CS 494/594
Computer and Network Security

Dr. Jinyuan (Stella) Sun
Dept. of Electrical Engineering and Computer Science
University of Tennessee
Fall 2010

Introduction to Computer and Network Security

- Why security?
- Security goals
- Security mechanisms
- Security services
- Security limitations

Threats, Vulnerabilities, Attacks

A **threat** is a set of circumstances that has the potential to cause loss or harm

A **vulnerability** is a weakness that may be exploited to cause loss or harm

A vulnerability can be exploited to perpetrate an **attack**

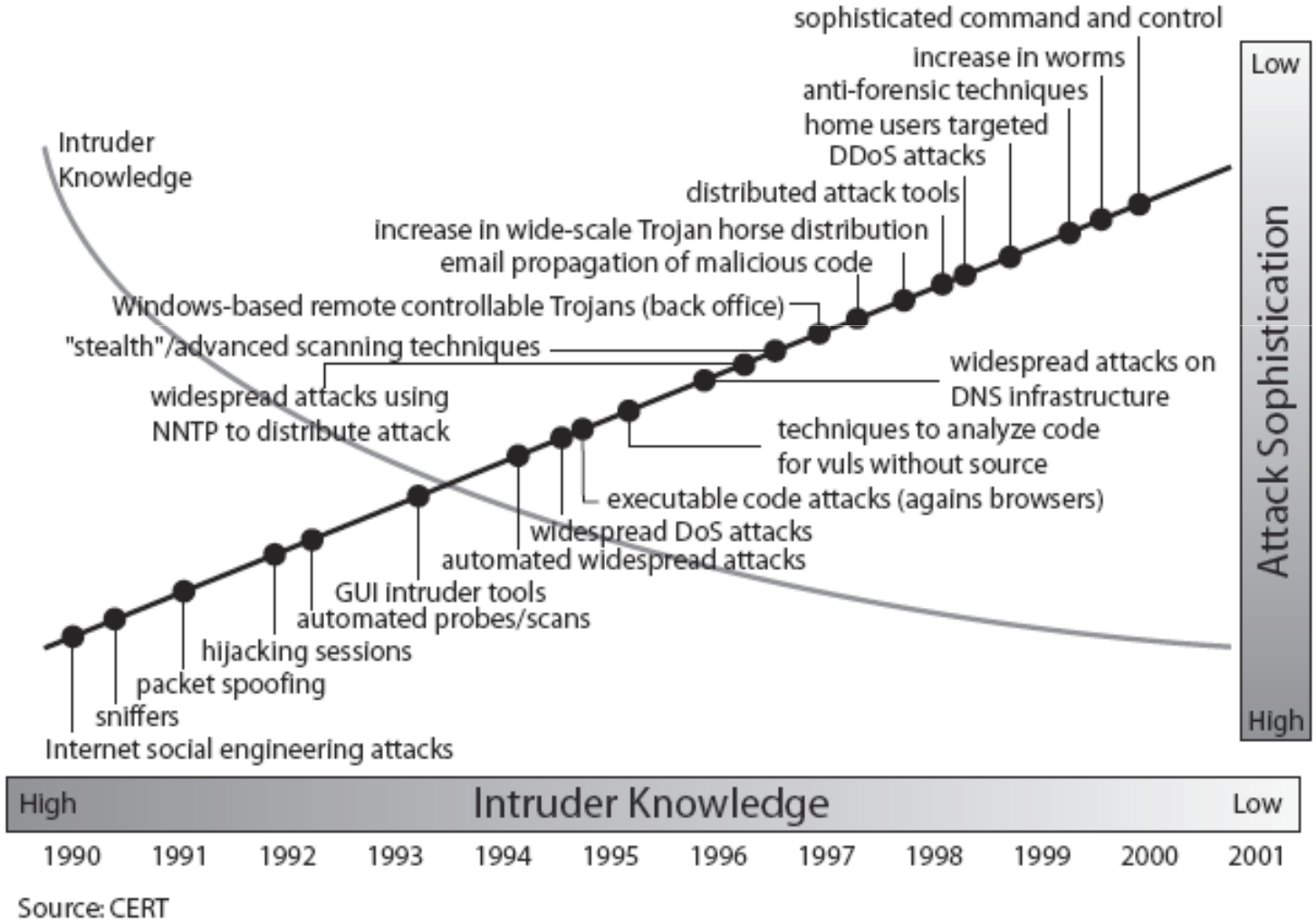
Threats, Vulnerabilities, Attacks

How to address these problems?

Control: an action, device, procedure, or technique that removes or reduces a vulnerability, and subsequently blocks threats and attacks

This class focuses on the various controls and how they enhance a system's security

Security Trends



Source: CERT

Malicious Software

- Trojan horse: instructions hidden inside an otherwise useful program that do bad things
- Virus: a set of instructions that inserts copies of itself into other programs
- Worm: a program that replicates itself on other machines across a network
- Trapdoor: an undocumented entry point in a program
- Logic bomb: malicious instructions that trigger on some event in the future
- Zombie: malicious instructions on comprised machines that are used to launch attacks
- Spyware: a software that installs itself on the user's computer, monitor user activities, browser hijacking, password sniffing
- Rootkit: a software that enables continued privileged access while hiding its presence

How Do They Spread?

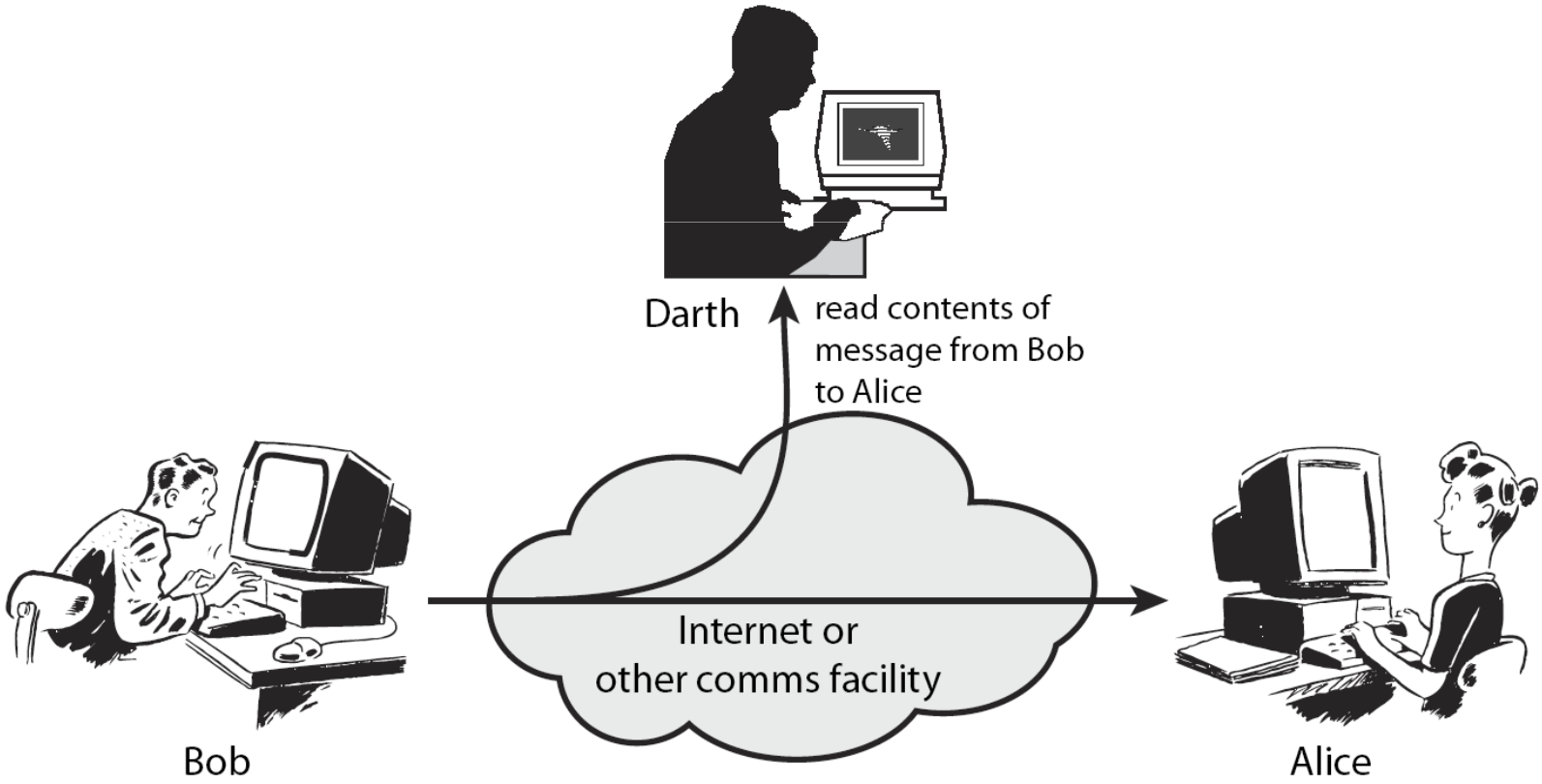
- Email
- Shared medium: CD, USB
- Mobile program
- Program bugs
- Buffer overflow

Defense

- Operating System: resource access control
- Virus Checker: instruction patterns, file lengths or digests
- Software Patch: bug fixes
- Intrusion Detection: host intrusion detection, network intrusion detection
- Firewall: filter unwanted/unauthorized traffic

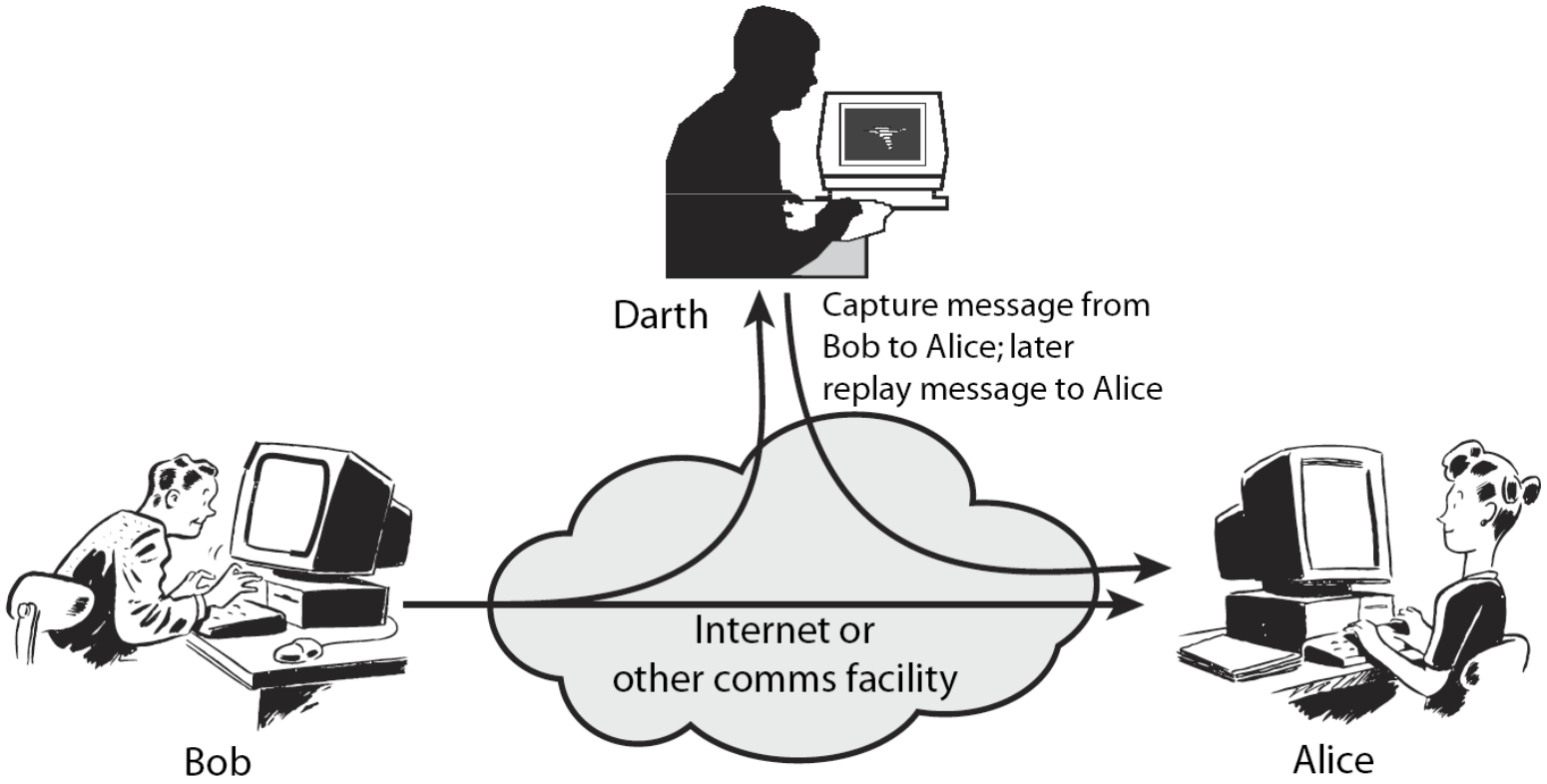
Passive Attacks

disclosure of message contents, traffic analysis



Active Attacks

delay, replay, deletion, modification, insertion

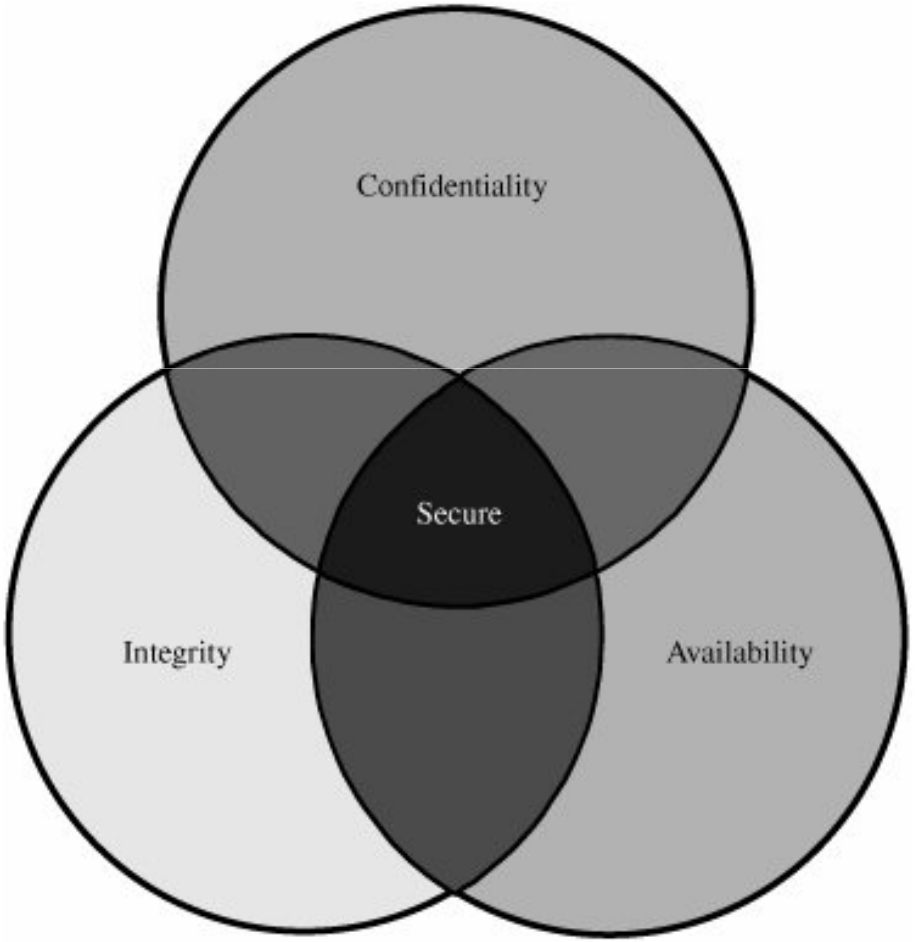


More Attacks Coming…

Security Goals

- Confidentiality: information or resources can only be accessed by authorized parties, sometimes called secrecy or privacy
- Integrity: information or resources can be modified only by authorized parties or only in authorized ways
- Availability: information or resources accessible to authorized parties at appropriate times; requirement for denial-of-service (DoS) prevention

Security Goals (Cont'd)



Example: Bank

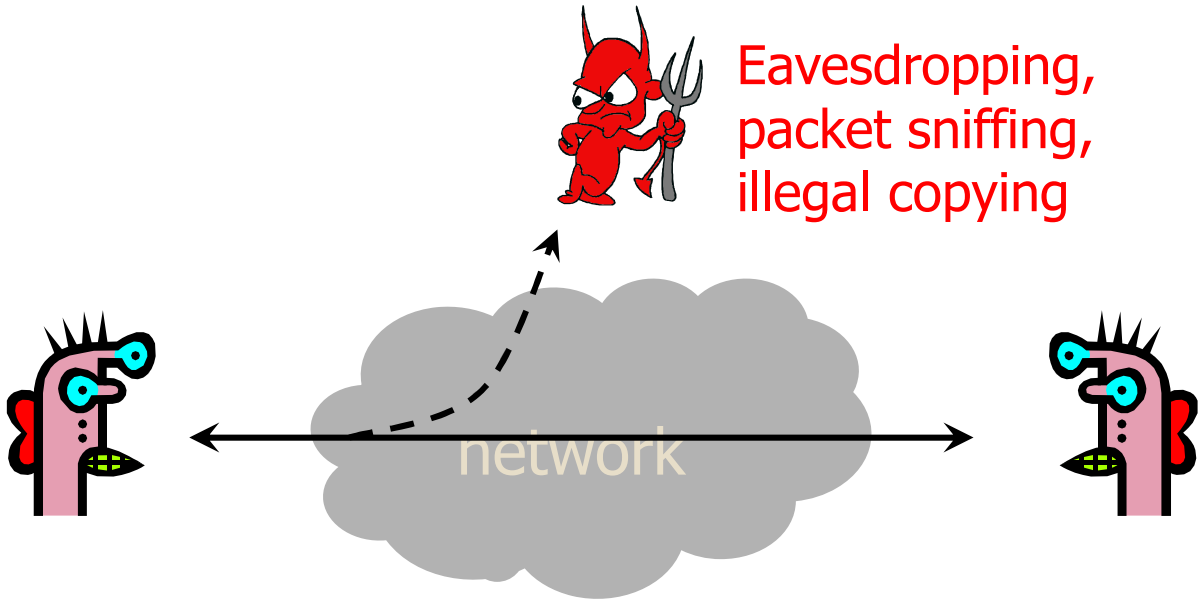
- Confidentiality: an employee should not disclose a customer's account information to another customer.
- Integrity: an employee should not improperly modify a customer's account balance.
- Availability: system should be usable when customers purchase with credit cards.

Example: Healthcare

- Confidentiality: patients' medical records should be access only by authorized personnel.
- Integrity: patients' medical records should not be illegally modified or deleted.
- Availability: patients' medical records should be accessible in case of emergencies.

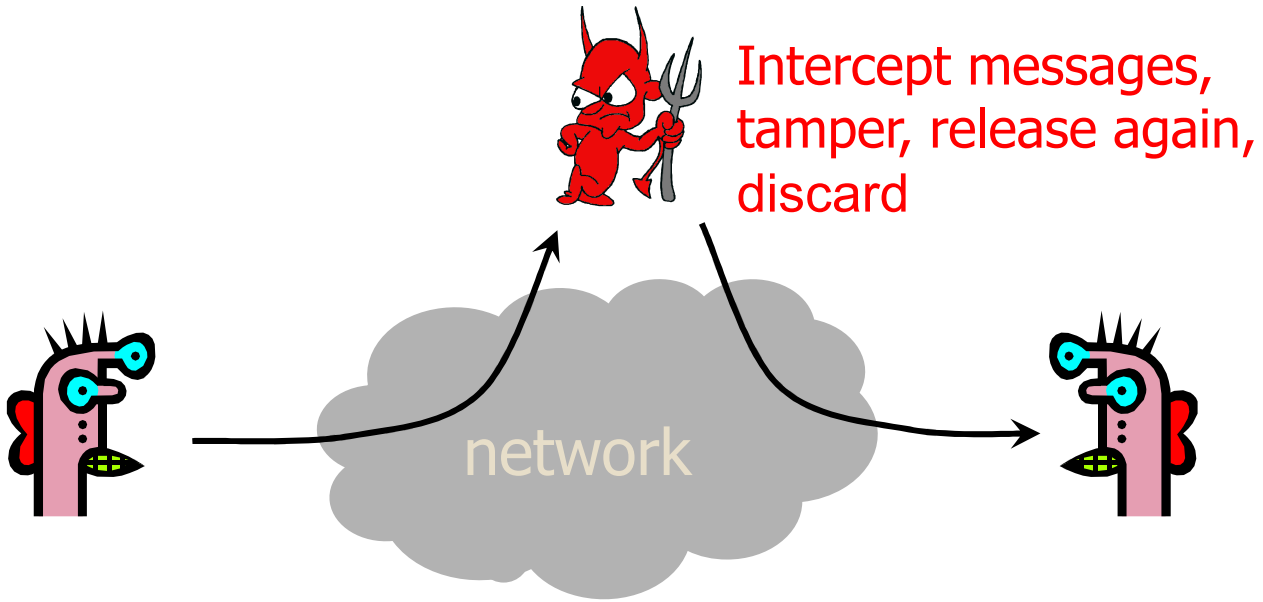
Attacks Continued…

Attacks on confidentiality:



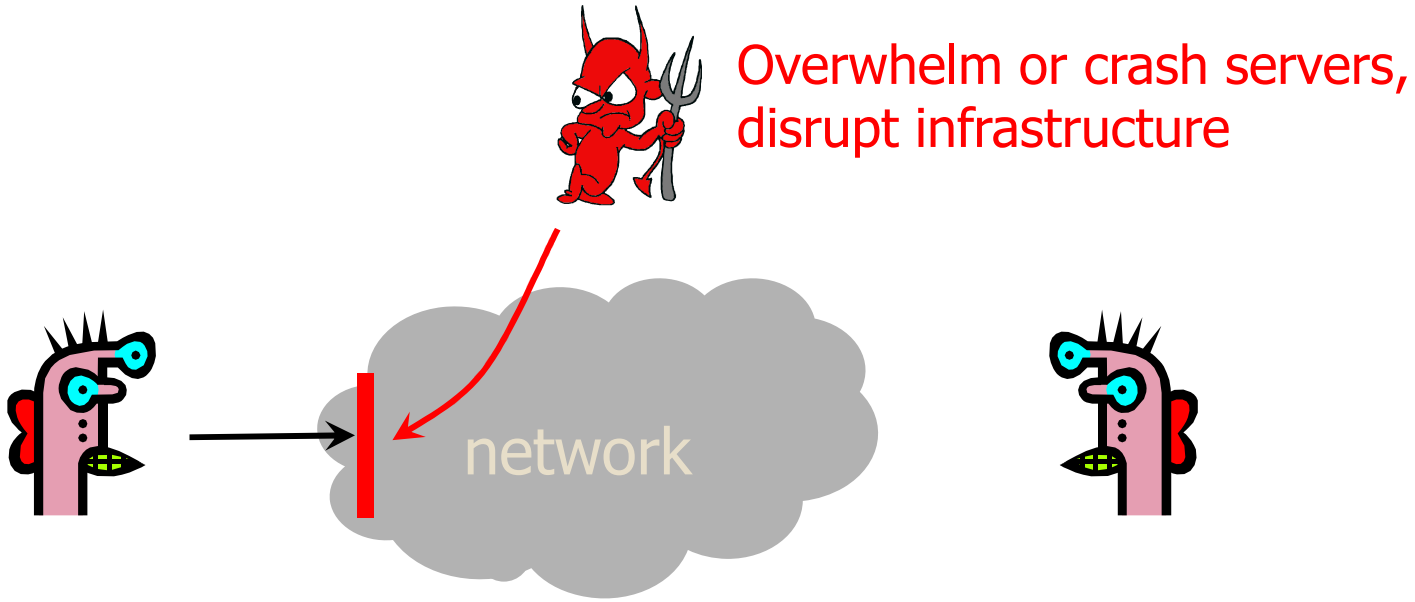
Attacks Continued…

Attacks on integrity:

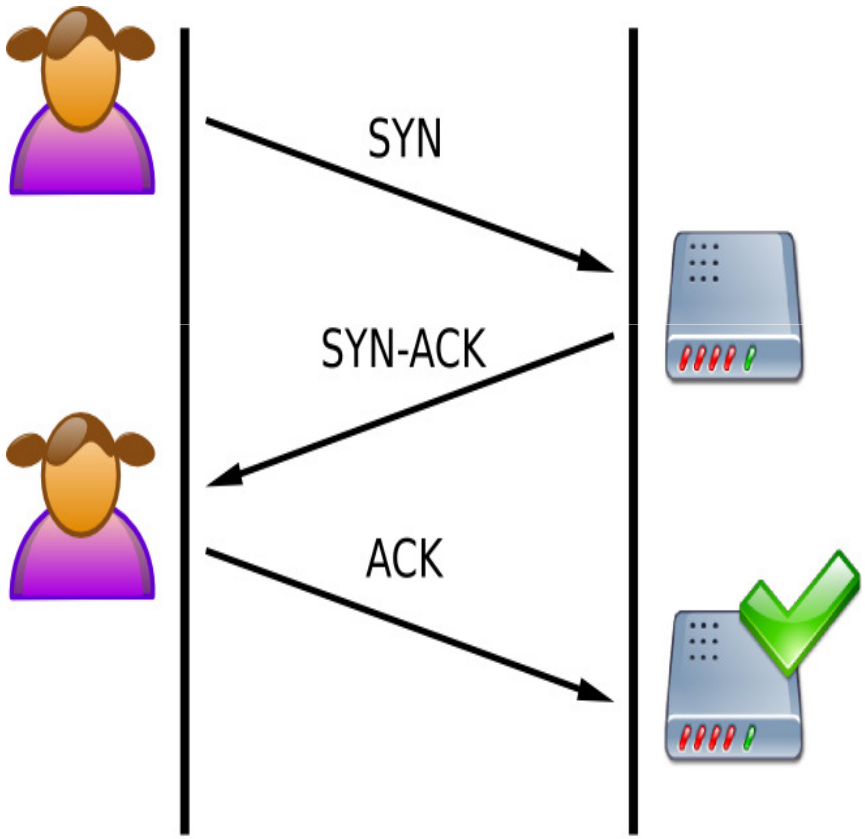


Attacks Continued…

Attacks on availability: DoS, DDoS attacks (SYN flooding, smurfing)

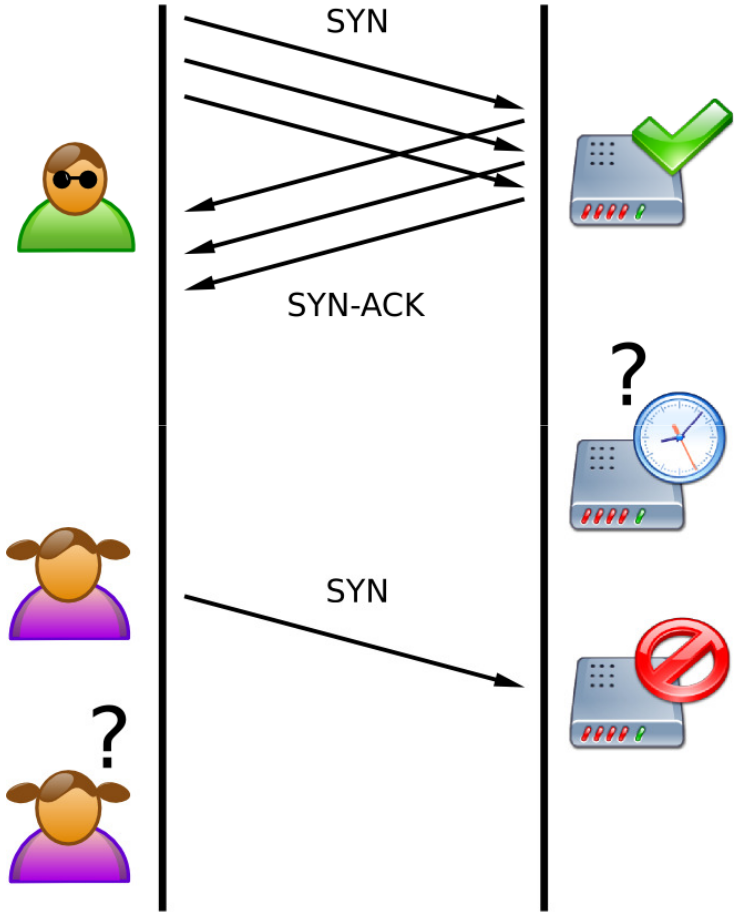


SYN Flooding



A normal connection between Alice and a server, the three-way handshake is correctly performed.

SYN Flooding (Cont'd)

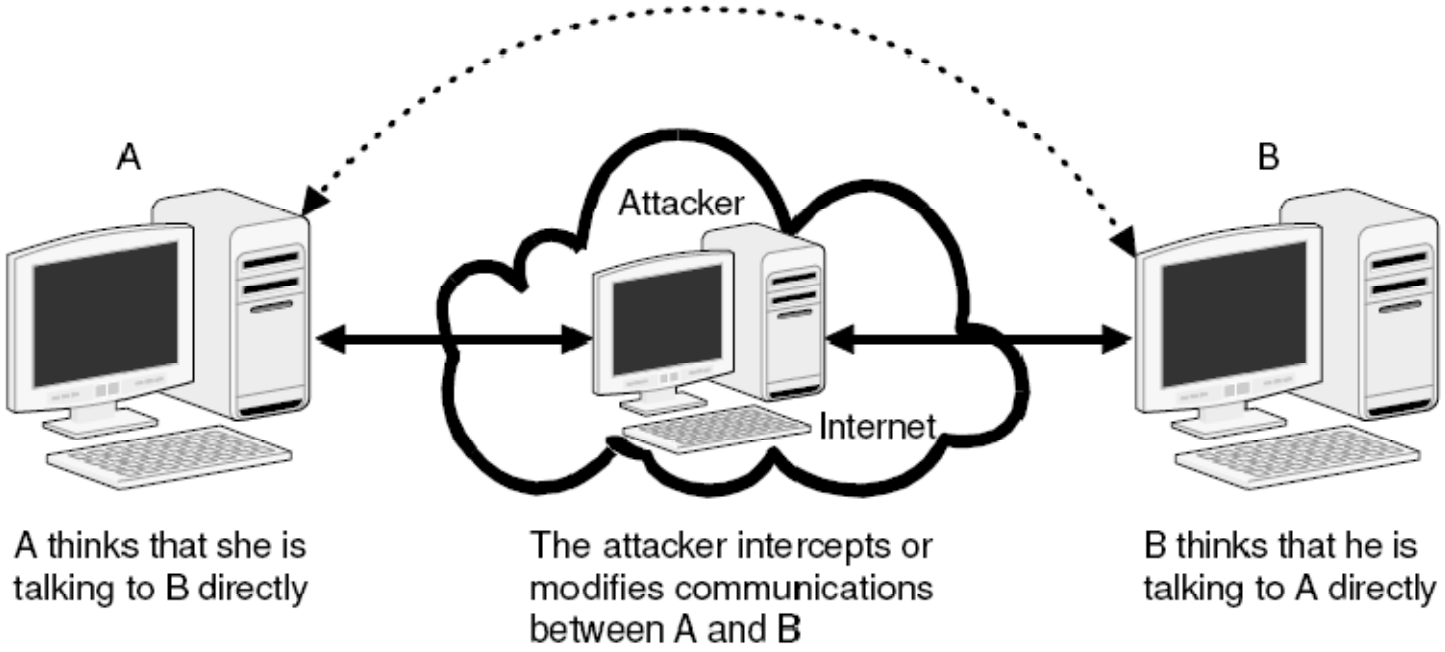


SYN flood: Darth the attacker sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources. Alice, a legitimate user, tries to connect but the server refuses to open a connection resulting in a denial of service.

SYN floods may appear with a wide range of source IP addresses, giving the appearance of a well distributed DDoS.

Spoofing/Masquerading

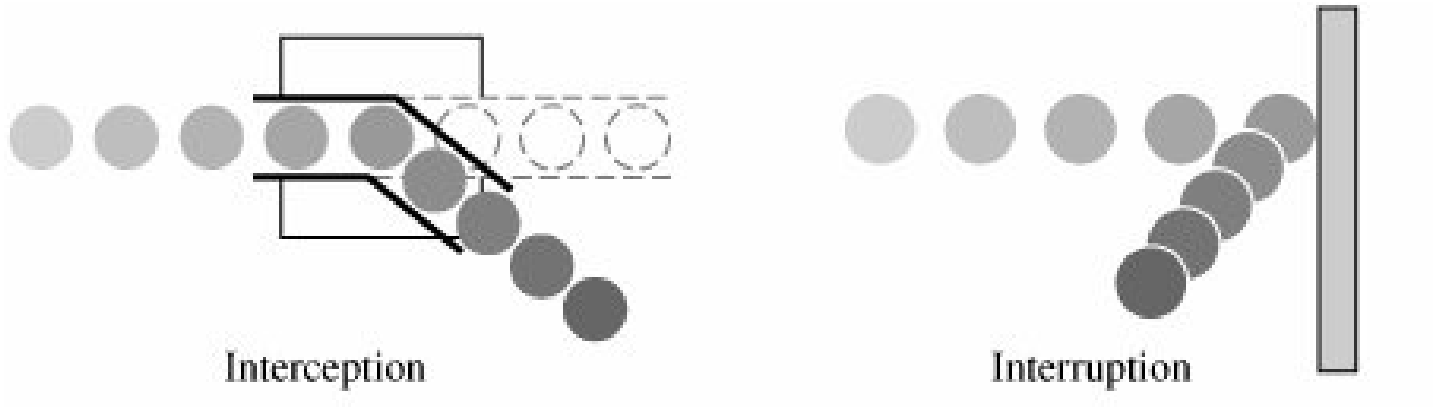
Attacks on authenticity: man-in-the-middle



Attacks on Password

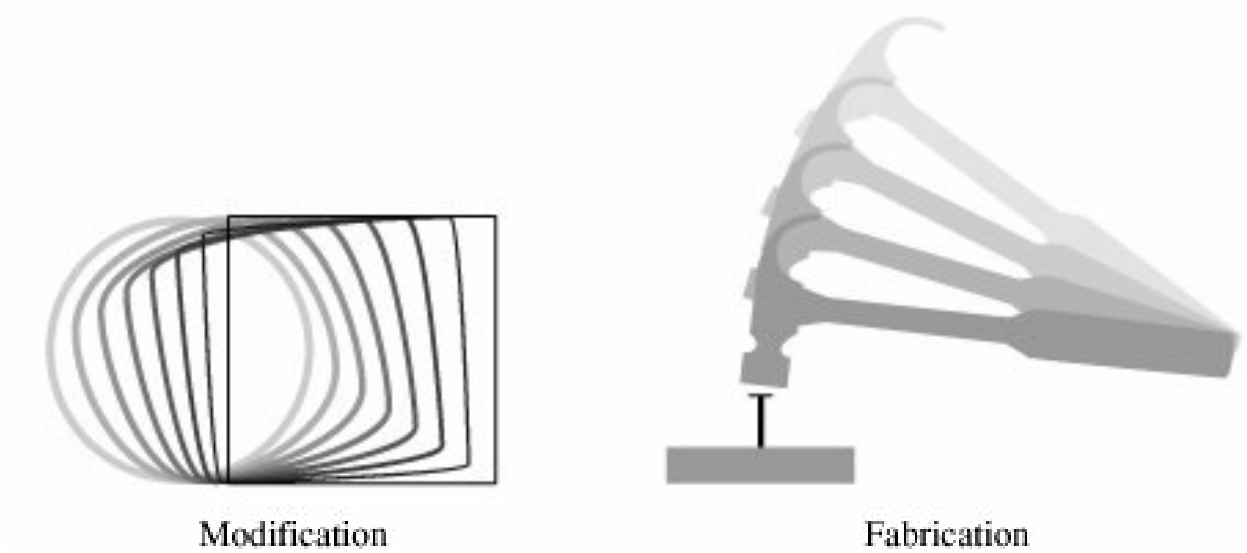
- Password sniffing
- Brute-force attack
- Dictionary attack
- Phishing
- Social engineering

Summary of the Kinds of Attacks



- Interception: some unauthorized party has gained access to information or resources, e.g., illicit copying of program or data files, wiretapping to obtain data in a network
- Interruption: information or resources become lost, unavailable, or unusable, e.g., malicious destruction of a hardware device, erasure of a program or data file

Summary of the Kinds of Attacks



- Modification: unauthorized parties tampering with the information or resources, e.g., alter a program so that it performs an additional computation, or modify data being transmitted electronically, or modify hardware
- Fabrication: an unauthorized party might create a fabrication of counterfeit objects on a computing system, e.g., insert spurious transactions to a network communication system or add records to an existing database

Security Mechanisms

- Any process (or a device incorporating such a process) designed to detect, prevent, or recover from a security attack
- Examples: encryption algorithms, digital signatures, authentication protocols
- Types:

  - prevention: password, encryption, digital signature, access control, authentication, data integrity, firewall

  - detection: monitoring, log, auditing, intrusion detection

  - recovery: backups, bug fixes, retaliation

Security Services

A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Security Services (Cont'd)

- Authentication: the assurance that the communicating entity is the one that it claims to be

  - Peer entity authentication: to provide confidence in the identity of the entities connected

  - Data origin authentication: to provide assurance that the source of received data is as claimed
- Access control: the prevention of unauthorized use of a resource
- Data confidentiality: the protection of data from unauthorized disclosure
- Data integrity: the assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
- Non-repudiation: provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication
- Availability: a system or a system resource being accessible and usable upon demand by an authorized system entity

Security Design Principles

- Easiest penetration
- Timeliness
- Effectiveness
- Weakest link

Security Limitations

- Human factors
- Cost-security tradeoff
- "Whoever thinks his problem can be solved using cryptography, doesn't understand his problem and doesn't understand cryptography"

  - Roger Needham and Butler Lampson to each other

Reading Assignments

- [Kaufman] Chapter 1