Course Logistics

- Course policy review.
- Office hours 2 - 4 Tuesdays. Else walk in.
- TA (Vikram) will be in lab for at least 10 hours a week. You can see him any time.
- HW 1 handed out. Due next week
- Lab open from this week. Hours posted on website. Basically 10 to 6 weekdays and 11 to 5 Saturday.
- No more travel planned this semester 😊

- **Security** - freedom from risk and danger.
- In early days of computers security meant physical security and confidentiality.
- Integrity and access control then became important with multi-tasking computers.
- In recent years availability is a big issue.
- Now security is hard to define!!

Computer Security Definitions.

- Security is the ability of a system to protect information and system resources with respect to confidentiality, integrity, and availability.
- Computer Security deals with the prevention and detection of unauthorized actions by users of a computer system.
- Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.
Goals of Security

- **Prevention**
  - Involves implementing mechanisms that users cannot override and are trusted to be implemented in correct and unalterable ways.

- **Detection**
  - Goal is to determine that an attack is underway, or has occurred and report it.

- **Recovery**
  - Resuming correct operation either after an attack or even while an attack is underway.


- Identification and Authentication.
- Access Control.
- Confidentiality.
- Privacy.
- Integrity.
- Non-Repudiation.
- Availability.
- Audit Trails
Methods of Defense

- Security policies.
- Cryptography and cryptographic protocols.
- Software controls.
  - Internal program controls.
  - Operating system controls.
  - Development controls.
- Hardware controls.
- Physical controls.

Policy and Mechanism

- A security policy is a statement of what is, and is not, allowed.
  - Expressed mathematically. Axiomatic.
  - List of allowed and disallowed actions
- A security mechanism is a procedure, tool, or method of enforcing security policy.
  - Can be non-technical
Computer Security and Trust.

- Tomas Olovsson – “A secure system is a system on which enough trust can be put to use it together with sensitive information.”
- “You can't trust code that you did not totally create yourself!!” - Reflections on trusting trust – Ken Thompson’s Turing Award Lecture.
- The open source movement and Linux. Install Linux today!!

Assumptions and Trust

Let A be the set of secure states (as specified by some security policy). Let the security mechanisms restrict the system to some set of states R.

- A security mechanism is secure if $R \subseteq A$; it is precise if $R = A$; and it is broad if there are states $r$ such that $r \in R$ and $r \notin R$
- Trusting the mechanism requires us to assume:
  - Each mechanism designed to implement part of policy
  - Union of mechanisms implement all aspects of policy
  - Implemented correctly
  - Installed and administered correctly
Assurance

- How do we quantify trust?
- System specification, design and implementation can provide a basis for determining how much to trust - assurance.
- When you buy a bottle of aspirin from a drug store you trust it. Why?
  - FDA, Manufacturing standards, safety seal on bottle provide assurance.

Specification, Design and Implementation

- A specification is a statement of the desired functioning of the system.
- Design of a system translates the specifications into components that will implement the specifications.
- Given a design, an implementation creates a system that satisfies the design.
Operational Issues

- Cost-Benefit Analysis: Difficult to do in a precise manner.
- Risk Analysis: Is often subjective.
- Laws and Custom.
- Human Issues

Security Life Cycle
Why is it difficult?

- Complexity.
- Resource sharing.
- Unknown Perimeter.
- Many points of attack.
- Anonymity.
- Unknown Paths.

Some interesting facts

- Common Causes of damage: Human Error 52%, Dishonest people 10%, Technical Sabotage 10%, Fire 15%, Water 10% and Terrorism 3%.
- Who causes damage? Current employees 81%, Outsiders 13%, Former employees 6%.
- Types of computer crime: Money theft 44%, Damage of software 16%, Theft of information 16%, Alteration of data 12%, Theft of services 10%, Trespass 2%.
Type of Threats in Networked Systems

- A threat is a danger which could affect the security (confidentiality, integrity, availability) of assets, leading to a potential loss or damage.
  - Interruption
  - Interception
  - Modification
  - Fabrication
Type of Threats

- Interruption: An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on the availability. Examples include destruction of a piece of hardware, such as a hard disk, the cutting of a communication link, or the disabling of the file management system.

- Interception: An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program, or a computer. Examples include wiretapping to capture data in a network. And the illicit copying of files or programs.

- Modification: An unauthorized party not only gains access to but tampers with an asset. This is an attack on the integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of a message being transmitted in a network.

- Fabrication: An unauthorized part inserts counterfeit objects into the system. This is an attack on the authenticity. Examples include the insertion of spurious messages in a network or the addition of records to a file.
Classification of Attacks

- Computer Security attacks can be classified into two broad categories:
  - **Passive Attacks** can only observe communications or data
  - **Active Attacks** can actively modify communications or data. Often difficult to perform, but very powerful
    - Mail forgery/modification
    - TCP/IP spoofing/session hijacking

Passive Attacks and Active Attacks

```
Passive Threats
  \------------------\   \------------------\   \------------------\   \------------------\  
| Interception (secrecy) | Traffic Analysis | Release of Message Contents | 
\------------------\   \------------------\   \------------------\   \------------------\  
Active Threats
  \------------------\   \------------------\   \------------------\   \------------------\  
| Interruption (availability) | Modification (integrity) | Fabrication (integrity) |
```
Passive Attacks

- Eavesdropping on or monitoring of transmission.
- The goal of the opponent is to obtain information that is being transmitted.
- Two types:
  - Release-of-message contents: Opponent finds out the contents or the actual messages being transmitted
  - Traffic Analysis: More subtle than release-of-message contents messages may be kept secret by masking or encryption but the opponent figures out information being carried by the messages based on the frequency and timings of the message

Passive Attacks Problems

- Difficult to detect because there is no modification of data
- Protection approach should be based on prevention rather than detection.
Active Attacks

- Active attacks involve some sort of modification of the data stream or the creation of a false stream.
- Four sub-categories:
  - Masquerade: An entity pretends to be another usually for the purpose of doing some other form of attack
  - Replay: First passive capture of data and then its retransmission to produce an unauthorized effect.
  - Modification of Messages: Some portion of a legitimate message is altered or messages are delayed or reordered to produce an unauthorized effect.
  - Denial of service: Prevents the normal use or management of communication facilities.
  - Man-in-the-middle attack: A double masquerade.

Problems with Active Attacks

- Easy to detect but difficult to prevent
- Efforts are directed to quickly recover from disruption or delays
- Good thing is that detection will have a deterrent effect.
Model for Network Security

Network Access Security Model
# Security Mechanisms

- Three basic building blocks are used:
  - Encryption is used to provide confidentiality, can provide authentication and integrity protection
  - Digital signatures are used to provide authentication, integrity protection, and non-repudiation
  - Checksums/hash algorithms are used to provide integrity protection, can provide authentication
- One or more security mechanisms are combined to provide a security service

# Services, Mechanisms, Algorithms

- A typical security protocol provides one or more services
- Services are built from mechanisms
- Mechanisms are implemented using algorithms

<table>
<thead>
<tr>
<th>SSL</th>
<th>Services (in security protocol)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signatures</td>
<td>Encryption</td>
</tr>
<tr>
<td>DSA  RSA  RSA  DES SHA1 MD5</td>
<td>Mechanisms  Algorithms</td>
</tr>
</tbody>
</table>