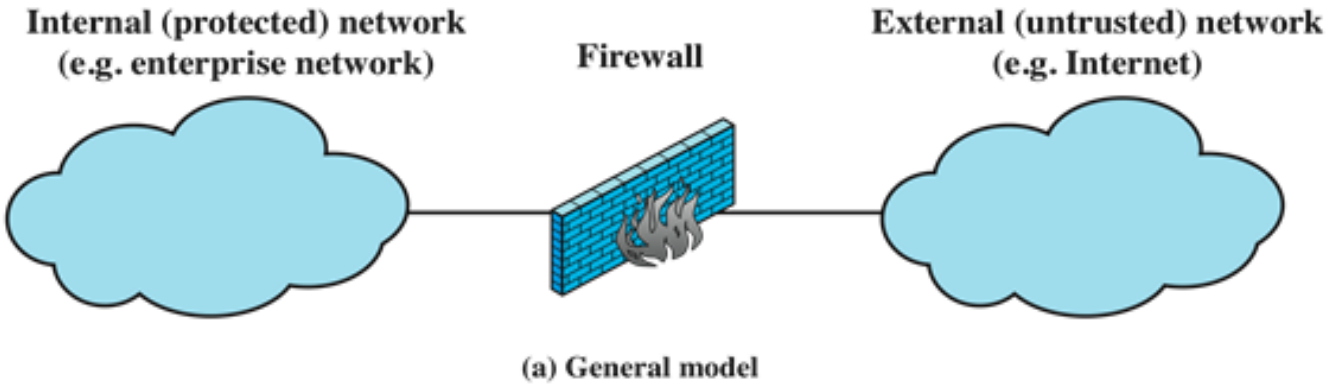
Types of Firewalls

- Packet filtering firewalls
- Stateful inspection firewalls
- Application-level firewalls
- Circuit-level firewalls



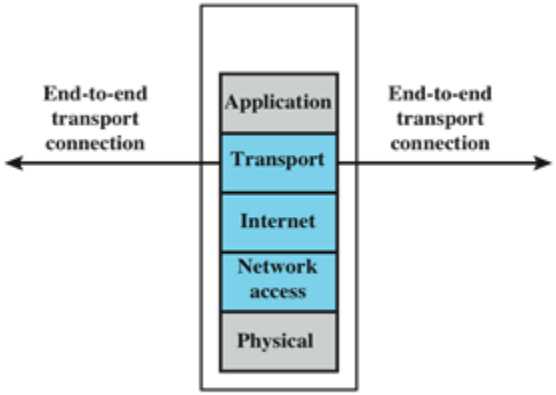
(a) General model

Packet Filtering Firewall

- applies rules to each incoming and outgoing IP packet
  - typically a list of rules based on matches in the TCP/IP header
  - forwards or discards the packet based on rules match

Filtering rules are based on information contained in a network packet

- Source IP address
- Destination IP address
- Source and destination transport-level address
- IP protocol field
- Interface



(b) Packet filtering firewall

- two default policies:
  - **discard** - prohibit unless expressly permitted
    - more conservative, controlled, visible to users
  - **forward** - permit unless expressly prohibited
    - easier to manage and use but less secure

Packet Filtering Rule 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

- Inbound mail is allowed (port 25 is for SMTP incoming)
- Allow a response to an inbound SMTP connection
- Outbound mail to an external source is allowed
- Allow a response to an inbound SMTP connection
- Discard default policy

Packet Filtering Rule 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

- Security threats: Rule 4 allows external traffic to any destination port above 1023—an external attacker can open a connection from **its port (e.g., 5150)** to an internal Web proxy server on port 8080 (not for mail).
- Countermeasure—add source port field for each row

Packet Filter Firewalls: Advantages And Weaknesses

- advantages
  - simplicity
  - typically transparent to users and are very fast
- weaknesses
  - cannot prevent attacks that employ application specific vulnerabilities or functions
  - do not support advanced user authentication
  - improper configuration can lead to breaches

Attacks to Packet Filtering Firewalls

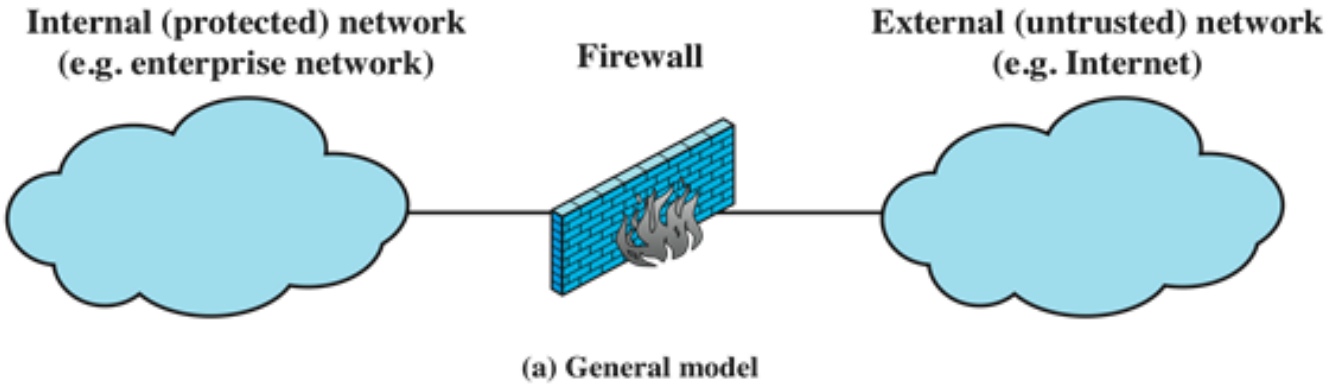
- IP address spoofing
  - The intruder transmits packets from the outside with a source IP address field containing an address of an internal host
  - Countermeasure– discard packets with an inside source address if the packet arrives on an external interface

Attacks to Packet Filtering Firewalls

- Tiny fragment attack
  - The intruder uses the IP fragment option to create small fragments; in some datalink protocol (Ethernet), the packet information is only contained in the first fragment packet; once the first fragment passes the test of firewall, the rest can pass as well
  - Countermeasure– enforce all the fragment packets contain necessary information

Types of Firewalls

- Packet filtering firewalls
- Stateful inspection firewalls
- Application-level firewalls (gateway)
- Circuit-level firewalls



(a) General model

Stateful Inspection Firewall

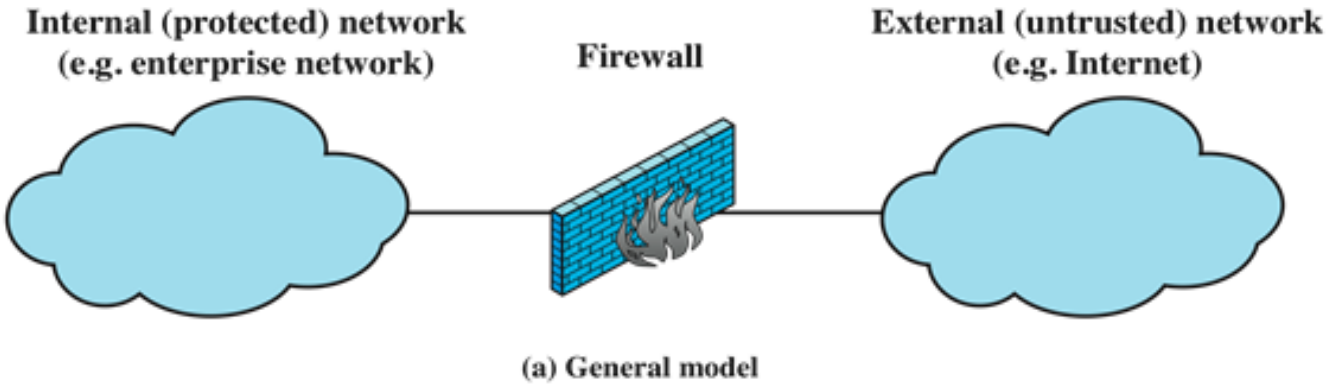
- tightens rules for TCP traffic by creating a directory of current TCP connections and their information (stateful)
  - there is an entry for each currently established connection
  - packet filter allows incoming packets that fit the profile of one of the entries
  - Consider the SMTP example ; the TCP client port value is valid if it belongs to 1024-65,535—wide accepting range for firewall filter; the attacker can exploit this property→stateful inspection
  - How about the first packet?

Stateful Firewall Connection State

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

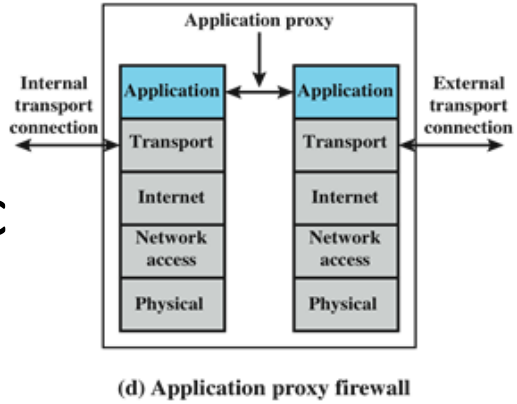
Types of Firewalls

- Packet filtering firewalls
- Stateful inspection firewalls
- Application-level firewalls (gateway)
- Circuit-level firewalls



(a) General model

Application-Level Gateway



(d) Application proxy firewall

- also called an **application proxy**
- acts as a relay of application-level traffic
  - user contacts gateway using a TCP/IP appl.
  - user is authenticated
  - gateway contacts application on remote host and relays TCP segments between server and user
- tend to be more secure than packet filters
  - The application-level gateway only needs to check a few allowable applications

Application-Level Gateway

- Disadvantage
  - Two split connections, one from external user to the gateway, the other from the gateway to the internal user
  - additional processing overhead on each connection

Lecture 23: Key Management and Distribution

Key Distribution Technique

- Term that refers to the means of delivering a key to two parties who wish to exchange data without allowing others to see the key
- For symmetric encryption to work, the two parties must share the same key, and that key must be protected from access by others
- Frequent key changes are desirable to limit the amount of data compromised if an attacker learns the key

Symmetric Key Distribution

Given parties A and B, key distribution can be achieved in a number of ways:

- **A can select a key and physically deliver it to B**
- **A third party can select the key and physically deliver it to A and B**
- **If A and B have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key**
- **If A and B each has an encrypted connection to a third party C, C can deliver a key on the encrypted links to A and B**

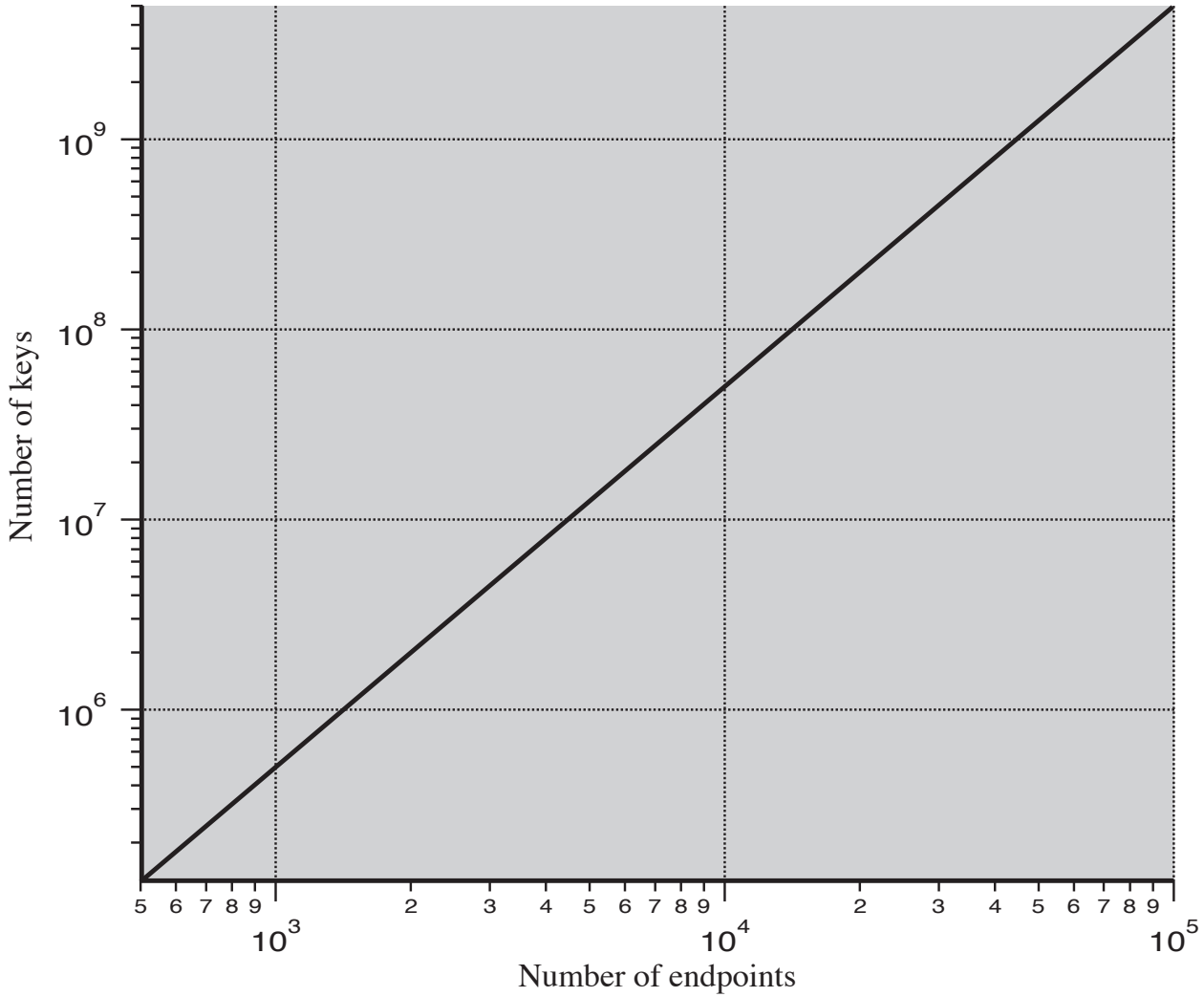


Figure 14.1 Number of Keys Required to Support Arbitrary Connections Between Endpoints

Symmetric Key Distribution

- Use symmetric encryption for symmetric key distribution
- Use asymmetric encryption for symmetric key distribution

Master Key and Session Key

- Master key: distributed by key distribution center (KDC) to each user, used for establish session key

- Session key: encrypt messages between A and B. The key used for message transmission

Symmetric Key Distribution Framework

- KDC first assigns a master key to each user
- when A and B wants to establish a session key
- KDC chooses this session key, encrypts the session key with A's (B's) master key, and sends the encrypted session key to A (B)
- Now A and B establish a session key for data delivery

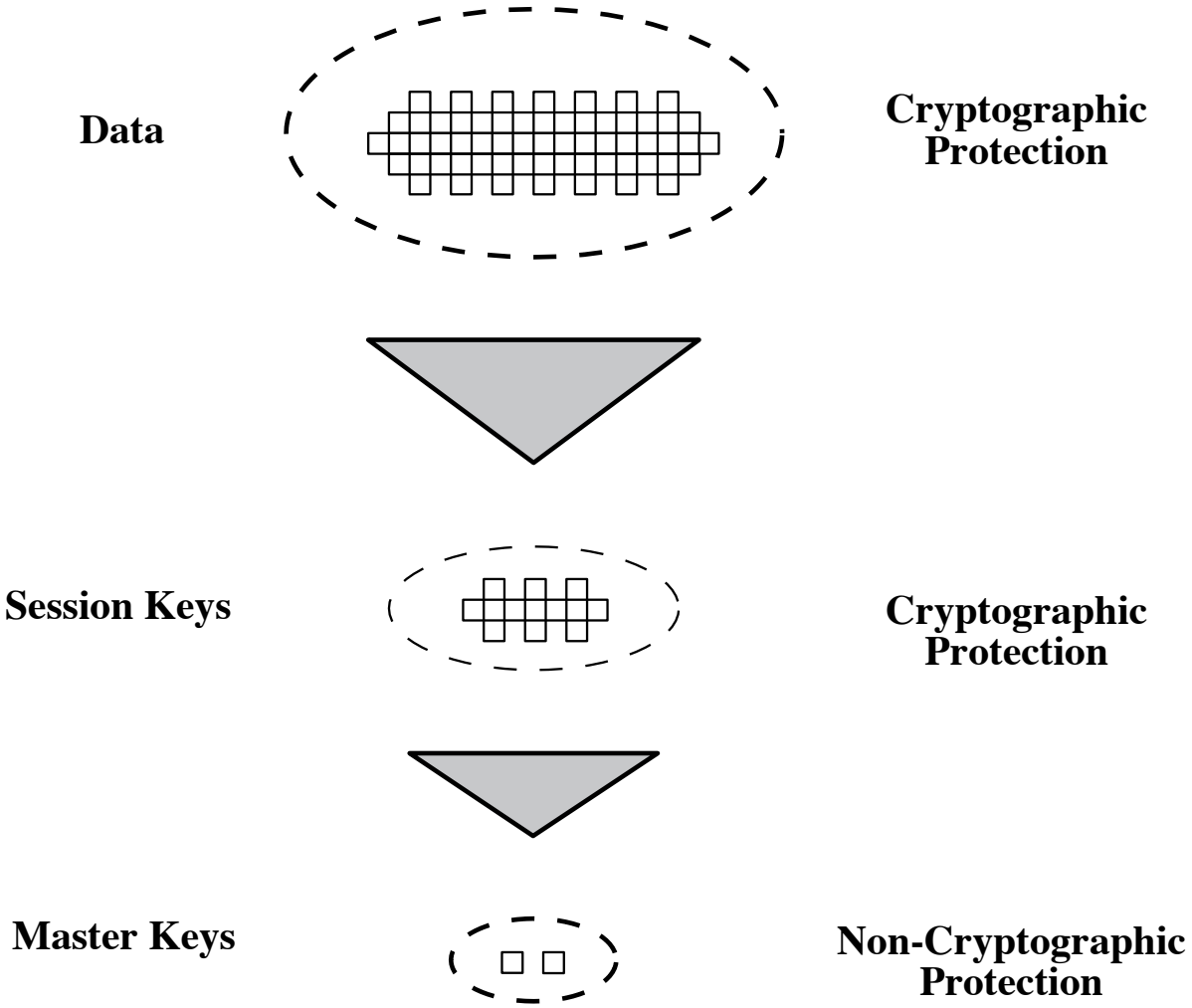


Figure 14.2 The Use of a Key Hierarchy

Hierarchical Key Control

- For communication among entities within the same local domain, the local KDC is responsible for key distribution
  - If two entities in different domains desire a shared key, then the corresponding local KDC's can communicate through a global KDC
- The hierarchical concept can be extended to three or more layers

Session Key Lifetime

For connection-oriented protocols one choice is to use the same session key for the length of time that the connection is open, using a new session key for each new session

A security manager must balance competing considerations:

- The more frequently session keys are exchanged, the more secure they are
- The distribution of session keys delays the start of any exchange and places a burden on network capacity

For a connectionless protocol there is no explicit connection initiation or termination, thus it is not obvious how often one needs to change the session key-update periodically

Asymmetric Encryption for Symmetric Key Distribution

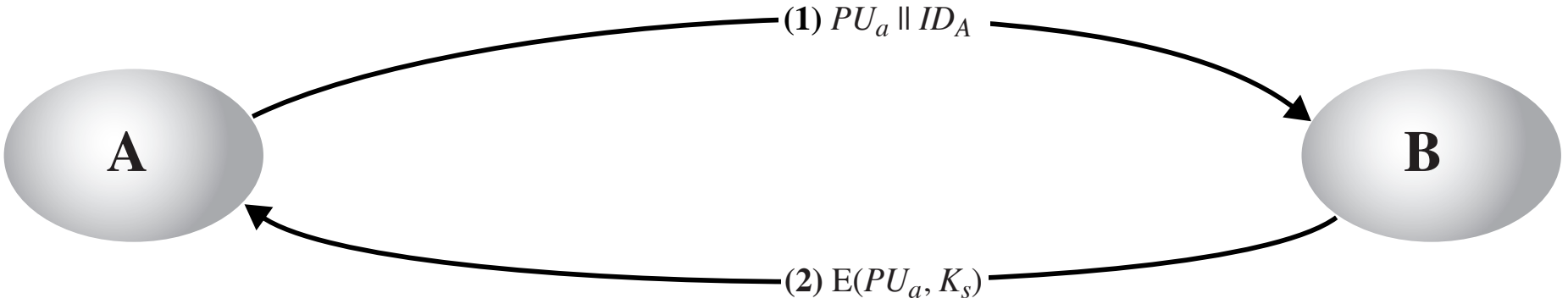


Figure 14.7 Simple Use of Public-Key Encryption to Establish a Session Key

Man-in-the-Middle Attack

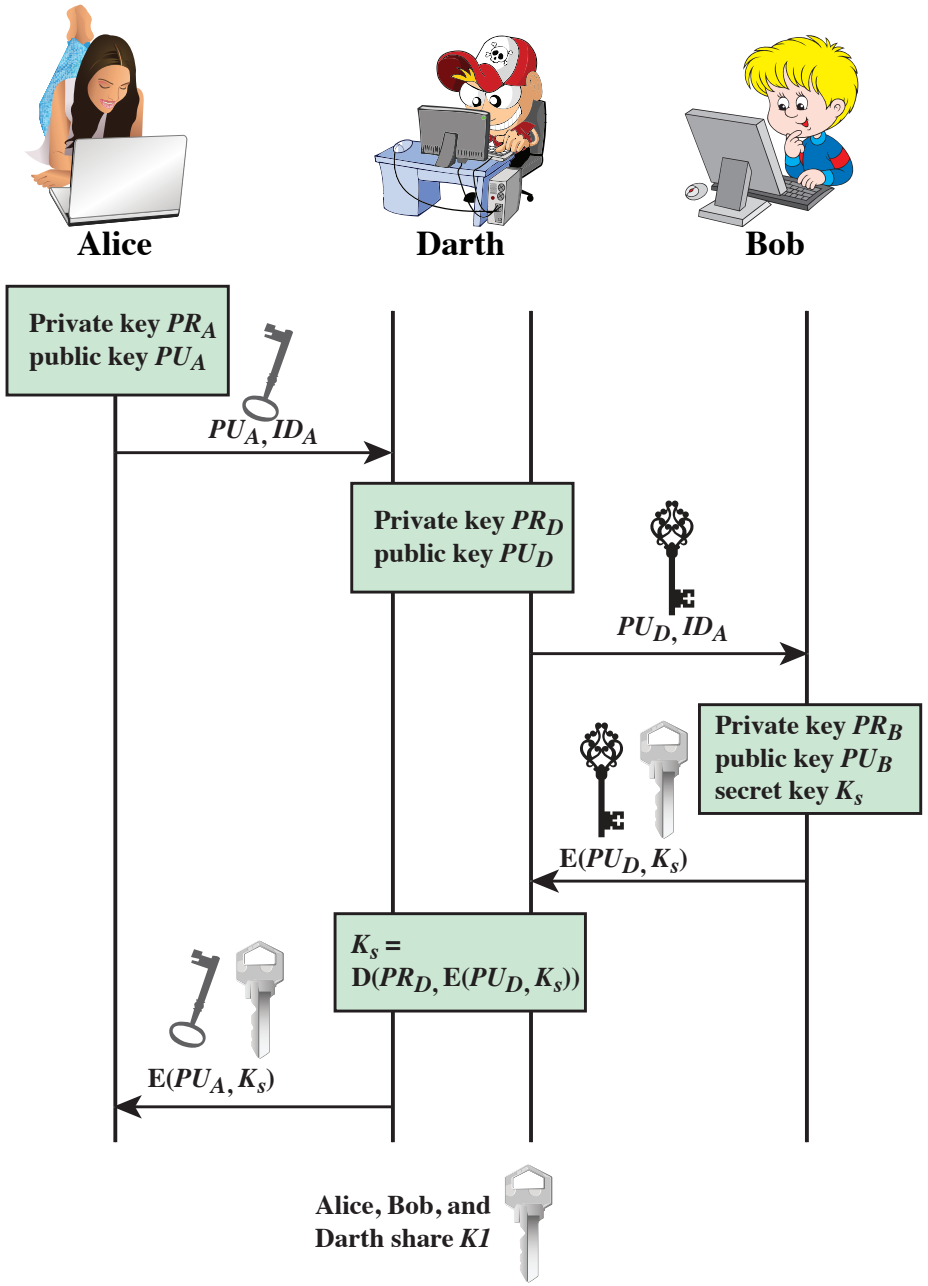


Figure 14.8 Another Man-in-the-Middle Attack

Secret Key Distribution with Confidentiality and Authentication

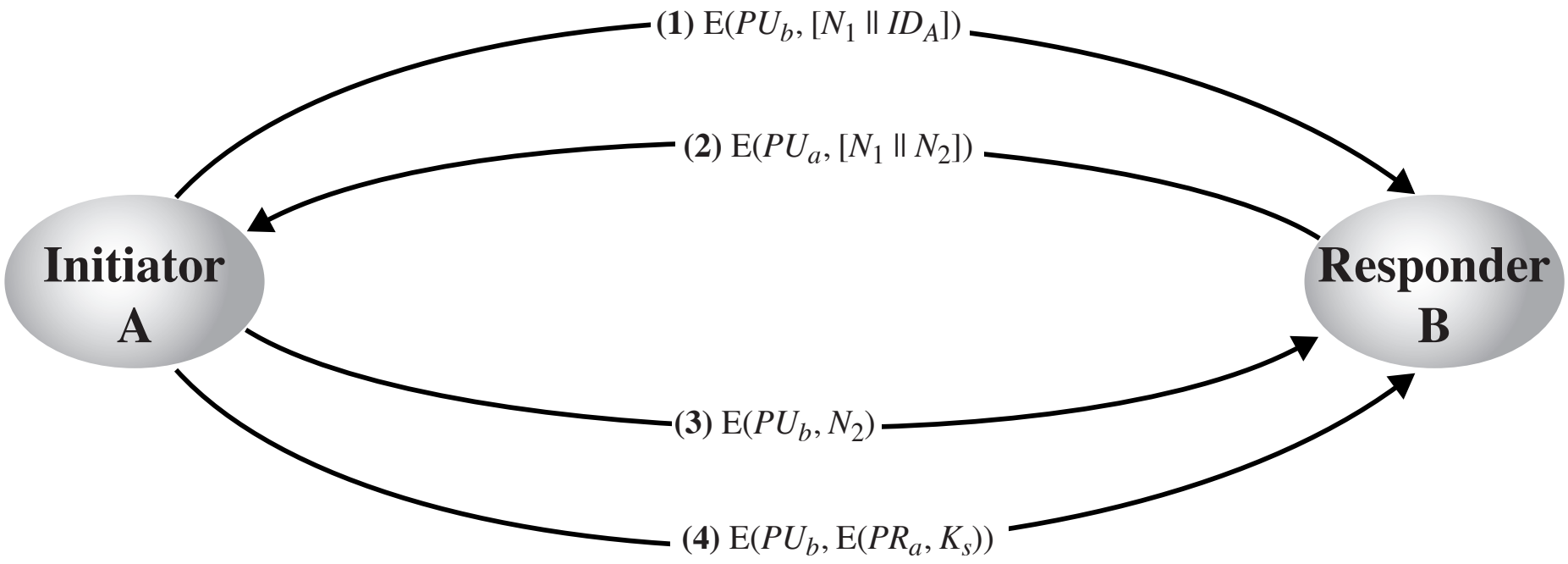
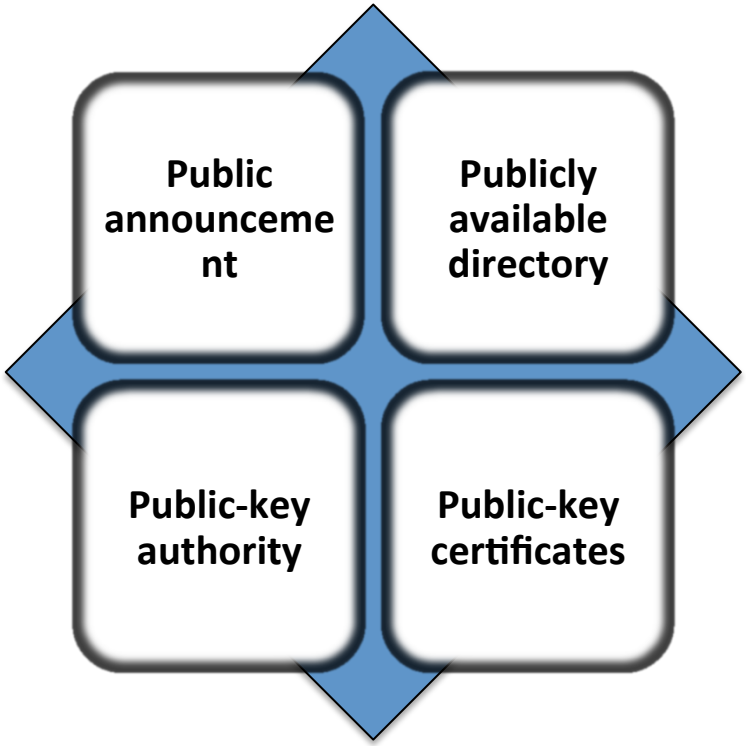


Figure 14.9 Public-Key Distribution of Secret Keys

Distribution of Public Keys

- Several techniques have been proposed for the distribution of public keys. Virtually all these proposals can be grouped into the following general schemes
- Core issue: how to make sure A's public key is from A



Public Announcement

Figure 14.10 Uncontrolled Public Key Distribution

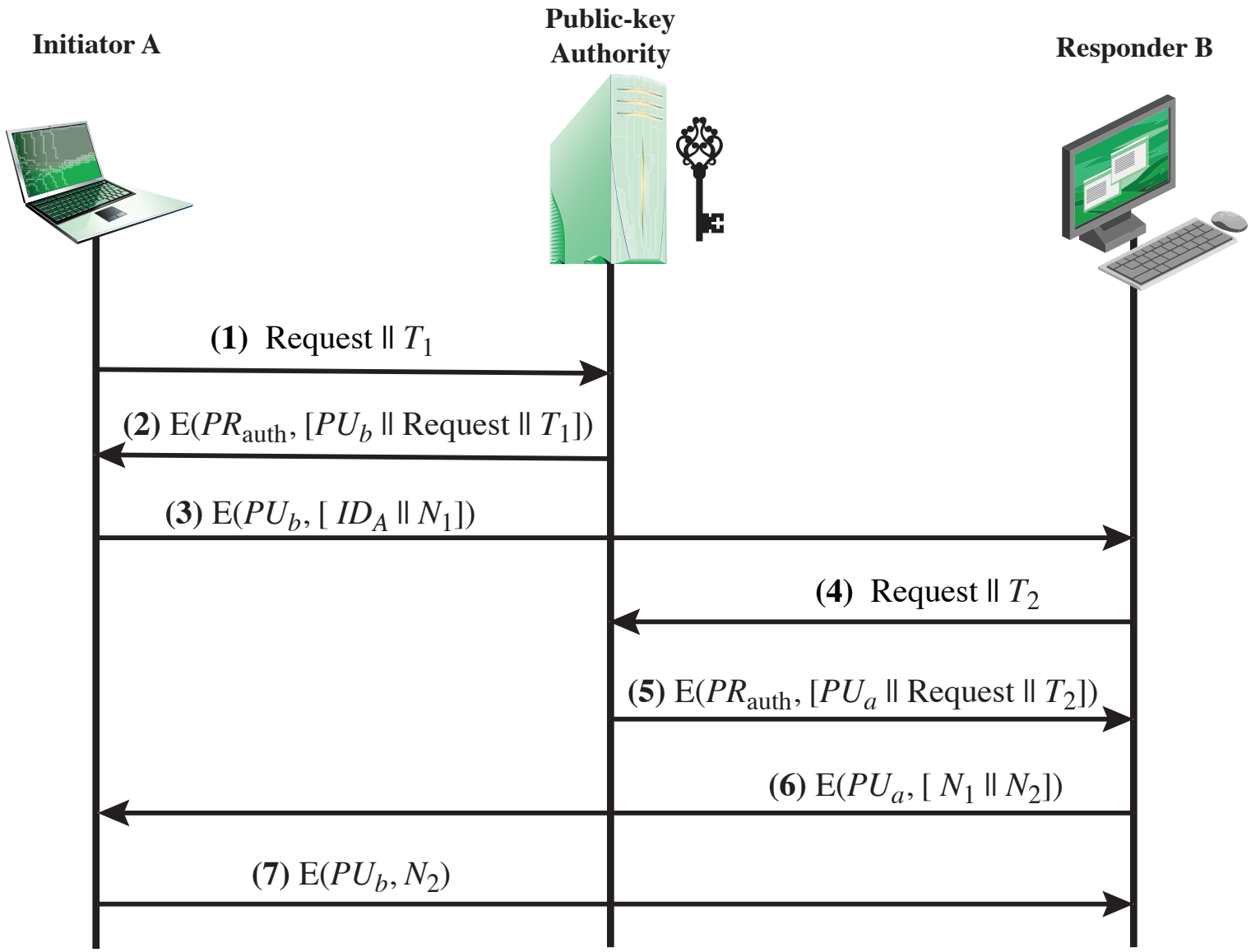
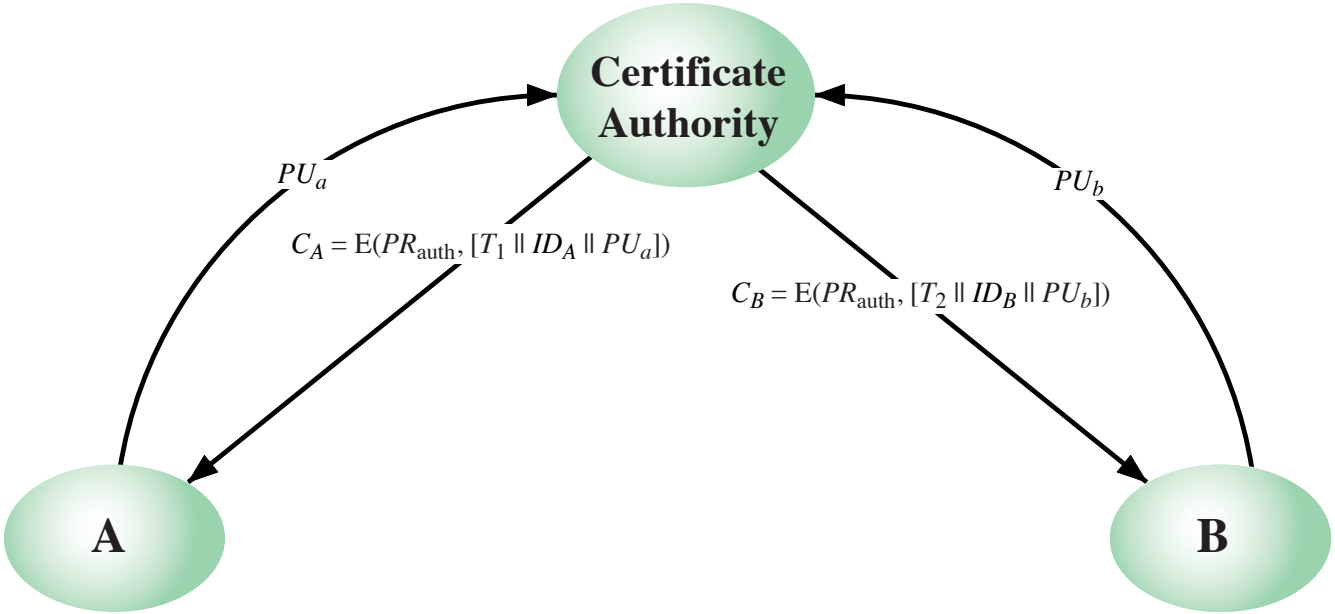
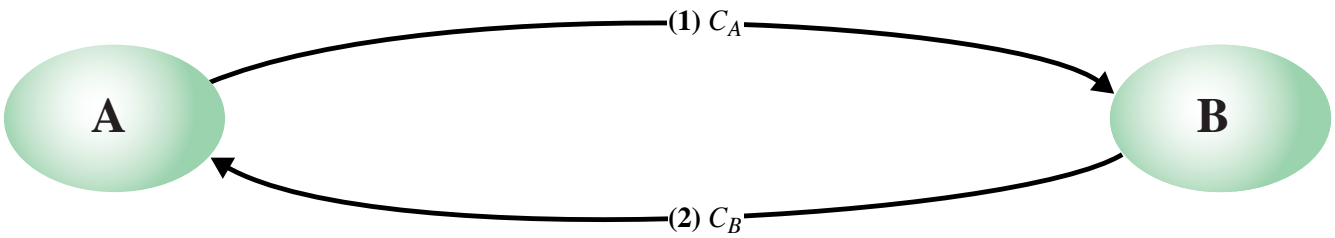


Figure 14.12 Public-Key Distribution Scenario



(a) Obtaining certificates from CA

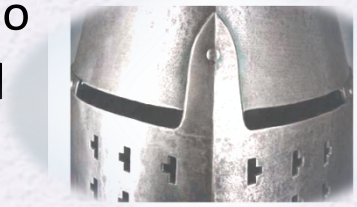


(b) Exchanging certificates

Figure 14.13 Exchange of Public-Key Certificates

Summary

- Symmetric key distribution using symmetric encryption
  - Key distribution scenario
  - Hierarchical key control
  - Session key lifetime
- Symmetric key distribution using asymmetric encryption
  - Simple secret key distribution
  - Secret key distribution with confidentiality and authentication



- Distribution of public keys
  - Public announcement of public keys
  - Public-key authority
  - Public-key certificates