INTRODUCTION TO COMPUTER SECURITY

Chapter 1

WHAT IS COMPUTER SECURITY?
(WE ACADEMICS LOVE OUR DEFINITIONS)

The NIST Computer Security Handbook defines computer security as:

- "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"
- This includes hardware, software, firmware, information, data, and telecommunications (among others that might not be listed)

CHALLENGES IN COMPUTER SECURITY

- Computer security is not as simple as it might first appear
- Attackers only need to find a *single* weakness, the engineer needs to find *all* weaknesses
- Users and system managers tend to not see the benefits of security until a failure occurs
- Potential attacks on the security features must be considered
- Procedures used to provide particular services are often counterintuitive
- Physical and logical placement needs to be determined
- Security requires regular and constant monitoring (at high cost)
- Often an afterthought to be incorporated into a system after the design is complete
- Additional algorithms or protocols may be involved (complexity, distribution of "secret" information to users)
- Thought of as an impediment to efficient and user-friendly operation

THE CIA TRIAD
(WHICH HAS LITTLE TO DO WITH THE CENTRAL INTELLIGENCE AGENCY)

The CIA Triad (2)

- Confidentiality

  Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

- Integrity

  Guarding against improper information modification or destruction,
  including ensuring information non-repudiation and authenticity. A loss of
  integrity is the unauthorized modification or destruction of information.

- Availability

  Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an
  information system.

Note: the CIA Triad is a *balancing act*. As soon as we emphasise one category, we sacrifice elements of the others. Meaning, we can't have high confidentiality and also high availability; those two things are *mutually exclusive*.

SECURITY CONCEPTS AND RELATIONS

ASSETS OF COMPUTING SYSTEMS

- Hardware
  - Including computer systems and other data processing, data storage, and data communications devices
- Software
  - Including the operating system, system utilities, and applications
- Data
  - Including files and databases, as well as security-related data, such as password files.
- Communication and Networks
  - Local and wide area network communication links, bridges, routers, and so on.

VULNERABILITIES, THREATS AND ATTACKS

- Categories
  - Leaks (loss of *confidentiality*)
  - Corruption (loss of *integrity*)
  - Unavailable or slow (loss of *availability*)
- Threats
  - Things that are capable of exploiting a vulnerability
- Attacks (executed threats)
  - Passive
    - An attempt to learn or make use of information from the system that does not affect system resources
  - Active
    - An attempt to alter system resources or affect their operation
  - Insider
    - Initiated by an entity inside the security perimeter or an authorized user
  - Outsider
    - Initiated from outside the perimeter or an illegitimate user

COUNTERMEASURES

Some means to deal with a security attack:

- Prevent
- Detect
- Recover

- Countermeasures are also not without their own issues:
  - May not fully neutralize threats
  - May introduce their own vulnerabilities
  - Ultimately, only used to minimize risk

THREAT CONSEQUENCES

ASSETS AND EXAMPLES OF THREATS

PASSIVE AND ACTIVE THREATS

- Passive
  - Attempts to learn about system without affecting resources
  - Can consist of eavesdropping or monitoring
- Active
  - Attempts to affect system resources or operations
  - Typically involve some modification of data or falsifying data
  - Four categories:
    - Replay
    - Masquerade
    - Modification of messages
    - Denial of Service (DoS)

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 SURFACES

Consist of the reachable and exploitable vulnerabilities in a system

- Examples:
  - Open ports
  - Services within a firewall
  - Interpretive code (eg. XML, PHP, Office Docs)
  - Interfaces (eg. SQL, web forms)
  - People! (eg. social engineering)

Attack Surfaces (2)

Attack Surfaces (3)

Consider an automated teller machine (ATM):

- In order of priority (high, medium, low) where each priority level has *one* item, how would you design an ATM machine using the CIA triad?
- Which item should have a high priority?
- Which item should have a medium priority?
- Which item should have a low priority?
- Why did you choose these priority levels?

Remember, you *cannot* make everything a high priority. You must make choices based on your design. What are the problems with your design? Would changing priorities fix your problems? What problems might be introduced by changing priorities?

ATTACK TREES