CHAPTER 15 - SYSTEM SECURITY

OBJECTIVES

- To discuss security threats and attacks
- To explain the fundamentals of encryption, authentication, and hashing
- To examine the uses of cryptography in computing
- To describe the various countermeasures to security attacks

THE SECURITY PROBLEM

THE SECURITY PROBLEM

- System secure if resources used and accessed as intended under all circumstances
  - Unachievable
- Intruders (crackers) attempt to breach security
- Threat is potential security violation
- Attack is attempt to breach security
- Attack can be accidental or malicious
- Easier to protect against accidental than malicious misuse

SECURITY VIOLATION CATEGORIES

- Breach of confidentiality
  - Unauthorized reading of data
- Breach of integrity
  - Unauthorized modification of data
- Breach of availability
  - Unauthorized destruction of data

SECURITY VIOLATION CATEGORIES

- Theft of service
  - Unauthorized use of resources
- Denial of service (DOS)
  - Prevention of legitimate use

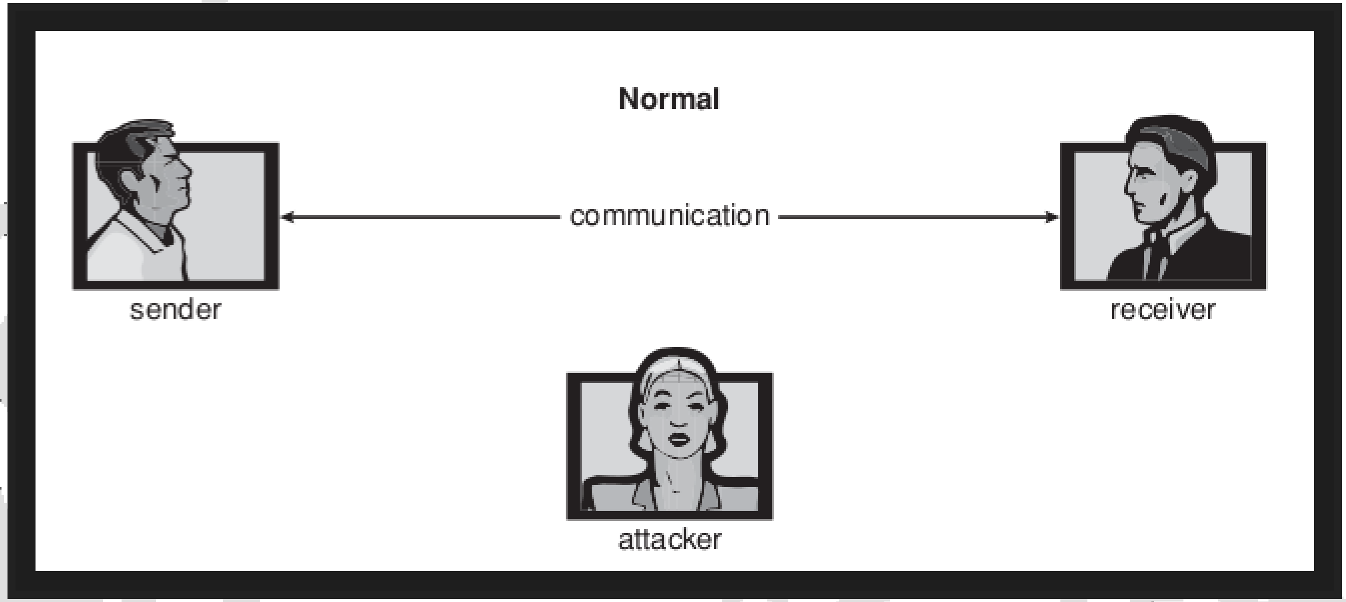
SECURITY VIOLATION METHODS

- Masquerading (breach authentication)
  - Pretending to be an authorized user to escalate privileges
- Replay attack
  - As is or with message modification

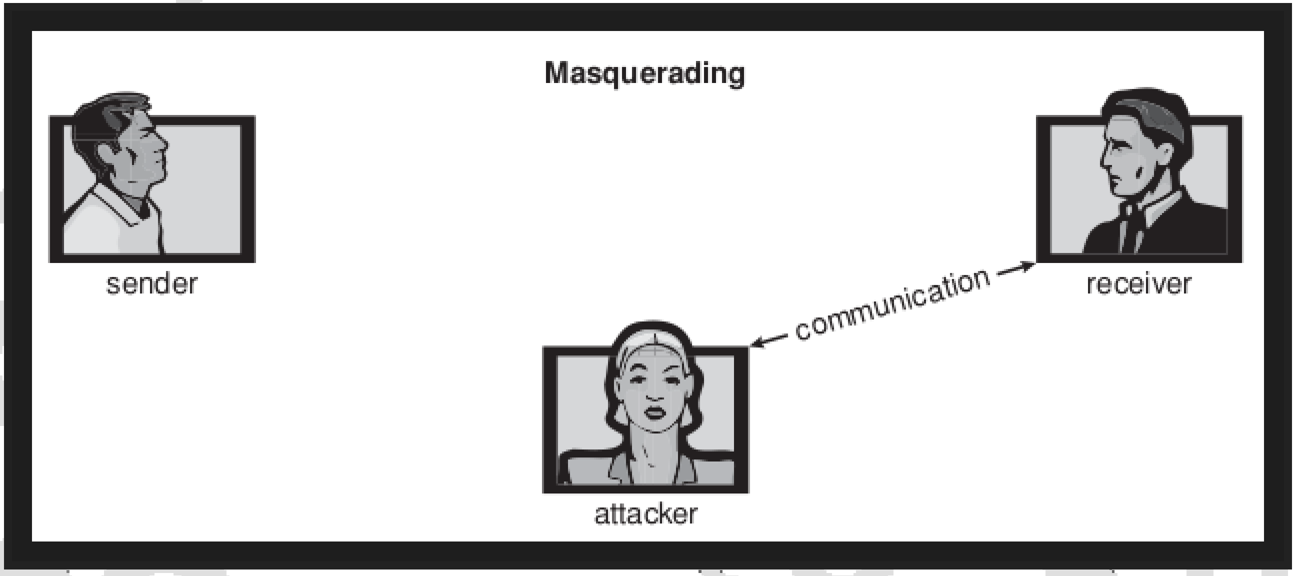
SECURITY VIOLATION METHODS

- Man-in-the-middle attack
  - Intruder sits in data flow, masquerading as sender to receiver and vice versa
- Session hijacking
  - Intercept an already-established session to bypass authentication

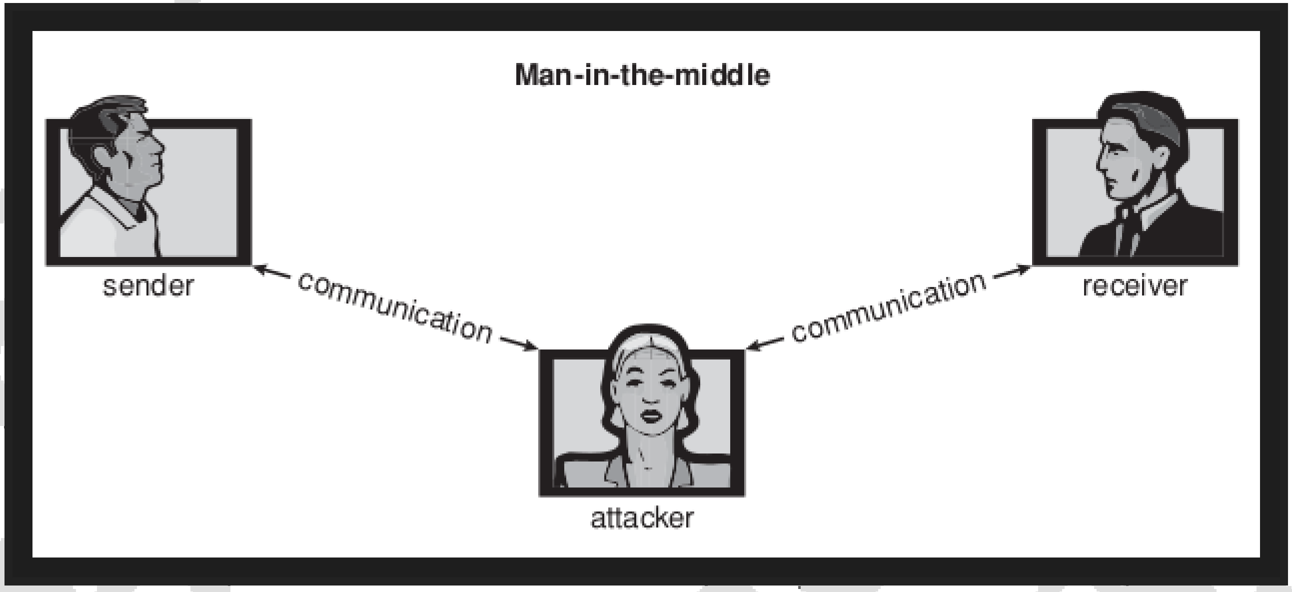
STANDARD SECURITY ATTACKS



STANDARD SECURITY ATTACKS



STANDARD SECURITY ATTACKS



SECURITY MEASURE LEVELS

Impossible to have absolute security, but make cost to perpetrator sufficiently high to deter most intruders

- Security must occur at four levels to be effective:

SECURITY LEVELS

- Physical
  - Data centers, servers, connected terminals
- Human
  - Avoid social engineering, phishing, dumpster diving
- Operating System
  - Protection mechanisms, debugging
- Network
  - Intercepted communications, interruption, DOS

SECURITY MEASURE LEVELS

- Security is as weak as the weakest link in the chain
  - But can too much security be a problem?

PROGRAM THREATS

PROGRAM THREATS

- Many variations, many names

TROJAN HORSE

- Code segment that misuses its environment
- Exploits mechanisms for allowing programs written by users to be executed by other users
- Spyware, pop-up browser windows, covert channels
- Up to 80% of spam delivered by spyware-infected systems

TRAP DOOR

- Specific user identifier or password that circumvents normal security procedures
- Could be included in a compiler
- How to detect them?

LOGIC BOMB

- Program that initiates a security incident under certain circumstances

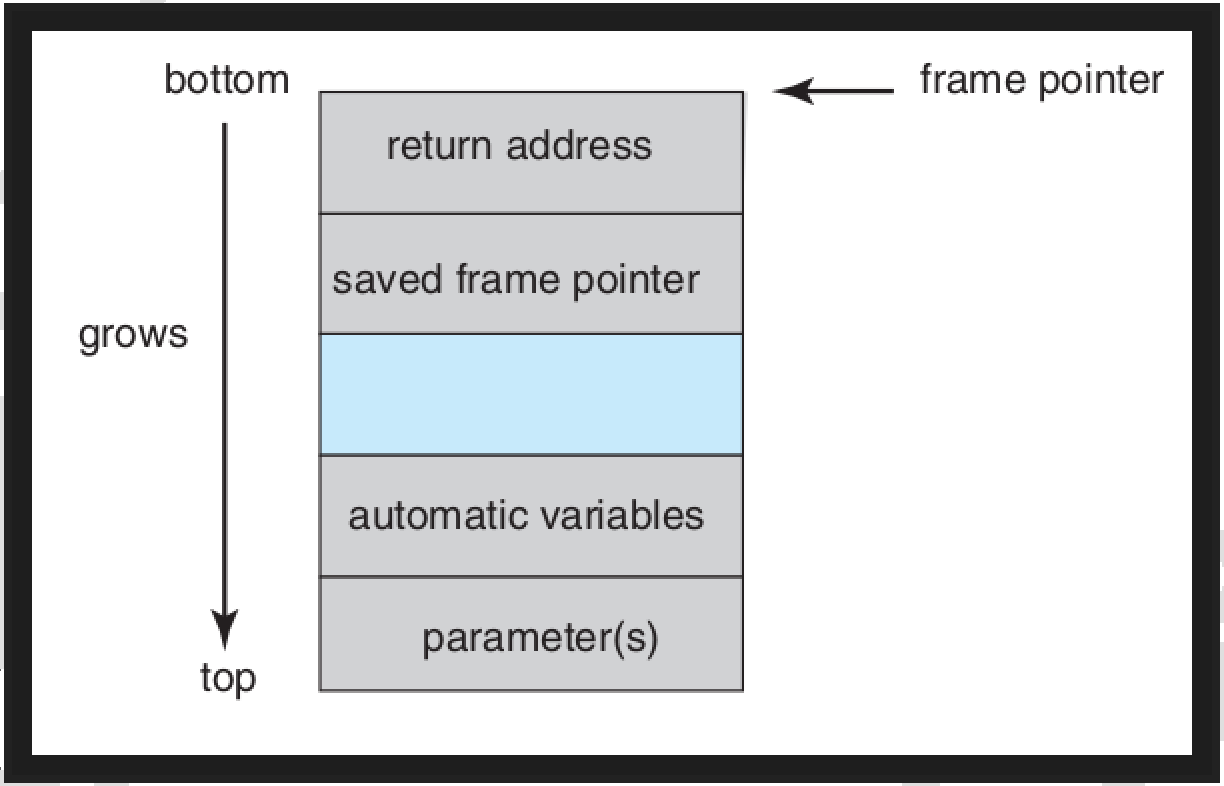
STACK AND BUFFER OVERFLOW

- Exploits a bug in a program (overflow stack or memory buffers)
- Failure to check bounds on inputs, arguments
- Write past arguments on the stack into the return address on stack
- When routine returns, returns to hacked address
  - Pointed to malicious code loaded onto stack
- Unauthorized user or privilege escalation

C PROGRAM WITH BUFFER-OVERFLOW CONDITION

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

LAYOUT OF TYPICAL STACK FRAME

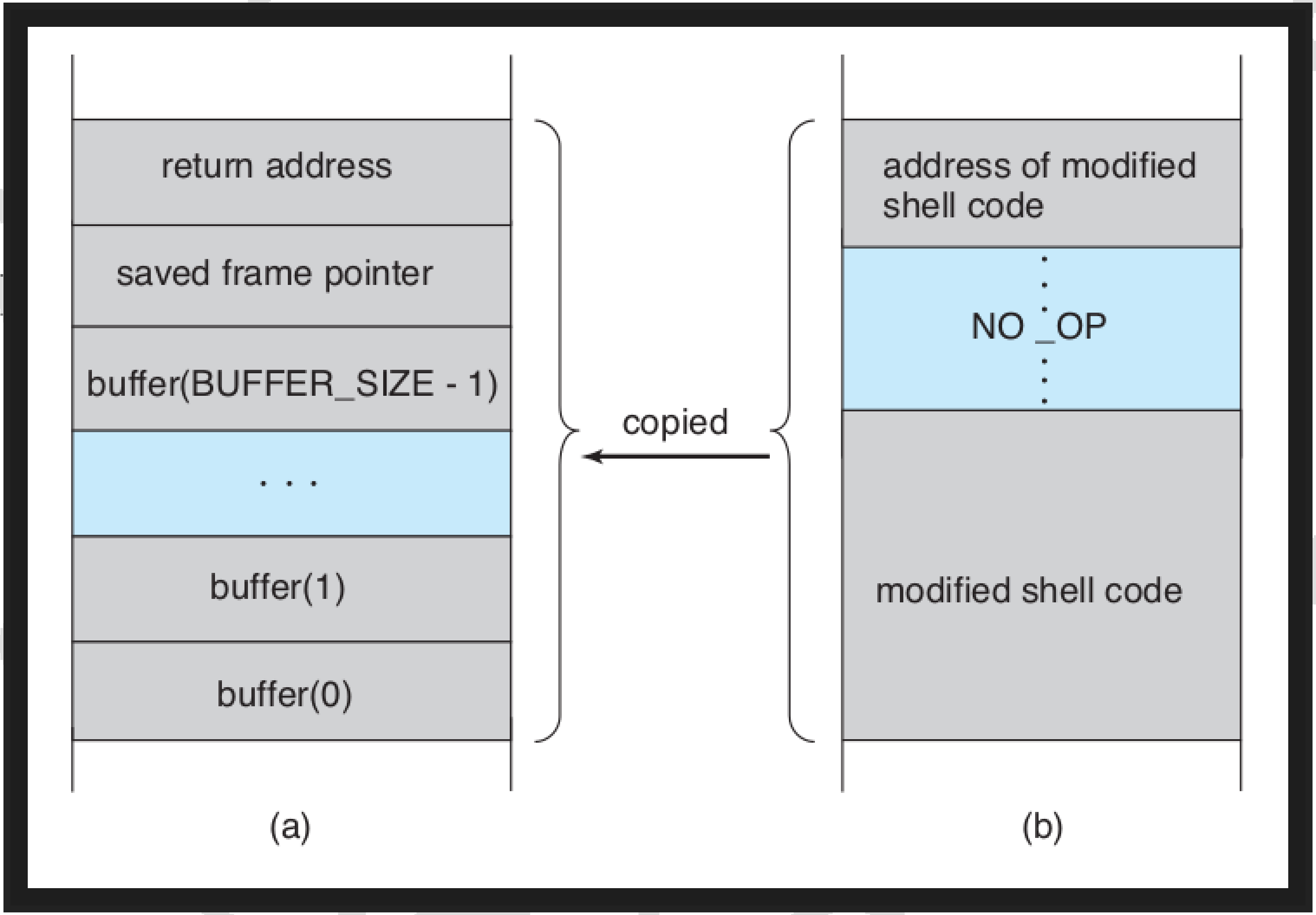


MODIFIED SHELL CODE

```
#include <stdio.h>

int main(int argc, char *argv[]) {
  execvp(‘‘\bin\sh’’,‘‘\bin \sh’’, NULL);
  return 0;
}
```

HYPOTHETICAL STACK FRAME



GREAT PROGRAMMING REQUIRED?

- For the first step of determining the bug, and second step of writing exploit code, yes
- Script kiddies can run pre-written exploit code to attack a given system
- Attack code can get a shell with the processes' owner's permissions
  - Or open a network port, delete files, download a program, etc

BUFFER OVERFLOW

- Depending on bug, attack can be executed across a network using allowed connections, bypassing firewalls
- Buffer overflow can be disabled by disabling stack execution or adding bit to page table to indicate “non-executable” state
  - Available in SPARC and x86
  - But still have security exploits

VIRUSES

- Code fragment embedded in legitimate program
- Self-replicating, designed to infect other computers
- Very specific to CPU architecture, operating system, applications
- Usually borne via email or as a macro
- Virus dropper inserts virus onto the system

VISUAL BASIC VIRUS

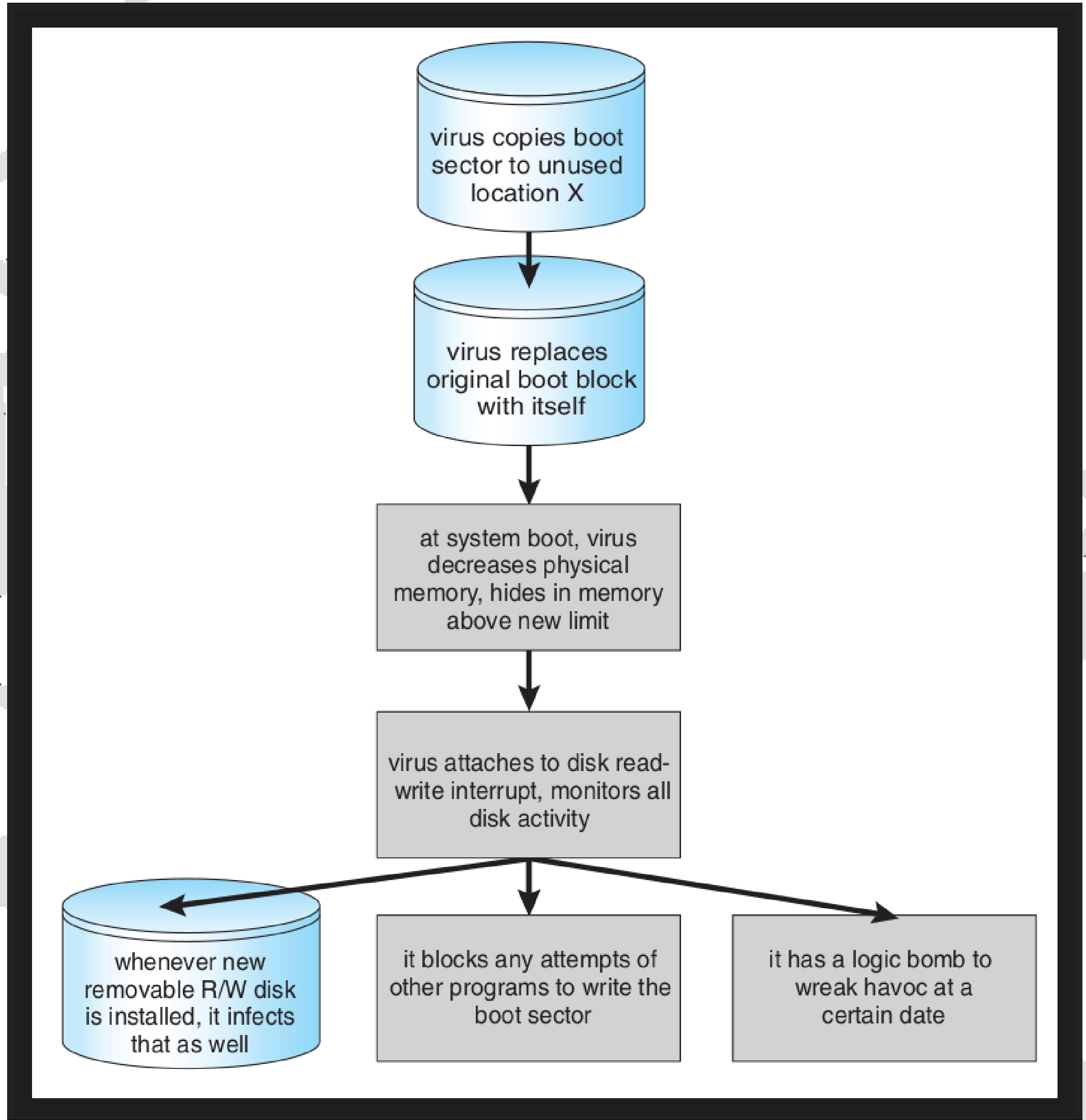
Visual Basic Macro to reformat hard drive

```
Sub AutoOpen()
Dim oFS
  Set oFS = CreateObject(’’Scripting.FileSystemObject’’)
  vs = Shell(’’c:command.com /k format c:’’,vbHide)
End Sub
```

VIRUS CATEGORIES

- File / parasitic
- Boot / memory
- Macro / Source code
- Polymorphic to avoid having a virus signature
- Encrypted
- Stealth
- Tunneling
- Multipartite
- Armored

A BOOT-SECTOR COMPUTER VIRUS



THE THREAT CONTINUES

- Attacks still common, still occurring
- Attacks moved over time from science experiments to tools of organized crime
  - Targeting specific companies
  - Creating botnets to use as tool for spam and DDOS delivery
  - Keystroke logger to grab passwords, credit card numbers

THE THREAT CONTINUES

- Why is Windows the target for most attacks?
  - Most common
  - Everyone is an administrator
    - Licensing required?
  - Monoculture considered harmful

SYSTEM AND NETWORK THREATS

SYSTEM THREATS

- Some systems “open” rather than secure by default
  - Reduce attack surface
  - But harder to use, more knowledge needed to administer

NETWORK THREATS

- Network threats harder to detect, prevent
- Protection systems weaker
- More difficult to have a shared secret on which to base access
- No physical limits once system attached to internet
    - Or on network with system attached to internet
- Even determining location of connecting system difficult
    - IP address is only knowledge

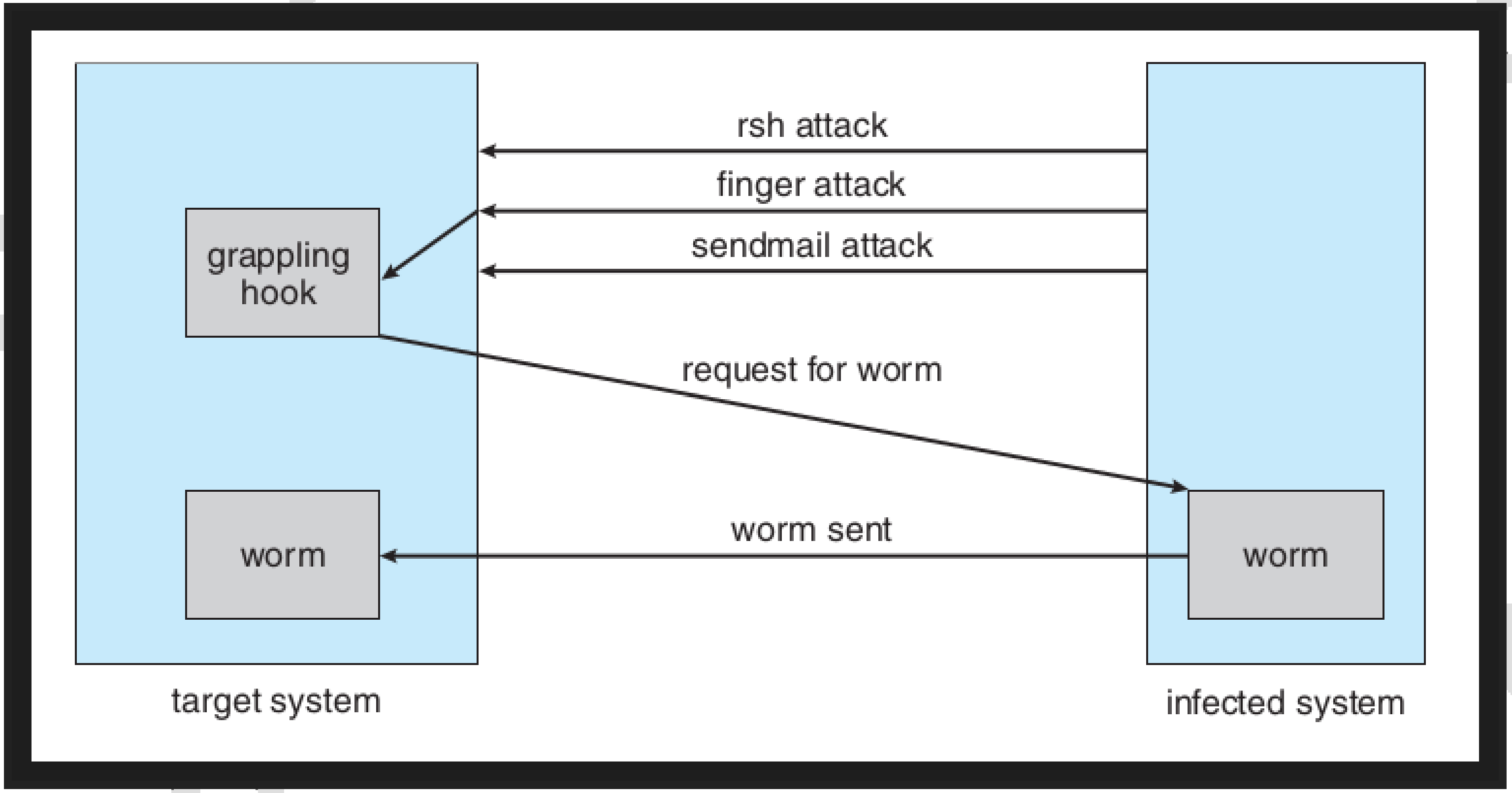
WORMS

- Worms – use spawn mechanism; standalone program
- Internet worm (Morris)
  - Exploited UNIX networking features (remote access) and bugs in finger and sendmail programs
  - Exploited trust-relationship mechanism used by rsh to access friendly systems without use of password
  - Grappling hook program uploaded main worm program
    - 99 lines of C code

WORMS

- Hooked system then uploaded main code, tried to attack connected systems
- Also tried to break into other users accounts on local system via password guessing
- If target system already infected, abort, except for every 7^{th} time

THE MORRIS INTERNET WORM



PORT SCANNING

- Automated attempt to connect to a range of ports on one or a range of IP addresses
- Detection of answering service protocol
- Detection of OS and version running on system
- **nmap** scans all ports in a given IP range for a response
- **nessus** and **metasploid** has databases of protocols and bugs (and exploits) to apply against a system
- Frequently launched from zombie systems

DENIAL OF SERVICE

- Overload the targeted computer preventing it from doing any useful work
- Distributed denial-of-service (DDOS) come from multiple sites at once

DENIAL OF SERVICE

- Consider the start of the IP-connection handshake (SYN)
  - How many started-connections can the OS handle?
    - Consider traffic to a web site
    - How can you tell the difference between being a target and being really popular?
  - Accidental – CS students writing bad fork() code
  - Purposeful – extortion, punishment

SOBIG.F WORM

- More modern example
- Disguised as a photo uploaded to adult newsgroup via account created with stolen credit card
- Targeted Windows systems
- Had own SMTP engine to mail itself as attachment to everyone in infect system’s address book
- Disguised with innocuous subject lines, looking like it came from someone known

SOBIG.F WORM

- Attachment was executable program that created WINPPR23.EXE in default Windows system directory Plus the Windows Registry

```
[HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"TrayX" = %windir%\winppr32.exe /sinc
[HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"TrayX" = %windir%\winppr32.exe /sinc
```

CRYPTOGRAPHY AS A SECURITY TOOL

CRYPTOGRAPHY AS A SECURITY TOOL

- Broadest security tool available
- Internal to a given computer, source and destination of messages can be known and protected
  - OS creates, manages, protects process IDs, communication ports

CRYPTOGRAPHY AS A SECURITY TOOL

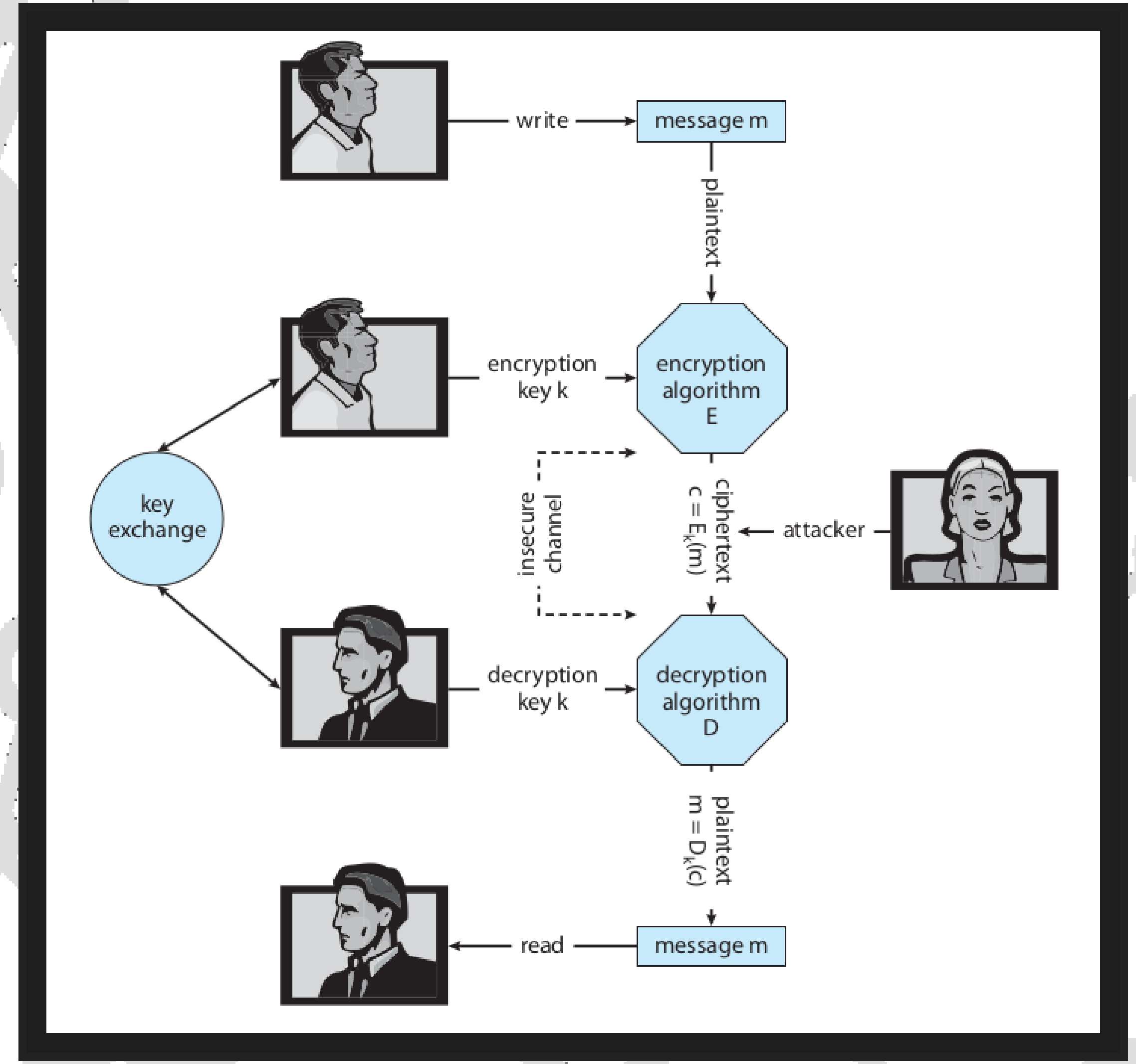
- Source and destination of messages on network cannot be trusted without cryptography
  - Local network – IP address?
    - Consider unauthorized host added
  - WAN / Internet – how to establish authenticity
    - Not via IP address

CRYPTOGRAPHY

- Means to constrain potential senders (sources) and / or receivers (destinations) of messages
- Based on secrets (keys)
- Enables:
  - Confirmation of source
  - Receipt only by certain destination
  - Trust relationship between sender and receiver

SECURE COMMUNICATION

over Insecure Medium



ENCRYPTION

- Encryption algorithm consists of
  - Set K of keys
  - Set M of Messages
  - Set C of ciphertexts (encrypted messages)

ENCRYPTION

- Encryption algorithm consists of
  - A function $E : K \rightarrow (M \rightarrow C)$. That is, for each $k \in K$, $E(k)$ is a function for generating ciphertexts from messages
    - Both E and $E(k)$ for any k should be efficiently computable functions
  - A function $D : K \rightarrow (C \rightarrow M)$. That is, for each $k \in K$, $D(k)$ is a function for generating messages from ciphertexts
    - Both D and $D(k)$ for any k should be efficiently computable functions

ENCRYPTION

- An encryption algorithm must provide this essential property: Given a ciphertext $c \in C$, a computer can compute m such that $E(k)(m) = c$ only if it possesses $D(k)$
- Thus, a computer holding $D(k)$ can decrypt ciphertexts to the plaintexts used to produce them, but a computer not holding $D(k)$ cannot decrypt ciphertexts
- Since ciphertexts are generally exposed (for example, sent on the network), it is important that it be infeasible to derive $D(k)$ from the ciphertexts

SYMMETRIC ENCRYPTION

Same key used to encrypt and decrypt, i.e. E(k) can be derived from D(k), and vice versa

- DES is commonly used symmetric block-encryption algorithm (created by US Govt)
  - Encrypts a block of data at a time
- Triple-DES considered more secure
- Advanced Encryption Standard (AES) much harder to break

SYMMETRIC ENCRYPTION

- RC4 is most common symmetric stream cipher, but known to have vulnerabilities
  - Encrypts/decrypts a stream of bytes (i.e., wireless transmission)
  - Key is a input to psuedo-random-bit generator
    - Generates an infinite keystream

ASYMMETRIC ENCRYPTION

- Public-key encryption 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
- Must be an encryption scheme that can be made public without making it easy to figure out the decryption scheme

RSA

- Most common is RSA block cipher
- Efficient algorithm for testing whether or not a number is prime
- No efficient algorithm is know for finding the prime factors of a number

RSA

- Formally, it is computationally infeasible to derive D(k_d, N) from E(k_e, N), and so E(k_e, N) need not be kept secret and can be shared
  - E(k_e, N) (or just k_e) is the public key
  - D(k_d, N) (or just k_d) is the private key
  - N is the product of two large, randomly chosen prime numbers p and q (for example, p and q are 512 bits each)

RSA

- Encryption algorithm is $E(k_e, N)(m) = m^{k_e} \bmod N$, where k_e satisfies $k_e\, k_d \bmod (p-1)(q-1) = 1$

- The decryption algorithm is then $D(k_d, N)(c) = c^{k_d} \bmod N$

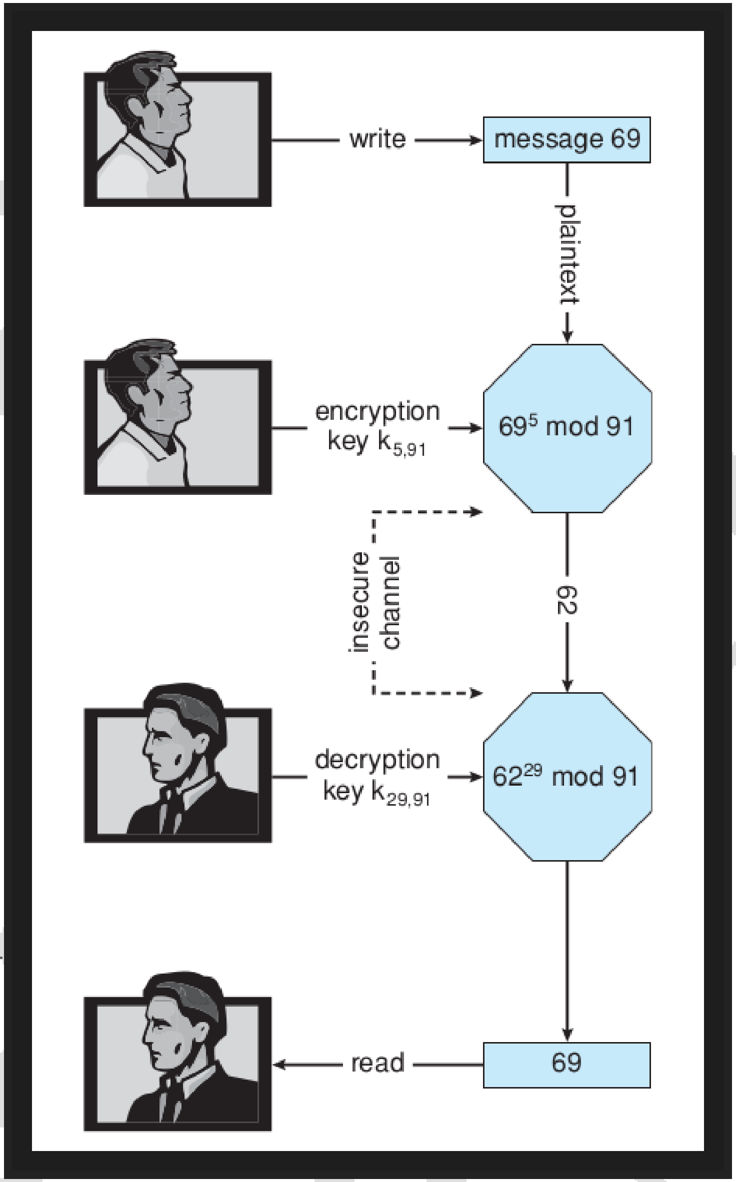
RSA EXAMPLE

- Make $p = 7$ and $q = 13$
- We then calculate $N = 7 * 13 = 91$ and $(p-1)(q-1) = 72$
- We next select k_e relatively prime to 72 and <72, → 5
- Finally,we calculate k_d such that $k_e\, k_d \bmod 72 = 1$, → 29
- We how have our keys
- Public key, k_e, N = 5, 91
- Private key, k_d, N = 29, 91

RSA EXAMPLE

- Encrypting the message 69 with the public key results in the cyphertext 62
- Cyphertext can be decoded with the private key
  - Public key can be distributed in cleartext to anyone who wants to communicate with holder of public key

RSA EXAMPLE



write
message 69
plaintext
encryption key $k_{5,91}$
69^5 mod 91
insecure channel
62
decryption key $k_{29,91}$
62^{29} mod 91
read
69

CRYPTOGRAPHY

- Note symmetric cryptography based on transformations, asymmetric based on mathematical functions
  - Asymmetric much more compute intensive
  - Typically not used for bulk data encryption

AUTHENTICATION

- Constraining set of potential senders of a message
  - Complementary and sometimes redundant to encryption
  - Also can prove message unmodified

AUTHENTICATION COMPONENTS

- Sets K of keys, M of messages and A of authenticators
- A function $S : K \rightarrow (M \rightarrow A)$
  - That is, for each $k \in K$, $S(k)$ is a function for generating authenticators from messages
  - Both S and $S(k)$ for any k is efficiently computable functions

AUTHENTICATION COMPONENTS

- A function $V : K \to (M \times A \to \{true, false\})$. That is, for each $k \in K$, $V(k)$ is a function for verifying authenticators on messages
  - Both V and V(k) for any k is efficiently computable functions

AUTHENTICATION

- For a message m, can generate an authenticator $a \in A$ such that $V(k)(m, a) = \text{true}$ only if it possesses $S(k)$
- Thus, holding $S(k)$ can generate authenticators on messages so that any other possessing $V(k)$ can verify them
  - Not holding $S(k)$ cannot generate authenticators on messages that can be verified using $V(k)$
  - Authenticators generally exposed (i.e. sent on the network with the messages themselves), must not be feasible to derive $S(k)$ from the authenticators

HASH FUNCTIONS

- Basis of authentication
- Creates small, fixed-size block of data (message digest, hash value) from m
- Hash Function H must be collision resistant on m
  - Infeasible to find an m’ ≠ m such that H(m) = H(m’)
- If H(m) = H(m’), then m = m’
  - The message has not been modified
- Common message-digest functions include MD5 → produces a 128-bit hash, and SHA-1 → outputs a 160-bit hash

AUTHENTICATION – DIGITAL SIGNATURE

- Based on asymmetric keys and digital signature algorithm
- Authenticators produced are digital signatures
- In a digital-signature algorithm, computationally infeasible to derive $S(k_S)$ from $V(k_V)$
  - V is a one-way function
  - Thus, k_V is the public key and k_S is the private key

DIGITAL SIGNATURE

- Consider the RSA digital-signature algorithm
  - Similar to the RSA encryption algorithm, but the key use is reversed

DIGITAL SIGNATURE

- Digital signature of message $S(k_s)(m) = H(m)^{k_s} \bmod N$
- The key k_s again is a pair d, N, where N is the product of two large, randomly chosen prime numbers p and q
- Verification algorithm is $V(k_v)(m,a) \equiv (a^{k_v} \bmod N = H(m))$
  - Where k_v satisfies $k_v\, k_s \bmod (p-1)(q-1) = 1$

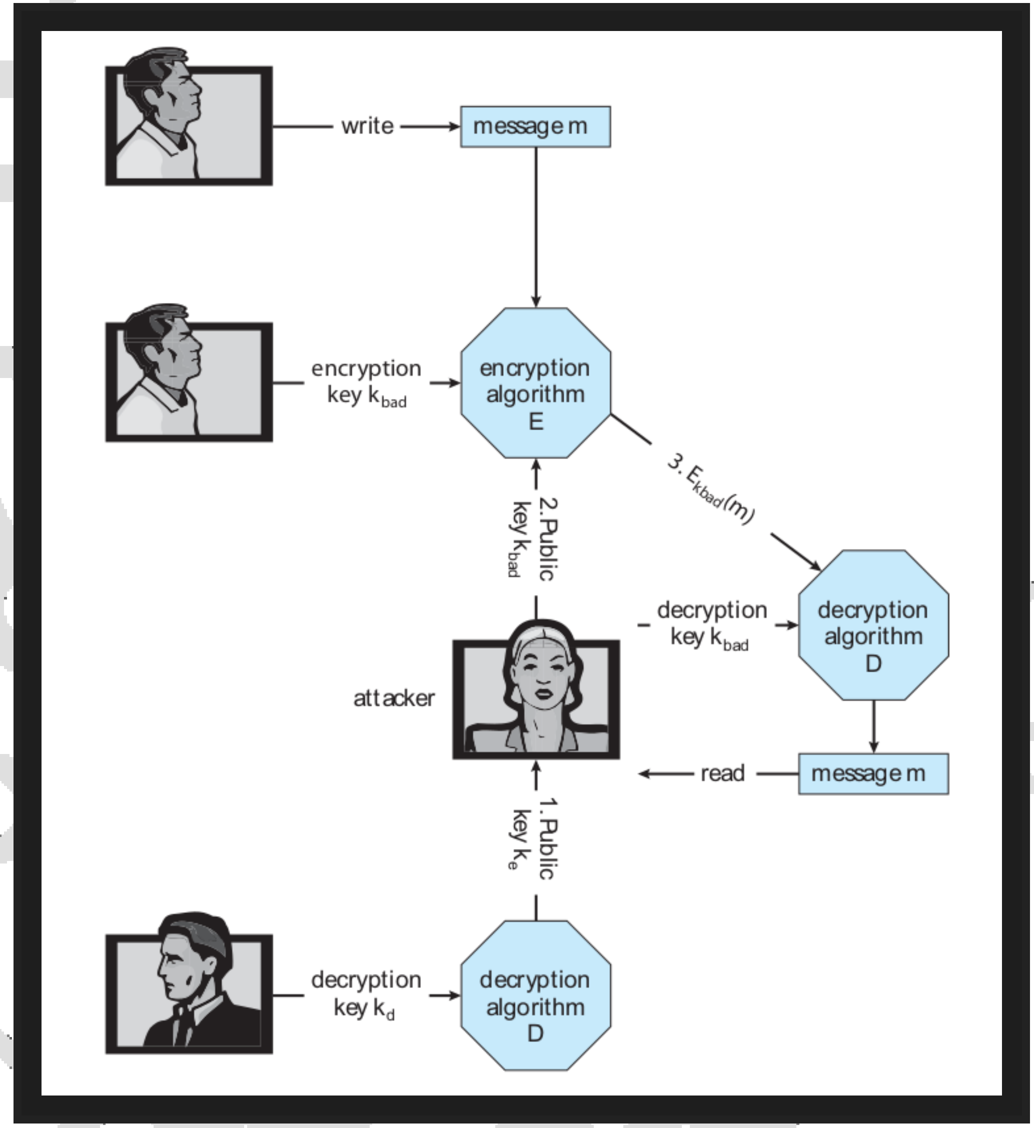
AUTHENTICATION

- Why authentication if a subset of encryption?
  - Fewer computations (except for RSA digital signatures)
  - Authenticator usually shorter than message
  - Sometimes want authentication but not confidentiality
    - Signed patches et al
  - Can be basis for non-repudiation

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



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

IMPLEMENTATION OF CRYPTOGRAPHY

- Can be done at various levels of ISO Reference Model
  - SSL at the Transport layer
  - Network layer is typically IPSec
    - IKE for key exchange
    - Basis of VPNs

IMPLEMENTATION OF CRYPTOGRAPHY

- Why not just at lowest level?
  - Sometimes need more knowledge than available at low levels
    - i.e. User authentication
    - i.e. e-mail delivery

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 (fx. credit card numbers)

ENCRYPTION EXAMPLE - SSL

- 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 then uses symmetric key cryptography

USER AUTHENTICATION

USER AUTHENTICATION

- Crucial to identify user correctly, as protection systems depend on user ID
- User identity most often established through passwords, can be considered a special case of either keys or capabilities

PASSWORDS

- Passwords must be kept secret
  - Frequent change of passwords
  - History to avoid repeats
  - Use of “non-guessable” passwords
  - Log all invalid access attempts (but not the passwords themselves)
  - Unauthorized transfer

PASSWORDS

- Passwords may also either be encrypted or allowed to be used only once
  - Does encrypting passwords solve the exposure problem?
    - Might solve sniffing
    - Consider shoulder surfing
    - Consider Trojan horse keystroke logger
    - How are passwords stored at authenticating site?

PASSWORDS

- Encrypt to avoid having to keep secret
  - But keep secret anyway (i.e. Unix uses superuser-only readably file /etc/shadow)
  - Use algorithm easy to compute but difficult to invert
  - Only encrypted password stored, never decrypted
  - Add “salt” to avoid the same password being encrypted to the same value

ONE-TIME PASSWORDS

- Use a function based on a seed to compute a password, both user and computer
- Hardware device / calculator / key fob to generate the password
    - Changes very frequently

PASSWORDS

- Biometrics
  - Some physical attribute (fingerprint, hand scan)
- Multi-factor authentication
  - Need two or more factors for authentication
    - i.e. USB “dongle”, biometric measure, and password

IMPLEMENTING SECURITY DEFENSES

IMPLEMENTING SECURITY DEFENSES

- Defense in depth is most common security theory – multiple layers of security
- Security policy describes what is being secured
- Vulnerability assessment compares real state of system / network compared to security policy

IMPLEMENTING SECURITY DEFENSES

- Intrusion detection endeavors to detect attempted or successful intrusions
    - Signature-based detection spots known bad patterns
    - Anomaly detection spots differences from normal behavior
        - Can detect zero-day attacks
    - False-positives and false-negatives a problem

IMPLEMENTING SECURITY DEFENSES

- Virus protection
- Auditing, accounting, and logging of all or specific system or network activities

FIREWALLING TO PROTECT SYSTEMS AND NETWORKS

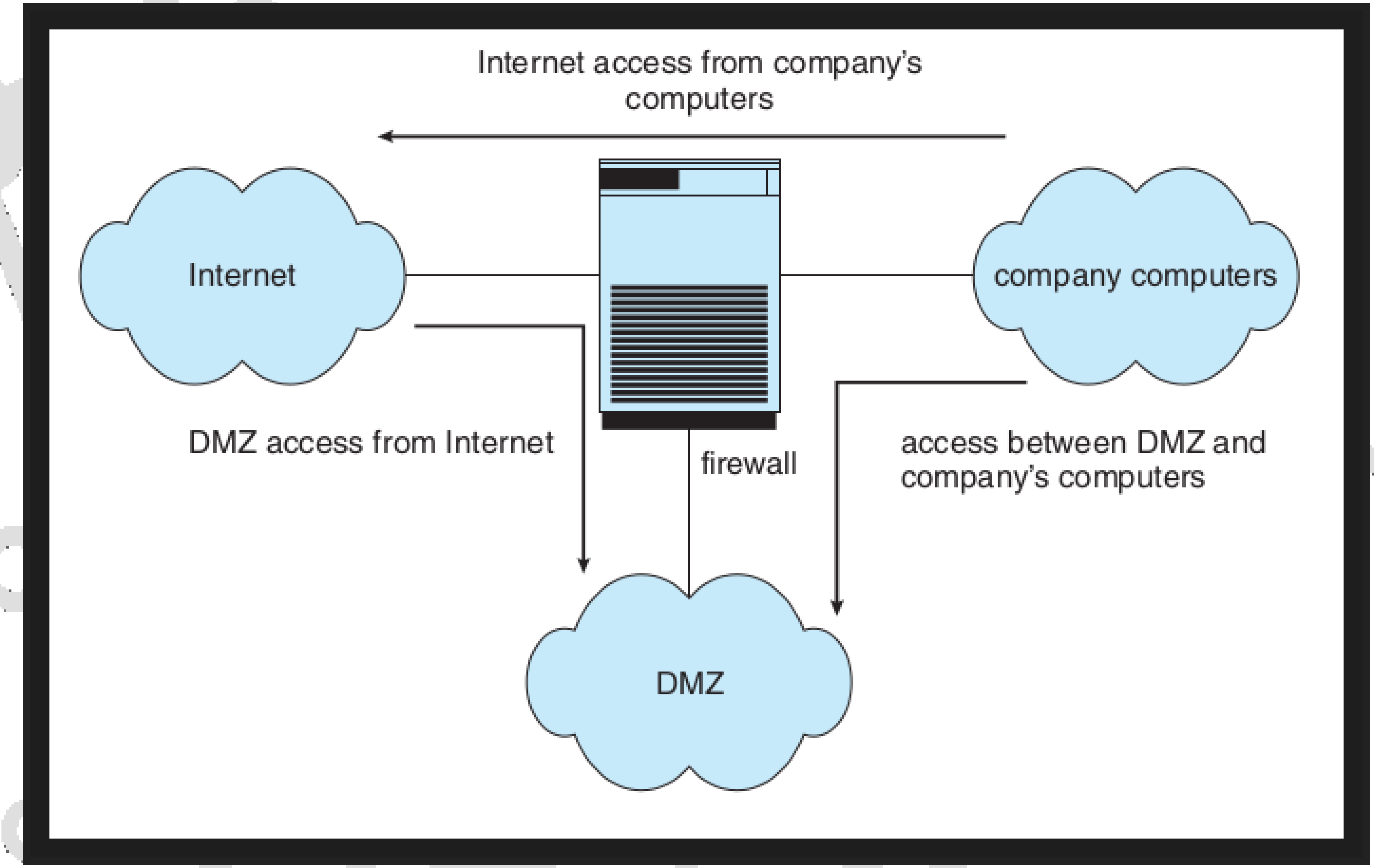
FIREWALLING

- A network firewall is placed between trusted and untrusted hosts
  - The firewall limits network access between these two security domains
- Can be tunneled or spoofed
  - Tunneling allows disallowed protocol to travel within allowed protocol (i.e., telnet inside of HTTP)
  - Firewall rules typically based on host name or IP address which can be spoofed

FIREWALLING

- Personal firewall is software layer on given host
  - Can monitor / limit traffic to and from the host
- Application proxy firewall understands application protocol and can control them (i.e., SMTP)
- System-call firewall monitors all important system calls and apply rules to them (i.e., this program can execute that system call)

NETWORK SECURITY THROUGH DOMAIN SEPARATION VIA FIREWALL



COMPUTER SECURITY CLASSIFICATIONS

SECURITY CLASSIFICATIONS

- U.S. Department of Defense outlines four divisions of computer security: A, B, C, and D
- D – Minimal security
- C – Provides discretionary protection through auditing
    - Divided into C1 and C2
        - C1 identifies cooperating users with the same level of protection
        - C2 allows user-level access control

SECURITY CLASSIFICATIONS

- B – All the properties of C, however each object may have unique sensitivity labels
  - Divided into B1, B2, and B3 A – Uses formal design and verification techniques to ensure security

EXAMPLE: WINDOWS 7

EXAMPLE: WINDOWS 7

- Security is based on user accounts
  - Each user has unique security ID
  - Login to ID creates security access token
    - Includes security ID for user, for user’s groups, and special privileges
    - Every process gets copy of token
    - System checks token to determine if access allowed or denied

EXAMPLE: WINDOWS 7

- Uses a subject model to ensure access security
  - A subject tracks and manages permissions for each program that a user runs
- Each object in Windows has a security attribute defined by a security descriptor
  - For example, a file has a security descriptor that indicates the access permissions for all users

QUESTIONS

BONUS

- Exam question number 11: **System Security**