Operating System Design

Dr. Jerry Shiao, Silicon Valley University

Security

- Overview
- Protection is an internal problem: Protection mechanisms provides controlled access to resources in Computer System.
- Security: Ensures the authentication of system users to protect the integrity of the information (i.e. data and code) and the physical resources of the Computer System.
  - Protection is ineffective if user authentication is compromised or a program is run by an unauthorized user.
- Computer Resources must be guarded against unauthorized access, malicious destruction or alterations.
- Key security enabler: Encryption. Explore encryption, authentication, and hashing.
- Mechanisms to guard against or detect attacks.
  - Uses of cryptography in computing.
- Implementing Security Defenses.
- Firewalling to Protect Systems and Networks.

Security

- The Security Problem
  - Impair Commercial Systems (payroll and financial data stolen), Corporate operations (company email and documents accessed) .
- Mechanism for protection work as long as users conform to the intended use of and access to those resources.
- Security must consider external environment of the system, and protect the system resources.
  - Intruders (crackers) attempt to breach security.
- Security Violations (or misuse) of the system:
  - Intentional (malicious): Attempt to breach security.
    - Threat is potential security violation.
    - Attack is the attempt to break security.
    - Difficult to protect.
  - Accidental: Protection mechanism was designed for accidents.
    - Easier to protect view Access Matrix.
- Attack can be accidental or malicious.

Security

- The Security Problem (Cont)
- Forms of accidental and malicious misuse.
  - Breach of Confidentiality: Unauthorized reading of data (or theft of information). ↑ impersonate s/o to access the unauthorized data.
    - Capturing secret data from a system or a data stream.
    - Credit-card information or identity information for identity theft.
  - Breach of Integrity: ← damage or destroy data. / modify
    - Unauthorized modification of data.
    - Passing of liability to innocent party or modification of source code of an important commercial application.
  - Breach of Availability: ← prevent s/o that has valid access to access
    - Unauthorized destruction of data by hackers causing havoc
    - Web-site defacement.

Security

- The Security Problem (Cont)
- Forms of accidental and malicious misuse (Cont)
  - Theft of Service:
    - Unauthorized use of resources.
    - Intruder (intrusion program) may install daemon that act as File Server.
  - Denial of Service:
    - Preventing legitimate use of the Computer System.
    - Sometimes accidental.

Security

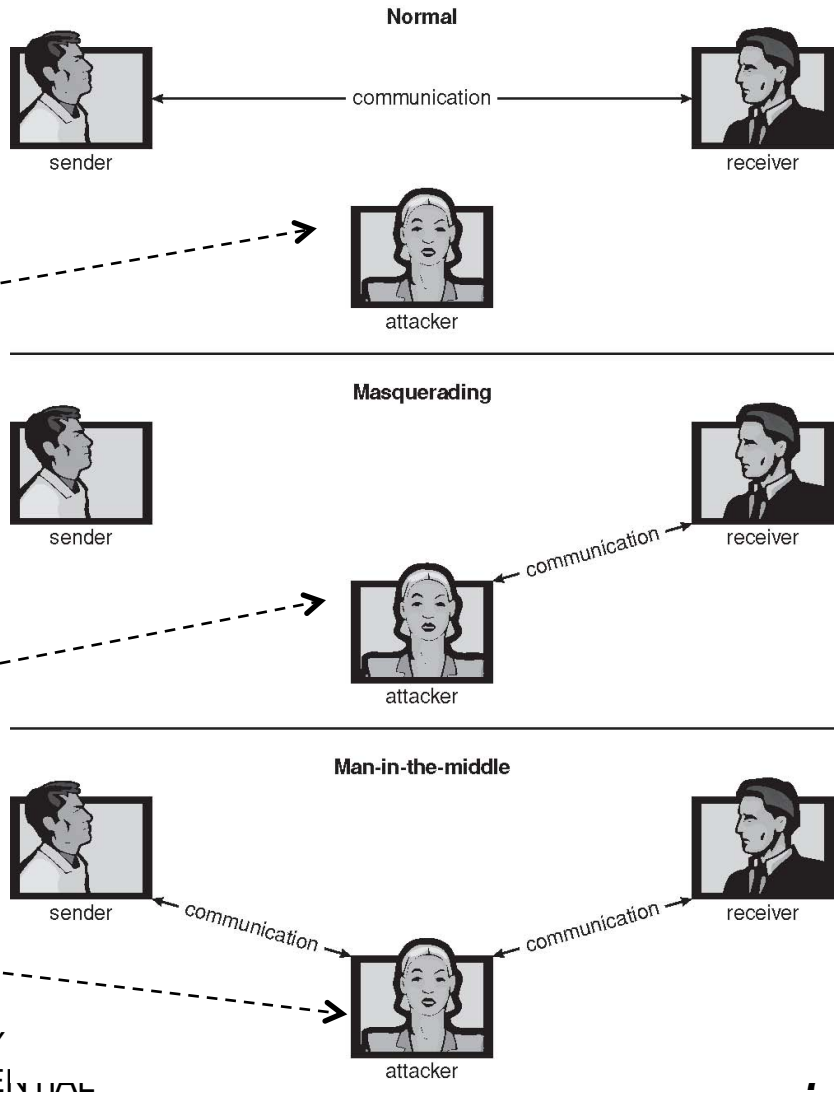
- The Security Problem (Cont)
- Attack Methods to breach Security:
  - Masquerading: ← pretend to be s/o.
    - Participant in communication pretends to be someone else.
    - Breach Authentiation: Gain access and obtain privilege that otherwise was prohibited.
  - Replay Attack: ← keep system busy.
    - Malicious or fraudulent repeat of a valid data transmission
  - Message Modification:
    - Repeat a request (Replay Attach) with message modification to escalate privileges.
    - Legitimate user's info replaced with unauthorized user's info.
  - Man-in-the-Middle Attack:
    - Attacker sits in the data flow of a communication, masquerading as the sender to the real receiver and as the receiver to the real sender.
  - Session Hijacking:
    - Man-in-the-Middle preceded by intercepting an active communication session.

Security

- The Security Problem (Cont)
- ~~Attach~~ Attack Methods (Cont)

Attacker in same Network is outside the flow of communication.

Attacker masquerades as Sender or Receiver.



Security

- The Security Problem (Cont)
- Protect a Computer System: Security Measure Levels.
  - Physical
    - Site containing Computer Systems physically secured.
    - Machine rooms, terminal, or workstations access secured.
  - Human
    - Authorization to ensure only appropriate users have access to the System.
    - Avoid social engineering (management and personnel issues):
      - Phishing: Web page misleads user into entering confidential info.
      - Dumpster diving: Gain unauthorized access by searching trash, phone books, or notes.
  - Operating System
    - System protects itself from accidental or purposeful security breach.
    - Programming error causing endless loop (accidental Denial-Of-Service).
  - Network
    - Computer data travels over internet and can be intercepted.

Focus

Security

- The Security Problem (Cont)
- Security Measures Levels (Cont)
  - Weakness at Security Levels 1 and 2 allows circumvention of low-level Operating System Security.
  - Operating System at Levels 3 and 4 provide protection and implementation of security features. Must be able to:
    - Provide protection to allow implementation of Security Features.
      - Implementing security measures requires: Authorizing Users and Processes, Controlling User Access, and Logging activities.
    - Hardware Memory Protection features needed (MMU).
    - Security Vulnerabilities being countered with Security Countermeasures causes more sophisticated attacks.
    - Improvements must be done at the Operating System and between Operating Systems (networking).

Security

- Program Threats ← worm, virus, etc.
- Processes, along with the Kernel, are the only means to accomplish work on Computer System.
- Goal of software intrusion to cause security breach:
  - Physically logging into Computer System not necessary, but leave back-door daemon to provide information or allows access.
  - Program creates a breach of security.
  - Cause a normal process to change its behavior and create a breach.
- What is a Trojan Horse?
  - Programs written by a user can grant permission for other users to execute it (i.e. text editor).
    - The program can misuse the access rights of the executing user (i.e. copy contents of the edited file to another location).

Security

- Program Threats
- Trojan House
  - Code Segment that misuses its environment.
  - Program inserted into search path list ($PATH contains "." character): Command executed from another user's account, instead of system library.
    - Programs using the Access Rights of executing user.
  - Terminal with Login emulation program: Collects username/password.
  - Spyware: Accompanies installed program (commercial or freeware/shareware).
    - Normally, download ads to display.
    - Capture information and return to central site.
    - Loading of Spyware daemon:
      - Destroying disk, crashing computer (Blue Screen of Death).
      - Using system to automate Spam or distribute Denial-of-Service attacks.

Program insert itself to the PATH env var to override login programs.

Security

- Program Threats
- Trap Door ← Backdoor
  - Software leaving secret access point, only designer of the program or system can use (i.e. password protected).
    - Compiler can generate trap door code, when compiled by certain user ID. Source code does not contain the code, but the compiler.
      - Have to analyze all the source code for all components of a system (i.e. millions of lines of code).
    - Implement: Program in bank checks if executed under specific user and deposit all account rounding errors to specific user account.
- Logic Bomb
  - Program initiates a security incident only under certain conditions.
    - Implement: Programmer write code to periodically check whether he is employed.

compiler may generate backdoor instead of sourcecode

Security

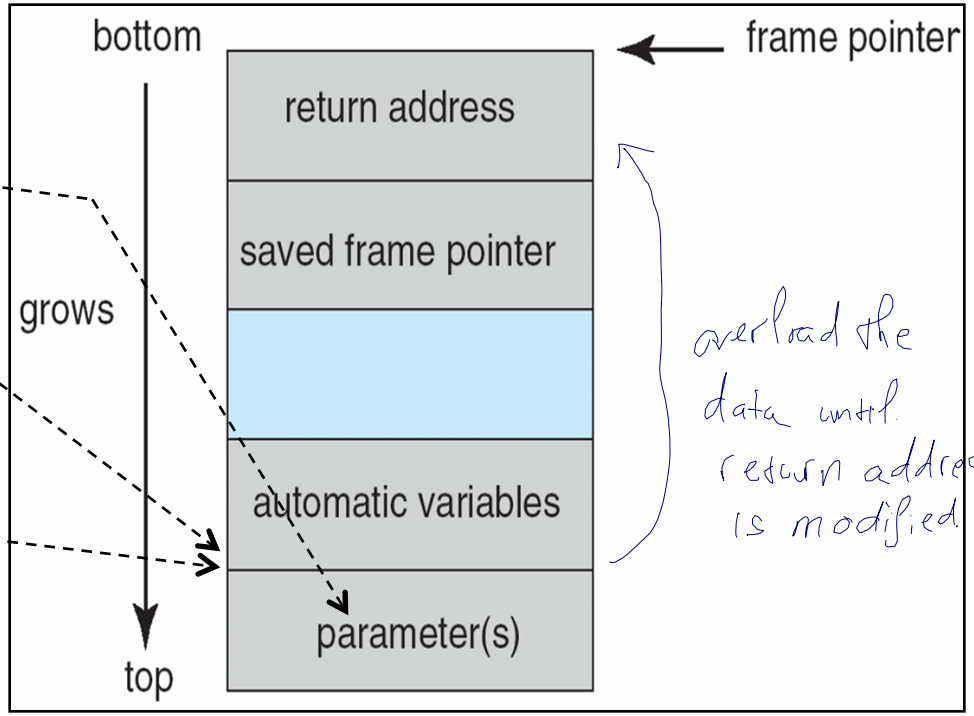
- Program Threats
- Stack and Buffer Overflow
  - Fraudulent Code Segment has unauthorized access to OS, when the executing program's stack is overwritten.

Q: how does Stack & Buffer overflow work?

```
#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;
    }
}
```

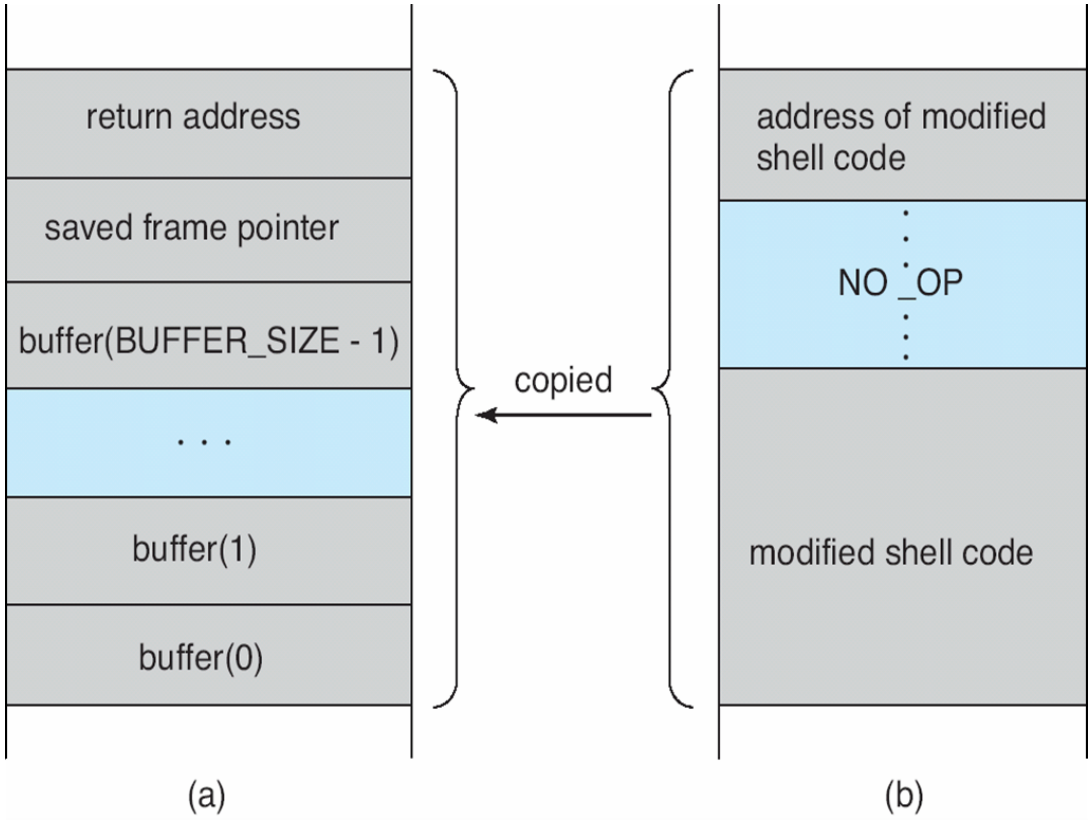
pass huge string



Security

- Program Threats
- Stack and Buffer Overflow

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



Security

- Program Threats
- Stack and Buffer Overflow
- Sun's SPARC and Solaris Operating Systems
  - Exception when executing from stack section of memory.
- Linux and Windows XP
  - AMD and Intel X86 Chip Sets
  - Hardware support bit in Page Table marking the page as nonexecutable.
    - Instructions cannot be read from the page and executed.

how these OSes prevent S& B overflow

Security

- Program Threats
- Viruses
  - Virus is a code fragment embedded in legitimate program.
    - Self-replicating and designed to "infect" other programs.
  - How do viruses work?
    - Usually a Trojan Horse, executed for other reasons, but installing the virus as its primary activity.
    - Thousands of viruses, falling into several main catagories.
    - Modify or destroy files causing system crashes and program malfunctions.

Security

- Program Threats
- Viruses (Cont)
  - Specific to CPU architecture, operating system, applications.
    - Viruses affect Windows PCs more often than UNIX/Linux systems.
    - UNIX/Linux Open Source (different distributions has different applications), designed with security for multiuser Operating System with networking capability (TCP/IP).
    - Windows initial architecture is desktop design, closed system, and networking later.
    - UNIX/Linux separation of users and root, whereas Windows user usually have administrative privilege.
    - Windows systems outnumber UNIX/Linux: Having computing community dominated by Microsoft increases threats.
      - Windows Servers affected, causing Microsoft Explorer to downloaded a browser virus that logged keystrokes, installed daemon for unrestricted access, and route spam.

reasons why viruses affect Windows more

Security

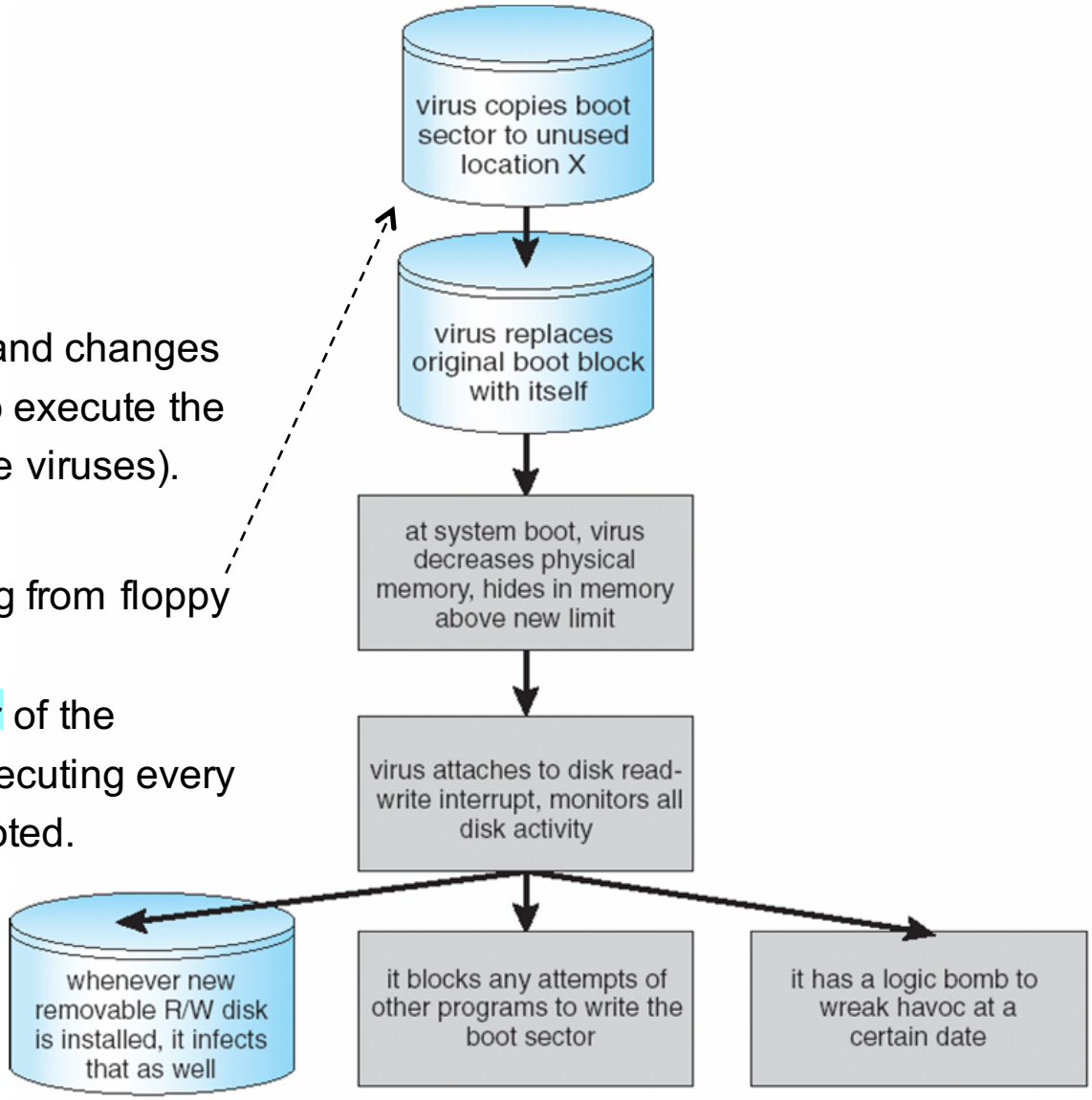
- Program Threats
- Viruses (Cont)
  - Another form of Virus transmission:
    - Microsoft Office Files with Macros (Visual Basic programs) in Word, PowerPoint, and Excel.
      - Virus use user's contact list to email itself.
      - Visual Basic Macro to reformat hard drive

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

    - Usually borne via email, with spam the most common.
      - Infected Word document propagated through email.
      - Opening email infects Computer System by using Visual Basic scripting language supported by the email system.

Security

- Program Threats
- Viruses Categories
  - File
    - Appended to the file, and changes start of the program to execute the appended file (parasite viruses).
  - Boot
    - Normally when booting from floppy or CD/DVD disk.
    - Infects the boot sector of the Operating System, executing every time the system is booted.



Security

- Program Threats
- Viruses Categories (Cont)
  - Macro
    - Written in high-level languages (Visual Basic).
    - Triggered when program capable of the macro is executed (i.e. MS Word).
  - Source Code
    - Virus spreads by looking for source code (i.e. C program), and modifies the source code to spread the virus.
  - Polymorphic
    - Changes each time its installed, so its virus signature (binary pattern of the machine code used to identify a virus) is changed.
  - Encrypted
    - Virus includes decryption code along with the encrypted virus. Virus first decrypts and then executes.

Security

- Program Threats
- Viruses Categories
  - Stealth
    - Virus maintains a copy of the original uninfected data and monitor system activity. When program (i.e. virus scan) attempts to access the affected data, the virus returns the original uninfected data.
  - Tunneling
    - Virus attempt to tunnel under anti-virus programs in order to bypass the anti-virus monitoring functions. Normally, the virus has access to the Operating System and installs itself underneath the anti-virus code in the interrupt-handler chain.
  - Multipartite
    - Infects multiple parts of a system, including boot sectors, memory and files.
  - Armored
    - Armored virus uses different mechanisms to make its detection difficult. The virus could be coded differently and compressed to change virus signature.

Security

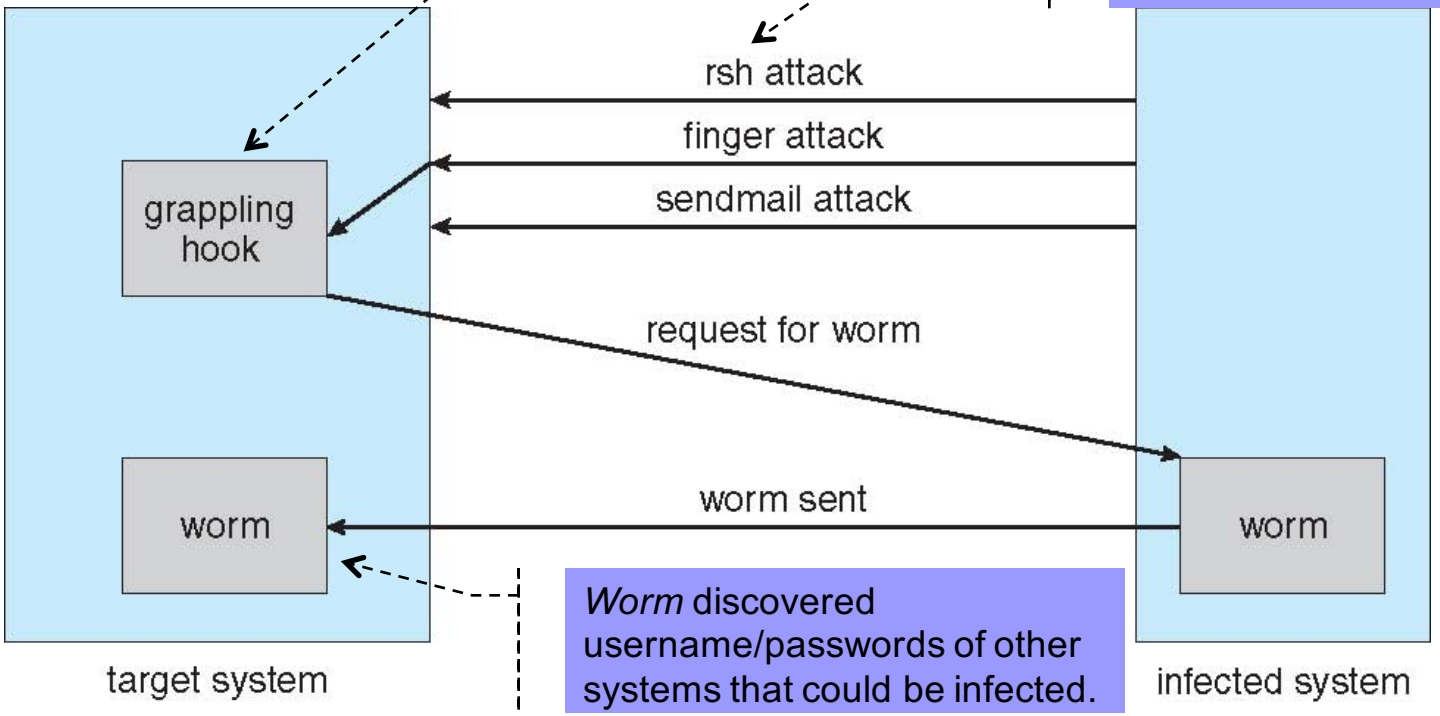
- System and Network Threats
- Program threats tries to bypass protection mechanisms of the Operating System to attach programs.
- System and Network threats creates situation where Operating System resources and files are misused.
  - Worms, Port Scanning, Denial-Of-Service, Masquerading, and Replay attacks.
- More open of an Operating System, more likely services will be exploited.
- Worms – Use spawn mechanism to over-extend system resources and cause performance issues.
  - Standalone program that copies itself.
  - Worms different from Viruses: Do not attach themselves to other files or program.

Security

- System and Network Threats
- Morris Internet worm
  - Exploited UNIX networking features (*rsh* for remote access) and bugs in *finger* and *sendmail* programs.

The stack overflow bug in *finger* utility provided a remote shell to run *rsh* utility and download the *worm* program. The *worm* program to discover username/passwords in other systems. The *sendmail* utility in debug mode was used to send and execute the *grappling hook* program.

rsh uses /etc/hosts.equiv to specify trusted hosts, where the password is not needed to login.



Worm discovered username/passwords of other systems that could be infected.

finger + stack overflow bug ⇒ rsh run. & use sendmail (debug) to send & execute grappling hook. of the worm, worm discover more user name/pwd in other system for further infection.

Security

- System and Network Threats
- **Port Scanning**
  - Automated attempt to connect to a range of ports on one or a range of IP addresses.
  - Could be used to detect whether Computer System contains a service, and the service's known bug can be exploited.
  - Frequently run from "zombie systems": Compromised systems that are being used by attackers for Denial-of-Service or Spamming.
  - Must be able to protect "inconsequential" systems as well as systems handling shared resources.

Security

- System and Network Threats
- **Denial of Service**
  - Overload the targeted computer preventing it from doing any useful work: Not at gaining information.
    - Website could download Trojan Horse Java applet that would continually pop-up windows.
  - Network based: Distributed denial-of-service (DDOS) come from multiple sites at once.
    - Difficult to prevent, uses the same mechanism as normal operations: Attack could be perceived as surge in system usage.
    - Attack on Computer System authentication that locks an account when password retry fails, could cause all authentication (valid users) to be blocked.
    - Typically launched by zombie systems.
    - Ransom asked to halt the attacks.

Security

- Review:

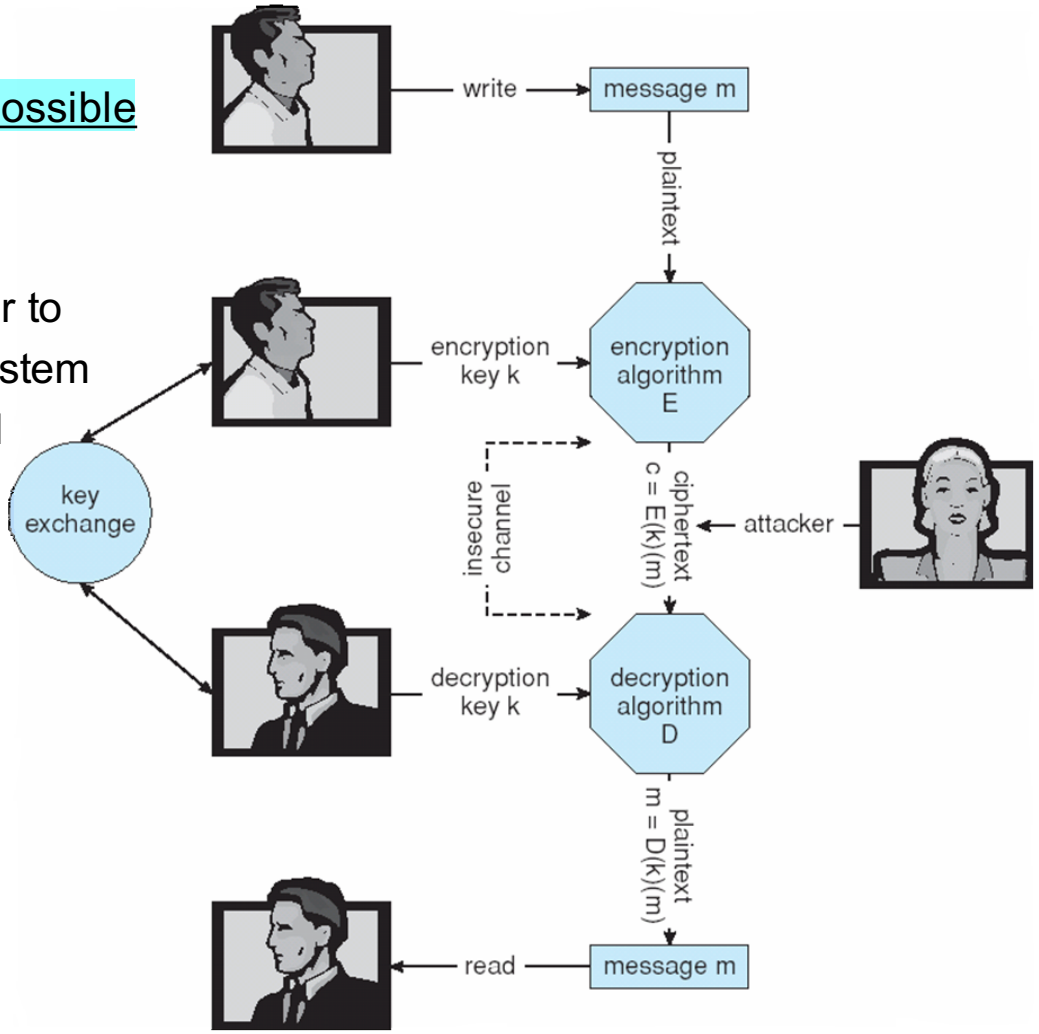
- A ***virus*** is a piece of computer code that attaches itself to a computer program. **When a computer runs the infected program, the virus launches and embeds itself in the computer's memory. It then looks for other programs or files to which it can attach.** This process repeats each time an infected program launches. A trigger activates the virus, which may be a date or the number of times a virus replicates itself, resulting in damaged software or computer files. **E-mail viruses may find an individual's address book and send copies of an infected document to everyone listed.**
- ***Worms*** are very similar to viruses in that they are computer programs that replicate functional copies of themselves and often, but not always, contain some functionality that will interfere with the normal use of a computer or a program. The difference is that, unlike viruses, worms exist as separate entities; they do not attach themselves to other files or programs. Worms are spread through email attachment (as separate entity), clicking on links on web page (separate entity), executing "legitimate" file from a friend. Virus would have been attached to a legitimate file, that is executed before the legitimate file is executed.
- ***Trojan Horse*** is a program that **appears to be useful software, but instead it compromises your security and causes a lot of damage**. Once it is downloaded and executed, the malicious code begins to work. **The difference between Trojan Horses and viruses is that Trojan Horses do not replicate or spread on their own.** They can only be transmitted intentionally via email or disk, or downloaded directly onto a PC. **Many Trojan Horses are designed to steal your login ID and password and then email them to someone** else who can make use of the account at your expense. Other Trojan Horses can **display obscene messages or delete the contents of your hard drive.**

Security

- Cryptography as a Security Tool
- Cryptography as become an important tool in Computer Security.
- Computer Security cannot completely trust the Network Packet's source and destination, because of the possibility of the packet being intercepted and modified.
  - Infeasible to build network of any scale in which source and destination address are trusted.
- Cryptography allows the use of the Network as a means for secure communication between Computer Systems.
  - Means to constrain potential senders (*sources*) and / or receivers (*destinations*) of *messages*.
- Based on secrets (**keys**) selectively distributed to Computer Systems in a network.
  - Receiver of a message use key to verify source of message.
  - Sender of a message use key to encode its message, so that only the destination with certain key can decode it.

Security

- Cryptography as a Security Tool
- Encryption
  - Means for constraining the possible receivers of a message.
- Encryption Algorithm
  - Enables the message sender to ensure only the computer system possessing the key can read the message.



Security

- Cryptography as a Security Tool
- Encryption algorithm consists of:
  - Set of K keys
  - Set of M Messages
  - Set of C ciphertexts (encrypted messages)
  - 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
- 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 $D(k)$. ← if it has decryption function D↑ compute original msg / key 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
  - Two types of encryption algorithms: Symmetric and Asymmetric

Security

Q: What is the most common used symmetric encryption algorithm ?

Q: what is symmetric encryption.?

- Cryptography as a Security Tool
- Encryption Algorithm: Symmetric Encryption
  - Same key to encrypt/decrypt: $E(k)$ can be derived from $D(k)$, and vice versa.
- DES (Data-Encryption Standard) is most commonly used symmetric block-encryption algorithm (created by US Govt).
  - 64-bit Value with 56-bit Key and perform "black-box" transformations.
  - Block Cipher: Encrypts a 64 bit block of data at a time.
  - Cipher-Block Chaining: XORed with previous ciphertext block before Encrypt.
- Triple-DES considered more secure.
  - DES algorithm repeated three times using two or three keys (168-bit Key).
  - C = E(k3)(D(k2)(E(k1)(m))).
- Advanced Encryption Standard (AES)
  - Uses Key lengths of 128, 192, and 256 bits and works on 128-bit blocks.
- twofish Algorithm
  - Uses variable length Key up to 256 bits and works on 128-bit blocks.
- RC5 Algorithm
  - Variable Keys(0-2040), transformations(0-255), and block size(32,64,128).

longer to decrypt (popular)

Q: which algo got the longest key length?

longest key length.

Security

Q: Compare block cipher v/s stream cipher.

- Cryptography as a Security Tool
- Symmetric Encryption (Cont)
- Stream Cipher: RC4 <— not block by block.
- Encrypt and Decrypt a stream of bytes or bits (not blocks).
  - Used when length of communication makes Block Cipher slow.
  - Key input into pseudo-random bit generator.
  - Keystream is infinite set of keys used for input plaintext stream.
- RC4 encrypts:
  - WEP, wireless LAN security protocol.
  - Communications between Web Browser and Web Server.
  - HTTPS connections to protect sensitive network traffic from eavesdroppers.

Security

Q: Compare Asymmetric Encryption v/s Symmetric Encryption.

- Cryptography as a Security Tool
- Asymmetric Encryption Algorithm
  - Different encryption and decryption keys.
- RSA (Rivest, Shamir, and Adleman): Block-Cipher Public-Key Algorithm.
- 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
- Asymmetric Cryptography based on Mathematical Functions, not Transformations.
  - More computational expensive.
  - Faster to encode/decode ciphertext with Symmetric Algorithms (block ciphers using series of transformations).
  - Not used for general-purpose encryption of large amounts of data.
  - Used for encryption of small amounts of data, authentication, confidentiality, and key distribution.

Security

- Cryptography as a Security Tool
- Asymmetric Encryption Algorithm (Cont)
- RSA (Rivest, Shamir, and Adleman): Block-Cipher Public-Key Algorithm.
- Computationally infeasible to derive $D(k_d, N)$ from $E(k_e, N)$.
- $E(k_e, N)$ need not be kept secret and can be widely disseminated.
  - $E(k_e, N)$ (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)
  - Encryption algorithm is $\boldsymbol{E(k_e, N)(m) = m^{k_e} \bmod N}$, where k_e satisfies $k_e k_d \bmod (p-1)(q-1) = 1$
  - The decryption algorithm is then $\boldsymbol{D(k_d, N)(c) = c^{k_d} \bmod N}$

Security

Q:. calculate encrypted msg of asymmetric algo

- Cryptography as a Security Tool
- Asymmetric Encryption Algorithm (Cont)

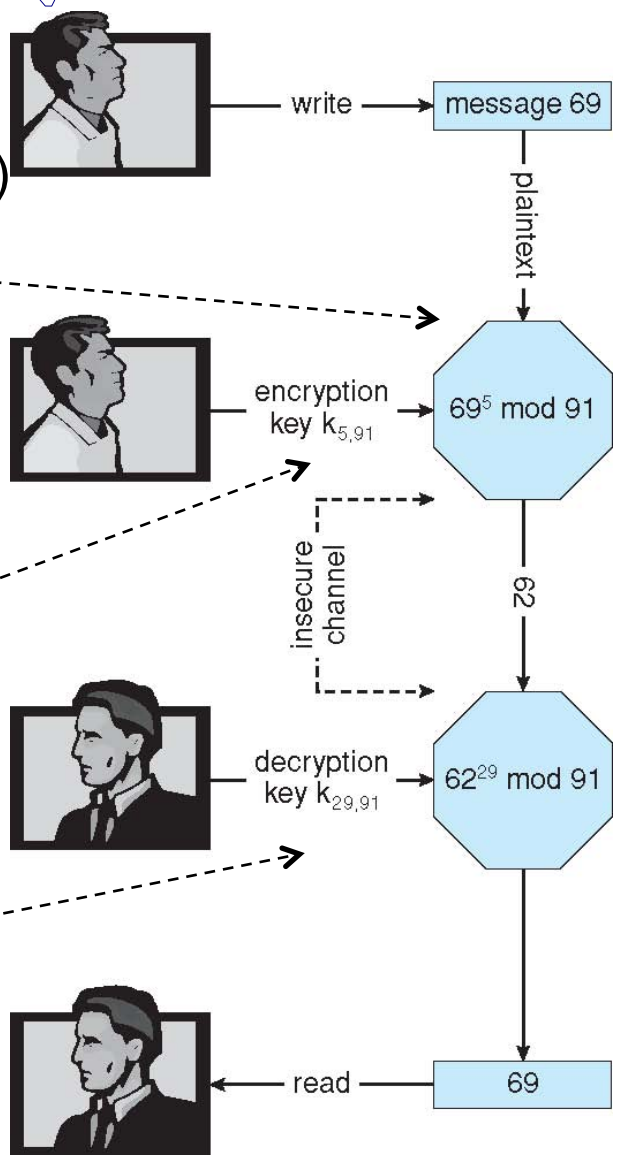
Prime Numbers: **p=7, q=13**
N=Product of 7*13 = **91**
(p-1)(q-1) = 72
Ke relative prime to 72 and <72 = **5**
Kd = KeKd mod 72 =1 = **29**

Encryption Algorithm:
E(Ke, N)(m) = mKe mod N
Ke satisfies KeKdmod(p-1)(q-1) = 1

Public Key, K<5,91>
encrypt Message 69,
result in Message 62.

Private Key, K<29,91>
decrypts Message 62,
result in Message 69.

Decryption Algorithm:
D(Kd,N)(c) = ckd mod N



Security

- Cryptography as a Security Tool
- Authentication
- Constraining set of potential senders of a message
  - Authentication is used to verify that a message or document was authored by a certain party, and that it was not altered or modified by anyone else. The process of verifying the integrity of a document.
  - Complementary to Encryption (constraint potential receivers).
- Algorithm components
  - A set K of keys
  - A set M of messages
  - A set 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 should be efficiently computable functions
  - A function $V : K \rightarrow (M \times A \rightarrow \{\text{true, false}\})$. 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 should be efficiently computable functions.

S: encryption method.
K: key
M: plain text
A: authenticated text

Security

- Cryptography as a Security Tool
- Authentication (Cont)
- For a message m, a computer can generate an authenticator $a \in A$ such that to verify authentication, $V(k)(m, a) =$ `true`, only if it possesses $S(k)$.
- A computer holding $S(k)$ can generate authenticators on messages so that any other computer possessing $V(k)$ can verify them.
- A computer not holding $S(k)$ cannot generate authenticators on messages that can be verified using $V(k)$.
- Since authenticators are generally exposed (for example, they are sent on the network with the messages themselves), it must not be feasible to derive the function $S(k)$ from the authenticators.

Security

Q: How many bits do MD5 & SHA1 produce?
How many types of Authentication Algorithms?

- Cryptography as a Security Tool
- Authentication
- Two types of Authentication Algorithms:
  - MAC (Message-Authentication Code) Algorithm.
  - Digital-Signature Algorithm.
- Involve Hash Function H(m): Creates small, fixed-size block of data (**Message Digest**, **hash value**) from *m*
  - Takes message in n-bit blocks and produce n-bit hash.
- Message Digest functions include **MD5**, which produces a 128-bit hash, and **SHA-1**, which outputs a 160-bit hash.
  - Message Digest can detect changed messages.
  - Message Digest must be encrypted if Hash Function is known, the message can be changed and the Message Digest recomputed.

is a mapping of org msg

Security

- Cryptography as a Security Tool
- Authentication
- Message-Authentication Code (MAC) Authentication Algorithm: Symmetric encryption
- Cryptographic Checksum generated from Secret Key.
- V(k) and S(k) can be derived from each other: "k" must be kept secret.
  - S(k) function for generating Authenticators from messages.
  - V(k) function for verifying Authenticators on messages.
  - MAC defines $S(k)(m) = f(k, H(m))$ hash m first, then generate authenticator for hash of m by key k.
    - Where f is a function that is one-way on its first argument
      - k cannot be derived from $f(k, H(m))$
    - Collision resistance in the hash function create unique MAC.
    - Verification Algorithm is $V(k)(m, a) \equiv (f(k,m) = a)$
    - Note that k is needed to compute both $S(k)$ and $V(k)$.

Security

Qn. Compare Digital signature algo v/s MAC algo
Qn: which Auth algo uses symmetric keys, which one uses asymmetric keys?

- Cryptography as a Security Tool
- Authentication
- Digital-Signature Algorithm: Based on Asymmetric Keys.
- $S(k_s)$ Authenticators produced are **Digital Signatures.**
- Computationally infeasible to derive $S(k_s)$ from $V(k_v)$
  - V is a one-way function.
  - k_v is the Public Key and k_s is the Private Key.

this is inverse version of encryption → sender holds public key, receiver holds private key.

- RSA Digital-Signature Algorithm:
  - Similar to the RSA encryption algorithm, but the key is reversed.
  - Digital signature of message $S(k_s)(m) = H(m)^{k_s} \bmod N$.
    - Where k_s is pair d,N, where N is prime numbers p times q.
  - Verification algorithm is $V(k_v)(m, a) \equiv (a^{k_v} \bmod N = H(m))$
    - Where k_v satisfies $k_v k_s \bmod (p-1)(q-1) = 1$

Security

- Cryptography as a Security Tool
- Authentication
- Why is Authentication needed, if it is a subset of Encryption?
  - Fewer computations (except for RSA digital signatures).
    - Large plaintext, resource and time substantially reduced.
  - Authenticator usually shorter than message.
    - Improves memory and transmission time.
  - Want authentication but not confidentiality.
    - Signed Software Signature.
  - Can be basis for **non-repudiation.**
    - Filling out electronic form as alternative to paper contracts.
    - Person filling out electronic form cannot deny it.

Security

- Cryptography as a Security Tool
- Authentication
- Key Distribution
  - Delivery of Symmetric Key to N users is huge challenge.
    - Changed frequently for security.
  - Asymmetric Key easier to manage.
    - Only one private key, use Key Rings to manage public keys.
  - Problem of authentication: Proof of who owns a public key.
    - Digital Certificate: Collection of identifying information (User Identifier/Name), a public key, and digital signature of a trusted party (Certification Authority).
    - Certification Authorities (CA Servers) database that allows users to submit and retrieve Digital Certificates.
    - Standard X.509 Digital Certificate Format.
    - CA public keys included in Web Browsers.

Security

- Cryptography as a Security Tool
- Authentication
- Implementation of Cryptography
  - Inserted into any layer in the networking ISO Reference Model.
  - SSL: Secure Socket Layer, Security at the Application Layer.
    - Asymmetric cryptography to setup symmetric encryption for a session key.
    - Web Brower used to communicate securely with Web Servers.
    - Unsecured HTTP URLs begin with "http://" and use port 80 by default.
    - Secure HTTPS URLs begin with "https://" and use port 443 by default.
  - IPSec: Network Layer Security.
    - Protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
    - Symmetric encryption and IKE Protocol for Key Exchange using X.509 Certificates.
      - IKE sets up a Security Association (SA) in the IPSec Protocol Suite.
    - Virtual Private Networks (VPN): Two IPSec Endpoints traffic are encrypted.

Security

Qn. what are the forms of user identification?

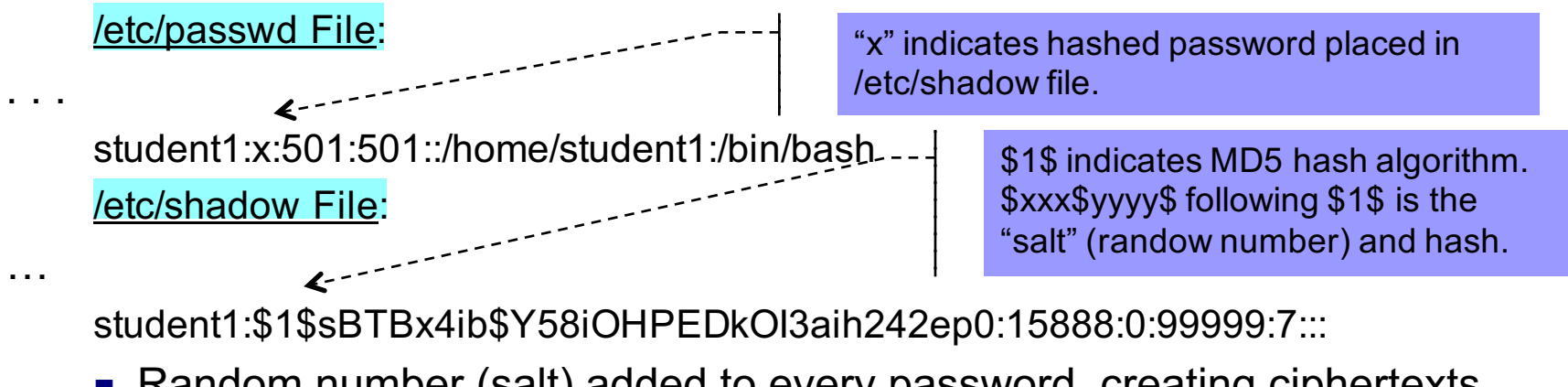
- User Authentication
- Authentication (symmetric and asymmetric encryption, authenticators) important for messages and sessions.
- Crucial to identify user: Protection Systems depend on identifying each user of the system.
  - Without User Identification, authentication for messages and session is not important.
- User Identification depends on:
  - User's possession of something (key or card).
  - User's knowledge of something (User Identifier and Password).
  - User's attribute (fingerprint, retina pattern, or signature).

Security

- User Authentication (Cont)
- Passwords: Considered a special case of either keys or capabilities (Accessing capabilities of a file).
- Passwords Vulnerabilities:
  - Using personnel information.
  - Exposure: Passwords written down.
    - Sniffing network for clear-text Username/Passwords.
  - Sharing accounts: Difficult to identify security breach.
- System Protection:
  - System enforces selection of "non-guessable" passwords.
  - Require number of characters and special characters.
    - Four digit passwords has 10,000 variations, average 5,000 guesses to crack, and computer trying every millisecond takes 5 seconds to crack.
  - Age passwords, requiring changing every 3 months.
  - New password after every session.

Security

- User Authentication
- Encrypted Passwords
  - UNIX stores encrypted passwords.
    - /etc/passwd file changed by superuser (setuid on passwd command).



    - Random number (salt) added to every password, creating ciphertexts.
  - Weaknesses of Encrypted Passwords
    - First eight characters as significant (UNIX).
    - Dictionary words not allowed as passwords.
    - Generate passwords using upper/lower/special characters.
      - Using phrase, first letter of each word is the password.

Security

Qn. what is SecurID?

- User Authentication
- One-Time Passwords
  - Password is different in each session.
  - SecurID: Commercial implementation generates an authentication code (password) at fixed intervals (60 seconds) using built-in clock and card's factory-encoded random key (seed). User entering PIN and code received by SecurID Server uses Personal Identification Number (PIN) to find user's seed and regenerates the authentication code.
  - S/Key System: Uses software calculators or code book.
    - One-time password: A user's real password is combined in an offline device with a short set of characters and a decrementing counter to form a single-use password.
    - Code book must be kept secret.
- Biometrics
  - Fingerprint Readers.
  - Convert finger ridge and calculate into sequence of numbers.

Security

Implementing Security Defenses

- **Defense in depth** is most common security theory: Many layers of security better than fewer layers.
- Security Policy (Living Document): Describes what is permissible, what is required, and what is NOT allowed.
  - Without document, users/administrators does not know what is allowed.
  - Applications must be code reviewed before being deployed.
  - Users have separate accounts (accounts NOT shared).
  - Software Port Scans performed periodically.
- Vulnerability Assessment: Compares real state of system / network compared to Security Policy. System scanned for possible vulnerabilities and fixed:
  - "Easy-to-Guess" Passwords.
  - Unauthorized programs in system directories.
  - Improper protections on user and system directories.
  - Improper protections on system data files (password file).
  - Changes to checksum values of system programs.
  - Unexpected or hidden network daemons.

Security

- Implementing Security Defenses
- Networked computers more susceptible to security attacks than standalone systems.
  - U.S. Government considers system as secure as its most far-reaching connection.
  - Scan a network for ports that have services enabled that should NOT be.
    - Determine if ports are misconfigured or needs to be updated.
  - Tools to test security can also be used to find security holes.
  - Security through obscurity? Misusing security tools.
- Securing System MUST have Intrusion Detection: Endeavors to detect attempted or successful intrusions and initiate responses.
- Techniques for Intrusion Detection: Q: What are techniques for Intrusion Detection?
  - Detection in real-time or after the fact.
  - Examine excess shell commands, system calls, network packets.
    - Off-hours or on test system.
  - Response capability: Alerting administrator, or killing a process engaged in intrusion activity.

Security

- Implementing Security Defenses (Cont)
- Detecting Intrusions have wide range of solutions.
- Intrusion-Detection Systems (IDS): Raise alarm when intrusion detected.
- Intrusion-Prevention System (IPS): Passes traffic, until intrusion is detected and traffic is blocked.
- What is an Intrusion?
  - Signature-based detection characterizes dangerous behavior patterns (Signatures) and detect when one of these behaviors occurs.
    - Analyze system input or Network Traffic .
    - Scan network packets for string "/etc/passwd/".
    - Virus-detection software which scans binaries and network packets.
  - Anomaly detection characterizes normal behavior and detect changes.
    - Monitoring daemon process for excessive system calls.
    - Monitoring shell commands for "odd" commands for a user.
    - Detecting anomalous login time for a user, late activity.
    - Can detect zero-day attacks (previously unknown intrusions).

Security

- Implementing Security Defenses (Cont)
- Anomaly Detection or Signature-Based Detection?
  - Anomaly Detection need benchmark of "normal" system behavior to be accurate.
  - Signature-Based Detection MUST continually upgrade new signatures as new viruses are detected manually.
    - Will identify ONLY known attacks that can be codified in a recognizable pattern.
- **False-Positives** (False Alarms) and **False-Negatives** (Missed Intrusions) always a problem.
  - For usability, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) must offer low False Alarm rates.
  - System Adminstrator investigating False Alarms wasteful and the System Administrator will eventually ignore the Alarms.

    Installation generating 10^6 (million) Audit Records per day.

    If 20 Audit Records reflect an actual attack, then

    20 divided by 10^6 = .00002 = .0002% represents an attack

Security

- Implementing Security Defenses (Cont)
- Virus Protection
  - Search all programs in the system for specific pattern of instructions known to make up the virus (antivirus programs has database of thousands of patterns).
  - Disinfecting virus by removing or quarantine the infected program.
  - Antivirus look for families of patterns rather than single pattern.
  - Decompress files before checking for signatures.
  - Search boot sectors, memory, inbound and outbound email files, downloaded files, removable devices (memory stick).
  - Microsoft Word documents exchanged in Rich Text Format (RTF) only, RTF cannot attach macros.
- Email Attachments
  - Avoid opening suspicious email (Love Bug virus in Visual Basic script).
- Auditing, Accounting, and Logging
  - All system-call executions can be logged for analysis of program behavior.
  - Suspicious Events:
    - User Authentication Failures (failed Logins).
  - Accounting can find performance changes and spot anomaly.

Security

- Firewalling to Protect Systems and Networks
- Firewall: Computer, Applicance, or Router that is inbetween the trusted and untrusted systems.
- Network Firewall:
  - Limits network access between two security domains.
  - Monitors and logs all connections.
  - Limits connections based on source or destination IP address, source or destination port, or direction of connection.
    - Firewall between Web Servers and Web Browers from Internet may allow ONLY HTTP protocol to pass.
  - Demilitarized Zone (DMZ):
    - Separate network into multiple domains, untrusted domain (Internet), semitrusted domain (DMZ), and secure domain (Company Computers).
    - Connections allowed:

      1) From Internet to DMZ Computers.

      2) From Company Computers to Internet.

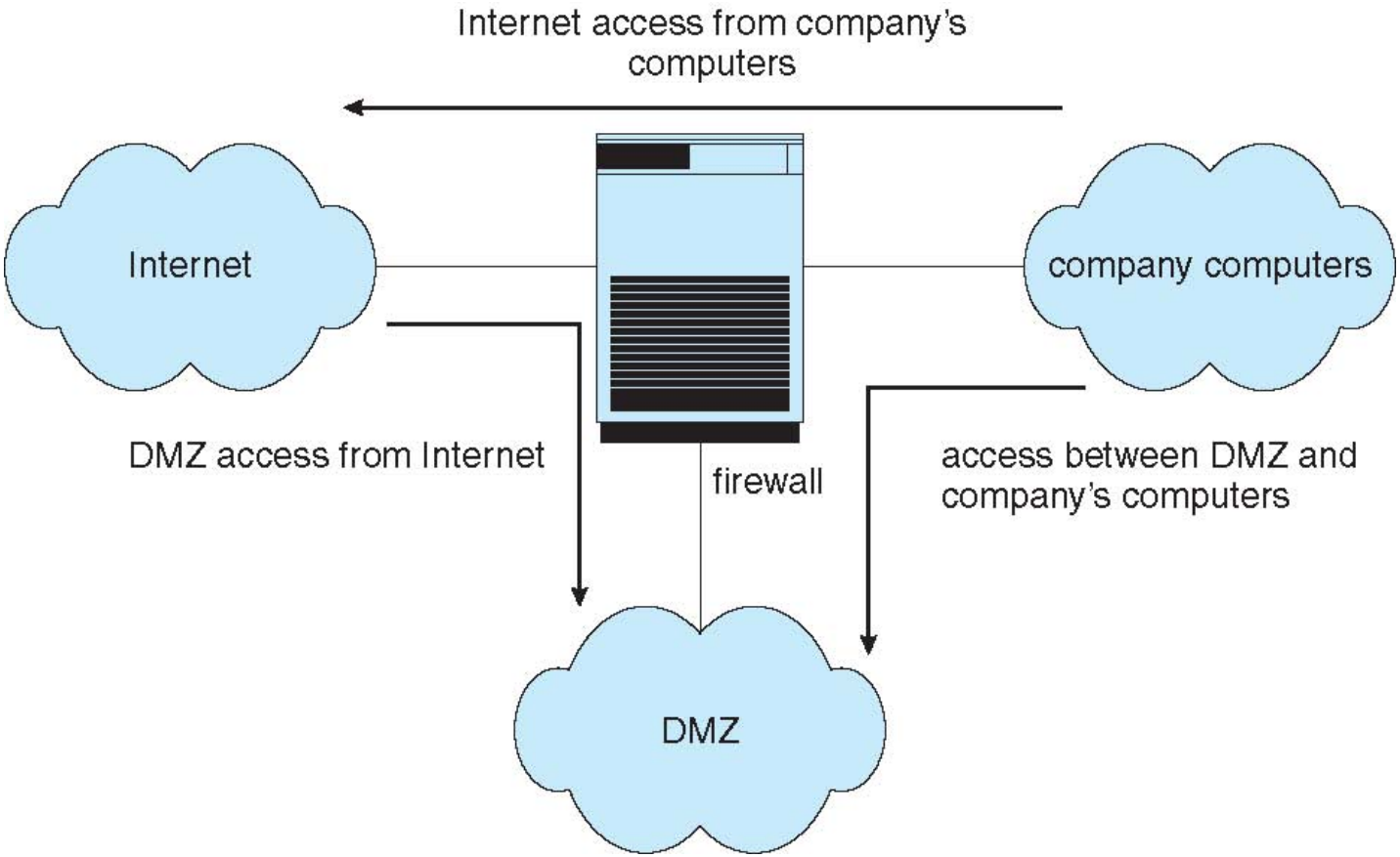
      3) NO connection from Internet or DMZ to Company Computers.

      4) Optional controlled access from Company Computer to DMZ Computer.

Qn: What types of servers are usually placed in the DMZ?

Security

- Firewalling to Protect Systems and Networks



Security

- Firewalling to Protect Systems and Networks
- Network Firewall cannot prevent tunnellling or spoofing
  - Tunneling allows attacker's 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.
- **Other Firewalls:**
  - **Personal firewall:** Software layer on given host
    - Can monitor / limit traffic to and from the host.
  - **Application Proxy Firewall:** Understands application protocol and intercepts traffic between the application and the network.
    - Application Proxy accepts SMTP connection (to SMTP Server) and initiates connection to SMTP Server.
    - Monitor traffic as it forwards traffic: Dropping illegal commands and attempts to exploit known SMTP problems.
  - **System-call Firewall:** Monitors all important system calls and apply rules to them (i.e., this program can execute limited system call).
    - Process can be prevented from spawning other processes.

Security

- Computer-Security Classification
- U.S. Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) outlines four divisions of computer security: **A**, **B**, **C**, and **D**.
- Trusted Computer Base (TCB): Total of all protection systems within a computer system (hardware, software, firmware) that correctly enforce a security policy.
- **D** – Minimal security:
  - Failed to meet requirements of A, B, or C. (MS-DOS and Windows).
- **C** – Provides discretionary protection through use of audit capabilities.
  - Divided into **C1** and **C2**
    - **C1** identifies cooperating users with the same level of protection. Allows users to protect private data and prevents other users from reading/destroying data. Users must identify themselves, username/password, before they start activities. Most UNIX systems.
    - **C2** allows user-level access control. Individual-level access control can be specified to the level of a single individual. Windows NT systems.

Security

- Computer-Security Classification (Cont)
- **B** – All the properties of **C**, however each object may have unique sensitivity labels
  - Divided into **B1**, **B2**, and **B3**
  - **B1** maintains security levels for selected objects in the Computer System. Clearance and authorization of individual users (users at confidential level cannot access a file at the secret level).
  - **B2** maintains security level to all system resources.
  - **B3** maintains access-control list that denote users or groups not granted access to named objects. Security Administrator role is defined.
- **A** – Uses formal design and verification techniques to ensure security
  - Functionally equivalent to B3 classification.
  - Uses formal design and verification techniques, granting high degree of assurance that the TCB has been implemented correctly.

Security

- Windows XP
- Security Access Token created for each User: Security ID of the User, Security ID of the Member Groups, Special Privileges.
  - Privileges to back-up Files and Directories.
  - Privilege to shutdown Computer, Logout, Change System Clock.
  - Process started by User has the privileges of the User's Security Token.
  - Access to System Objects permitted by User's Security Token.
- Subject concept: Track and manage permissions for each program.
  - Composed of User's Security Token and program access rights.
  - Assigned a Security Context based on Security Access Token of the User.
- Windows XP Client-Server Model: Server Subject is a protected server process that uses the security context of the client (user).
- Windows Security Descriptor for objects: Owner Security ID, Group Security ID, Access-Control List of Users or Group with access.
  - Object are Container Objects (Directories) or Noncontainer Objects (Files).

Summary

- Protection is an internal problem.
- Security must consider the Computer System and environment within which the system is used.
- Data in Computer System must be protected from unauthorized access, malicious destruction or alteration.
- Threats on program threats and threats on System and Network.
  - Worms, Viruses, Trojan Horse, Denial-of-Service.
- Network Computer Systems Authentication: Trusted environment (messages and sessions).
  - Encryption limits receivers. Authentication limits senders.
  - Symmetric encryption requires a shared key (DES, RC4).
  - Asymmetric encryption provides a public key and a private key (RSA).
  - Authentication limits senders (MD5, digital-signature, Certification Authorities)
- User Authentication: identify legitimate users of a system.
  - Authentication Methods: One-time passwords, Pin and hardware calc (SecurID).
- Methods of preventing or detecting security incidents.
  - Intrusion Detection System, Intrusion Prevention System, antivirus software.