Introduction

- Security is a problem whenever you use a shared medium, whether it’s the neighborhood in which you live or a computer network.
- There are a lot of bad guys out there doing a lot of naughty things.
- So how can you protect your information and communications from security breaches?

Aspects of Security

- There's no definition of network security in the abstract.
  - Security means different things to different people.
  - A college will have a different idea of security than a military installation.
- To begin, a person or an institution must define a security policy. There are many considerations:
  - Data accessibility.

    What data is to be made accessible to whom?

Aspects of Security

- Data integrity.

  What data is to be protected from change?
- Data confidentiality.

  What data is to be kept private?
- Messages traversing networks.
- Internal vs external access to a network.
- Read-write vs read-only access to data.
- Delegation and control of responsibility.

  Accountability.

  Who is responsible for what data? How are records kept?

Aspects of Security

Authorization.

Who is responsible for who gets special privileges? How is this done?

Types of Security Threats

- Can an intruder listen to and record network messages?

  Yes—by using a packet sniffer.
- Can an intruder add and remove messages?

  Yes—by IP spoofing.
- Denial-of-service attacks.

  These typically create so much work for the infrastructure under attack that legitimate work cannot be performed.

Integrity Mechanisms

- Parity checks, checksums, CRCs are used to help insure data integrity.
- Passwords are used to control access to certain systems and data.
- Data encryption is used to ensure the privacy of a message.
- Encryption is used for:
  - Secrecy.
  - Sender and receiver authentication.
  - Message integrity.

A Big (Unfounded?) Fear

- One of the biggest fears is that someone will steal a credit-card number over the Internet and run up whopping charges.
- In reality, it's far more likely that a clerk in a department store or a waiter in a restaurant will steal a credit-card number from a receipt than it is for a hacker to grab a number in transit across the Internet.
- As of 2000, all major on-line thefts of credit-card numbers were accomplished by stealing the information from poorly secured databases and files *after* the information had been safely transmitted.

A Big (Unfounded?) Fear

- Nevertheless, to make the Internet more secure, encryption is used for:
  - Confidentiality.
  - Authentication.
  - Transmission accuracy.

Encryption

- Encryption is a complex subject.
- Performing encryption properly requires a detailed understanding of the mathematical algorithms used to encrypt and decrypt data and the protocols used to exchange keys and encrypted data.
- Even a small mistake can open a large hole in your armor and reveal your communications to an eavesdropper.
- Fortunately, non-experts can secure their communications with software designed by experts.

Encryption

- Confidential communication through an open channel such as the public Internet absolutely requires that data be encrypted.
- For example, every time you order something from an on-line store using a browser, chances are the transaction is encrypted and authenticated.
- You should expect no less!

Packet Filtering

- Routers and other packet-forwarding devices can be configured to drop certain packets.
- Filtering is usually based on network addresses and ports.
- Examples:
  - Traffic coming in from the Class C network address 193.28.25.0 may be rejected because of bad experiences with hackers in the past.
  - Outgoing Telnet connections may be allowed, but incoming Telnet connections may not be.

Packet Filtering

- Incoming connections on port 80 (Web) may be allowed but only to the corporate Web server.

Firewalls

- firewall - a packet filter at the edge of an intranet which protects the entire intranet from unwanted outside traffic.
- Packets can be restricted to just a few computers.
- It's less expensive and more convenient to install a firewall than to make each individual computer secure.

Proxies

- We already say how a proxy server can be used to cache documents for multiple users (HTTP).
- If a firewall protects hosts on a network by preventing them from making direct connections to the outside world, a proxy server can act as a go-between.
- A machine that is prevented from connecting to the Internet by a firewall can make a request for a Web page from a local proxy server instead of requesting the Web page directly from the remote Web server.

Proxies

- The proxy server then requests the page from the remote Web server and forwards the response to the original requester.
- Proxies can also be used for FTP services and other types of connections.

Why Do This?

- One reason is that external hosts find out only about the proxy server.
- They do not learn the names and IP addresses of internal machines, making it more difficult to hack into the internal systems.
- Another reason is that access to the Internet can be controlled.
  - A company can block access to certain Websites and allow access to others.
  - A company can allow incoming FTP but block outgoing FTP so that confidential data cannot be smuggled out.

Why Do This?

- A company can use proxy servers to keep track of employees' Web usage.

  Controversial and not an indication of enlightened management techniques.