Computer & Network Security Overview

Guofei Gu
CSCE 665 Advanced Networking & Security

Roadmap

- Security definition, components, overview
- Security Policy, Mechanism, Services
- Security Threats and Vulnerabilities

Security: Definition

- *Security* is a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable
- Security rests on confidentiality, authenticity, integrity, and availability

Basic Components

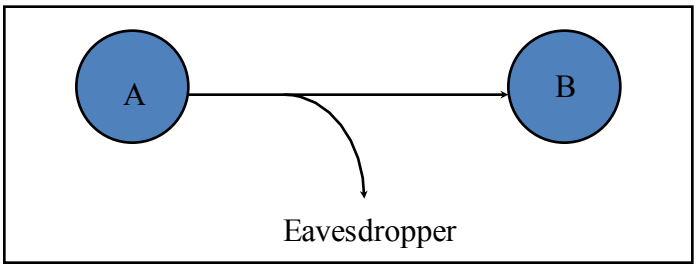
- **Confidentiality** is the concealment of information or resources
- **Authenticity** is the identification and assurance of the origin of information
- **Integrity** refers to the trustworthiness of data or resources in terms of preventing improper and unauthorized changes
- **Availability** refers to the ability to use the information or resource desired

Security Threats and Attacks

- A threat is a *potential* violation of security
  - Flaws in design, implementation, and operation
- An attack is any *action* that violates security
  - Active vs. passive attacks

Eavesdropping - Message Interception (Attack on Confidentiality)

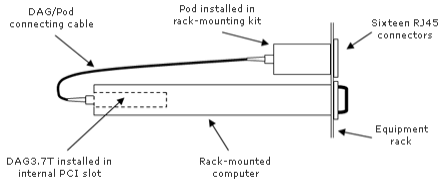
- Unauthorized access to information
- Packet sniffers and wiretappers
- Illicit copying of files and programs

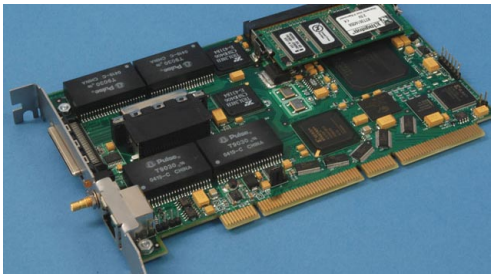


Full Packet Capture (Passive)

Example: OC3Mon

- Rack-mounted PC
- Optical splitter
- Data Acquisition and Generation (DAG) card





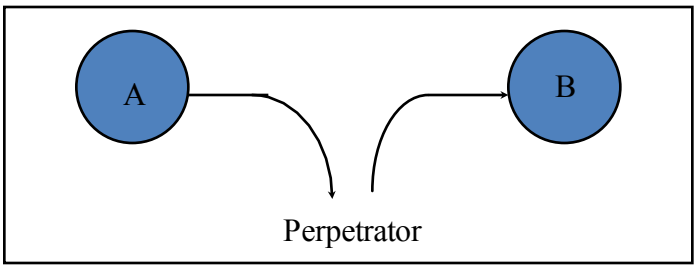
Source: endace.com

Eavesdropping Attack: Example

- tcpdump with promiscuous network interface
  - On a switched network, what can you see?
- What might the following traffic types reveal about communications?
  - DNS lookups (and replies)
  - IP packets without payloads (headers only)
  - Payloads

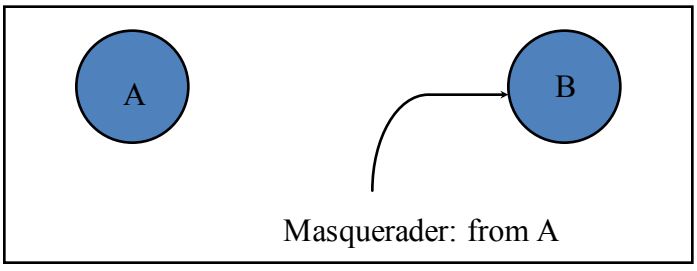
Integrity Attack - Tampering

- Stop the flow of the message
- Delay and optionally modify the message
- Release the message again



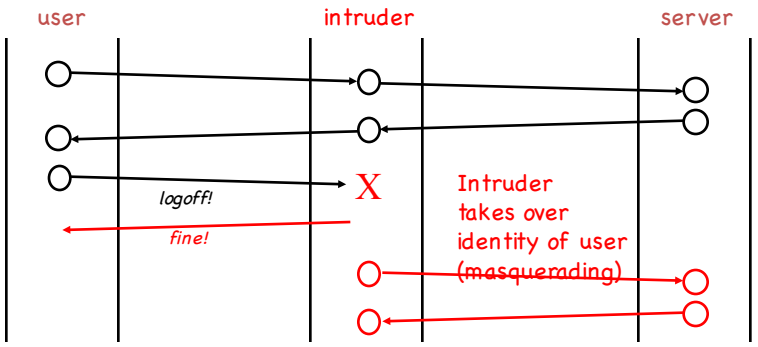
Authenticity Attack - Fabrication

- Unauthorized assumption of other's identity
- Generate and distribute objects under this identity



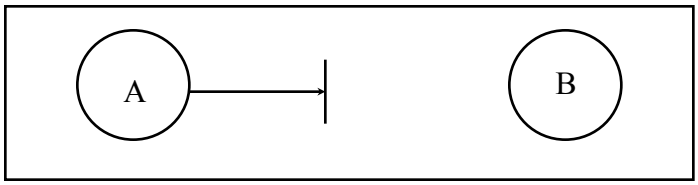
Man-In-The-Middle: Example

- **Passive tapping**
  - Listen to communication without altering contents.
- **Active wire tapping**
  - Modify data being transmitted
  - Example:



Attack on Availability

- Destroy hardware (cutting fiber) or software
- Modify software in a subtle way (alias commands)
- Corrupt packets in transit



- Blatant *denial of service* (DoS):
  - Crashing the server
  - Overwhelm the server (use up its resource)

Impact of Attacks

- Theft of confidential information
- Unauthorized use of
  - Network bandwidth
  - Computing resource
- Spread of false information
- Disruption of legitimate services

All attacks can be related and are dangerous!

Security Policy and Mechanism

- **Policy:** a statement of what is, and is not allowed
- **Mechanism:** a procedure, tool, or method of enforcing a policy

- Security **mechanisms** implement functions that help *prevent, detect, and respond to recovery from* security attacks
- Security functions are typically made available to users as a set of *security services* through APIs or integrated interfaces
- Cryptography underlies many security mechanisms.

Security Services

- **Confidentiality:** protection of any information from being exposed to unintended entities
  - Information content
  - Parties involved
  - Where they are, how they communicate, how often, etc.

Security Services - Cont'd

- **Authentication:** assurance that an entity of concern or the origin of a communication is authentic - it's what it claims to be or from
- **Integrity:** assurance that the information has not been tampered with
- **Non-repudiation:** offer of evidence that a party indeed is the sender or a receiver of certain information

Security Services - Cont'd

- **Access control:** facilities to determine and enforce who is allowed access to what resources, hosts, software, network connections
- **Monitor & response:** facilities for monitoring security attacks, generating indications, surviving (tolerating) and recovering from attacks

Security Services - Cont'd

- **Security management:** facilities for coordinating users' service requirements and mechanism implementations throughout the enterprise network and across the Internet
  - Trust model
  - Trust communication protocol
  - Trust management infrastructure

Assumptions and Trust

- A security policy consists of a set of axioms that the policy makers believe can be enforced
- Two assumptions
  - The policy correctly and unambiguously partitions the set of system states into secure and nonsecure states
    - The policy is correct
  - The security mechanisms prevent the system from entering a nonsecure state
    - The mechanisms are effective

Assumptions and Trust – Cont'd

- Trusting the mechanisms work require the following assumptions
  - Each mechanisms enforces part(s) of the security policy
  - The union of the mechanisms enforce all aspects of the policy
  - The mechanisms are implemented, installed, and administered correctly

How to Make a System Trustworthy

- Specification
  - A statement of desired functions
- Design
  - A translation of specifications to a set of components
- Implementation
  - Realization of a system that satisfies the design
- *Assurance*
  - The process to insure that the above steps are carried out correctly
  - Inspections, proofs, testing, etc.

Operational Issues

- Risk Analysis
- Cost-Benefit Analysis
- Laws and Custom

Human Issues

- Organizational Problems
- People Problems

"The data breaches came from a variety of mishaps, including theft of laptops, hacking, employees improperly handling data, accidental disclosure and problems with subcontractors."

The Security Life-Cycle

- **Threats**
- Policy
- Specification
- Design
- Implementation
- Operation and Maintenance

24

Taxonomy of Threats

- Taxonomy – a way to classify and refer to threats (and attacks) by names/categories
  - Benefits – avoid confusion
  - Focus/coordinate development efforts of security mechanisms
- No standard yet
- **One possibility:** by results/intentions first, then by techniques, then further by targets, etc.
  - Associate severity/cost to each threat

25

A Taxonomy Example

- By results first, then by (high-level) techniques:
  - Illegal root
    - Remote, e.g., buffer-overflow a daemon
    - Local, e.g., buffer-overflow a "root" program
  - Illegal user
    - Single, e.g., guess password
    - Multiple, e.g., via previously installed back-door
  - Denial-of-Service
    - Crashing, e.g., teardrop, ping-of-death, land
    - Resource consumption, e.g., syn-flood
  - Probe
    - Simple, e.g., fast/regular port-scan
    - Stealth, e.g., slow/"random" port-scan

26

Threat Examples - IP Spoofing

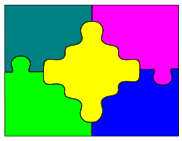
- A common first step to many threats
- Source IP address cannot be trusted!

SRC: source DST: destination	
IP Header	IP Payload
SRC: 18.31.10.8 DST: 128.194.7.237	Is it really from MIT?

27

Similar to US Mail (or E-mail)

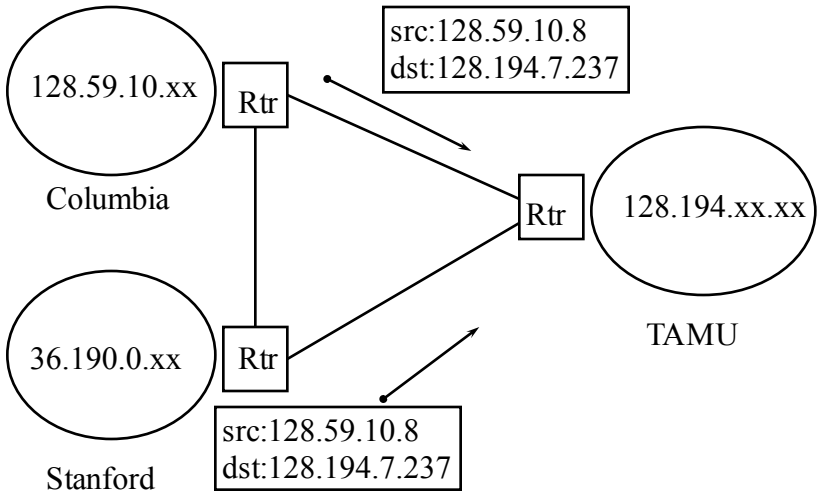
From:
Guofei Gu
TAMU



To:
William Smith
M.I.B. Corp.

US mail maybe better in the sense that there is a *stamp* put on the envelope at the *location* (e.g., town) of collection...

Most Routers Only Care About Destination Address



29

Why Should I Care?

- Attack packets with spoofed IP address help hide the attacking source.
- A *smurf* attack launched with your host IP address could bring your host and network to their knees.
- Higher protocol layers (e.g., TCP) help to protect applications from direct harm, but not enough.

30

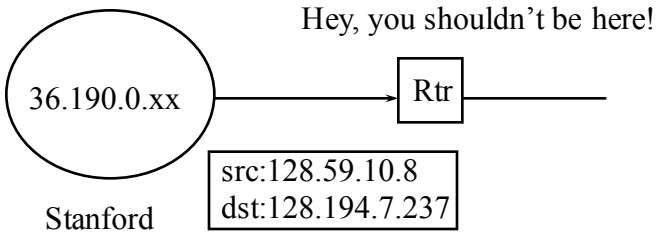
Current IPv4: IP Spoofing

- No authentication for the source
- Various approaches exist to address the problem:
  - Router/firewall filtering
  - TCP handshake

31

Router Filtering

- Decide whether this packet, with certain source IP address, should come from this side of network.



- Local policy

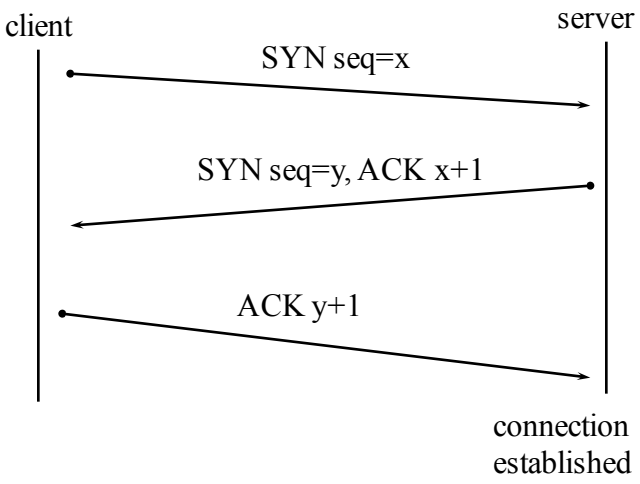
32

Filtering at Routers

- Very effective for some networks (ISP should always do that!)
  - At least be sure that this packet is from some particular subnet
- Problems
  - Hard to handle frequent add/delete hosts/subnets or mobile IP
  - Upsets customers should legitimate packets get discarded
  - Need to trust other routers

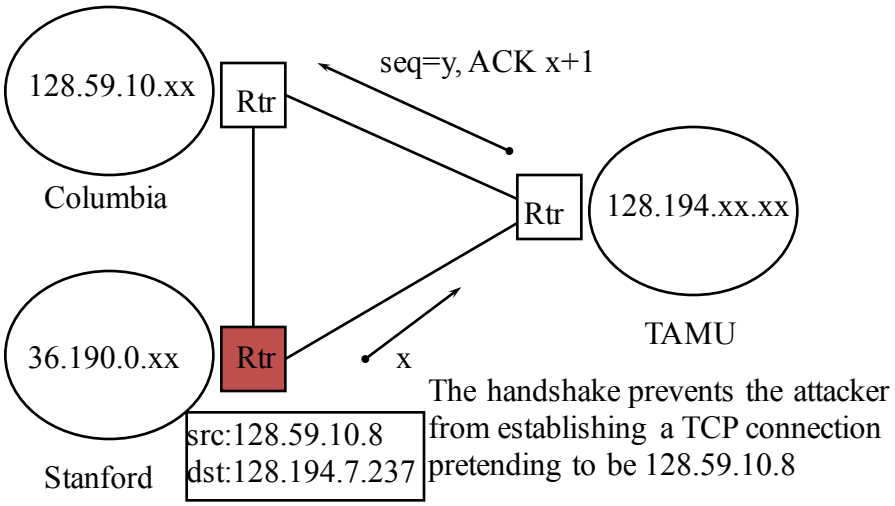
33

TCP Handshake



34

TCP Handshake



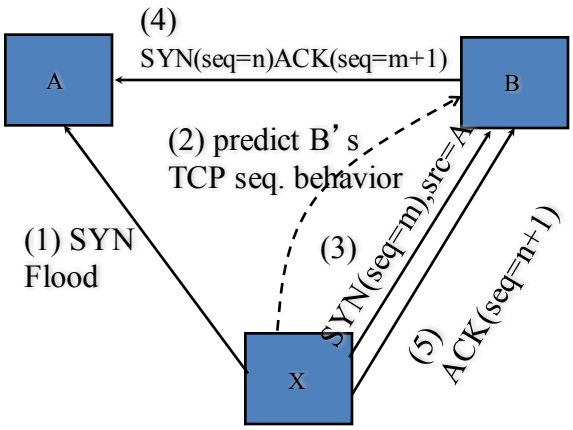
TCP Handshake

- Very effective for stopping most such attacks
- Problems
  - The attacker can succeed if "y" can be predicted
  - Other DoS attacks are still possible (e.g., TCP SYN-flood)

36

IP Spoofing & SYN Flood

- X establishes a TCP connection with B assuming A's IP address



37

Vulnerability

- A vulnerability (or security flaw) is a specific failure of the security controls
- Using the failure to violate the site security: exploiting the vulnerability; the person who does this: an attacker
- It can be due to
  - Lapses in design, implementation, and operation procedures.
  - Even security algorithms/systems are not immune!
    - We will go over some examples in this course

38

Example: IP Protocol-related Vulnerabilities

- Authentication based on IP source address
  - But no effective mechanisms against IP spoofing
- Consequences (possible exploits)
  - Denial of Service attacks on infrastructures, e.g.
    - IP Spoofing and SYN Flood
    - Redirection attacks

39