Week 7
Network Security: Basic concepts and terminology

Slides by J.F Kurose and K.W. Ross and lecture notes from CMU are used in this lecture

Computer Networking: A Top Down Approach Featuring the Internet, 2nd edition.
Jim Kurose, Keith Ross
Addison-Wesley, July 2002.

What is Computer Security?

Computer Security = CIA

CIA = *Confidentiality* + *Integrity* + *Availability*

What is Computer Security?

- *Confidentiality*: The protection of information from unauthorized disclosure
  - need to know
  - sample mechanisms: access controls, cryptography, resource hiding
  - existence of data as well as content

What is Computer Security

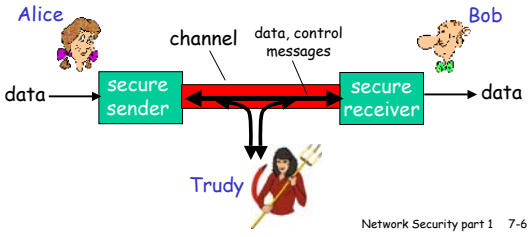
- *Integrity:* The protection from unauthorized modification of information
  - *data* integrity and *origin* integrity (authentication)
    - Prevention mechanisms block unauthorized access
    - Detection mechanisms report when information is no longer trustworthy

What is Computer Security

- *Availability:* Resources are usable or operational during a given time period despite attacks or failures.

Friends and enemies: Alice, Bob, Trudy

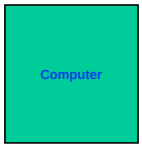
- well-known in network security world
- Bob, Alice (lovers!) want to communicate "securely"
- Trudy (intruder) may intercept, delete, add messages



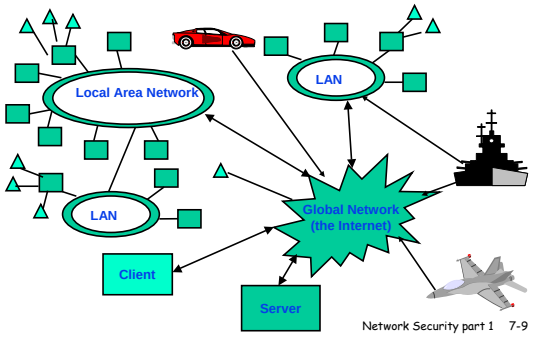
Who might Bob, Alice be?

- … well, *real-life* Bobs and Alices!
- Web browser/server for electronic transactions (e.g., on-line purchases)
- on-line banking client/server
- DNS servers
- routers exchanging routing table updates
- other examples?

We Have Gone From This ….

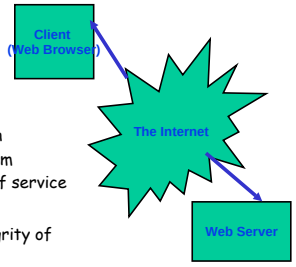


To This ….

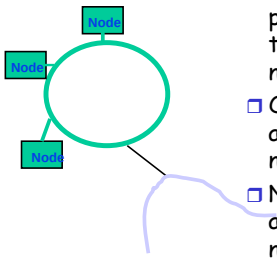


Web Security

- **Client side**
  - Privacy protections
  - Integrity protections
- **Server side**
  - Protection from break in
  - Protection from vandalism
  - Protection from denial of service
- **Both**
  - Confidentiality and integrity of transmitted information



Network Security Issues

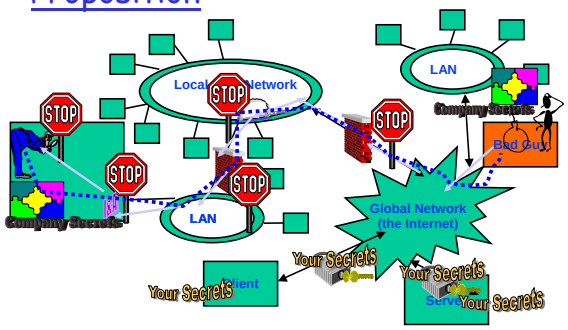


- Information must be protected when travelling across the network
- Only authorized access is allowed to a node
- Nodes handle security appropriately within node itself

Network Security Does Not Preclude Node Security!!

- Firewalls don't provide complete protection.
- "Whoever thinks his problem can be solved using cryptography, doesn't understand his problem and doesn't understand cryptography."

Think of Security as a Layered Proposition



There are bad guys (and girls) out there!

Q: What can a "bad guy" do?

A: a lot!

- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (e.g., by overloading resources)

more on this later ……

Threats, Vulnerabilities, Risks, Attacks

- A *Threat* is any situation or event that poses harm to a computer system.
- *Vulnerabilities* is a potential weakness whose exploitation can cause a threat to be realized.
- A *Risk* is a potential problem, with causes and effects.
  - Definition 1: Risk is the harm that can result if a threat is actualized
  - Definition 2: Risk is a measure of the extent of that harm.
- An *Attack* is an attempt to exploit a vulnerability to make a threat a reality.

Fundamental Threats

- *Disclosure or Compromise:* Unauthorized disclosure of information.
  - Has received the most attention in R&D over the past 30 years.
- *Deception:* Acceptance of false data
- *Disruption:* interruption or prevention of correct operation
- *Usurpation:* unauthorized control of some part of the system

Snooping

- Unauthorized viewing
- Disclosure threat
- Passive
- Example: Wiretapping, or *passive wiretapping*
- Counter with confidentiality mechanisms

Modification or Alteration.

- Unauthorized tweaking
- Deception threat
- May involve disruption or usurpation if controls are modified
- Active
- Example: *Active wiretapping*
- Counter with integrity mechanisms

Masquerading or Spoofing

- Impersonation, misleading user
- Deception and usurpation threat
- Passive attacks:
  - user falls into trap with no overt actions by spoofer
  - Spoofer gives me a different file than I asked for. I do not ask for authentication of file.
- Active attacks:
  - spoofer intentionally misleads user
  - Counter with authentication mechanisms

Delegation Can Lead to a Masquerade

- One user is authorized to act on behalf of another.
- Can be used appropriately
- Can be used inappropriately to affect a masquerade

Repudiation of Origin

- Denial that you sent or created something
- Deception threat
- Counter with integrity mechanisms

Denial of Receipt

- User claims messages were not received.
- Deception threat
- Counter with integrity and availability mechanisms

Delay

- Temporarily inhibit a service.
- Usurpation threat
  - Can support deception in the form of masquerading
- Counter with availability mechanisms

Denial of Service

- Long term inhibition of service
- Usurpation and sometimes deception
- Counter with availability mechanisms.

Vulnerabilities

- Design Flaws
  - Inadequate logging of security relevant events
  - Incorrect or incomplete access controls.
- Programming Flaws
  - Improper array bounds allowing buffer overflow.
- Operational Flaws
  - Insecure default setup conditions
  - Failure to address security issues from external sources.