CSCI 455: Principles of Computer Security

Set 01: Overview.

Reading: Chapter 1 in Stallings & Brown

Slide Sources

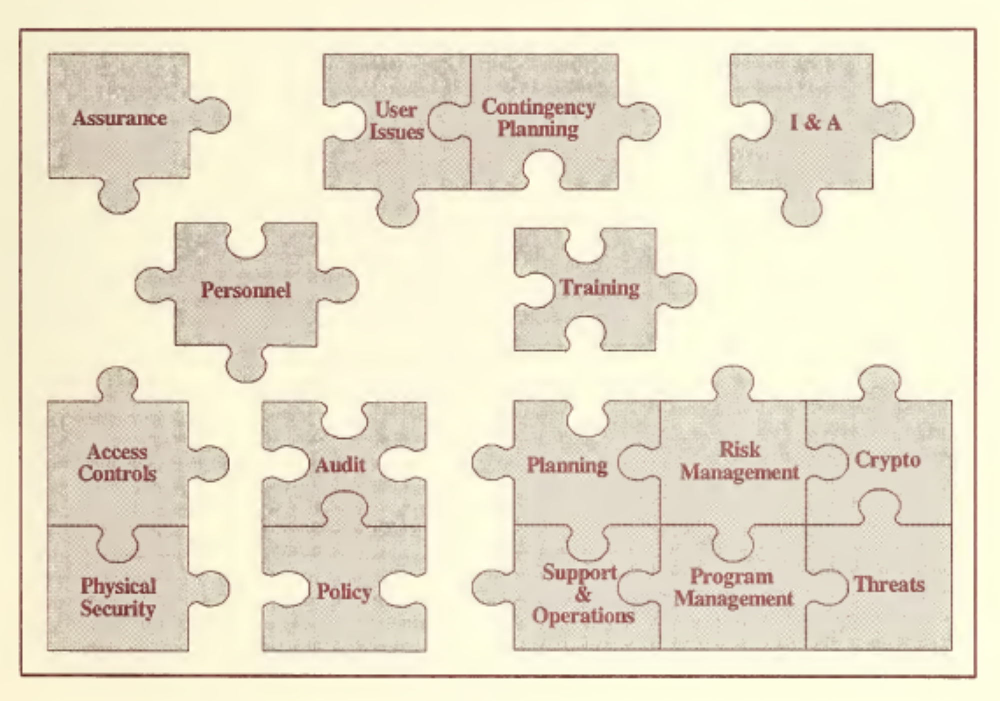
- Multiple sources including
  - Stallings & Brown textbook materials
  - Other readings including NIST publications
  - My prior slides
  - Others

What is Computer Security?

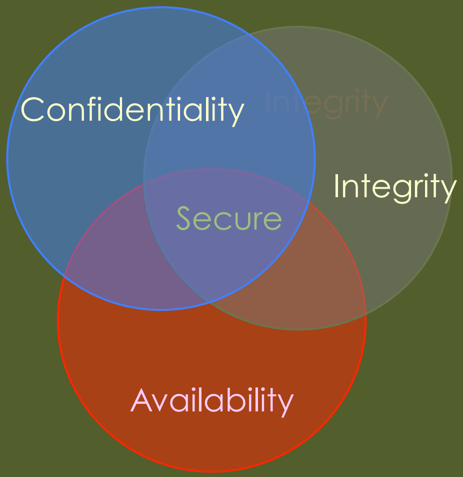
- Discussion

Overview: What is Computer Security?

- "The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/ data, and telecommunications)."
  - NIST Computer Security Handbook
  - http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf



C-I-A Triad (Pillars): Three Objectives



- Confidentiality: two related concepts
  - Data confidentiality: private or confidential information is not made available or disclosed to unauthorized individuals
  - Privacy: Assures that individuals can control or influence what information related to them may be collected/stored, and by whom, and to whom it may be disclosed
- Integrity: Also covers two related concepts
  - Data integrity: Assures that information and programs are changed only in a specified and authorized manner
  - System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
- Availability
  - Assures that systems work promptly and service is never denied to authorized users

What makes A different from C and I?

From CIA to CIANA: The CIANA Pentad

- Non-repudiation
  - Assures that system has the ability to correlate, with high certainty, a recorded action with its originating individual or entity
- Authentication
  - Assures that the system has the ability to verify the identity of an individual or entity

Security Breach Impact (C-I-A Loss) — 1

- Impact levels
  - FIPS 199: Standards for Security Categorization of Federal Information and Information Systems)
    - http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- Low
  - Loss expected to have limited adverse effect on operations, assets, or individuals.
  - Some degradation, minor asset damage, some financial loss, and minor individual harm

Security Breach Impact (C-I-A Loss) — 2

- Moderate
  - Serious adverse effect on operations, organizational assets, or individuals
  - Significant degradation, damage to assets, financial loss; or harm to individuals that does not involve loss of life or serious, life-threatening injuries
- High
  - Severe or catastrophic adverse operations, organizational assets, or individuals.
  - Organization not able to perform one or more of its primary functions, or major damage to organizational assets, or major financial loss; or severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries

Terminology

- Building up a glossary of common terms
  - A worthwhile exercise
- Good news
  - Many such glossaries are available online
- Bad news
  - Too many of them, some contradict one another!
- Earlier document URLs have some definitions
- Here's one more
  - Internet Security Glossary, Version 2
    - https://tools.ietf.org/html/rfc4949

Security Concepts and Relationships

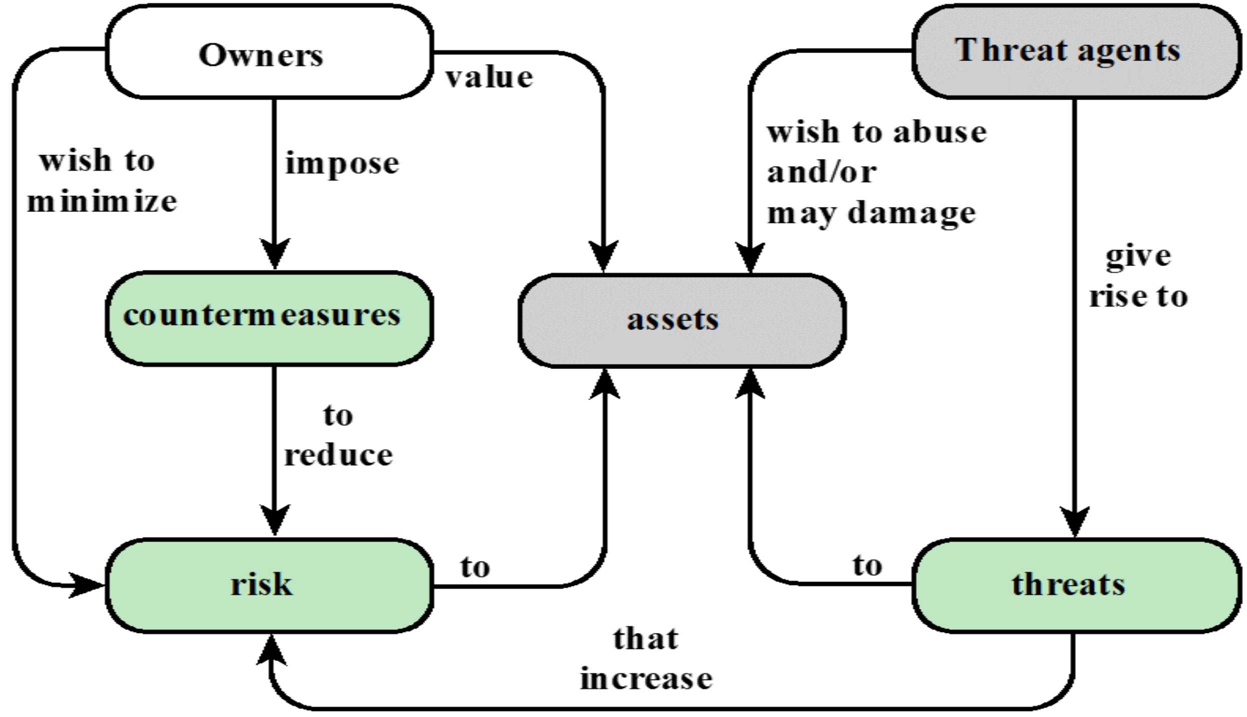


Figure 1.1 Security Concepts and Relationships

Some Security Challenges — 1

- Computer security is not as simple as it might first seem
  - Requirements seem straightforward, but mechanisms meeting them can be complex and subtle
- In developing a particular security mechanism or algorithm, one must always consider potential attacks (often unexpected) on those security features
- Procedures to provide services are often counterintuitive
- Once security mechanisms are designed, need to decide where to use them
- Security mechanisms often involve more than one particular algorithm/protocol,
  - Also, users need secret information, and how create, distribute, and protect this secret information

Some Security Challenges — 2

- Battle of wits between perpetrator finding holes and designer/administrator closing them
- Natural tendency of users and managers to perceive little benefit from security investment until a security failure occurs
- Requires regular monitoring, which is difficult in today's short-term environment
- Still too often an afterthought—incorporated after the design is complete
- Users/security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

Computer Assets

- Hardware
  - Computers, data processors/storage, communications units, special-purpose units, ..
- Mobile systems
  - Laptops, tablets, smartphones, …
- Software
  - Operating system, system utilities, apps
- Data
  - Files and databases,
  - Security-related data: passwords, logs
- Communication
  - LANs, WANS, links, bridges, routers
- …

Think of each threat terms of the C-I-A
Hardware & C: loss of unencrypted laptop
Hardware and I: ???
… and so on

Vulnerabilities, Threats and Attacks

- Vulnerabilities come from loss of the C-I-A
  - Corruption (loss of integrity)
  - Leaks (loss of confidentiality)
  - Slowness or inaccessibility (loss of availability)
  - Threats (capability to exploit vulnerabilities)
  - Represent potential security harm to an asset

Attacks (Threats Carried Out)

- Passive: attempt to learn or use data from system without affect on system resources
  - Eavesdropping, traffic analysis, message release
  - Difficult to detect because they do not involve any alteration of the data
  - Need to be prevented as top priority

- Active: attempt to alter system resources or affect their operation
  - Replay, masquerade, message modification, and denial of service
  - Difficult to prevent active attacks as full protection of all paths at all times
  - Detection and recovery mechanisms also have a deterrent effect, and prevent attacks

Insider v. Outsider Attacks

- Insider
  - Initiated by entity inside the security parameter
  - Is this difficult to prevent, detect and recover from?

- Outsider
  - Initiated from outside the security perimeter
  - Is this difficult to prevent, detect and recover from?

Countermeasures

- Any means deal with a security attack
- Ideally prevents a given type of attack
  - When prevention not possible or fails, it should detect and recover from the attack
- It may itself introduce new vulnerabilities, or residual vulnerabilities can be exploited by threat agents
  - Owners seek to minimize risk given other constraints
- Need to minimize residual level of risk to assets

Threat Consequences/Corresponding Attacks

- Unauthorized disclosure (threat to confidentiality)
- Exposure, Interception, Inference, Intrusion
- Deception (threat to either system or data integrity)
- Masquerade, falsification, repudiation
- Disruption (threat to availability or system integrity)
- Incapacitation, corruption, obstruction
- Usurpation (threat to system integrity)
- Misappropriation, misuse

Security Requirements: FIPS PUB 200

http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

- Policies & procedures
  - 17 security-related areas re. protecting C-I-A of federal information systems and information processed, stored, and transmitted by those systems
  - Broad-based, balanced information security program
    - Addresses management, operational, technical aspects of protecting federal information and information systems

1. Access control
2. Awareness and training
3. Audit and accountability
4. Certification, accreditation, and security assessments
5. Configuration management
6. Contingency planning
7. Identification and authentication
8. Incident response
9. Maintenance
10. Media protection
11. Physical and environmental protection
12. Planning
13. Personnel security
14. Risk assessment
15. Systems and services acquisition
16. System and communications protection
17. System and information integrity

The Sad Truth

- Despite decades of R&D, …
  - It has not been possible to develop security design and implementation techniques that systematically exclude security flaws and prevent all unauthorized actions
- In the absence of such foolproof techniques
  - Useful to have a set of widely agreed design principles that can guide the development of protection mechanisms

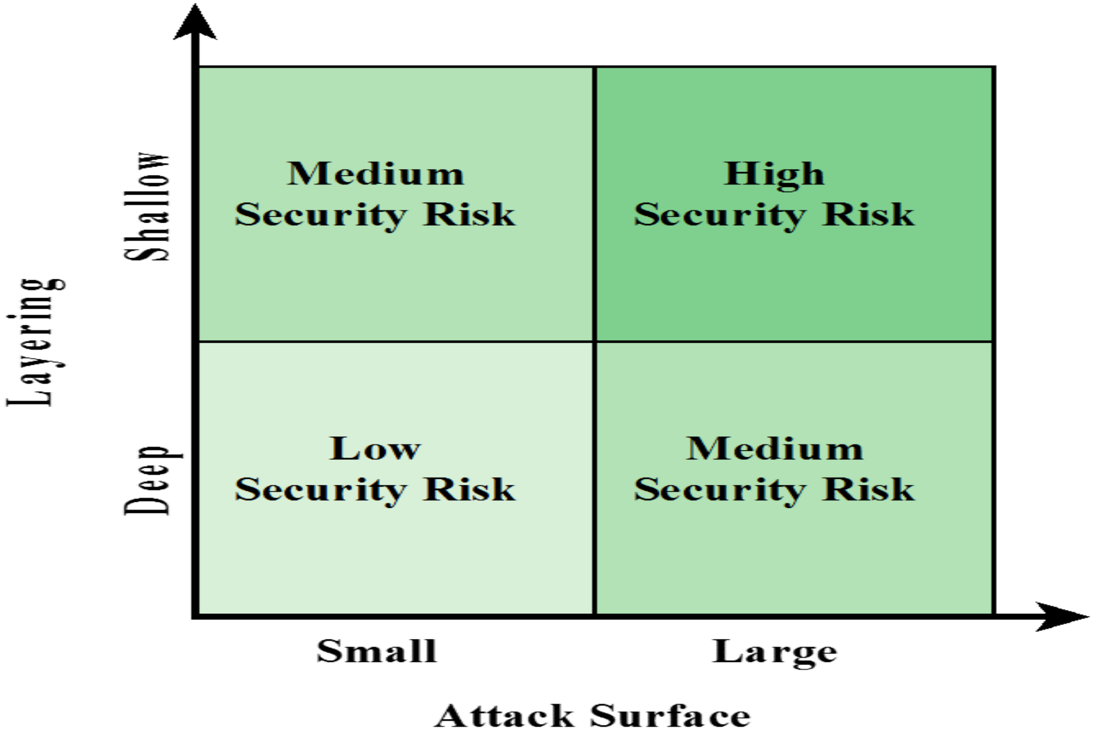
Fundamental Security Design Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Layering
- Least astonishment

Attack Surface — 1

- Consists of reachable and exploitable system vulnerabilities
  - Open ports with code listening on those ports
  - Code that processes incoming data, email, XML, office documents, and similar formats
  - Interfaces, SQL, and Web forms
  - Employee with access to sensitive information vulnerable to a social engineering attack
  - Different attack surfaces: network, software, human
- Attack tree
  - Branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities

Attack Surface — 2



	Small	Large
Shallow	Medium Security Risk	High Security Risk
Deep	Low Security Risk	Medium Security Risk

Figure 1.3 Defense in Depth and Attack Surface

A Dumb Idea (Or Not?)

- To protect computer systems and protecting data, just simply turn off the computer and hard drives and store them in a truly safe vault
  - Great idea, right?
- Why is this not acceptable?
  - Because we need to continue to provide services while maintaining CIANAs

Food for Thought

- True or false
  - Security is only possible in two situations
    1. A world in which everybody trusts everybody else or
    2. A world where nobody trusts anybody else!
- Discussion!