Internet/Computer Security

Terminology

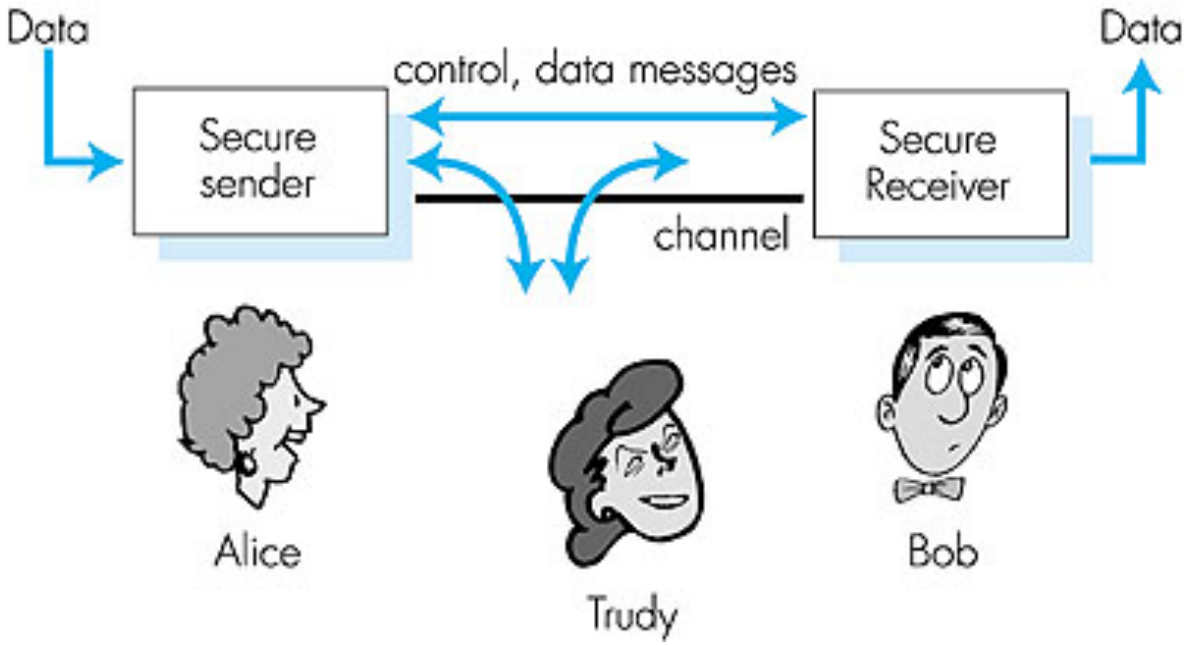
Introduction to Computer Security

- What is Computer Security?

A first definition:

To prevent and detect unauthorized actions by users or *others* of a system.

Simple Scenario



- Well-known in network security world
- Friends and enemies: Alice, Bob, Trudy/Eve
- Bob, Alice want to communicate "securely" (they maybe "lovers")
- Trudy/Eve, the "intruder", the "evil person" may intercept, delete, add, and/or modify messages

Introduction into Computer Security

- How to achieve Computer Security?
  - Security principles/concepts: explore general principles/concepts that can be used as a guide to design secure information processing systems.
  - Security mechanisms: explore some of the security mechanisms that can be used to secure information processing systems.
  - Physical/Organizational security: consider physical & organizational security measures (policies).

Introduction into Computer Security

- Security is about protecting assets.

This involves:

  - Prevention
  - Detection
  - Reaction (recover/restore assets)

Introduction into Computer Security

- Computer Security is:
  1. Confidentiality: prevent unauthorized disclosure of information.
  2. Integrity: prevent unauthorized modification of information.
  3. Availability: prevent unauthorized withholding of information.
- In addition:
  - Authenticity, accountability, reliability, safety, dependability, survivability, …

Introduction into Computer Security

- Even at this general level there is disagreement on the precise definitions of some of the required security aspects.

References:

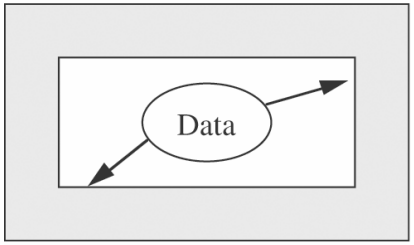
- *Orange book* – US Dept of Defense, Trusted Computer System Evaluation Criteria.
- *ITSEC* – European Trusted Computer System Product Criteria.
- *CTCPEC* – Canadian Trusted Computer System Product Criteria.

Confidentiality

- Historically, security is closely linked to secrecy. Security involved a few organizations dealing mainly with classified data.

  However, nowadays security extends far beyond confidentiality.

- Confidentiality involves:



Confidentiality

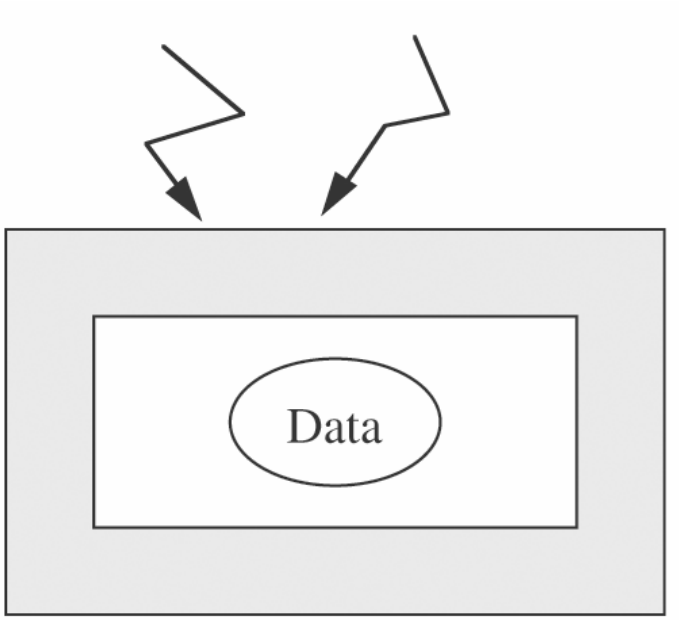
  - Privacy: protection of private data,
  - Secrecy: protection of organizational data.

Integrity

- "Making sure that everything is as it is supposed to be."

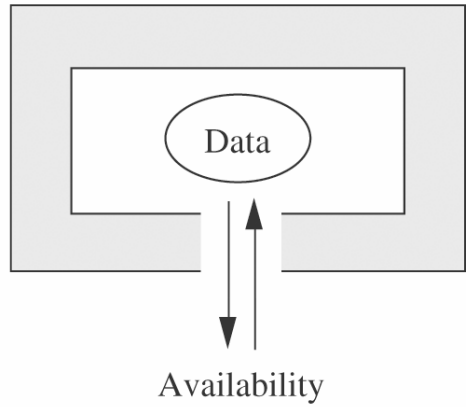
For Computer Security this means:

Preventing unauthorized writing or modifications.



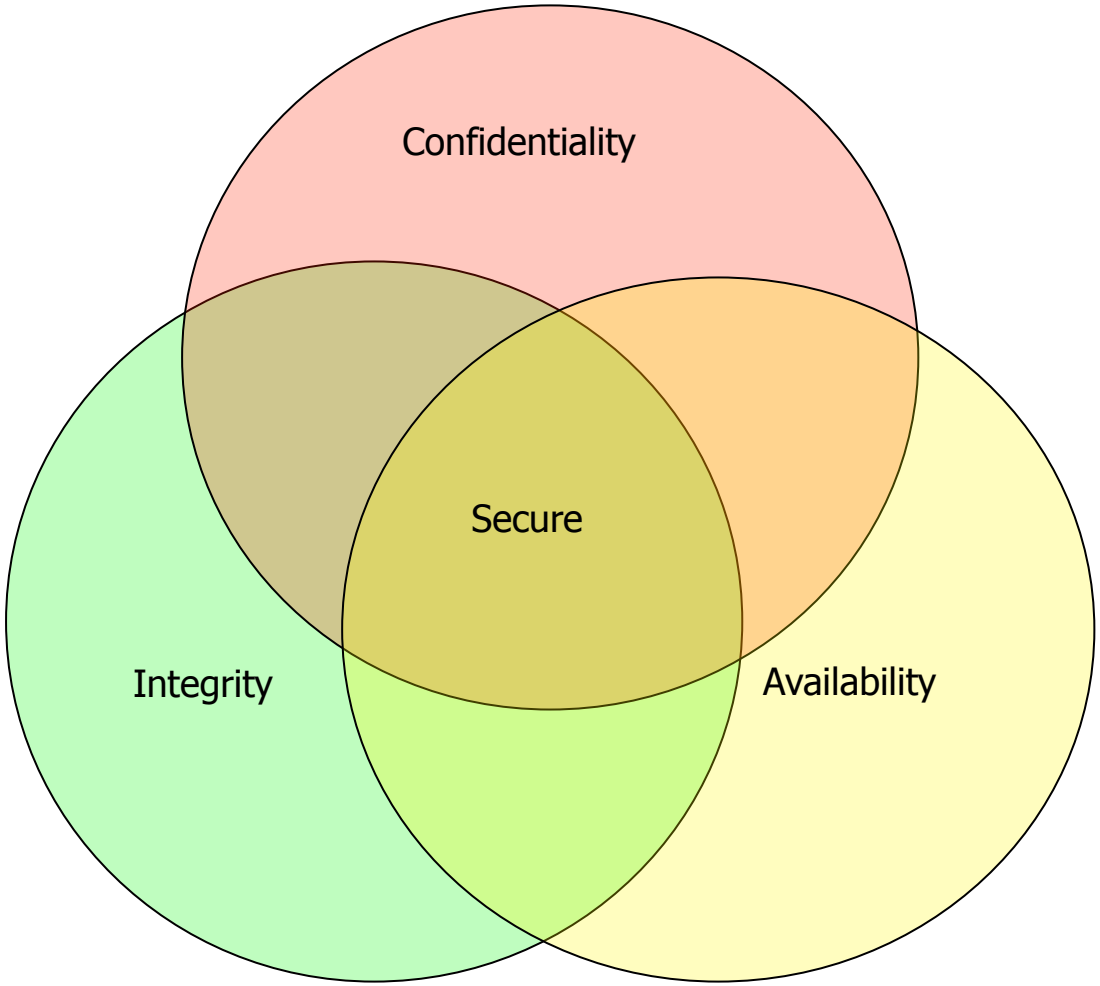
Availability

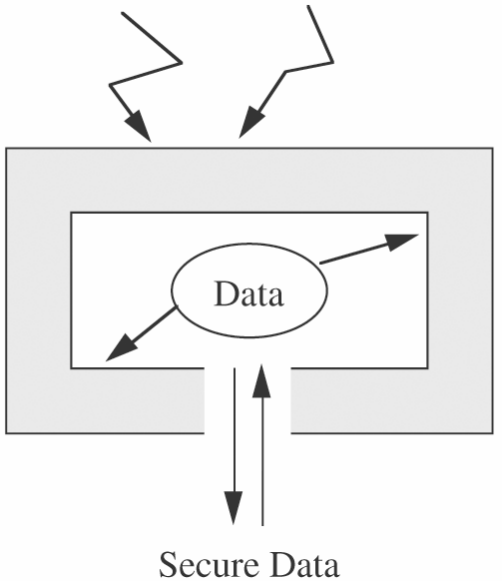
- For Computer Systems this means that:
  - Services are accessible and useable (without undue delay) whenever needed by an authorized entity.
- For this we need fault-tolerance:
  - Faults may be accidental or malicious (Byzantine).



  - Denial of Service attacks are an example of malicious attacks.

Relationship between Confidentiality Integrity and Availability



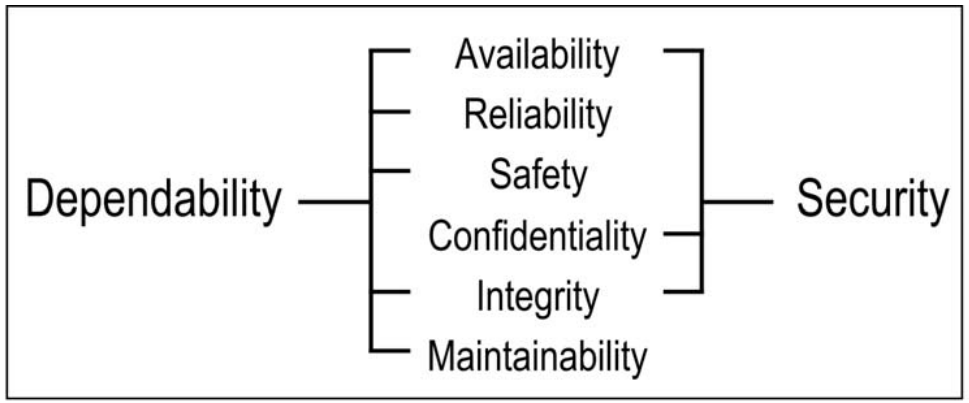


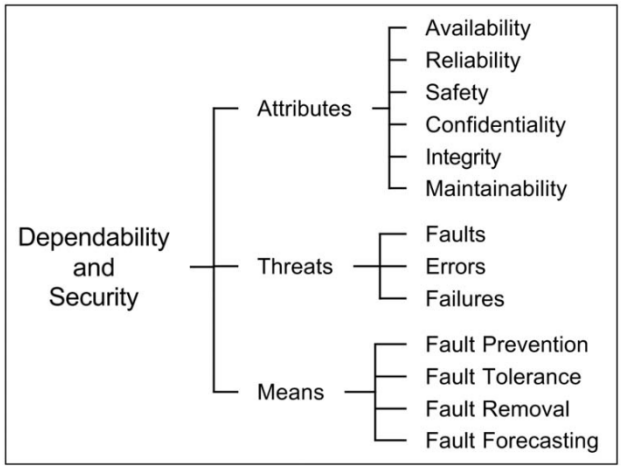
Accountability

- Actions affecting security must be traceable to the responsible party.
  - For this, Audit information must be kept and protected,
  - Access control is needed.

Other security requirements

- Reliability – deals with accidental damage,
- Safety – deals with the impact of system failure on the environment,
- Dependability – reliance can be justifiably placed on the system,
- Survivability – deals with the recovery of the system after massive failure.





Computer Security

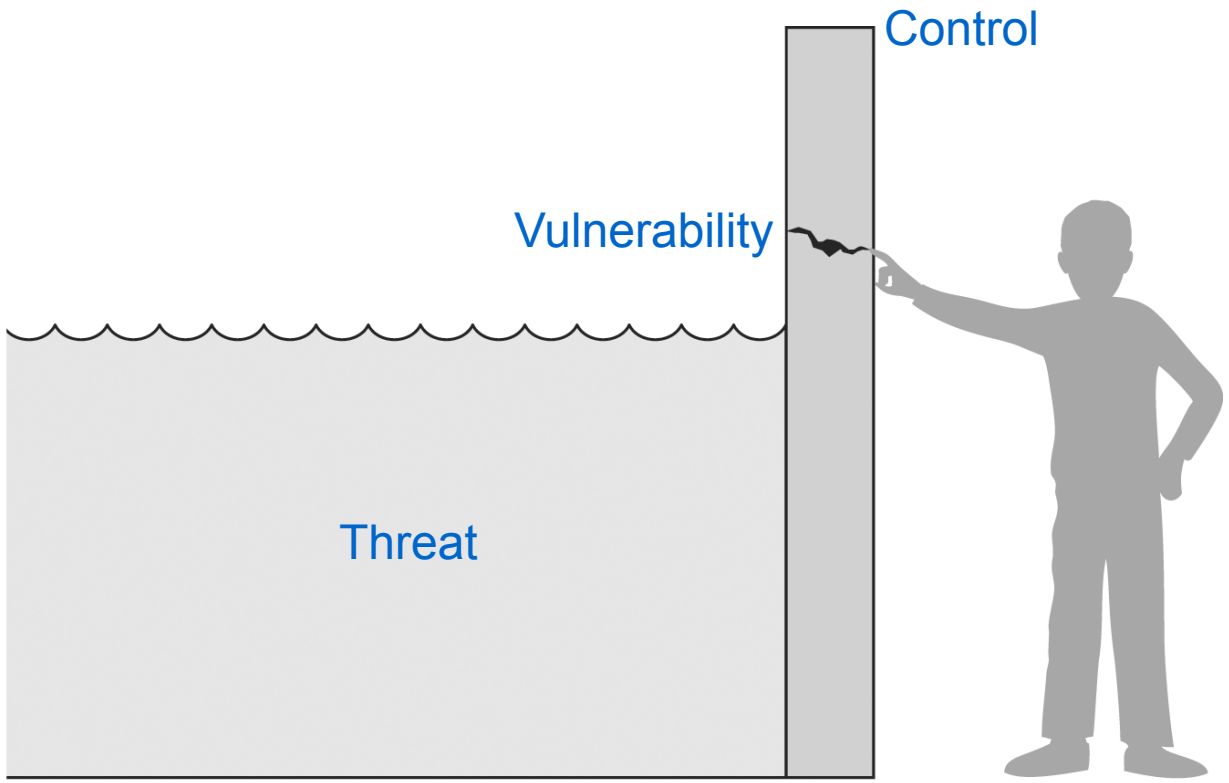
a definition ... (again)

- **Computer Security deals with the prevention and detection of unauthorized actions by users or others of a System.**

Additional terms

- Vulnerability: „An error or weakness in the design, implementation, or operation of a system“
- Attack: „A means of exploiting some vulnerability in a system“
- Threat: „An adversary that is motivated and capable of exploiting a vulnerability“

Vulnerabilities vs. Threats

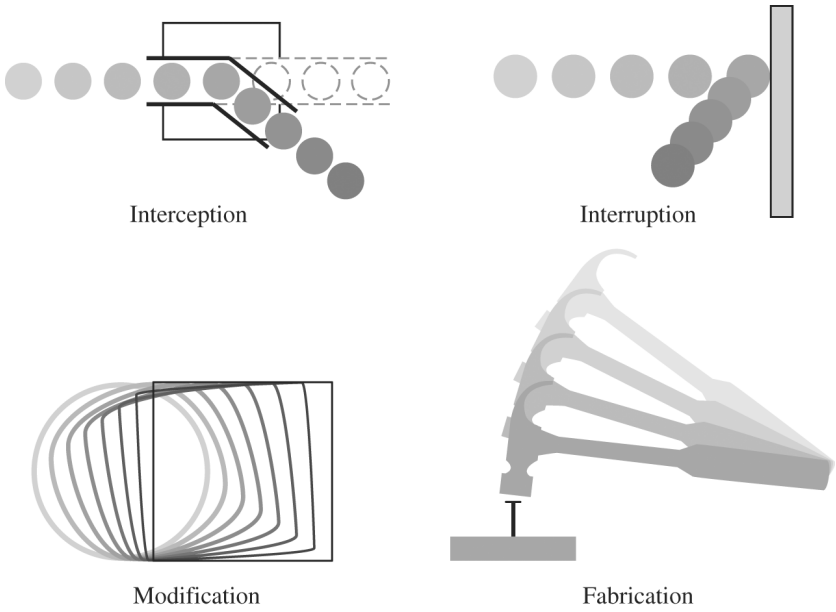


Pfleeger/Pfleeger Fig. 01-01

Vulnerabilities vs. Threats

- Vulnerability
  - Technical failure in a system
  - Primary focus of most computer security classes
  - Close all vulnerabilities => threats don ‘t matter? Or do they?
- Threats
  - Different enemies have different abilities
  - Teenage joy-hackers can ‘t crack modern cryptosystems
  - Serious enemies can exploit the „three B ‘s“: burglary, bribery, and blackmail (in addition to social engineering)
  - Cannot design a security system unless one knows who the enemy is!

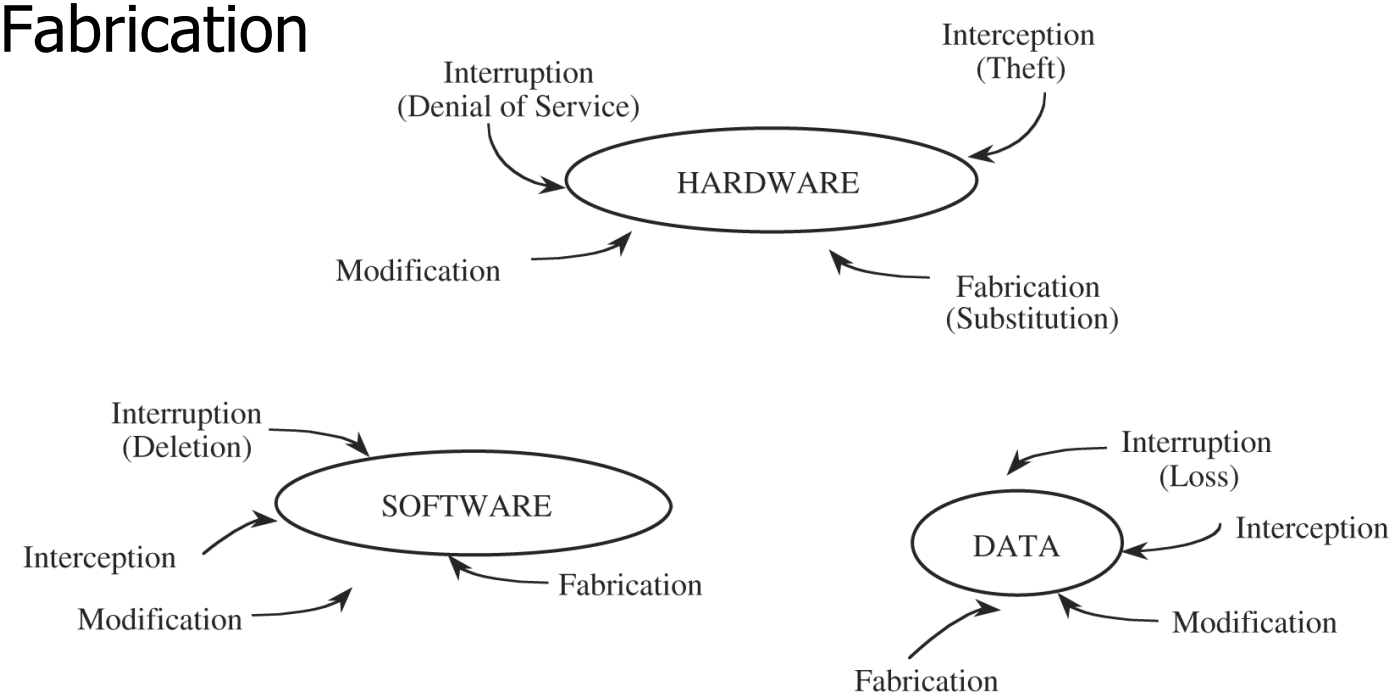
- Much of this course is devoted to describing a variety of controls and understanding the degree to which they enhance a system's security.



Pfleeger/Pfleeger Fig. 01-02

Vulnerabilities

- Hardware: Interruption (DoS), Modification, Interception (Theft), Fabrication (Substitution)
- Software: Interruption (Deletion), Modification, Interception, Fabrication
- Data: Interruption (Loss), Modification, Interception, Fabrication



Threats: Joy hackers

- Who are they
  - Many are „script kiddies“; some are very competent
    ⇒The scripts are very sophisticated
  - The hackers share tools more than the good guys do!
    ⇒Very little useful and working tools are existing ***for*** security
- Are they a problem?
  - What would it cost you to rebuild a machine?
  - What would your CEO say if you ended up on the front page of the NYTimes?
  - What if they’re working for someone else?
  - Their target selection has improved

Threats: Hacking for profit

- Hackers have allied themselves with the spammers and the phishers
- Primary motivation for most current attacks:
  money!
- The market works – the existence of a profit motive has drawn new talent into the field
  - East Europe!
- We are seeing, in the wild, sophisticated attacks
- We are seeing less pure vandalism
- Most of today ‘s worms and viruses are designed to turn victim computers into „bots“

Threats: Organized (disorganized) crime

- Often hacking is just another venue for ordinary criminal activity
- The same people who hack
  - Steal credit card numbers
  - Launder money
  - ...

Threats: Industrial espionage

- Less than 5% of attacks are detected

- Professionals who are after you won ‘t use your machine to attack other companies, and that ‘s how successful penetrations are usually found
- Professionals are more likely to use non-technical means, too:
  - social engineering, bribery, etc.
- Professionals tend to know what they want

Threats: Inside jobs

- Insiders know what you have
- Insiders often know the weak points
- Insiders are on the inside of your firewall
- ....

⇒ What if your system administrator turns to the „Dark Side“???

Threats: Spies

- Governments may want your technology
- Some governments lend tangible support to companies in their own countries
- Spies tend to be sophisticated, well-funded, etc.
- What about cyber warfare?

Threats: Why does it matter?

- You have to build your defenses accordingly
- Security is fundamentally a matter of economics
  - How much security can you afford?
  - How much do you need?

Assets: What are you protecting?

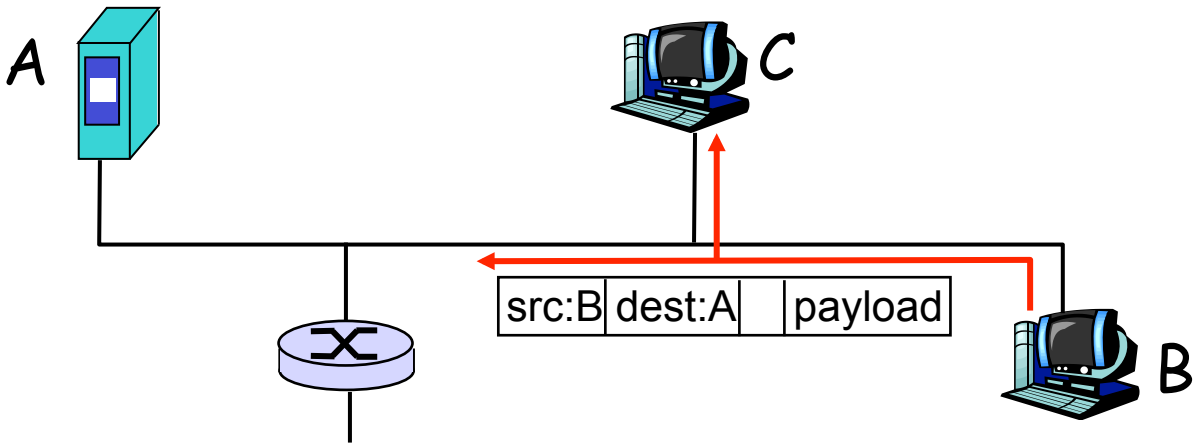
- Host-resident data?
- Bandwidth?
- CPU time?
- Knowledge of what hosts exist?
  - Network scans
  - Why (1)? The # of computers == # of people
    How large is your competitor?
  - Why (2)? Attack power
    MAC addresses can only be determined on-LAN
    Does the attacker have this ability?

Attacks

- Bandwidth attacks
  - Clog your bandwidth via DoS attacks
  - Use your bandwidth to attack someone else, e.g.,
  - Reflector attacks:
    - UDP-based service where response is > than request
    - Forge source address to victims address
  - Network identity attack:
    - Run the server with illegal content on hacked machine
  - Eavesdropping
    - Pick up traffic, e.g., passwords/credit cards via sniffer
    - Done to major backbones in 1993-4
    - e.g., http://monkey.org/~dugsong/dsniff/

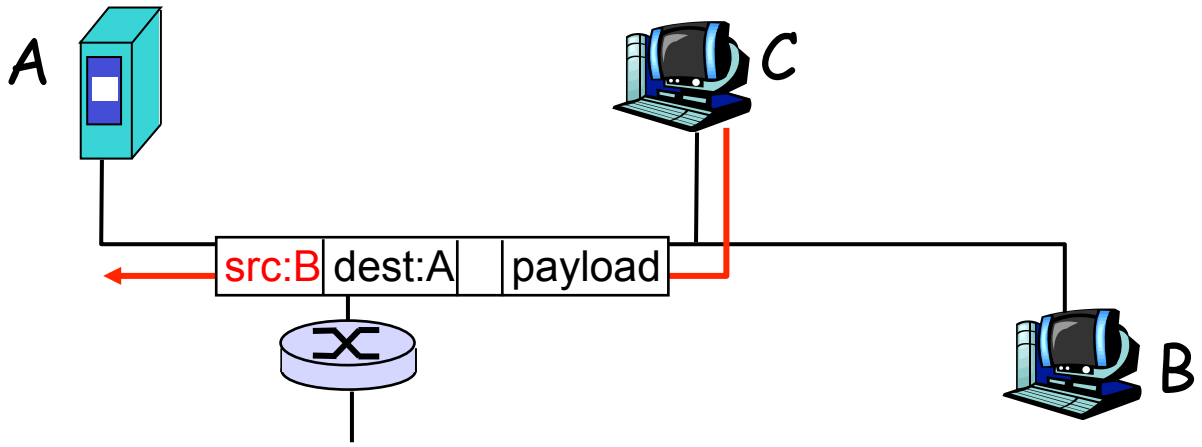
Packet sniffing: How

- Easiest case: Broadcast media
- Promiscuous NIC reads all packets passing by. Can read all unencrypted data (e.g., passwords)
- E.g.: C sniffs B's packets



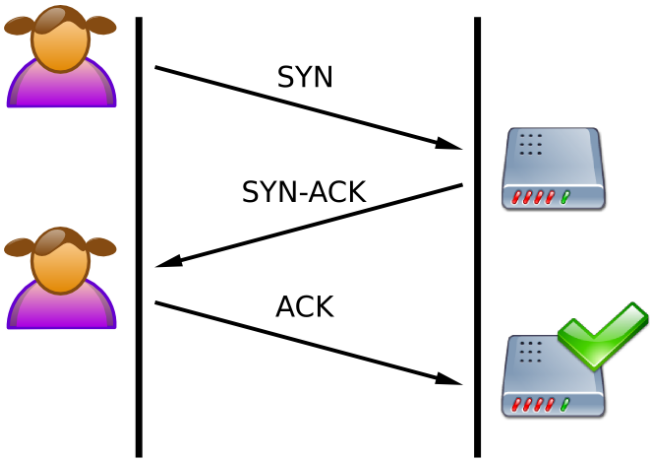
IP Spoofing: How (2.)

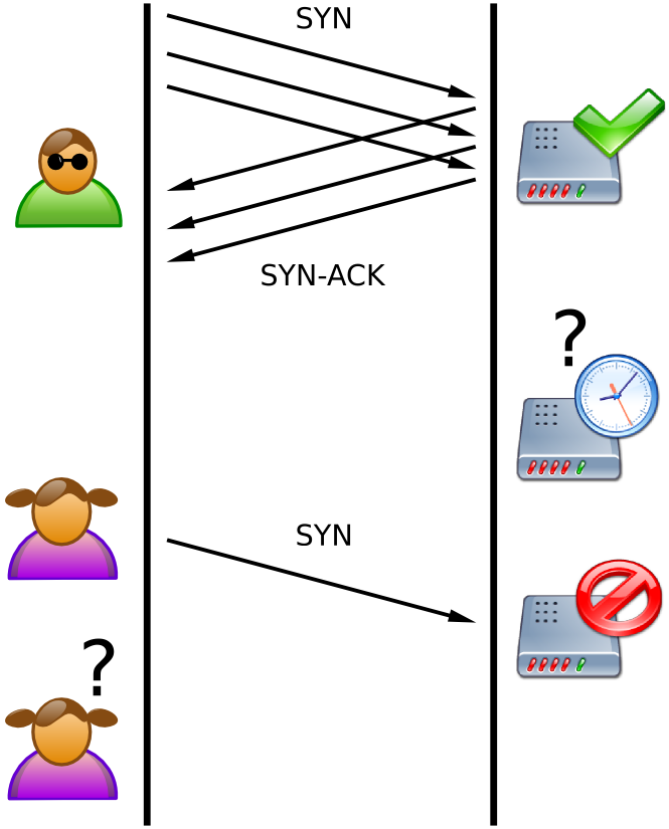
- Can generate "raw" IP packets directly from application, putting any value into IP source address field
  - Receiver can't tell if source is spoofed
  - E.g.: C pretends to be B



Denial of service attack: how

- Maliciously generated packets “swamp” receiver
- Distributed DoS (DDoS):
  multiple coordinated sources swamp receiver





SYN Flood. The attacker sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources. Alice, a legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.

Vulnerabilities:

- Dichotomy: Host vs. network
- We deal with both!
- We need protect **both**!
- Techniques differ

Vulnerabilities: Hosts (Seifert)

- Goal: keep the bad guy from penetrating the networked host (generally via a buggy application)
- If a penetrated application is used to break host security, it is probably an OS and application security issue
- If the application itself can be tricked into doing nasty things, it is probably a network security problem
- No clean categories

Vulnerabilities: Network (Feldmann)

- What can the attacker do?
- Where is the attacker located?
- What are you trying to protect?

Vulnerabilities: Different network layers

- Examples
  - Link layer: ARP-spoofing
    - ARP (Address Resolution Protocol): maps IP addresses to Ethernet addresses
    - Send fake, or "spoofed", ARP messages to an Ethernet LAN.
    - Associate the attacker's MAC address with the IP address of another node.
  - Transport layer: TCP sequence number guessing
    - Initial sequence number (ISB) used to be incremented by some constant k after each connection and every half-second
    - X opens legitimate connection to S to learn ISB
    - X can now impersonate T
      - Spoofs T ‘s source IP
      - Blocks RST (RESET the connection) from T

Protecting a network

- Analysis
  - What are you trying to protect?
  - Against whom?
  - Enumerate vulnerabilities
  - Deploy protective measures

Protection mechanisms

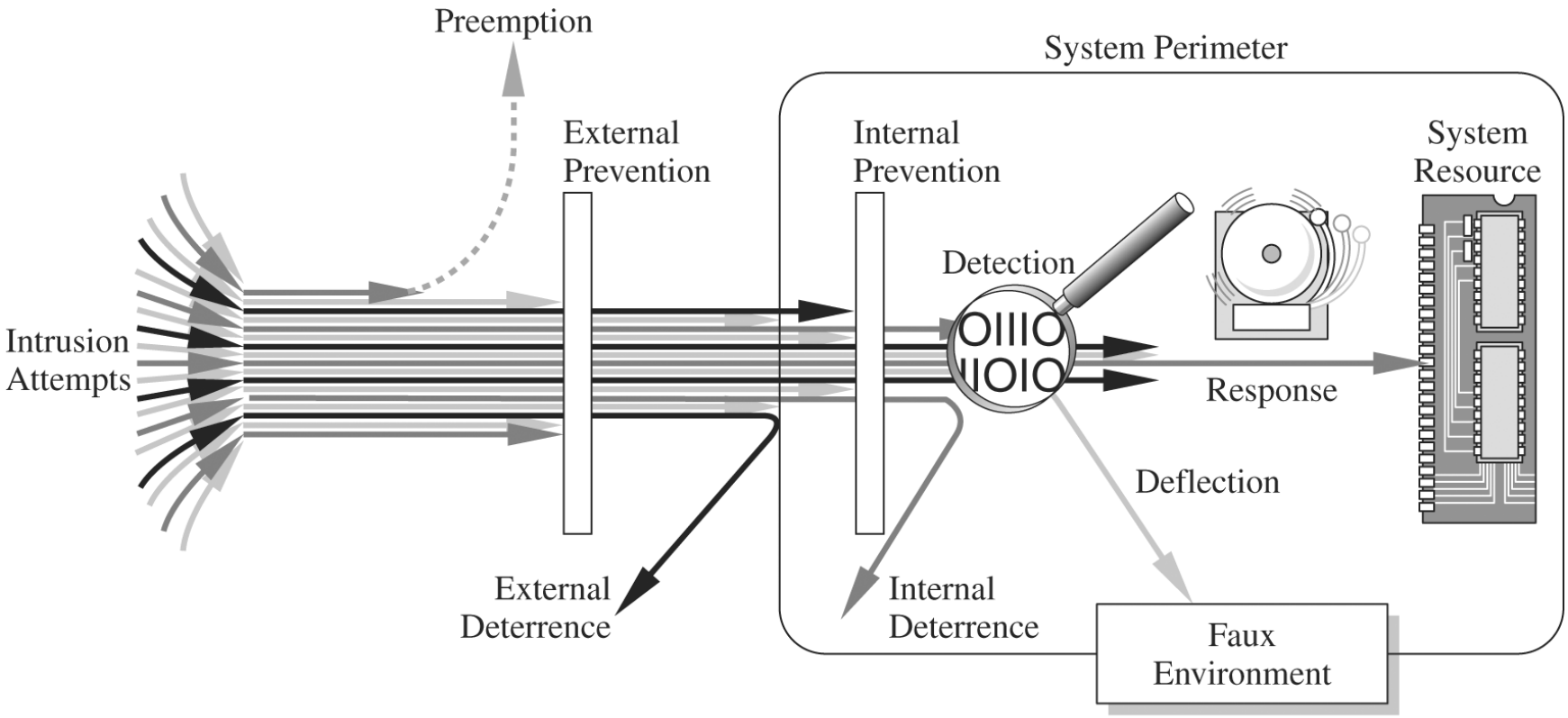
- Replace vulnerable mechanisms by strong ones
  Example: Address-based authentication with cryptography
- Use filters or firewalls to limit access to important but insecure services
  Example: Do not permit outside access to Windows file-sharing ports
- Use procedural mechanism as last resort
  Example: There is no way to block ARP-spoofing) have to keep would-be spoofers of your LAN
  (the attack only works locally)

Human element (important!)

„Humans are incapable of securely storing high-quality cryptographic keys, and they have unacceptable speed and accuracy when performing cryptographic operations. They are also large, expensive to maintain, difficult to manage, and they pollute the environment. It is astonishing that these devices continue to be manufactured and deployed, but they are sufficiently pervasive that we must design our protocols around their limitations.“

Kaufman et al.

Course Summary: Methods of Defense



Pfleeger/Pfleeger Fig. 01-06