Network and Cloud Security
CSC 3207: Computer Security

Outline

- Model for Network Security
- Encryption for Network Security
- Firewalls
- Intenet Security.
- Intrusion detection and prevention systems
- References: Stallings,William, and Lawrie Brown. Computer security: principles and practice. Pearson,2015.

Network Security

What do you want to protect?

- Your data: Information stored in your computer
- Your resources: The computers themselves
- Your reputation: Your risk to be blamed for intrusions or cybercrime
- Security aspects for your data are the "usual" ones:
  - Confidentiality, Integrity, Availability
  - E.g., when communicating, the other party's identity must be verified - authentication

Network Security

Reasons for security problems in networks

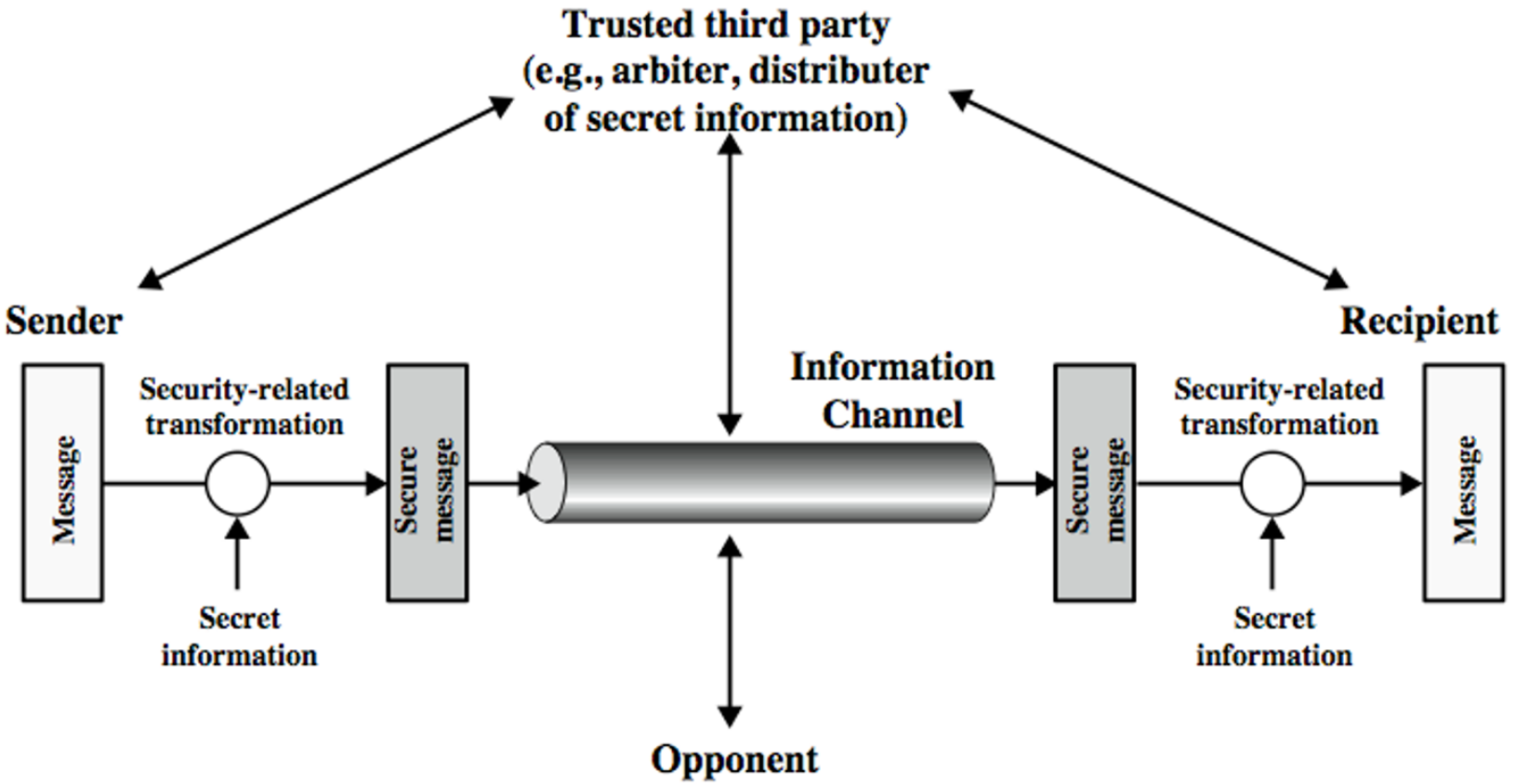
- Resource sharing: Access by many users to many systems
  - How to establish access control - Single sign on (SSO)
- Complexity of systems: Diversity, Changeability, Heterogeneity
- Unknown perimeter boundary
  - Difficult to define and/or know. Where are the Intranet boundaries
  - To which systems are you connected – what are the security policies
  - Mobile devices also make it worse
- Several points of attack
  - Targets as well as attack origins
  - Increases threat level significantly

Network Security

Reasons for security problems in networks

- Anonymity
  - Your identity will most likely be revealed
  - The attacker will be anonymous
- Unknown communication path
  - Several routes between two nodes
  - Lack of control of the network
- Insecure Medium: It is almost impossible to secure the network itself, i.e., the communication links
  - You must always assume that attackers are able to bug and modify all traffic

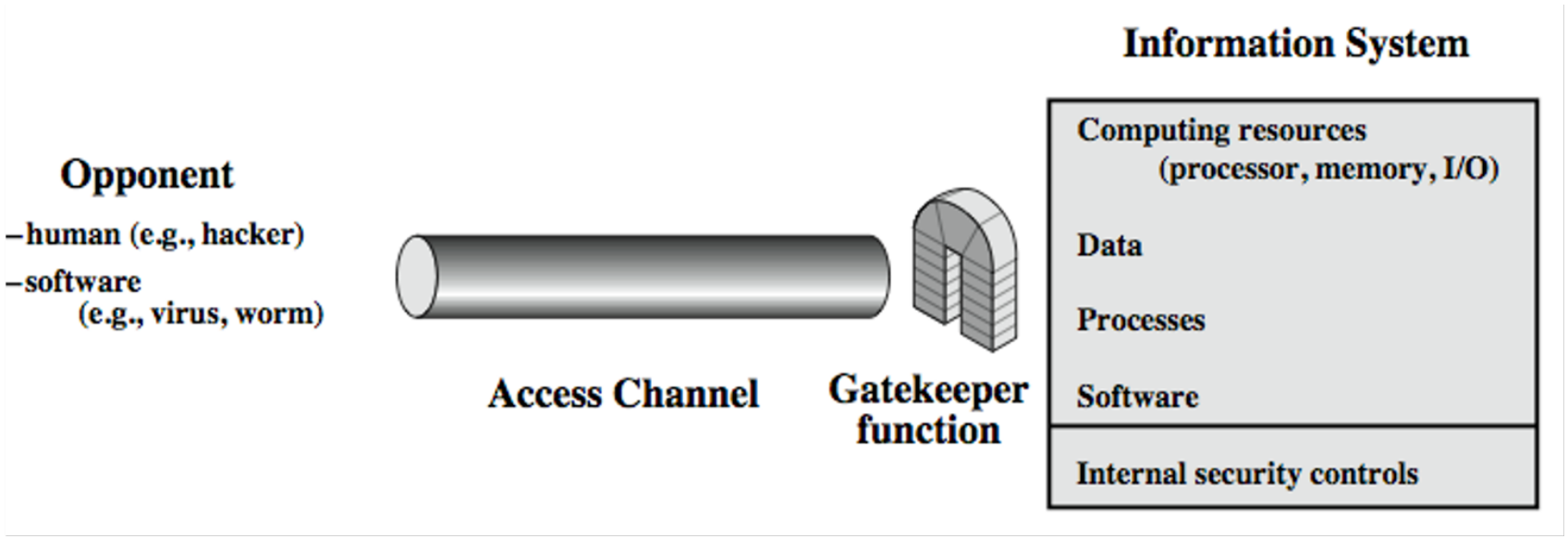
Model for Network Security



Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



Model for Network Access Security

- using this model requires us to:
  - select appropriate gatekeeper functions to identify users
  - implement security controls to ensure only authorised users access designated information or resources
- note that model does not include:
  - monitoring of system for successful penetration
  - monitoring of authorized users for misuse
  - audit logging for forensic uses, etc.

Encryption

- *Encryption* involves transforming a message into undecipherable message
  - only a user with knowledge of transformation algorithm/key can obtain original message
- Components of encryption:
  - Plaintext: the original message
  - Ciphertext: the encrypted message
  - Key: used to change the output of the encryption algorithm for a given plaintext
  - Encryption algorithm: transforms the plaintext into ciphertext
  - Substitution algorithm: replace characters in plaintext with others
  - Transposition algorithm: re-arrange characters
  - Decryption algorithm: transforms ciphertext into plaintext

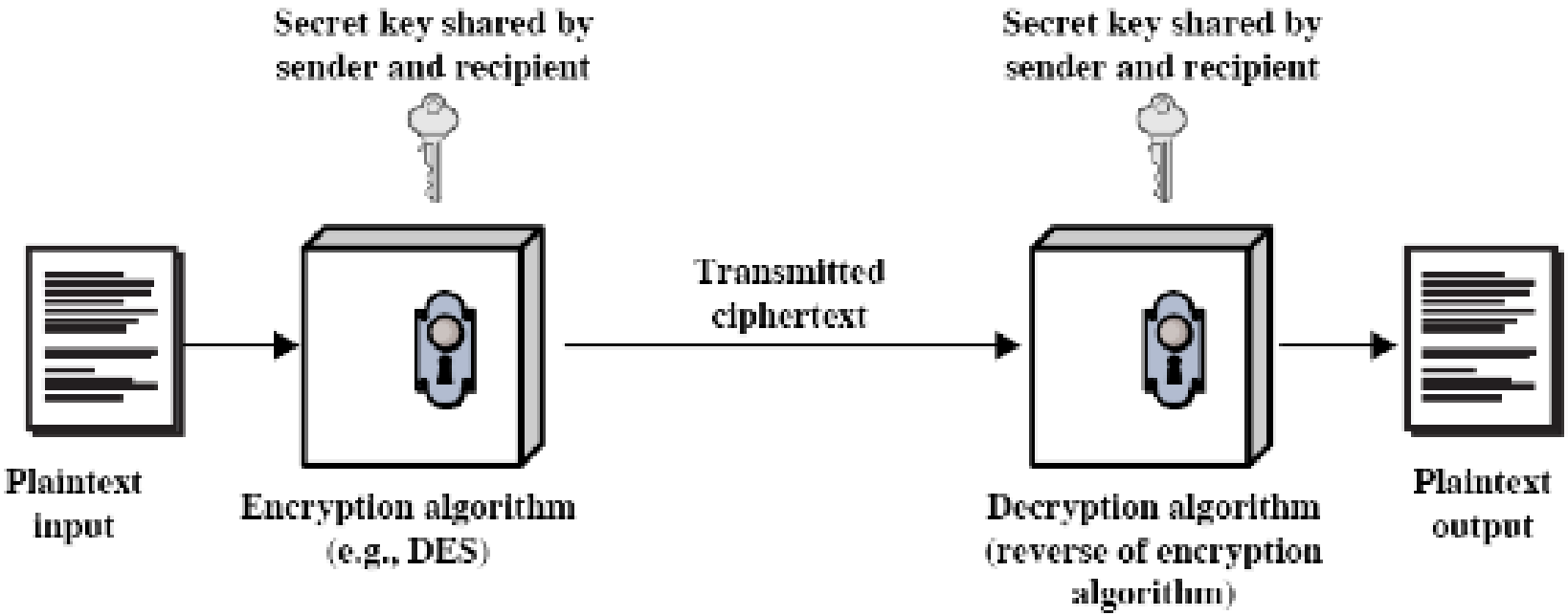
Encryption

- Encryption plays an important role in network security
  - Used to provide almost all security services
- Two types of encryption:
  - Symmetric Key Encryption (or Secret Key, or Shared Key)
  - Public Key Encryption (or Asymmetric Key)

Symmetric Key Encryption

- A key is shared between sender and recipient: this is the secret
- Secure if:
  - Encryption algorithm is strong: Given the algorithm and ciphertext, an attacker cannot obtain the key or plaintext
  - Sender and receiver have knowledge of the secret key (and keep it secret)
- No need to keep the algorithm secret (only the key)
  - Allows for mass and cheap manufacturing of devices that perform symmetric key encryption

Symmetric Key Encryption



A Simple Example: Caesar Cipher

- Take the plaintext p, where letters are mapped to numbers (a=0, b=1, . . .)
- Shift the letters in plaintext by k positions (in example, k=3)
  Plain (p): *a b c d e f g h i j k l m n o p q r s t u v w x y z*
  Cipher (C): *D E F G H I J K L M N O P Q R S T U V W X Y Z A B C*
- Encryption: Ciphertext, $C = E(p) = (p + k) \bmod (26)$
- Decryption: Plaintext, $p = D(C) = (C - k) \bmod (26)$
  Cipher: VHFXULWBDQGFUBSWRJUDSKB
  Plain: ?

A Simple Example: Caesar Cipher

- Breaking the Caesar Cipher
  - Try all 25 possible combinations of k (the key)
  - If the output (plaintext) is something you recognise (e.g. English words), then that is highly likely the key
  - This is called Brute Force Attack
- Brute Force Attack
  - Try every key possible until readable text is obtained from the ciphertext
- Cryptanalysis: Use knowledge of algorithm and/or plaintext patterns to "intelligently" decipher the ciphertext
  - Attacks differ based on amount of information known to attacker

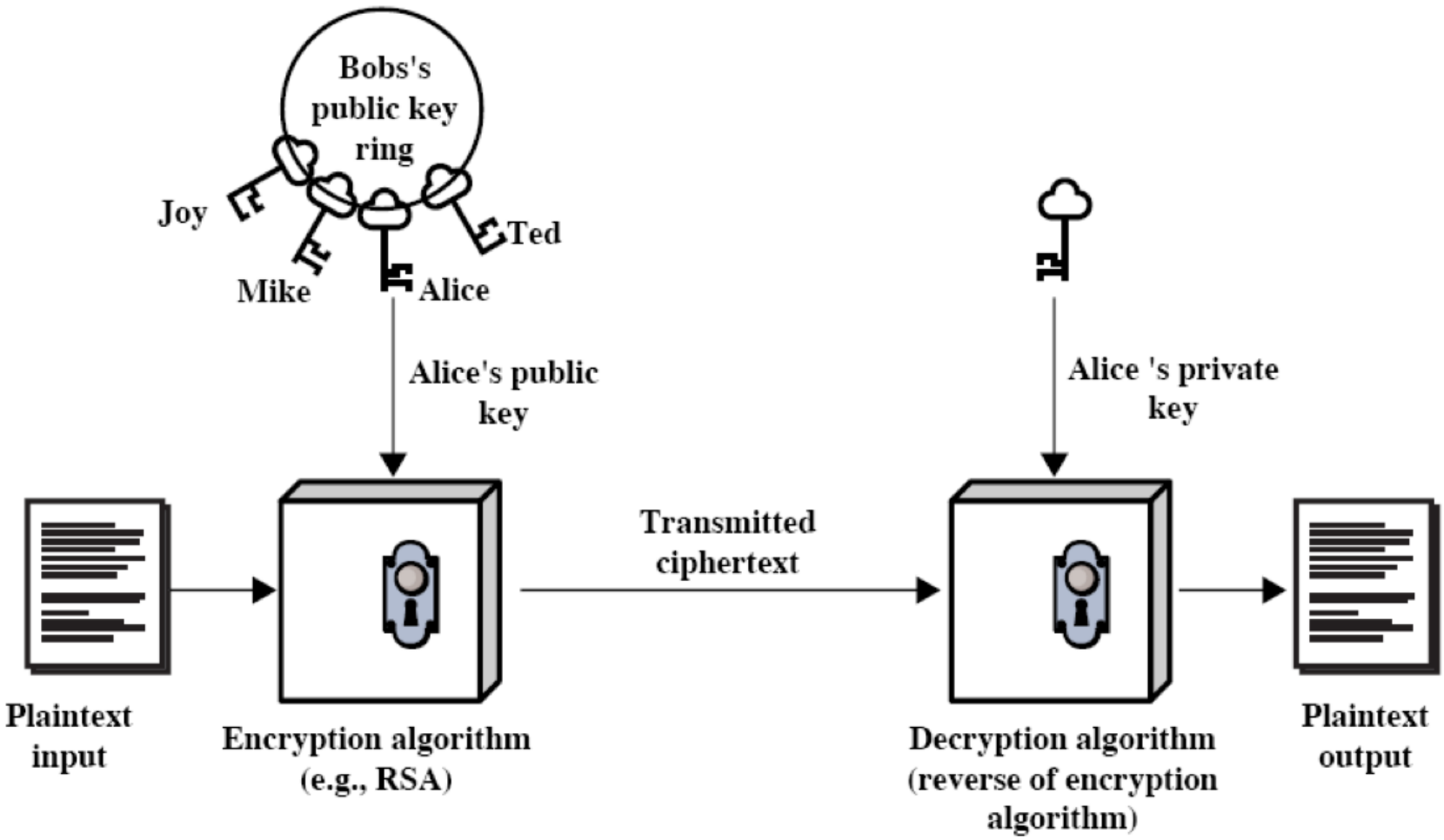
Real Symmetric Key Algorithms

- Data Encryption Standard (DES)
  - Published as standard in 1977 by NIST
  - 56-bit key – today it is not strong enough
  - In 1999 NIST recommended Triple DES (3DES) to be used: 128-bit keys
- Advanced Encryption Standard (AES)
  - Published as standard in 2001 by NIST
  - Keys of 128, 192 or 256 bits
  - Used today in many network standards/products
- Others: IDEA, RC4/RC5, Skipjack, Blowfish, ...

Public Key Encryption

- Public key uses two different keys
- Main concept: Given the encryption key and algorithm, too hard to determine the decryption key
- Public key: key used by sender to encrypt plaintext
  - Owned by the receiver
  - Anyone can know the public key
- Private (Secret) Key: key used to decrypt ciphertext
  - Must be kept secret by the receiver
- The public key and private key are related
- Each user must have their own pair of keys
- For confidentiality, the pair belong to the receiver: (Public, Secret) or (P, S)

Symmetric Key Encryption



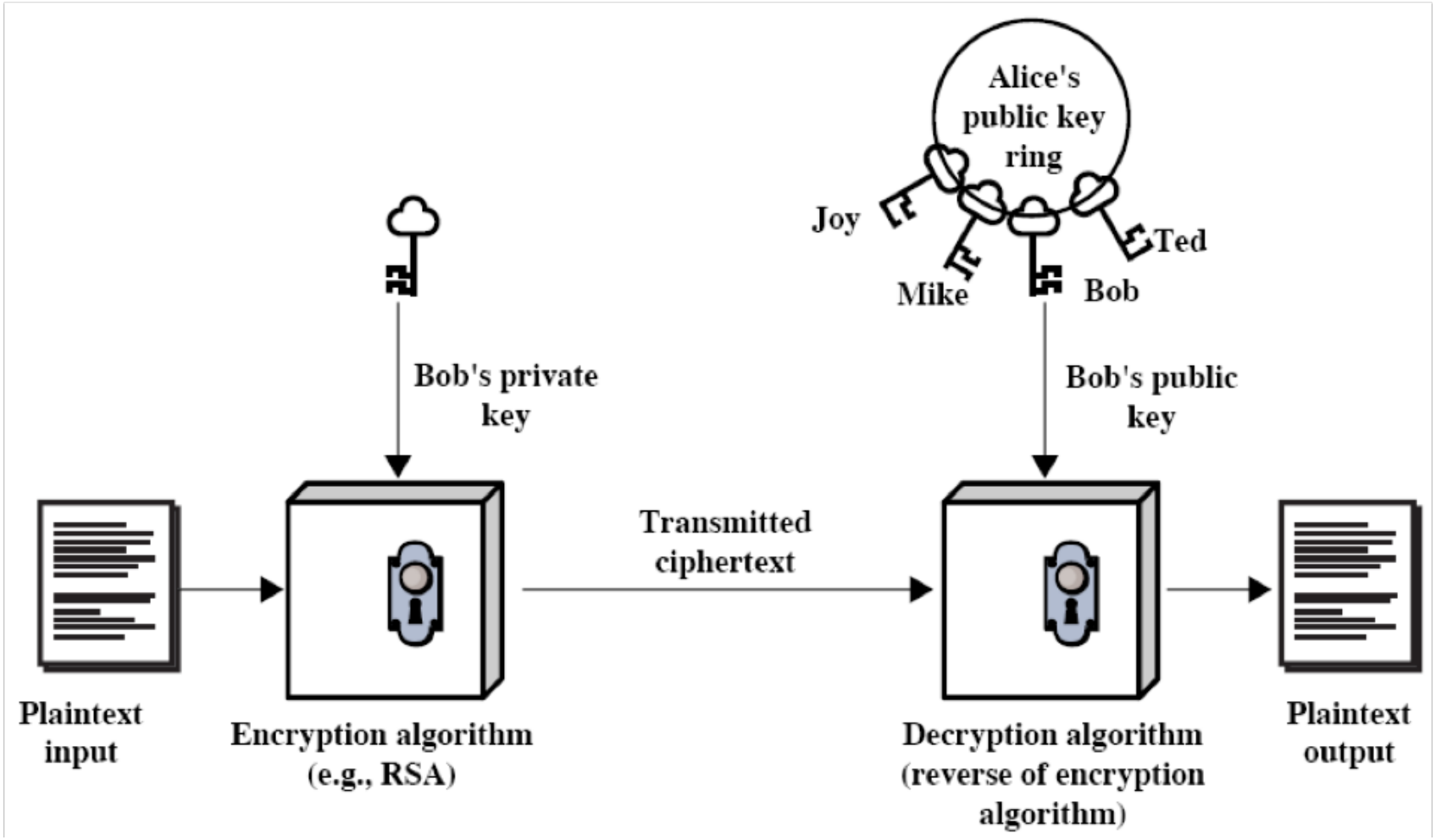
Public Key Algorithm

- If plaintext is encrypted with Public key, can only successfully decrypt with corresponding Private key
- Or if plaintext is encrypted with Private key, can only successfully decrypt with corresponding Public key
- Public key encryption requires:
  - Very hard (impossible) for someone to recover plaintext if they only know ciphertext and Public key
  - Very hard (impossible) for someone to determine Private key if they only know Public key

Public Key Authentication

- Authentication: assure that the message comes from the correct person
- If we trust that Bob's private/public key actually is Bob's private/public key ...
- If Bob encrypts a message with his private key, anyone can decrypt with Bob's public key (so this does not provide confidentiality)
- But since only Bob has Bob's private key, we know the message comes from Bob (and not someone pretending to be Bob); hence authentication is successful
- Encrypt with private key is used for Digital Signatures
  - Requires some Authority (government, company) to issue/validate Public/Private keys e.g. Verisign, Thawte

Symmetric Key Authentication



Public Key Algorithms

- RSA: Created in1978
  - Now most used Public Key algorithm
  - Key sizes of 1024 are generally considered secure
  - Attacks have been developed for key sizes up to 640 bits
- Others: Elliptic curve, Diffie Hellman, DSS, ...
- Practical applications:
  - Encryption/decryption for confidentiality
  - Digital Signature (authentication)
  - Key exchange (e.g. to securely exchange Symmetric Secret keys)

Symmetric vs Public Key

- Differentiate between Symmetric and Public Key encryption
- Symmetric
  - Sender and receiver use same shared Secret key
  - Requires secure distribution of Secret key
  - Difficult to manage
  - Encryption/decryption algorithms are fast, computationally efficient
- Public Key
  - Each user has a public/private key pair
  - One key used to encrypt, the other to decrypt
  - Easy to distribute the Public key
  - Post on web page, email, tell everyone – its public!
  - Encryption/decryption algorithms are slower
- Often Public Key encryption is used to exchange Symmetric Secret keys, then Symmetric key encryption to encrypt data

Internet Security

- Most Internet protocols did not initially include security mechanisms
  - But today, security can be an "optional extra" for almost all protocols
  - Tradeoff: more security leads to more complex implementations and less performance
- Most protocols use encryption for confidentiality
- Physical layer security
  - Encryption can be applied for high security applications
- Data Link Layer Security
  - LAN and WANs often don't have built-in encryption because the network/link is owned by one organisation ("trusted")
  - But options are available, especially in wireless networks e.g. WEP and WPA for IEEE 802.11 wireless LANs

Internet Security

- Network Layer
  - IP does not provide security
  - IPsec is an option of IP
  - Provides encryption (confidentiality and data integrity) of IP datagrams
  - Also authentication of senders (verify the sender)
  - If IPsec is used, all higher layer traffic can be secured (TCP, UDP, ICMP; web browsing, voice, instant message, . . .)
  - Requires implementation on PCs and routers
- Transport Layer
  - TCP and UDP do not provide security
  - Secure Sockets Layer (SSL) (also called Transport Layer Security (TLS)) is an optional extra for TCP
  - Provides encryption (confidentiality and data integrity) of TCP traffic
  - Does not support UDP applications
  - Requires implementation on PCs (in OS or application)

Internet Security

- Application Layer Security
  - HTTP can be configured to use SSL/TLS – called HTTPS
  - Secure web access
  - Secure Shell (SSH)
  - Secure remote login
  - And many others: SFTP, SMIME, ...
- Firewalls
  -

Firewalls

- A firewall is an access control device between two networks
  - Provide access control at edge of local network
- A firewall monitors all traffic (in both directions) and filters away (denies) unwanted traffic
- It protects against attacks from outside
- All traffic from inside to outside, and vice versa, must pass through the firewall – physical blocking all access to local network
- Only authorized traffic as defined by the local security policy will be allowed to pass - Look at each packet entering/leaving the local network
  - Check a set of rules as to whether the packet is allowed
  - Rules based on source/destination addresses, port numbers, protocols, users, and other policies
- The firewall itself is immune to penetration

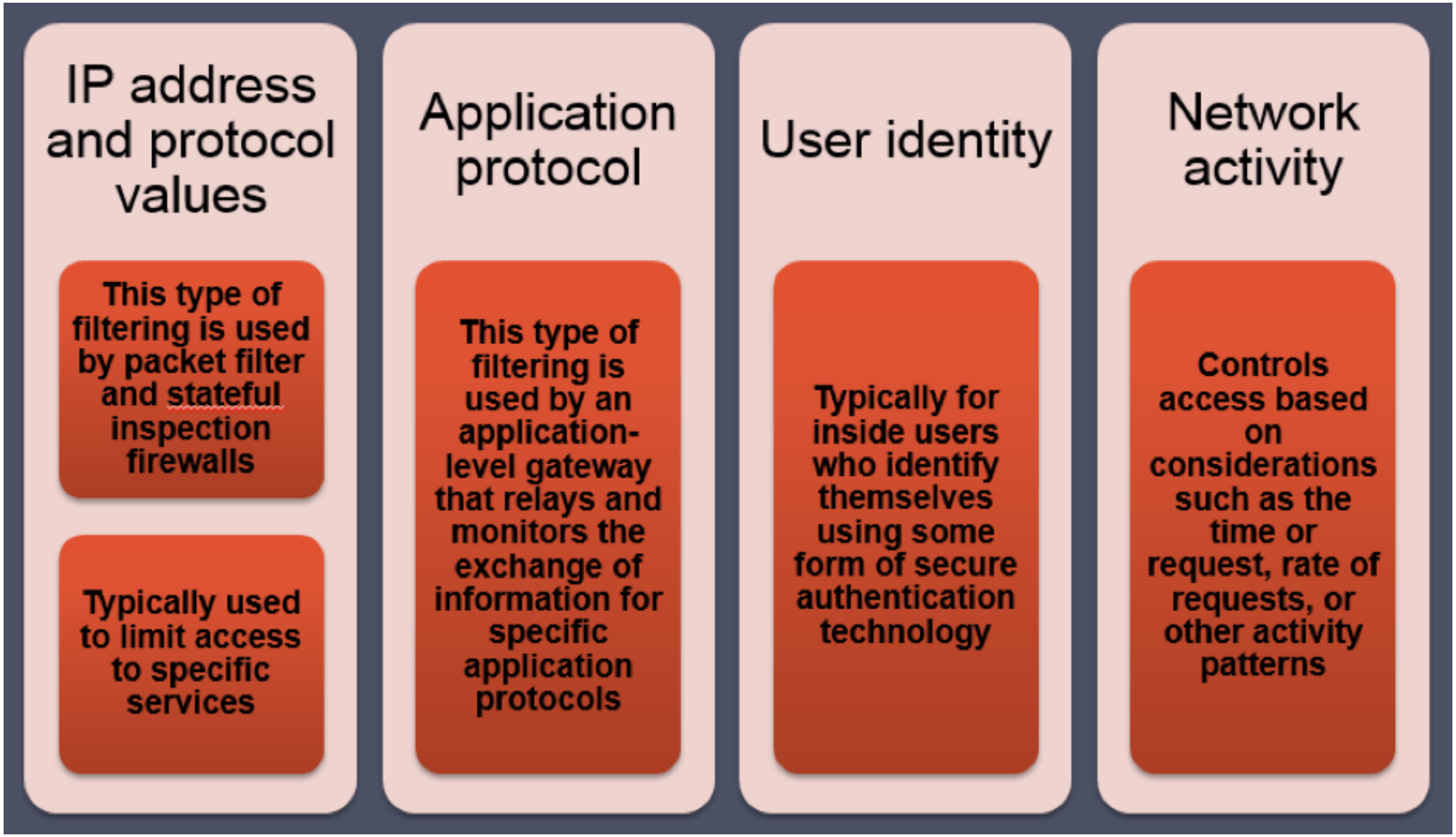
The Need for Firewalls

- Internet connectivity is essential but it creates a threat
- Effective means of protecting LANs
- Inserted between the premises network and the Internet to establish a controlled link
- Can be a single computer system or a set of two or more systems working together
- Used as a perimeter defense
- Single choke point to impose security and auditing
- Insulates the internal systems from external networks

Firewall Capabilities & Limitations

- Capabilities
  - Defines a single choke point
  - Provides a location for monitoring security events
  - Convenient platform for some Internet functions such as NAT, usage monitoring, IPSEC, VPNs
- Limitations
  - Cannot protect against attacks bypassing firewall
  - May not protect fully against internal threats
  - Improperly secure wireless LAN
  - Laptop, PDA, portable storage device infected outside then used inside

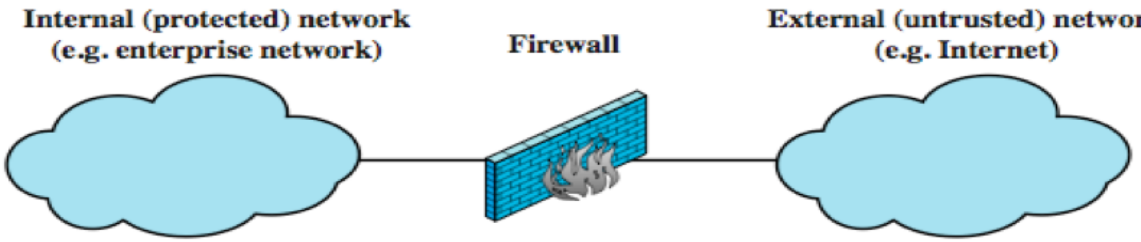
Firewall Filter Characteristics



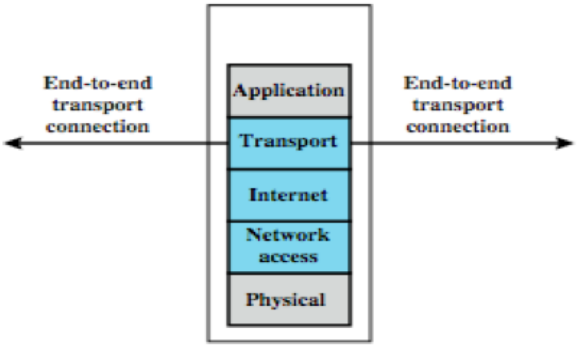
Firewalls - Basic Functionality

- A firewall implements an organization's security policy with respect to Internet.
- The stance of a firewall describes the fundamental security philosophy of the organization
- The default deny (discard) stance: everything is denies unless specifically permitted
  - More conservative, controlled, visible to users
- The default permit (forward) stance: everything is permitted unless specially denied
  - Easier to manage and use but less secure

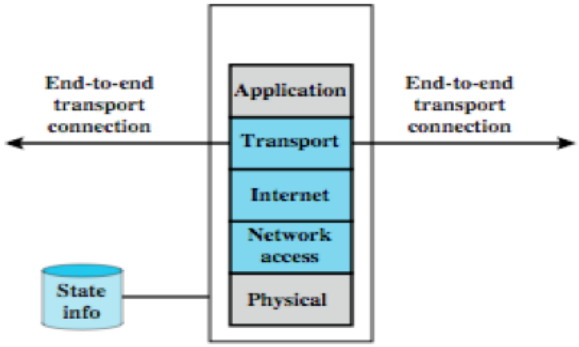
Firewall Types



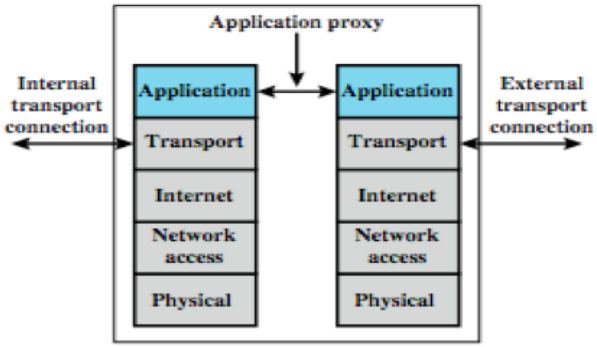
(a) General model



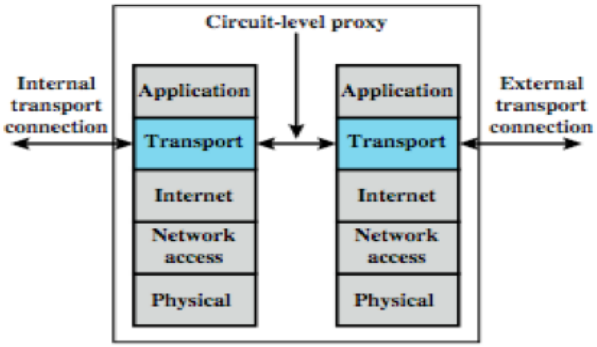
(b) Packet filtering firewall



(c) Stateful inspection firewall



(d) Application proxy firewall



(e) Circuit-level proxy firewall

Packet Filtering Firewall

- Applies rules to packets in/out of firewall based on information in packet header: Source IP address, Destination IP address & port, IP protocol, interface
- Applies rules to each incoming and outgoing IP packet
  - Typically a list of rules based on matches in the IP or TCP header
  - Forwards or discards the packet based on rules match
  - Does not understand the content of the message.

Packet Filtering Example

- Simplified example of a rule set for SMTP traffic.
- The goal is to allow inbound and outbound email traffic but to block all other traffic.
- The rules are applied top to bottom to each packet.

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Packet Filtering Example

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

1. Inbound mail from an external source is allowed (port 25 is for SMTP incoming).
2. This rule is intended to allow a response to an inbound SMTP connection.
3. Outbound mail to an external source is allowed.
4. This rule is intended to allow a response to an inbound SMTP connection.
5. This is an explicit statement of the default policy. All rule sets include this rule implicitly as the last rule

Packet Filtering - Pros and Cons

- Advantages
  - Simplicity
  - Typically transparent to users and are very fast
- Weaknesses
  - Cannot prevent attacks that employ application specific vulnerabilities or functions
  - Limited logging functionality
  - Do not support advanced user authentication
  - Vulnerable to attacks on TCP/IP protocol bugs
  - Improper configuration can lead to breaches

Stateful Inspection Firewall

- Tightens rules for TCP traffic by creating a directory of outbound TCP connections
- There is an entry for each currently established connection
- Packet filter allows incoming traffic to high numbered ports only for those packets that fit the profile of one of the entries in this directory
- Reviews packet information but also records information about TCP connections
- Keeps track of TCP sequence numbers to prevent attacks that depend on the sequence number
- Inspects data for protocols like FTP, IM and SIPS commands

Example Stateful Firewall Connection State Table

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Application-Level Gateway

- Also called an application proxy
- Acts as a relay of application-level traffic
  - User contacts gateway using a TCP/IP application
  - User is authenticated
  - Gateway contacts application on remote host and relays TCP segments between server and user
- Must have proxy code for each application
  - May restrict application features supported
- Tend to be more secure than packet filters
- Disadvantage is the additional processing overhead on each connection

Circuit-Level Gateway

- Circuit level proxy
- Sets up two TCP connections, one between itself and a TCP user on an inner host and one on an outside host
- Relays TCP segments from one connection to the other without examining contents
- Security function consists of determining which connections will be allowed
- Typically used when inside users are trusted
- May use application-level gateway inbound and circuit level gateway outbound
- Lower overheads

Firewall Locations: Bastion Hosts

- System identified as a critical strong point in the network's security
- Serves as a platform for an application-level or circuit-level gateway
- Common characteristics:
  - Runs secure O/S, only essential services
  - May require user authentication to access proxy or host
  - Each proxy can restrict features, hosts accessed
  - Each proxy is small, simple, checked for security
  - Each proxy is independent, non-privileged
  - Limited disk use, hence read-only code

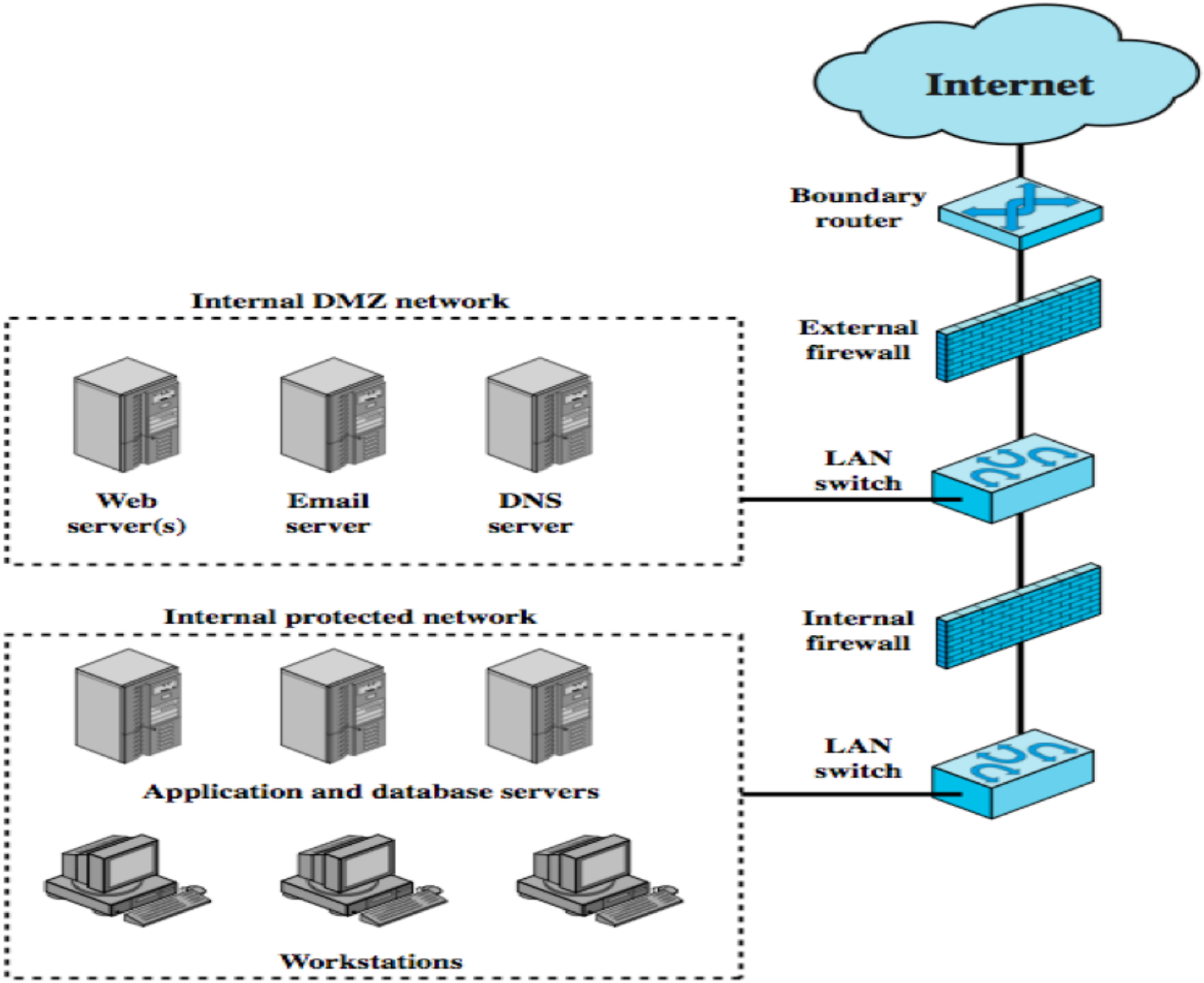
Host-based Firewalls

- Used to secure an individual host
- Available in operating systems or can be provided as an add-on package
- Filter and restrict packet flows
- Common location is a server
- Advantages:
  - Filtering rules can be tailored to the host environment
  - Protection is provided independent of topology
  - Provides an additional layer of protection

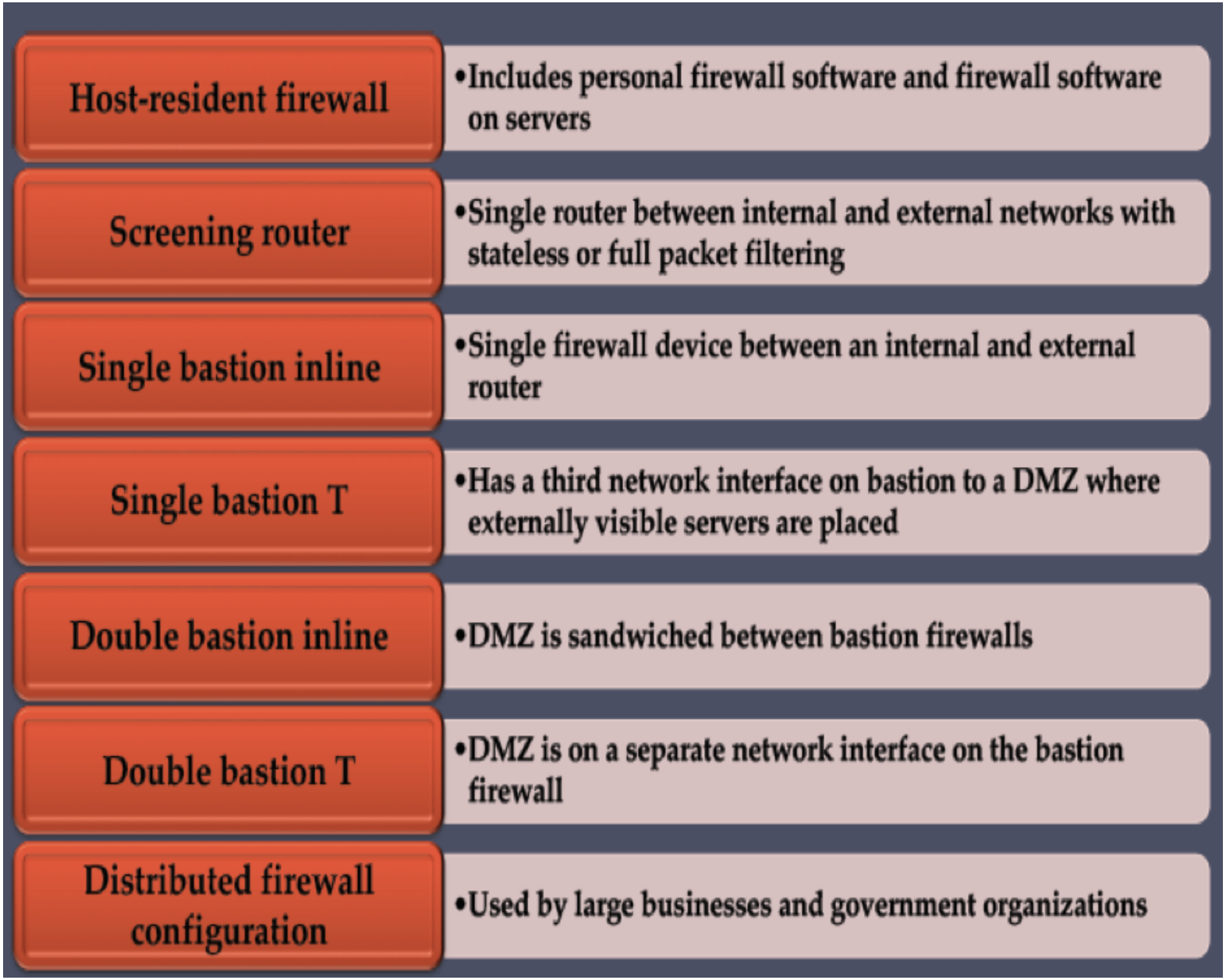
Personal Firewalls

- Controls traffic between a personal computer or workstation and the Internet or enterprise network
- For both home or corporate use
- Typically is a software module on a personal computer
- Can be housed in a router that connects all of the home computers to a DSL, cable modem, or other Internet interface
- Typically much less complex than server-based or standalone firewalls
- Primary role is to deny unauthorized remote access
- May also monitor outgoing traffic to detect and block worms and malware activity

Example Firewall Configuration



Firewall Topologies



Intrusion Detection and Prevention Systems

- Examples of Intrusion
  - Remote root compromise
  - Web server defacement
  - Guessing/cracking passwords
  - Copying databases containing credit card numbers
  - Viewing sensitive data without authorization
  - Running a packet sniffer
  - Distributing pirated software
  - Using an unsecured modem to access internal network
  - Impersonating an executive to get information
  - Using an unattended workstation

Intruders

- Criminals: individuals or members of an organized crime group with a goal of financial reward
  - Identity theft
  - Theft of financial credentials
  - Corporate espionage
  - Data theft
  - Data ransoming
- Masquerader: unauthorized individuals who penetrates a system
- Misfeasor: legit user who accesses unauthorized data
- User trespass: unauthorized logon, privilege abuse
- Software trespass: virus, worm, or Trojan horse

Criminal intruder behavior

- Act quickly and precisely to make their activities harder to detect
- Exploit perimeter via vulnerable ports
- Use Trojan horses (hidden software) to leave back doors for re-entry
- Use sniffers to capture passwords
- Do not stick around until noticed
- Make few or no mistakes

Insider Intrusion Behavior

- Create network accounts for themselves and their friends
- Access accounts and applications they wouldn't normally use for their daily jobs
- E-mail former and prospective employers
- Conduct furtive (covert) instant-messaging chats
- Visit web sites that cater to disgruntled employees
- Perform large downloads and file copying
- Access the network during off hours

Insider Attacks

- Among most difficult to detect and prevent
- Employees have access & systems knowledge
- May be motivated by revenge/entitlement
  - When employment terminated
  - Taking customer data when move to competitor

Intrusion Detection and Prevention Systems

- Security intrusion: a security event, or combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so
- Intrusion detection: a security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an unauthorized manner.
- Intrusion Detection/Intrusion Prevention Systems may help against insider attacks
  - Least privilege, monitor logs, strong authentication, termination process to block access
  - Take mirror image of employee's hard drive (for future purposes)

Intrusion Detection Systems

- Host-based IDS: monitor single host activity
- Network-based IDS: monitor network traffic
- Distributed or hybrid: Combines information from a number of sensors, often both host and network based, in a central analyzer that is able to better identify and respond to intrusion activity
- 3 logical components
  - Sensors: collect data. Input to a sensor includes network packets, log files, and system call traces
  - Analyzers: receive input from one or more sensors or from other analyzers and determine if intrusion has occurred
  - User interface: enables a user to view output or control the behavior of the system

Intrusion Detection Systems

- Assumption: intruder behavior differs from legitimate users
- Expect overlap as shown for legit users
- Observe major deviations from past history
- Problems of: false positives, false negatives, must compromise
- Detection techniques:
  - Anomaly (behavior) detection
  - Signature/heuristic detection

Intrusion Detection Systems

- Anomaly (behavior) detection:
  - Involves the collection of data relating to the behavior of legitimate users over a period of time
  - Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder
- Threshold detection
  - Checks excessive event occurrences over time
  - Alone a crude and ineffective intruder detector
  - Must determine both thresholds and time intervals
  - Lots of false positive/false negative may be possible
- Profile based
  - Characterize past behavior of users/groups
  - Then detect significant deviations
  - Based on analysis of audit records: gather metrics

Anomaly (behavior) detection: Example of Metrics

- Counters: e.g., number of logins during an hour, number of times a cmd executed
- Gauge: e.g., the number of outgoing messages - packets
- Interval time: the length of time between two events, e.g., two successive logins
- Resource utilization: quantity of resources used (e.g., number of pages printed)Mean and standard deviations

Intrusion Detection Systems

Signature/Heuristic Detection

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior
- Also known as misuse detection
- Can only identify known attacks for which it has patterns or rules (signature)
- Very similar to anti-virus (requires frequent updates)
- Rule-based penetration identification
  - Rules identify known penetrations/weaknesses
  - Often by analyzing attack scripts from Internet (CERTs)

Intrusion Detection Systems

Example of Rules in a Signature Detection IDS

- Users should not be logged in more than one session
- Users do not make copies of system, password files
- Users should not read in other users' directories
- Users must not write other users' files
- Users who log after hours often access the same files they used earlier
- Users do not generally open disk devices but rely on high-level OS utils

Audit Records

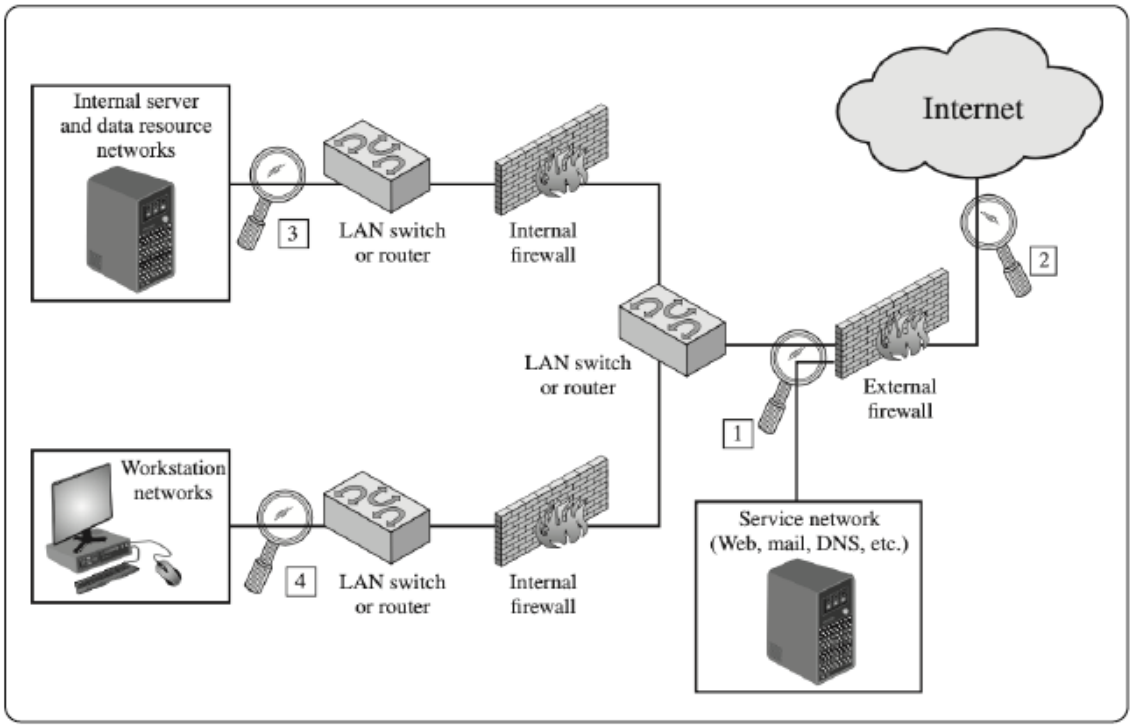
- A fundamental tool for intrusion detection
- Two variants:
  - Native audit records: provided by Operating system
  - Always available but may not be optimum
- Detection-specific audit records: IDS specific
  - Additional overhead but specific to IDS task
  - Often log individual elementary actions

  -May contain fields for: subject, action, object, exception-condition, resource-usage, time-stamp
  - Possible overhead (two such utilities)

Network-based IDS (NIDS)

- Monitor traffic at selected points on a network (e.g., rlogins to disabled accounts) In (near) real time to detect intrusion patterns
- May examine network, transport and/or application level protocol activity directed toward systems
- Comprises a number of sensors
  - Inline (possibly as part of other net device) – traffic passes through it
  - Passive (monitors copy of traffic)

NIDS Sensor Deployment



Logging of Alerts

Typical information logged by a NIDS sensor

- Timestamp- usually date and time
- Connection or session ID Event or alert type
- Rating
- Network, transport, and application layer protocols
- Source and destination IP addresses
- Source and destination TCP or UDP ports, or ICMP types and codes
- Number of bytes transmitted over the connection
- Decoded payload data, such as application requests and responses
- State-related information

Summary

- Introduced need for & purpose of firewalls
- Types of firewalls - packet filter, stateful inspection, application and circuit gateways
- Firewall hosting, locations, topologies
- Introduced intruders & intrusion detection
  - Hackers, criminals, insiders
- Intrusion detection approaches - Host-based (single and distributed); Network