attacker to gain access to an asset.
  - A possible threat to the Mentcare system might be a situation where an attacker gains access to the records of an individual patient.
- Interruption threats that allow an attacker to make part of the system unavailable.
  - A possible threat might be a denial of service attack on a system database server so that database connections become impossible.

Threat types

- Modification threats that allow an attacker to tamper with a system asset.
  - In the Mentcare system, a modification threat would be where an attacker alters or destroys a patient record.
- Fabrication threats that allow an attacker to insert false information into a system.
  - This is perhaps not a credible threat in the Mentcare system but would be a threat in a banking system, where false transactions might be added to the system that transfer money to the perpetrator's bank account.

Security assurance

- Vulnerability avoidance
  - The system is designed so that vulnerabilities do not occur. For example, if there is no external network connection then external attack is impossible
- Attack detection and elimination
  - The system is designed so that attacks on vulnerabilities are detected and neutralized before they result in an exposure. For example, virus checkers find and remove viruses before they infect a system
- Exposure limitation and recovery
  - The system is designed so that the adverse consequences of a successful attack are minimized. For example, a backup policy allows damaged information to be restored

Security and dependability

- Security and reliability
  - If a system is attacked and the system or its data are corrupted as a consequence of that attack, then this may induce system failures that compromise the reliability of the system.
- Security and availability
  - A common attack on a web-based system is a denial of service attack, where a web server is flooded with service requests from a range of different sources. The aim of this attack is to make the system unavailable.

Security and dependability

- Security and safety
  - An attack that corrupts the system or its data means that assumptions about safety may not hold. Safety checks rely on analyzing the source code of safety critical software and assume the executing code is a completely accurate translation of that source code. If this is not the case, safety-related failures may be induced and the safety case made for the software is invalid.
- Security and resilience
  - Resilience is a system characteristic that reflects its ability to resist and recover from damaging events. The most probable damaging event on networked software systems is a cyberattack of some kind so most of the work now done in resilience is aimed at deterring, detecting and recovering from such attacks.

Security and organizations

Security is a business issue

- Security is expensive and it is important that security decisions are made in a cost-effective way
  - There is no point in spending more than the value of an asset to keep that asset secure.
- Organizations use a risk-based approach to support security decision making and should have a defined security policy based on security risk analysis
- Security risk analysis is a business rather than a technical process

Idaho State University
Computer Science

Organizational security policies

- Security policies should set out general information access strategies that should apply across the organization.
- The point of security policies is to inform everyone in an organization about security so these should not be long and detailed technical documents.
- From a security engineering perspective, the security policy defines, in broad terms, the security goals of the organization.
- The security engineering process is concerned with implementing these goals.

Security policies

- The assets that must be protected
  - It is not cost-effective to apply stringent security procedures to all organizational assets. Many assets are not confidential and can be made freely available.
- The level of protection that is required for different types of asset
  - For sensitive personal information, a high level of security is required; for other information, the consequences of loss may be minor so a lower level of security is adequate.

Security policies

- The responsibilities of individual users, managers and the organization
  - The security policy should set out what is expected of users e.g. strong passwords, log out of computers, office security, etc.
- Existing security procedures and technologies that should be maintained
  - For reasons of practicality and cost, it may be essential to continue to use existing approaches to security even where these have known limitations.

Risk assessment and mgmt

- Risk assessment and management is concerned with assessing the possible losses that might ensue from attacks on the system and balancing these losses against the costs of security procedures that may reduce these losses.
- Risk management should be driven by an organizational security policy.
- Risk management involves
  - Preliminary risk assessment
  - Life cycle risk assessment
  - Operational risk assessment

Preliminary risk assessment

- The aim of this initial risk assessment is to identify generic risks that are applicable to the system and to decide if an adequate level of security can be achieved at a reasonable cost.
- The risk assessment should focus on the identification and analysis of high-level risks to the system.
- The outcomes of the risk assessment process are used to help identify security requirements.

Design risk assessment

- This risk assessment takes place during the system development life cycle and is informed by the technical system design and implementation decisions.
- The results of the assessment may lead to changes to the security requirements and the addition of new requirements.
- Known and potential vulnerabilities are identified, and this knowledge is used to inform decision making about the system functionality and how it is to be implemented, tested, and deployed.

Operational risk assessment

- This risk assessment process focuses on the use of the system and the possible risks that can arise from human behavior.
- Operational risk assessment should continue after a system has been installed to take account of how the system is used.
- Organizational changes may mean that the system is used in different ways from those originally planned. These changes lead to new security requirements that have to be implemented as the system evolves.

Security requirements

Security specification

- Security specification has something in common with safety requirements specification – in both cases, your concern is to avoid something bad happening.
- Four major differences
  - Safety problems are accidental – the software is not operating in a hostile environment. In security, you must assume that attackers have knowledge of system weaknesses
  - When safety failures occur, you can look for the root cause or weakness that led to the failure. When failure results from a deliberate attack, the attacker may conceal the cause of the failure.
  - Shutting down a system can avoid a safety-related failure. Causing a shut down may be the aim of an attack.
  - Safety-related events are not generated from an intelligent adversary. An attacker can probe defenses over time to discover weaknesses.

Idaho State University
Computer Science

Types of security requirement

- Identification requirements.
- Authentication requirements.
- Authorization requirements.
- Immunity requirements.
- Integrity requirements.
- Intrusion detection requirements.
- Non-repudiation requirements.
- Privacy requirements.
- Security auditing requirements.
- System maintenance security requirements.

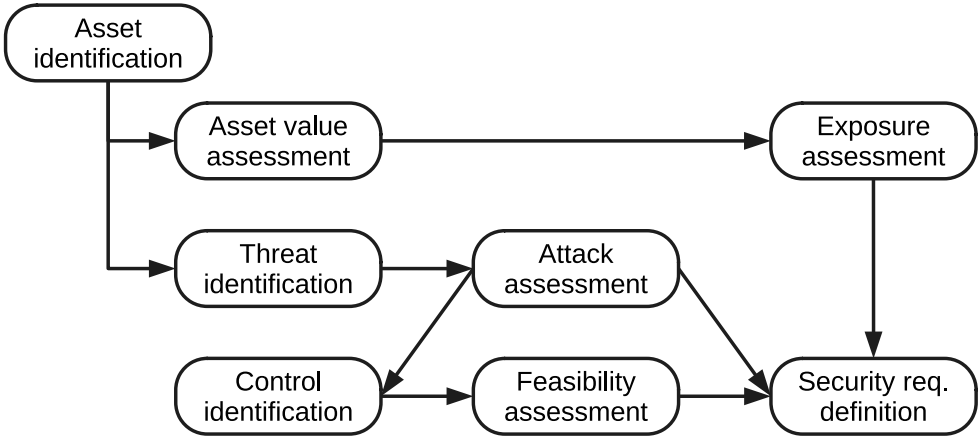
ROAR

Security requirement classification

- Risk avoidance requirements set out the risks that should be avoided by designing the system so that these risks simply cannot arise.
- Risk detection requirements define mechanisms that identify the risk if it arises and neutralize the risk before losses occur.
- Risk mitigation requirements set out how the system should be designed so that it can recover from and restore system assets after some loss has occurred.

Idaho State University
Computer Science

Preliminary risk assessment



ROAR

Security risk assessment

- Asset identification
  - Identify the key system assets (or services) that have to be protected.
- Asset value assessment
  - Estimate the value of the identified assets.
- Exposure assessment
  - Assess the potential losses associated with each asset.
- Threat identification
  - Identify the most probable threats to the system assets

Security risk assessment

- Attack assessment
  - Decompose threats into possible attacks on the system and the ways that these may occur.
- Control identification
  - Propose the controls that may be put in place to protect an asset.
- Feasibility assessment
  - Assess the technical feasibility and cost of the controls.
- Security requirements definition
  - Define system security requirements. These can be infrastructure or application system requirements.

Asset analysis

- **The information system**
  - Value: High. Required to support all clinical consultations. Potentially safety-critical.
  - Exposure: High. Financial loss as clinics may have to be canceled. Costs of restoring system. Possible patient harm if treatment cannot be prescribed.
- **The patient database**
  - Value: High. Required to support all clinical consultations. Potentially safety-critical.
  - Exposure: High. Financial loss as clinics may have to be canceled. Costs of restoring system. Possible patient harm if treatment cannot be prescribed.
- **An individual patient record**
  - Value: Normally low although may be high for specific high-profile patients.
  - Exposure: Low direct losses but possible loss of reputation.

Threat and control analysis

- Threat: An unauthorized user gains access as system manager and makes system unavailable
  - Probability: Low
  - Control: Only allow system management from specific locations that are physically secure.
    - Feasibility: Low cost of implementation but care must be taken with key distribution and to ensure that keys are available in the event of an emergency.

Threat and control analysis

- Threat: An unauthorized user gains access as system user and accesses confidential information
  - Probability: High
  - Control: Require all users to authenticate themselves using a biometric mechanism.
    - Feasibility: Technically feasible but high-cost solution. Possible user resistance.
  - Control: Log all changes to patient information to track system usage.
    - Feasibility: Simple and transparent to implement and also supports recovery.

Mentcare security req’ts

- Patient information shall be downloaded at the start of a clinic session to a secure area on the system client that is used by clinical staff.
- All patient information on the system client shall be encrypted.
- Patient information shall be uploaded to the database after a clinic session has finished and deleted from the client computer.
- A log on a separate computer from the database server must be maintained of all changes made to the system database.

Are there any questions?