Chapter 15: Security

Outline

- Secure Communication
- Cryptography overview
- Cryptography as a Security Tool
- User Authentication

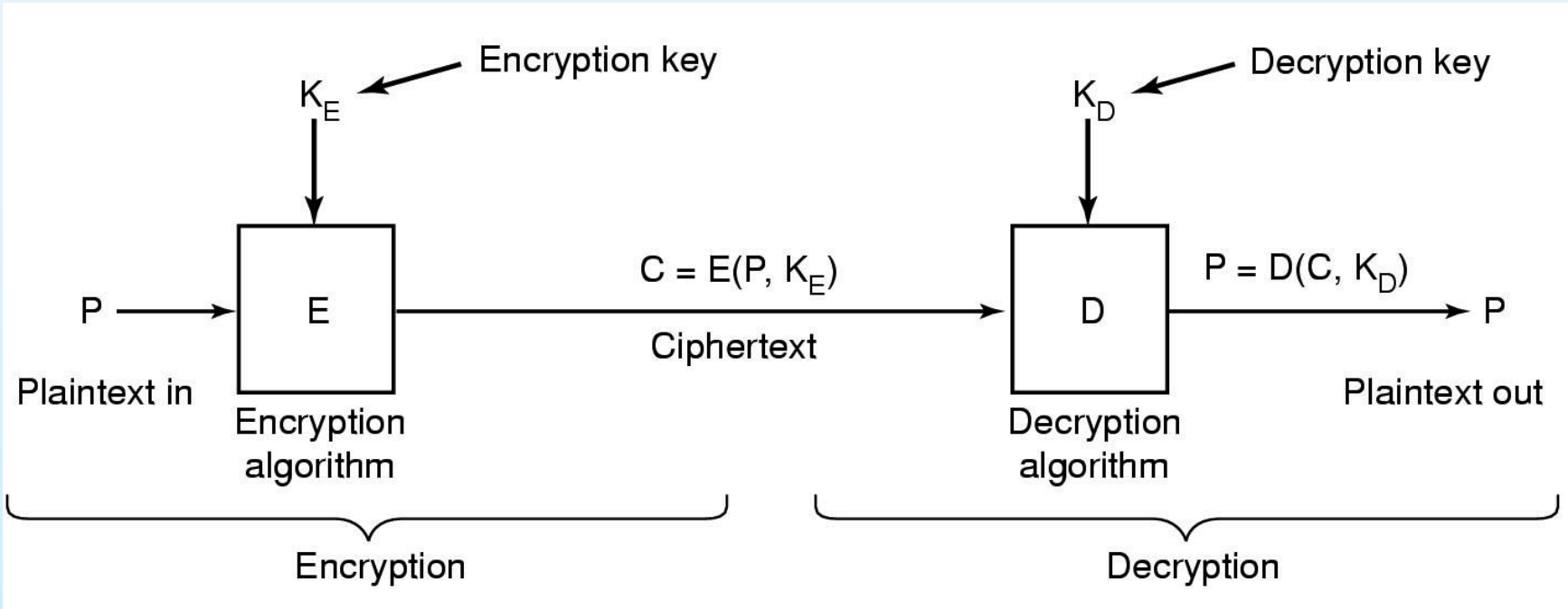
- Program Threats
- System and Network Threats
- Implementing Security Defenses
- Firewalling to Protect Systems and Networks

Secure Communication

- Confidentiality (secrecy)
  - only an authorized recipient should be able to read the contents of the message
- Integrity
  - the recipient should be able to determine if the message has been altered during transmission.
- Authentication
  - the recipient should be able to identify the sender, and verify that the purported sender actually did send the message

Cryptography Overview

- Encrypt data so it only makes sense to authorized users
  - Input data is a message or file called plaintext
  - Encrypted data is called ciphertext
- Encryption and decryption functions should be public



Type of Cryptographic Functions

- Symmetric key cryptography (secret-key cryptography)
  - DES, IDEA, AES, RC4
- Asymmetric key cryptography (public-key cryptography)
  - RSA, Diffie-Hellman
- Hash algorithms
  - MD4, MD5, SHA-1, SHA-2

Symmetric Cryptography

- Symmetric cryptography based on each user having shared secret key
- Same key used to encrypt and decrypt
  - *E(K)(message)=ciphertext* *D(K)(ciphertext)=message*
- Block cipher
  - Takes fixed-length block of message (64bit, 128bit..)
  - Takes fixed-length key (54bit, 128bit)
  - Generates a block of output (same length as the input)
  - When encrypting messages larger than the block size
    - Mode of operation i.e. ECB, CBC
  - Examples: DES, AES
- Stream cipher
  - Takes the key and generate a one-time pad
  - Applies it to the stream of plaintext with XOR
  - Example: RC4

Basic Structure of DES

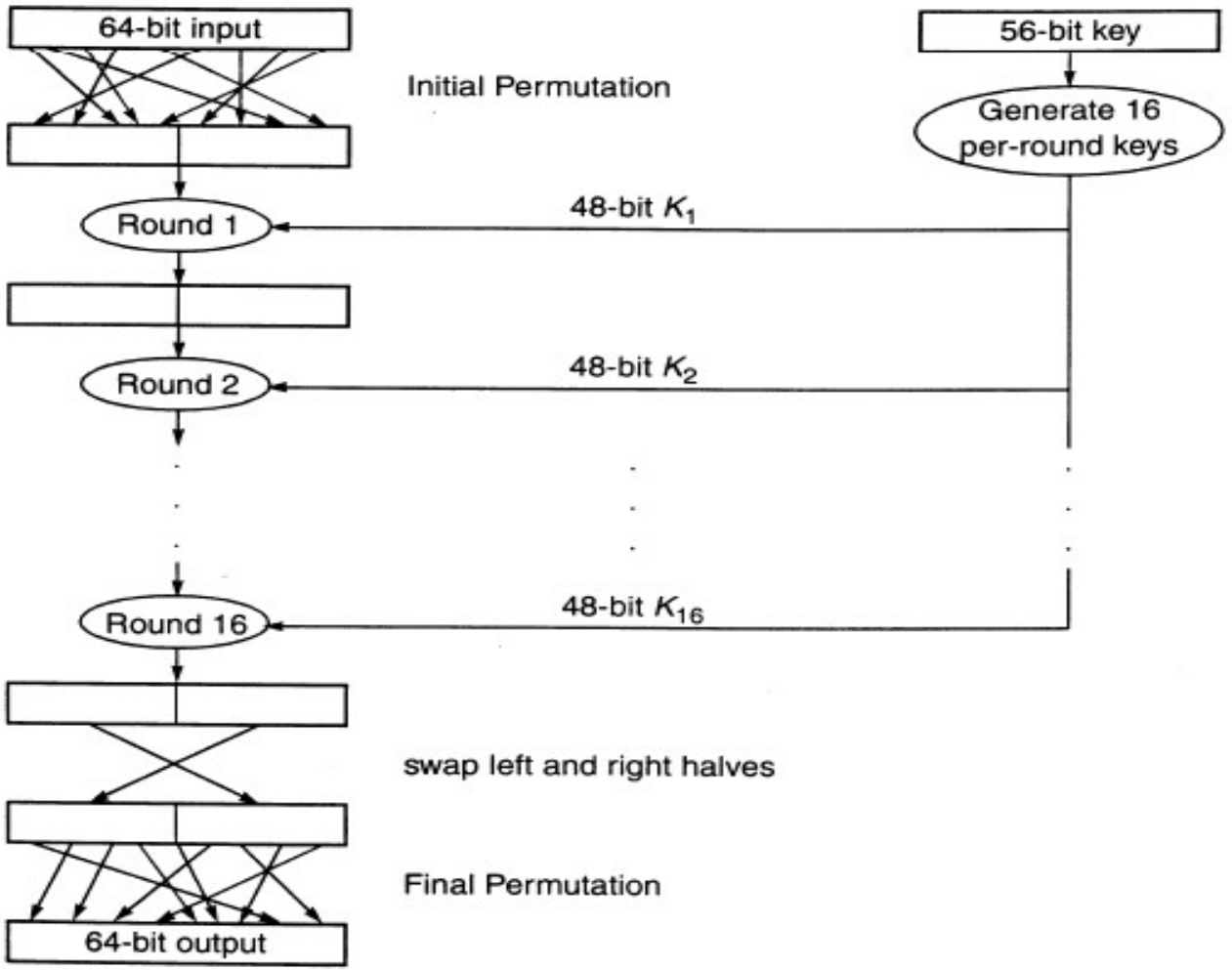


Figure 3-2. Basic Structure of DES

Symmetric cryptography (cont.)

- DES was proposed in the 1970s
  - Encrypts 64 bits of data with 56 bit key to give 64-bit ciphertext
    - Uses 16 rounds of substitution and permutation
    - EFF invested $250000 to break DES message in 56 hours
- Current standard is AES
  - A result of 3-year competition with entries from 12 countries
  - Block size 128 bit, key size 128, 192, 256
- Symmetric cryptography is based on transformations, much less computationally intensive than asymmetric algorithms

Asymmetric Cryptography

- Asymmetric cryptography based on each user having two keys:
  - public key – published key used to encrypt data
  - private key – key known only to individual user used to decrypt data
- If Alice has a packet to send to Bob
  - She encrypts the packet with Bob's public key
  - Bob uses his private key to decrypt Alice's packet
- Private key linked mathematically to public key, but it is computationally infeasible to drive private key from the public key
  - RSA: factoring large integers
  - Diffie-Hellman: finding discrete logarithms
- Asymmetric cryptography based on mathematical functions, much slower than symmetric cryptography
  - Typically not used for bulk data encryption

RSA

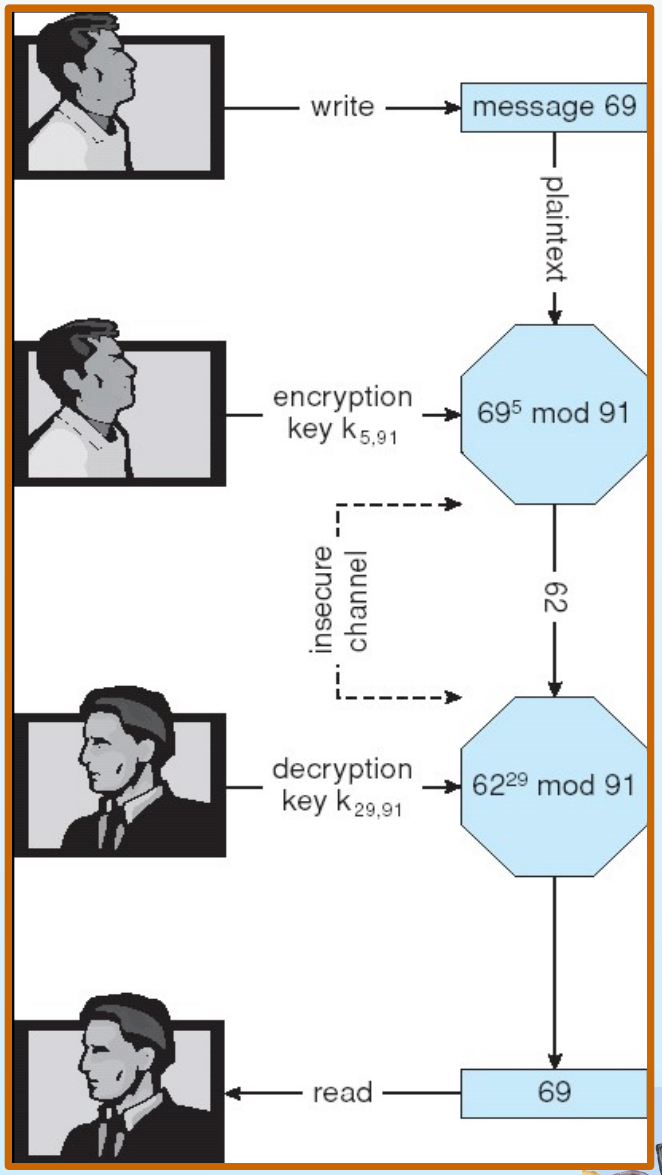
- Generate Keys
  - Randomly chose 2 large prime numbers p, q (for example, *p* and *q* are 512 bits each) let $N = pq$
  - Select k_e that is relative prime to $(p-1)(q-1)$
  - Select k_d that satisfies $k_e k_d \bmod (p-1)(q-1) = 1$
  - $[k_e , N]$ is the **public key**
  - $[k_d , N]$ is the **private key**
- Encrypt message *m*
  - $E(k_e , N)(m) = m^{k_e} \bmod N$,
- Decrypt ciphertext c
  - $D(k_d , N)(c) = c^{k_d} \bmod N$

RSA Example

- For example. make p = 7and q = 13
- We then calculate N = 7x13 = 91 and $(p-1)(q-1)$ = 72
- We next select k_e relatively prime to 72 and< 72, yielding 5
- Finally,we calculate k_d such that $k_e k_d$ mod 72 = 1, yielding 29
- We how have our keys
  - Public key, $[k_e, N] = [5, 91]$
  - Private key, $[k_d, N] = [29, 91]$

RSA Example (cont.)

- Encrypting the message 69 with the public key results in the ciphertext 62
- Ciphertext 62 can be decoded with the private key to obtain original message 69



Hash Algorithms

- A hash is a *one-way* function
  - Takes a message of any length
  - Produces a fixed length output
  - it should be easy to compute, it must be very difficult to invert
- Hash Function *H* must be collision resistant on *m*
  - Must be infeasible to find an $m' \neq m$ such that $H(m) = H(m')$
- Keyed-hash function
  - Assume users share a secret key, *K*
  - Generate hash $H(K|m)$
- Common hash functions include
  - **MD5**, which produces a 128-bit hash
  - **SHA-1**, which outputs a 160-bit hash

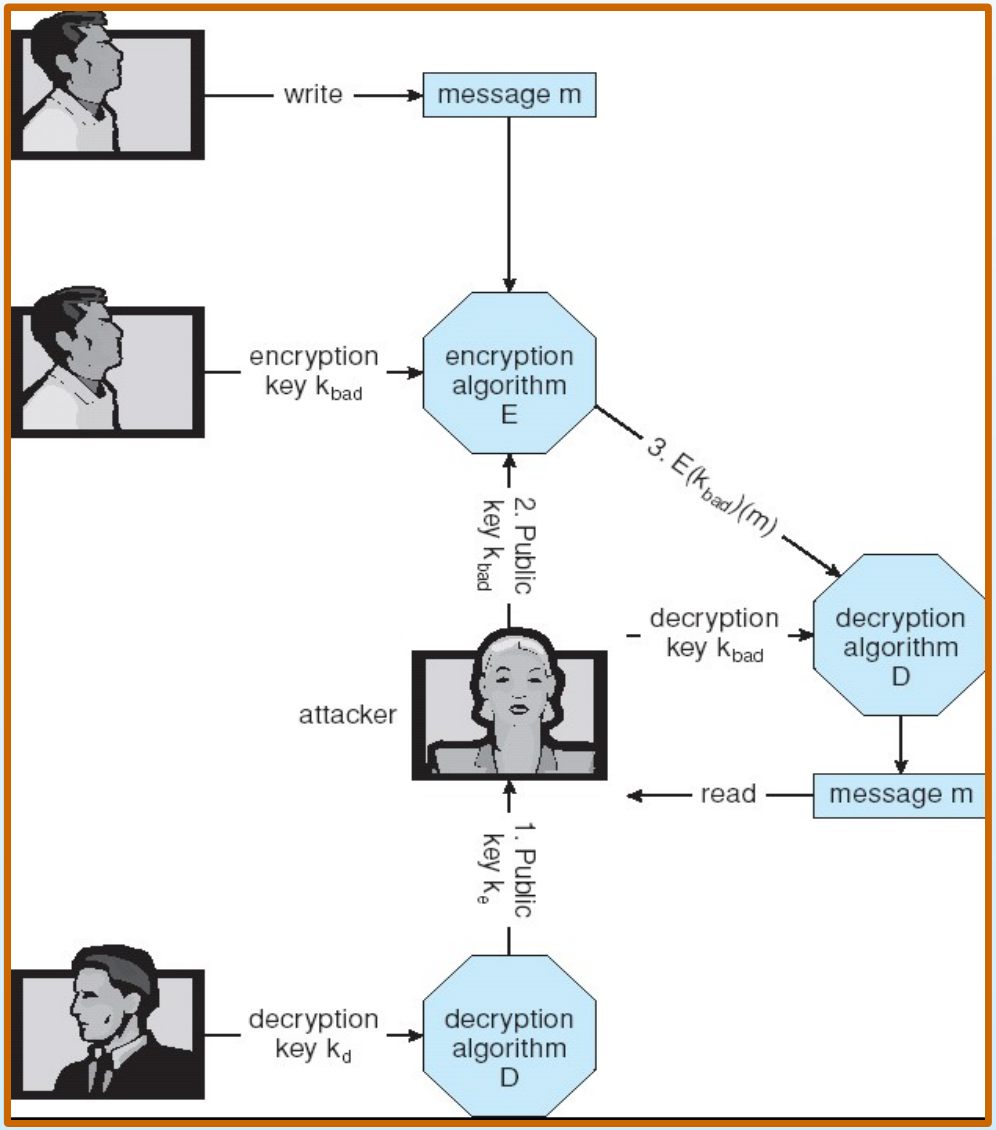
Cryptography as a Security Tool

- Confidentiality
  - Symmetric, asymmetric, even hash
  - Symmetric encryption is used to for bulk data
- Integrity
  - Most often use hash function
- Authentication
  - Symmetric/hash:
    - MAC: A cryptographic checksum generated from the message using a secret key
  - Asymmetric: digital signatures
    - To sign (RSA): $s = E(k_d, N)(m) = m^{k_d} \bmod N$
    - To verify (RSA): $v = \mathrm{D}(k_e, N)(s) = s^{k_e} \bmod N$
    - More usually, message is hashed before signing

Key Distribution

- Delivery of symmetric key is huge challenge
  - Sometimes done **out-of-band**
- Asymmetric keys can proliferate – stored on **key ring**
  - Even asymmetric key distribution needs care – man-in-the-middle attack

Man-in-the-middle Attack on Asymmetric Cryptography



Digital Certificates

- Proof of who or what owns a public key
- Public key digitally signed a trusted party
- Trusted party receives proof of identification from entity and certifies that public key belongs to entity
- Certificate authority are trusted party – their public keys included with web browser distributions
  - They vouch for other authorities via digitally signing their keys, and so on

Encryption Example - SSL

- Insertion of cryptography at one layer of the ISO network model (the transport layer)
- SSL – Secure Socket Layer (also called TLS)
- Cryptographic protocol that limits two computers to only exchange messages with each other
  - Very complicated, with many variations
- Used between web servers and browsers for secure communication (credit card numbers)
- The server is verified with a **certificate** assuring client is talking to correct server
- Asymmetric cryptography used to establish a secure **session key** (symmetric encryption) for bulk of communication during session
- Communication between each computer uses symmetric key cryptography

SSL (cont.)

- Client sends a *ClientHello* message specifying the list of cipher suites, compression methods and the highest protocol version it supports. It also sends random bytes which will be used later.
- Then it receives a *ServerHello*, in which the server chooses the connection parameters from the choices offered by the client earlier.
- When the connection parameters are known, client and server exchange certificates (depending on the selected public key cipher).
- Client and server negotiate a common secret called "master secret". All other key data is derived from this secret

SSL (cont.)

- Certificate
  - Various attributes of the server: name, DNS
  - Public key of this server
  - Validity interval during which the certificate should be considered valid
  - A digital signature a on the above information by the CA
- Master secret
  - Client sends 28byte random n_c
  - Server replies random n_s and the certificate
  - Client verify the certificate, generate 46byte random **pms** and send to server E(k_e)(**pms**)
  - Server recover **pms**
  - Both side construct a master secret using n_c, n_s and **pms**

Computer Security

- What are we trying to protected
  - secrecy and confidentiality: improper disclosure of information
  - integrity: improper alteration of data
  - availability: a service should be there when it is sought
- Gold Standard of Security
  - Authorization
  - Authentication
  - Audit
- The Security Problem
  - Vulnerability: A weakness that can be exploited to cause damage.
  - Attack: A method of exploiting a vulnerability. Attempt to breach security

Security Measure Levels

- Security must occur at four levels to be effective:
  - Physical
  - Human
    - Avoid social engineering, phishing, dumpster diving
  - Operating System
  - Network
- Security is as week as the weakest chain

Threats and Attacks

- Trojan horse
- Trap door
- Worms
- Virus
- Buffer overflow
- Bombs
- Spoofing
- Denial of Service

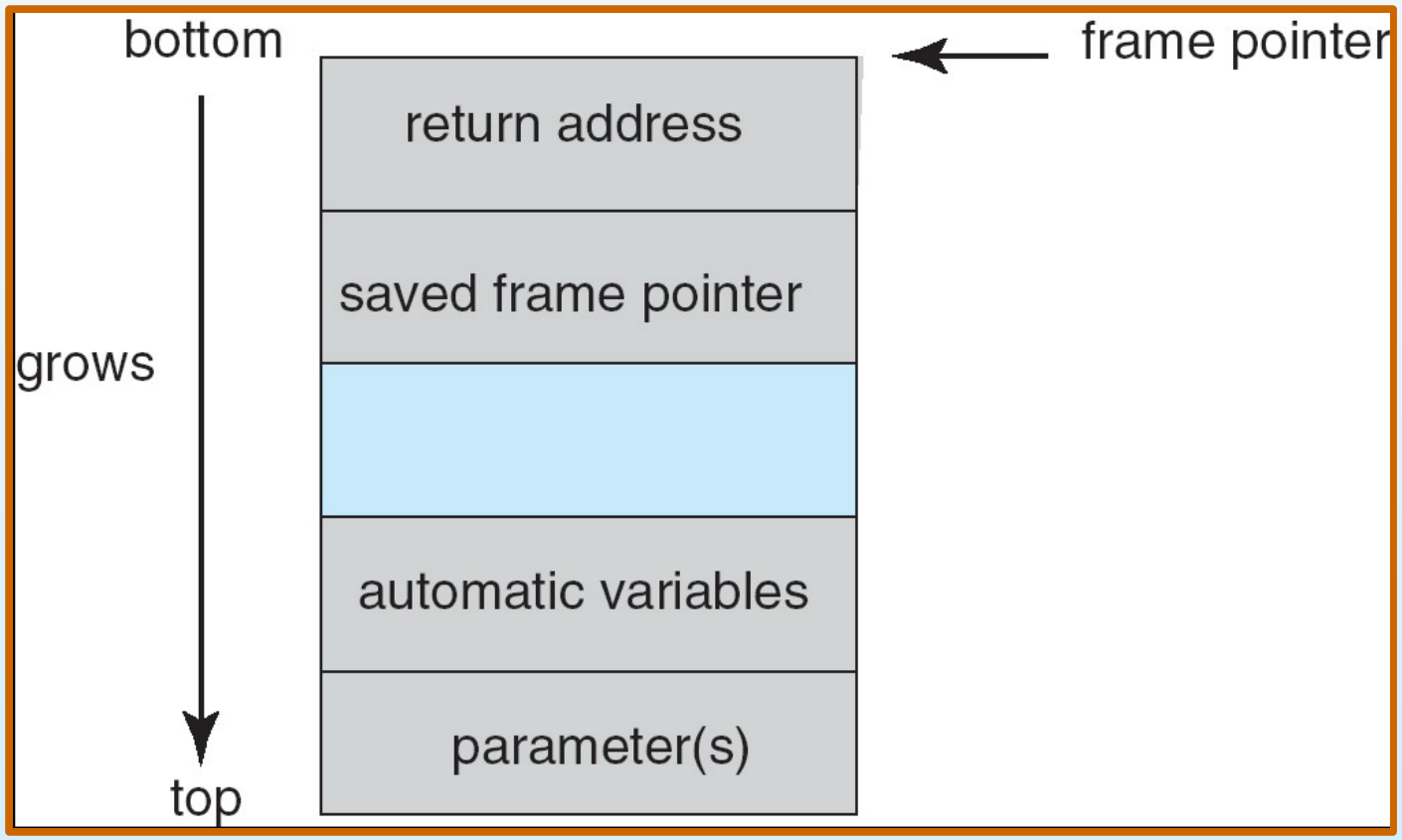
Buffer-overflow

- Buffer overflow vulnerabilities are one of the most common vulnerabilities
- "Smashing the Stack for Fun and Profit", in Phrack magazine
- Stack based or heap based
- Prevention
  - Choice of programming language
  - Stack-smashing protection
  - Executable space protection

Buffer-overflow Example

```
#include <stdio.h>
#define BUFFERSIZE 256
int main(int argc, char *argv[])
{
   char buffer[BUFFERSIZE];
   if (argc < 2)
    return -1;
   else {
    strcpy(buffer,argv[1]);
    return 0;
   }
}
```

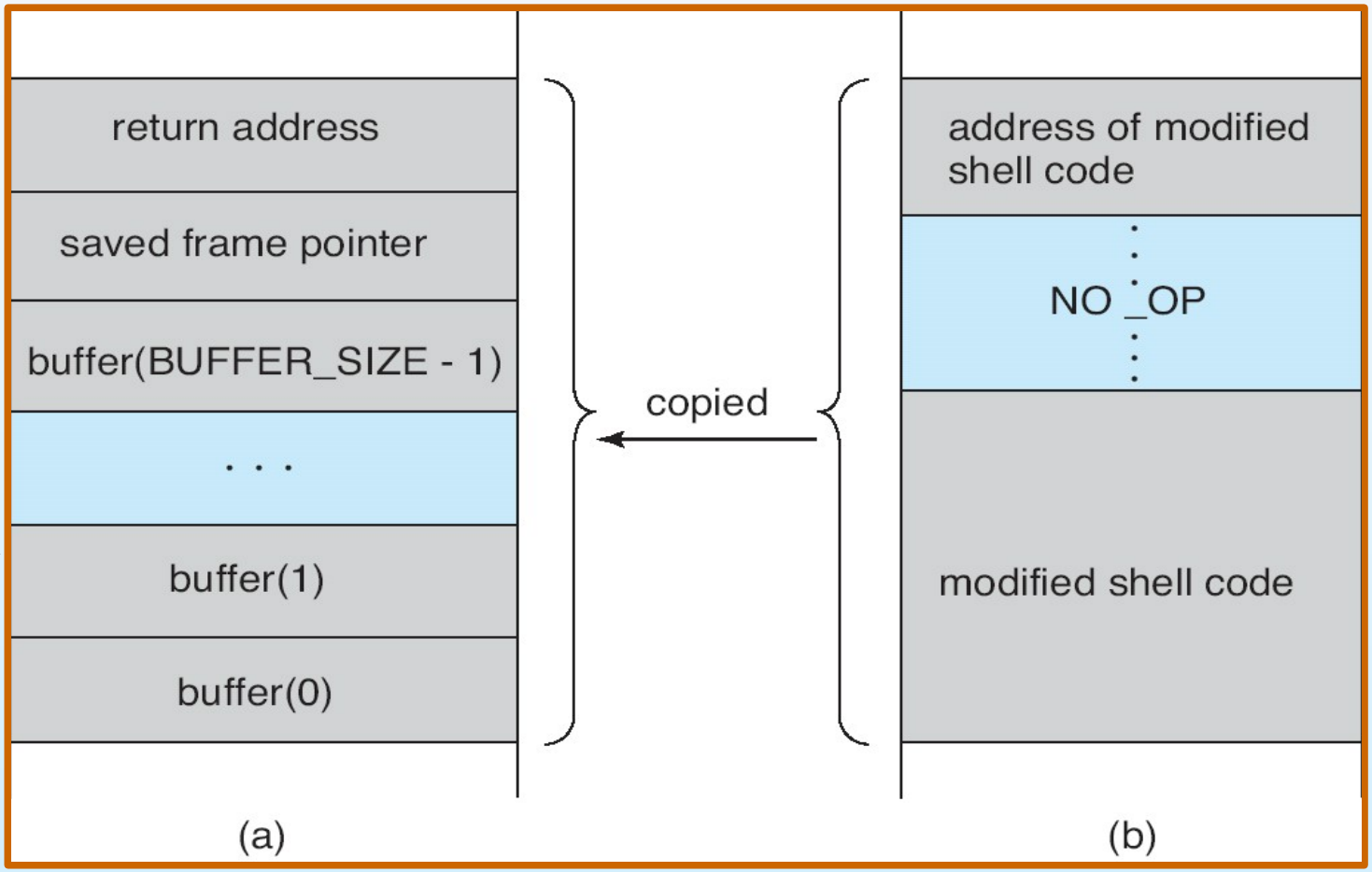
Buffer-overflow
Layout of Typical Stack Frame



Buffer-overflow
Modified Shell Code

```
#include <stdio.h>
int main(int argc, char *argv[])
{
  execvp(‘‘\bin\sh’’,‘‘\bin \sh’’,
  NULL);
  return 0;
}
```

Buffer-overflow
Hypothetical Stack Frame



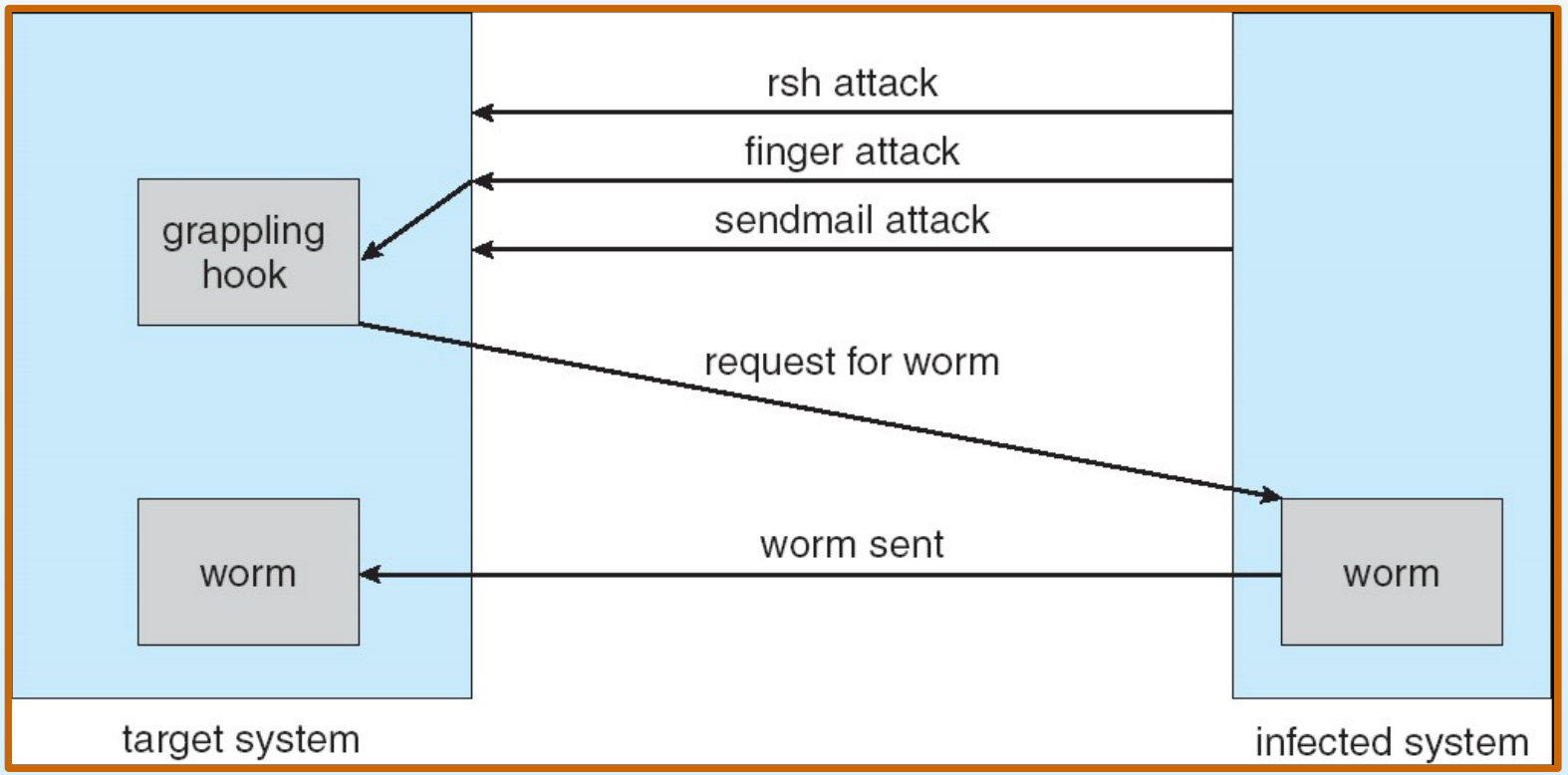
Before attack

After attack

Worm

- Self-replicating computer program
- Morris worm: first worm to attract wide attention
- Designed to do any number of things
  - delete files
  - install a backdoor for future use
  - send spam or launch DOS attack
  - etc.
- Worm can wreak havoc just with the network traffic generated by its reproduction
- Famous worms
  - Morris worm
  - Code Red worm
  - SQL slammer worm

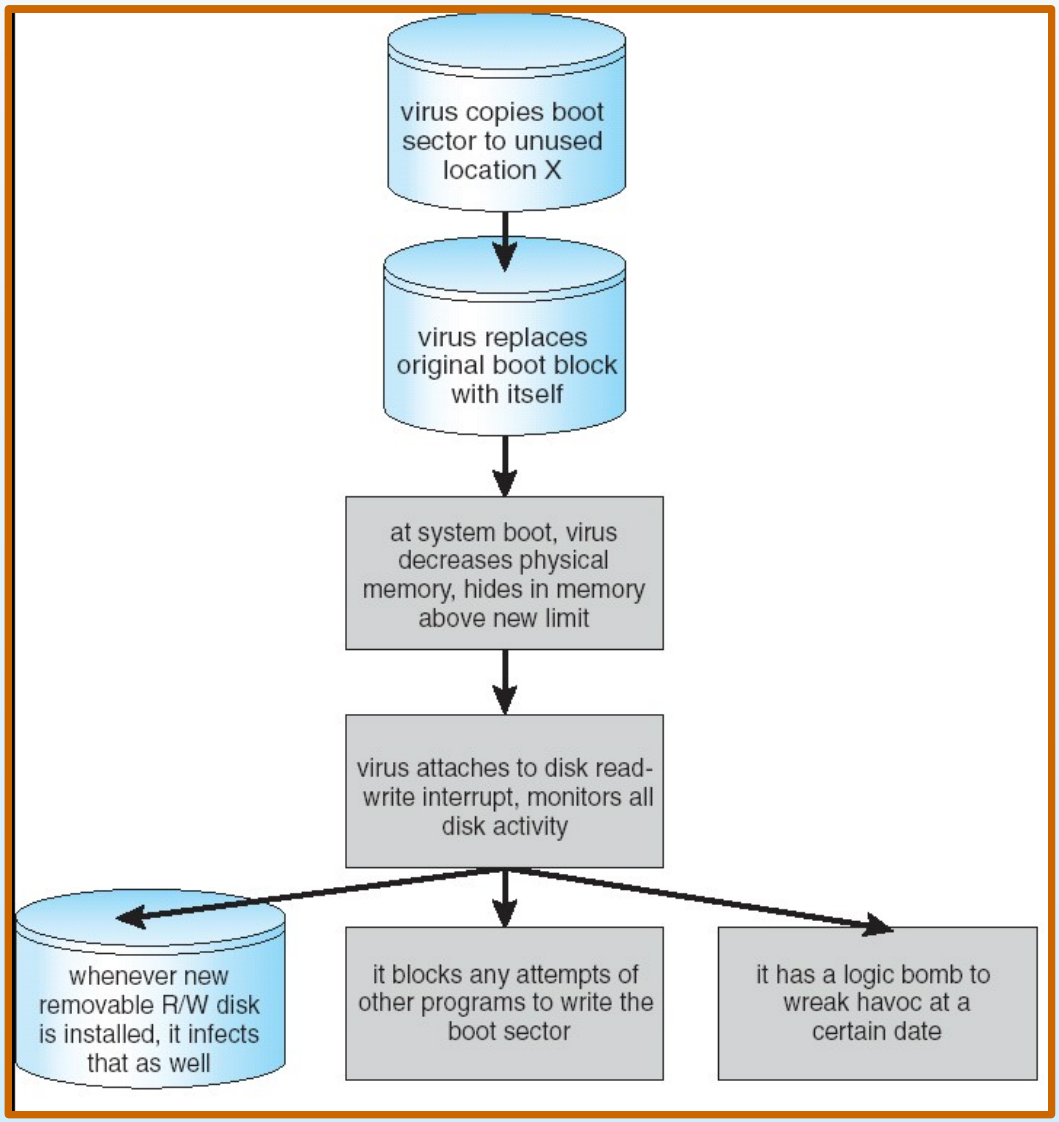
The Morris Internet Worm



Virus

- A self-replicating program that spreads by inserting copies of itself into other executable code or documents.
- Viruses have targeted various types of documents
  - Binary executable files
  - Boot sectors of floppy disks and hard disk partitions
  - General-purpose script files
  - Documents that can contain macros
  - etc.
- **Anti-virus software**
  - Examining (scanning) files to look for known viruses matching definitions in a virus dictionary (virus signature)
  - Identifying suspicious behavior from any computer program which might indicate infection.
- Polymorphic, encrypted

A Boot-sector Computer Virus



Denial of Service Attacks (DoS)

- An attack on a computer system or network that causes a loss of service to users typically by
  - consuming the bandwidth of the victim network
  - overloading the computational resources of the victim system
- Examples:
  - ping of death
  - SYN flood
- Distributed denial-of-service attack (DDoS)
  - the attacking computer hosts are **zombie computers** that have been compromised.
  - the perpetrator to remotely control the machine and direct the attack
- IP source address spoofing

DoS (cont.)

Figure 4: A DDoS Attack

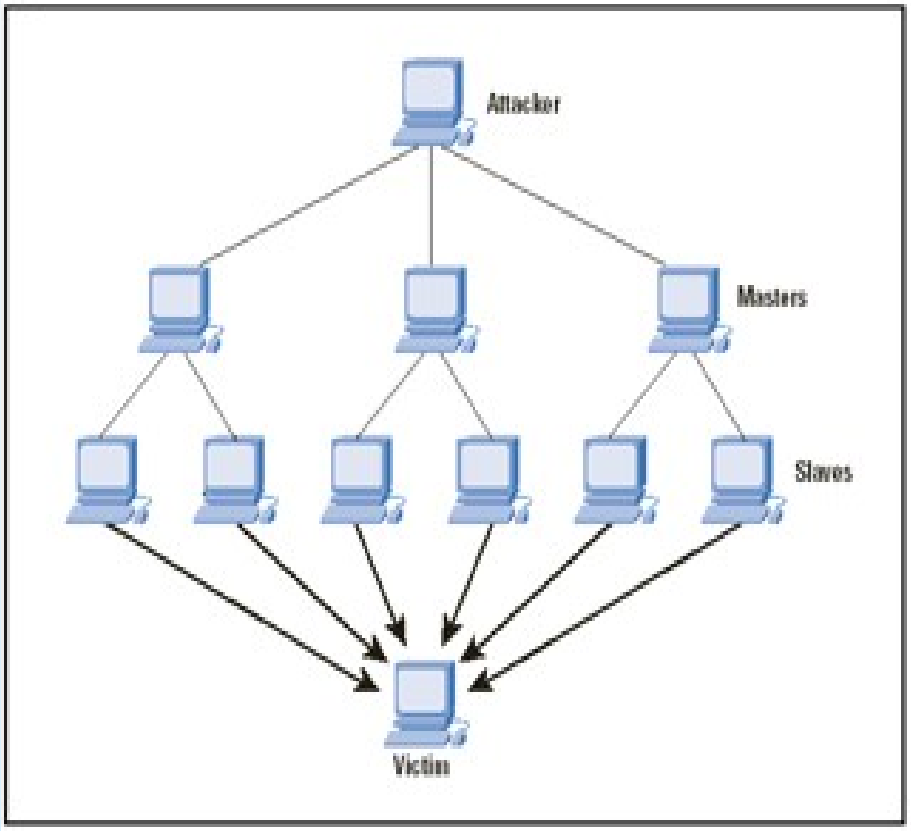
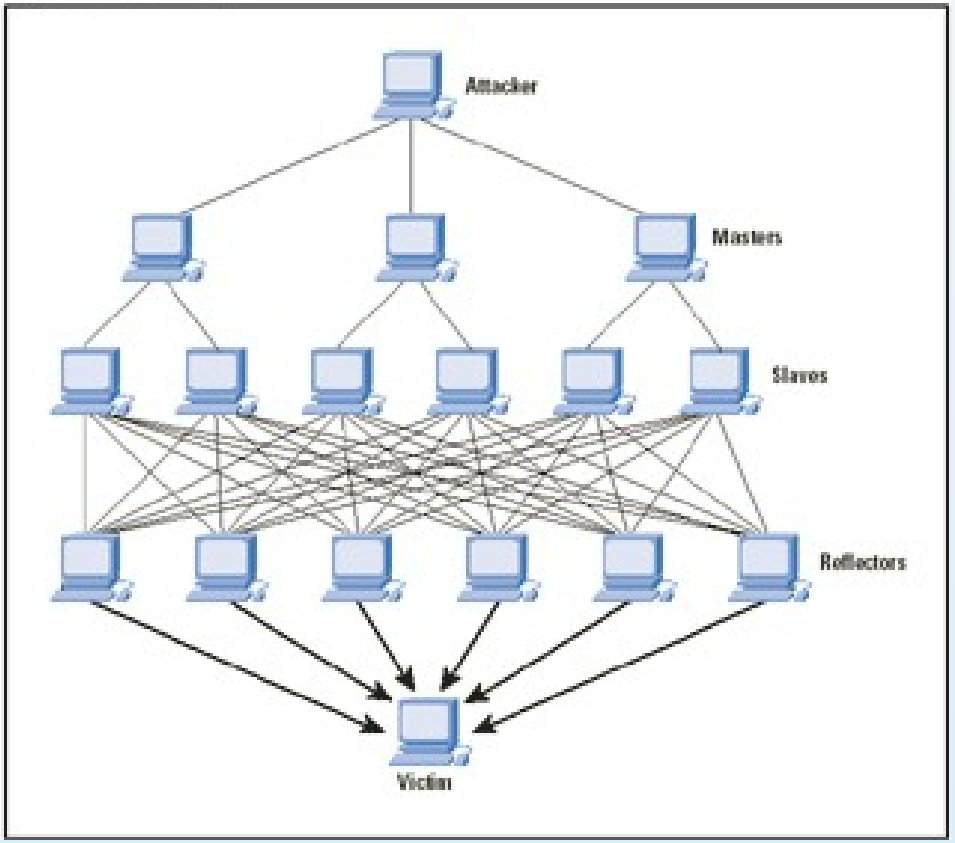


Figure 5: A DRDoS Attack



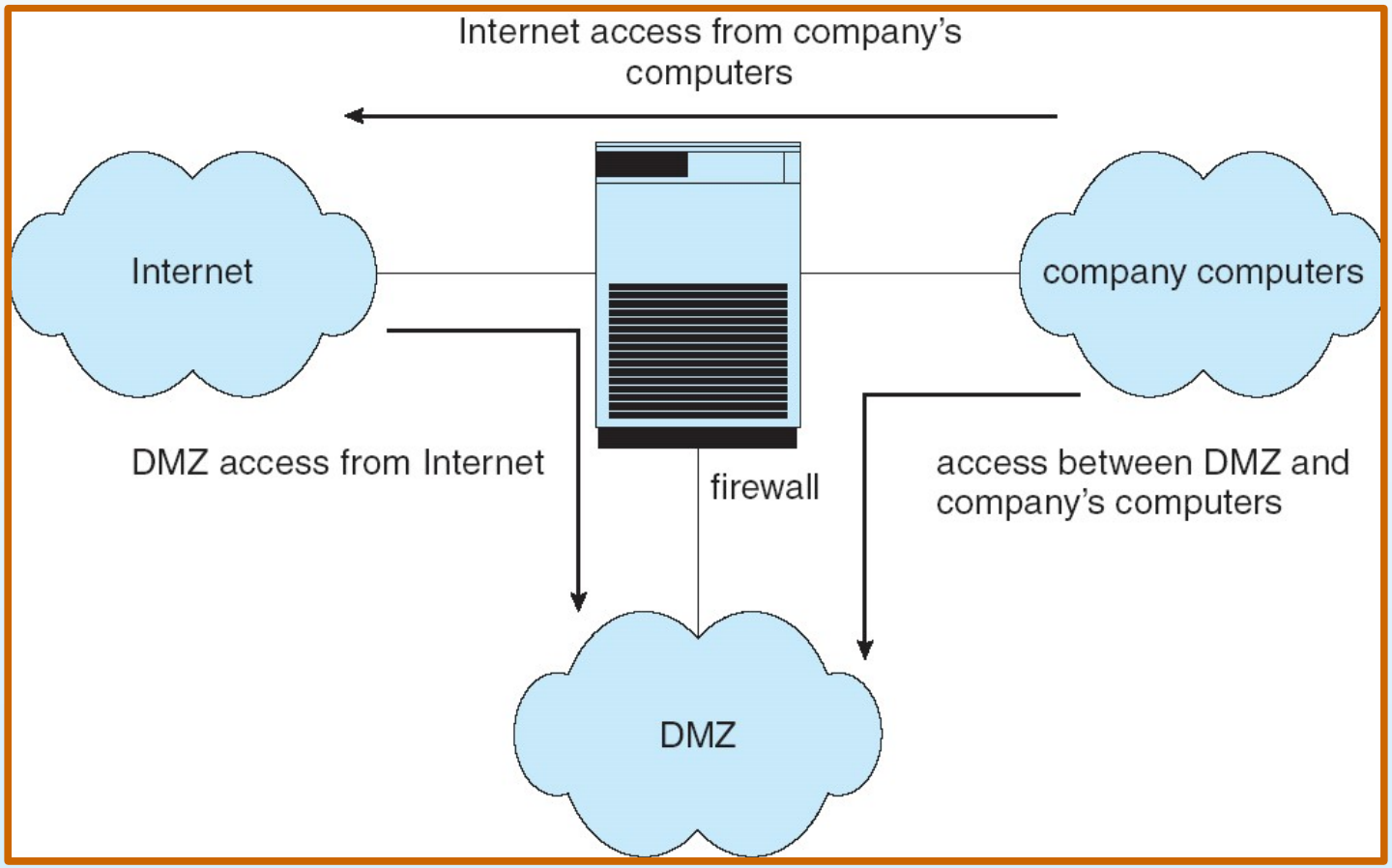
Intrusion Detection System

- Intrusion detection endeavors to detect attempted or successful intrusions
  - Signature-based detection spots known bad patterns
  - Anomaly detection spots differences from normal behavior
    - system administrator defines the baseline, or normal, state of the network's traffic load, breakdown, protocol, and typical packet size
  - False-positives and false-negatives a problem

Firewalls

- A firewall is a piece of hardware and/or software which functions in a networked environment to prevent some communications forbidden by the security policy
- Network Layer Firewall
  - Controlling traffic between different zones of trust
    - Internet (a zone with no trust)
    - Internal network (a zone with high trust)
    - DMZ (demilitarized zones)
  - works as a packet filter by deciding what packets will pass the firewall according to rules defined by the administrator
- Personal firewall is software layer on a given host
  - monitor and limit the traffic to and from the host

Network Security Through Domain Separation Via Firewall



End of Chapter 15