NETWORK SECURITY

Farooq Ashraf

Department of Computer Engineering

King Fahd University of Petroleum and Minerals

Dhahran 31261, Saudi Arabia

Outline of the Presentation

- What is Security
- Introduction to Computer Network Security
- Attacks, Services, and mechanisms
- Security Threats
- Cryptosystems
- Firewalls
- E-mail Security

Security and Why do we need it ?

Security is a concern of organizations with assets that are controlled by computer systems. By accessing or altering data, an attacker can steal tangible assets or lead an organization to take actions it would not otherwise take. By merely examining data, an attacker can gain a competitive advantage, without the owner of the data being any wiser.

Computers at Risk: Safe Computing in the Information Age

U.S. National Research Council, 1991.

Data Security

- Impossible to have 100% secure system.
- Given enough time and skill, the system can be broken.
- Strategies for data security:
  - » Physical Security: Lock, Guard, Alarm
  - » Personal Identification: Badges, user IDs, passwords
  - » Encryption
- Passwords should be:
  - » Chosen by the system;
  - » Changed regularly;
  - » Encrypted during login;

Introduction

Two Major Developments During the Past Decade:

1. Widespread Computerization
2. Growing Networking and Internetworking
   - ➧ The Internet

- Need for Automated Tools for Protecting Files and Other Information.
- Network and Internetwork Security refer to measures needed to protect data during its transmission from one computer to another in a network or from one network to another in an internetwork.

Introduction (Cont'd)

Network security is complex. Some reasons are:

- Requirements for security services are:
  - ï Confidentiality
  - ï Authentication
  - ï Integrity
- Key Management is difficult.

  Creation, Distribution, and Protection of Key information calls for the need for secure services, the same services that they are trying to provide.

cks, Services, and Mechanisms

- Assessment of security needs of an organization involves the evaluation of types of services needed and the types of attacks that could occur and the cost of such attacks.
- Classification of Security Services:
  - ï Confidentiality
  - ï Authentication
  - ï Integrity
  - ï Nonrepudiation
  - ï Access Control
  - ï Availability

cks, Services, and Mechanisms (Cont'd)

- Security Attacks:___
  - ï Interruption
  - ï Interception
  - ï Modification
  - ï Fabrication
- Passive Attacks:
  Interception (confidentiality)
  - ï Release of message contents
  - ï Traffic Analysis

cks, Services, and Mechanisms (Cont'd)

- Active Attacks:
  - Interruption (availability)
  - Modification (integrity)
  - Fabrication (integrity)

Security Threats

- Unauthorized access
- Loss of message confidentiality or integrity
- User Identification
- Access Control
- Players:
  - User community
  - Network Administration
  - Introducers/Hackers
- The bigger the system, the safer it is
  - MVS mainframe users (5%)
  - UNIX users (25%)
  - Desktop users (50%)

C r

- The Science of Secret writing.
- Encryption: Data is transformed into unreadable form.
- Decryption: Transforming the encrypted data back into its original form.

- Types of Cipher
  - » Transposition
  - » Substitution

Types of Cryptosystems

1- Conventional Cryptosystems

- ï Secret key Cryptosystems.
- ï One secret key for Encryption and Decryption.

» Example: DES

2- Public key cryptosystems

» Two Keys for each user

- ï Public key (encryptions)
- ï Private key (decryptions)

» Example: RSA

s of Cryptosystems (Secret Key)

- Both the encryption and decryption keys are kept secret.

Example:

To encrypt, map each letter into the third letter forward in the alphabet order;

To decrypt, map each letter into the third letter back.

- Problems with Secret Key Cryptosystems:
  - ï Key transfer
  - ï Too many keys

Key Cryptosystems (DES)

- Data Encryption Standard (1977)
- Started with an IBM Project called LUCIFER (1971)
- DES key length: 56-bits
- Uses 16 iterations with
  - » Transportation
  - » Substitution
  - » XOR operations
- DES Criticism
  - ï Key length
  - ï Design of S-Boxes in hidden
- Future
  - ï Multiple DES
  - ï IDEA (International Data Encryption Algorithm)

s of Cryptosystems (Public Key)

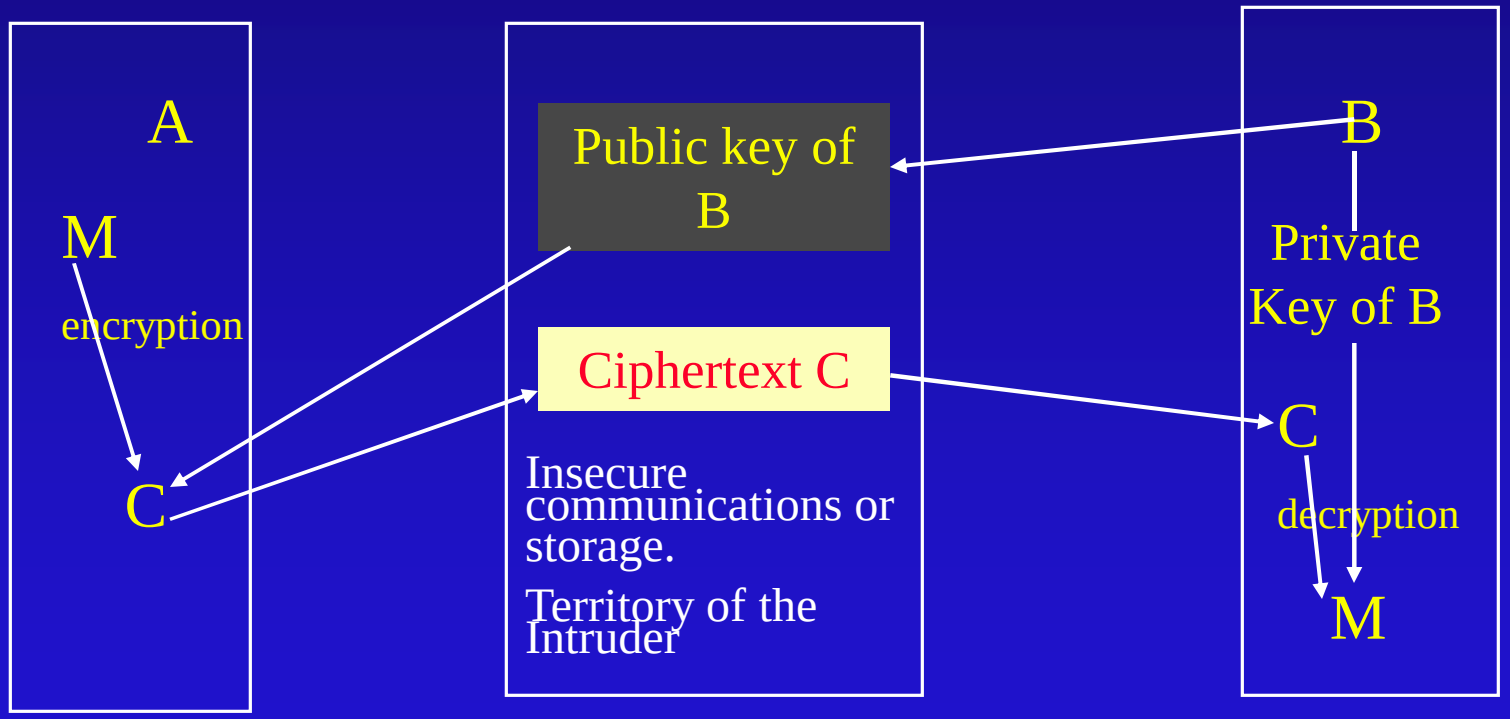
- Only the decryption key is kept secret. The encryption key is made public.
- Each user has two keys, one secret and one public.
- Public keys are maintained in a public directory.
- To send a message M to user B, encrypt using the public key of B.
- B decrypts using his secret key.

Signing Messages

For a user Y to send a signed message M to user X.

1. **Y encrypts** M using his secret key.
2. X decrypts the message using Yôs public key.

Public Key



A wants to send M in a secure manner to B

RSA Public Key Cryptosystem

- Proposed by Rivest-Shamir-Adelman in 1978.
- Each user chooses two large primes p and q. Let $n = p*q$; $k = (p-1)*(q-1)$.
- Also calculate two integers d and e such that

$$d*e \bmod k = 1$$

- The user publishes the pair (n,e) as his public key, where a message M is encrypted as,

$$C = M^e \bmod n$$

- The message C is decrypted as follows:

$$C^e \bmod n = M$$

RSA Example

- Let $n = 3 * 7 = 21$; $k = 2 * 6 = 12$.
- $d * e \bmod k = 17 * 5 \bmod 12 = 85 \bmod 12 = 1$
  - ☑ $d = 17$ and $e = 5$
- The pair $(e,n) = (5,21)$ is the public key.
- The message $M = 2$ is encrypted as

$$2^5 \bmod 21 = 9$$

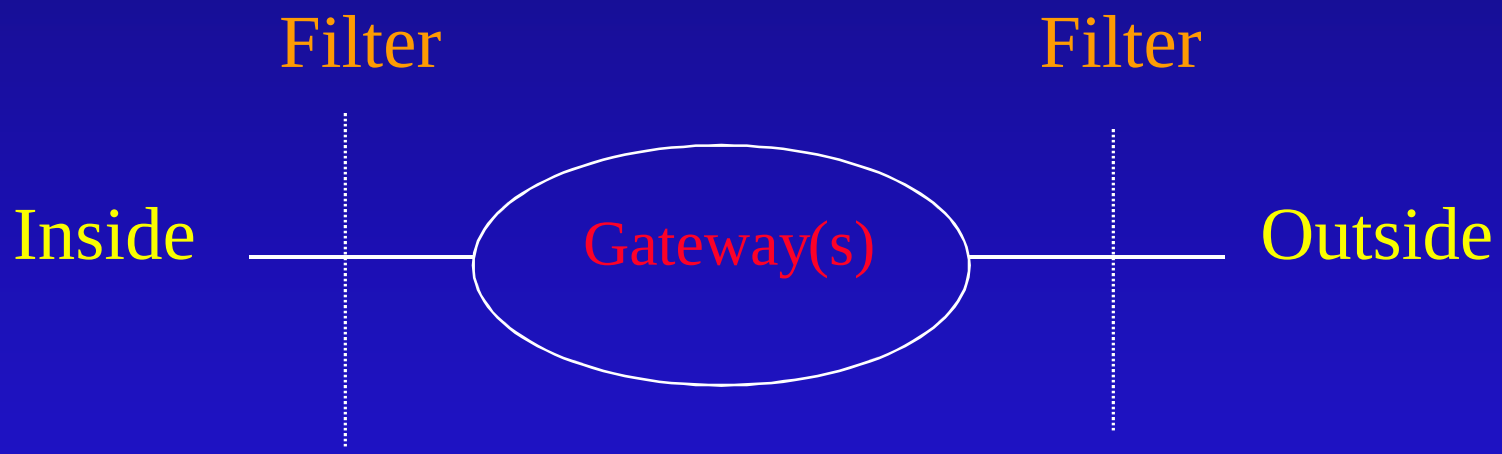
- The receiver decrypts as follows:

$$9^{17} \bmod 21 = 2$$

Firewalls

- A firewall is a barrier placed between the private network and the outside world.
- All incoming and outgoing traffic must pass through it.
- Can be used to separate address domains.
- Control network traffic.
- **Cost:** ranges from no-cost (available on the Internet) to $ 100,000 hardware/software system.
- **Types:**
  - Router-Based
  - Host Based
  - Circuit Gateways

Firewall



Schematic of a firewall

Firewall Types (Router-Based)

- Use programmable routers
- Control traffic based on IP addresses or port information.

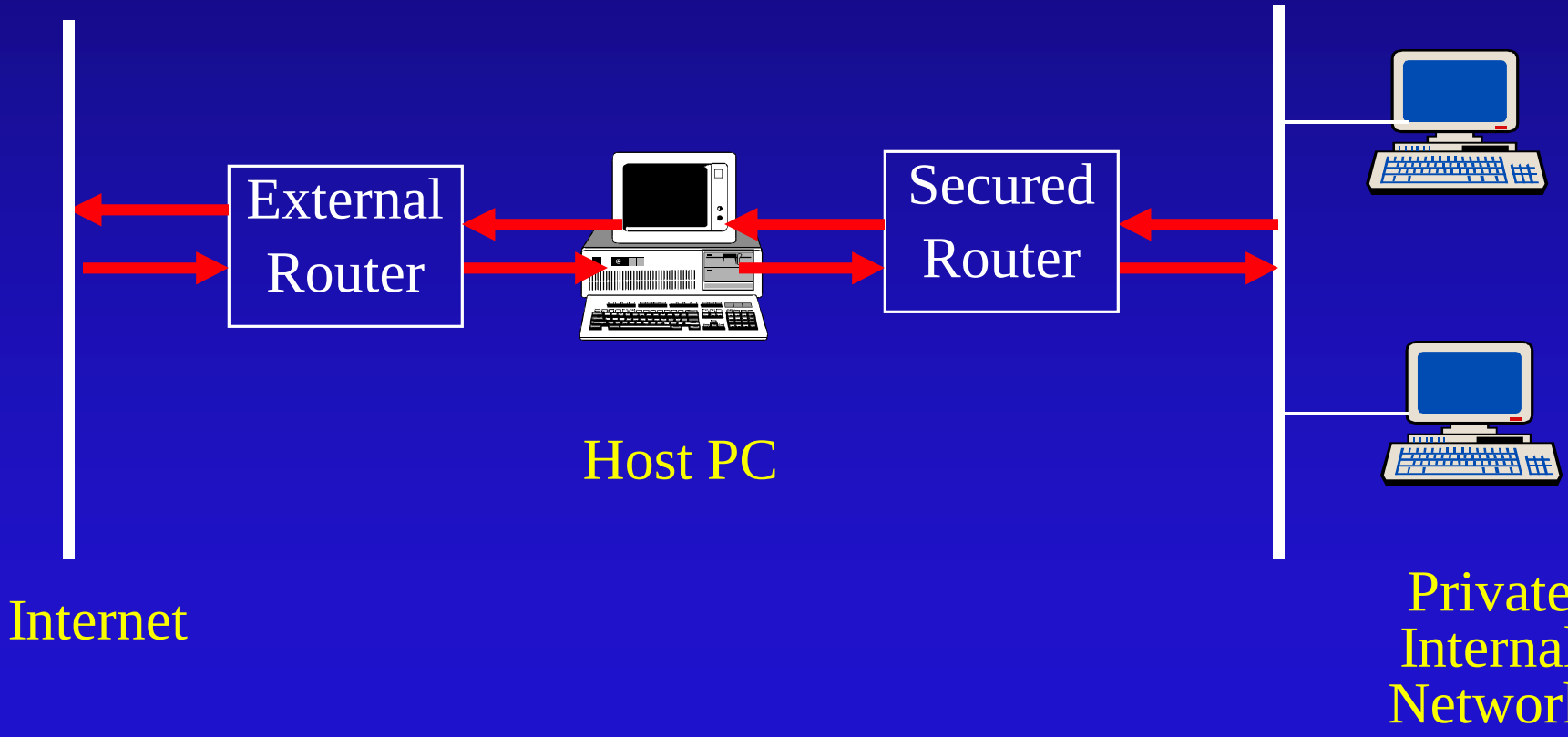
Examples:

- » Bastion Configuration
- » Diode Configuration

To improve security:

- Never allow in-band programming via Telnet to a firewall router.
- Firewall routers should never advertise their presence to outside users.

Bastion Firewalls

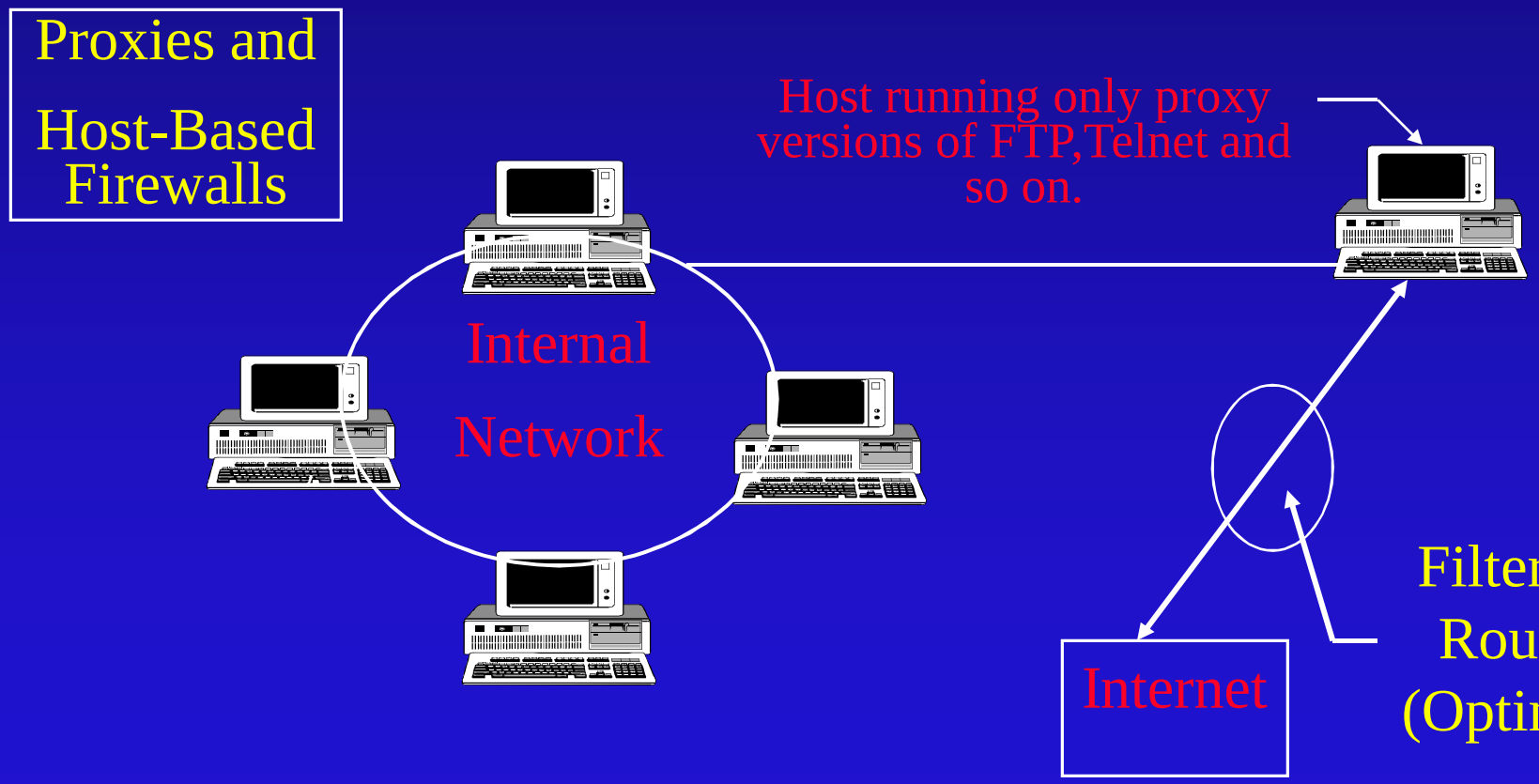


Firewall Types (Host-Based)

- Use a computer instead of router.
- More flexible (ability to log all activities)
- Works at application level
- Use specialized software applications and service proxies.
- Need specialized programs, only important services will be supported.

Firewall Types
Host-Based (Cont'd)

- **Example:** Proxies and Host-Based Firewalls



Electronic Mail Security

- E-mail is the most widely used application in the Internet.
- Who wants to read your mail ?
  - » Business competitors
  - » Reporters,Criminals
  - » Friends and Family
- Two approaches are used:
  - » PGP: Pretty Good Privacy
  - » PEM: Privacy-Enhanced Mail

E-mail Security (PGP)

- Available free worldwide in versions running on:
  - » DOS/Windows
  - » Unix
  - » Macintosh
- Based on:
  - » RSA
  - » DIDEA
  - » MD5

E-mail Security (PGP cont'd)

- Where to get PGP
  - » Free from FTP site on the Internet
  - » Licensed version from ViaCrypt in USA

Example:

pgp -kg ID-A	⟶	Signature
pgp esa m.txt ID-B	⟶	Encryption
pgp message	⟶	Decryption

Function	Algorithms used	Description
Message encryption	IDEA, RSA	A message is encrypted using IDEA with a one time session key generated by the sender. The session key is encrypted using RSA with the recipientôs public key, and included with the message.
Digital signature	RSA, MD5	A hash code of a message is created using MD5. This message digest is encrypted using RSA with the senderôs private key, and included with the message.
Compression	ZIP	A message may be compressed, for storage or transmission, using ZIP.

Summary of PGP Services

Function	Algorithms used	Description
E-mail compatibility	Radix 64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.
Segmentation	——	To accommodate maximum message size limitations, PGP performs segmentation and reassembly.

E-mail Security (PEM)

- A draft Internet Standard (1993).
- Used with SMTP.
- Implemented at application layer.
- **Provides:**
  - » Disclosure protection
  - » Originator authenticity
  - » Message integrity

E-mail Security (PEM cont'd)

- **Does not address**
  - » Access Control
  - » Traffic Flow
  - » Routing Control
  - » Assurance of message receipt.

Summary of PEM Services

Function	Algorithms used	Description
Message encryption	DES-CBC	A message is encrypted using DES-CBC with a one-time session key.The session key is encrypted using RSA with with the recipientôs public key and included with the message.
Authentication and Digital sig-Nature (asymmetric encryption)	RSA with MD2 or MD5	A hash code of a message is created using MD2 or MD5. This message digest is encrypted using RSA with the senderôs private key,and included with the message.

ary of PEM Services (cont'd)

Function	Algorithms used	Description
Authentication (asymmetric encryption)	DES-ECB or DES-EDE with MD2 or MD5	A hash code of a message is created using MD2 or MD5. This message digest is encrypted using either DES-ECB or DES-EDE (triple DES) using a symmetric key shared by sender and receiver, and included with the message.
Symmetric key Management	DES-ECB or DES-EDE	The session key is encrypted using either DES-ECB or DES-EDE (triple DES) using a symmetric key shared by sender and receiver, and included with the message.

ary of PEM Services (cont'd)

Function	Algorithms used	Description
Asymmetric key management	RSA, MD2	Public-key certificates are created and signed using MD2 to hash the certificate and RSA to encrypt the hash code. The session key is encrypted using RSA with the recipient's public key, and included with the message.
E-mail compatibility	Radix 64 conversion	To provide transparency for e-mail applications, an encrypted message may be converted to an ASCII string using radix-64 conversion.