CS 372 Lecture #41

Security

- threats
- policies
- mechanisms

Note: Many of the lecture slides are based on presentations that accompany *Computer Networking: A Top Down Approach,* 6th edition, by Jim Kurose & Keith Ross, Addison-Wesley, 2013.

Cyber Crime

- Internet enables new types of crime
- Explosive growth of the problem
  - laws have been reactive instead of proactive
    - types of activities not anticipated
    - many "crimes" are not illegal yet
  - cost of protection
  - cost of security breaches
- Perpetrators
  - Criminal hackers (crackers)
  - Terrorists
  - Governments
  - Unknowing accomplices

2012 Poneman Report

- Most costly types of attacks
  - Malicious code
  - Denial of services
  - Web-based attacks
  - Stolen devices
  - Malicious insiders
  - Social Engineering, Phishing
  - Viruses, worms, trojans
  - Botnets
  - Malware
- Wireless/mobility makes crimes easier to commit, harder to trace

- Costs of attacks
  - Norton/Symantec estimates cost of internet theft
    - to US companies $250 billion/year
    - to US consumers $110 billion/year (not including costs passed on from companies)
    - globally $388 billion (including downtime)
  - McAfee estimates that $1 trillion was spent globally for remediation.
  - National security
    - cyber attacks now considered greater threat than terrorism
  - Personal security
    - identity theft, privacy
  - Interruption of essential services
    - power, water, medical, etc.
  - etc.

Security policies

- "Secure" is not an absolute term
- Need to define *security policy* for organization
- Costs and benefits of security policies must be assessed
  - What is the value of information?
- Policies must consider stored information as well as transmitted information.
- Users must be educated
  - Security policy is useless if users respond to "phishing", etc.

Maintaining security

- Data integrity
  - Data should be transmitted unchanged
  - Stored data should be "safe"
- Data availability
  - Authorized users should have access
  - Access should not be interrupted
- Data confidentiality
  - Only authorized users should have access
  - No snooping, wiretapping, etc.
- Privacy
  - User identity is protected
  - Private transactions are protected

Security mechanisms

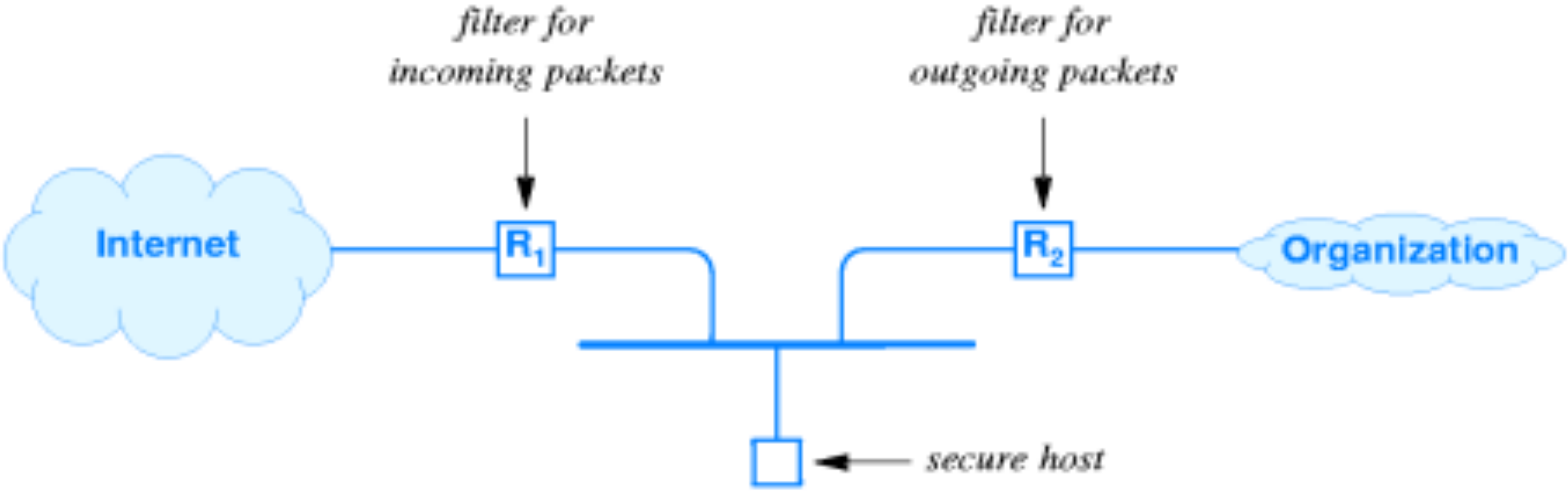
- Perimeter security
- Password / data encryption
- Others
  - Virtual private networks
    - Use Internet to transfer data among organization's sites but ensure that data cannot be read by others
  - Message authentication codes (MAC)
  - Digital signatures
  - etc.

Perimeter security

- Using *packet filters* to create a *firewall*
- Secure host ("bastion" host) runs application-layer gateways or proxies
- There are many variations.

Firewalls can't protect against …

- Malicious insiders
- Connections that don't go through it
  - E.G., dial-up connections
- Completely new threats
- Unknown viruses



Commercial / open-source security systems

- IDS Intrusion Detection System
- Kerberos from MIT
- SSH and OpenSSH Secure Shell
- SSL and OpenSSL Secure Socket Layer
- … and many others

Summary Lecture #41

- Cyber crime
  - scope of the problem
  - types of attacks
- Security
  - policies
  - mechanisms