Chapter - Seven

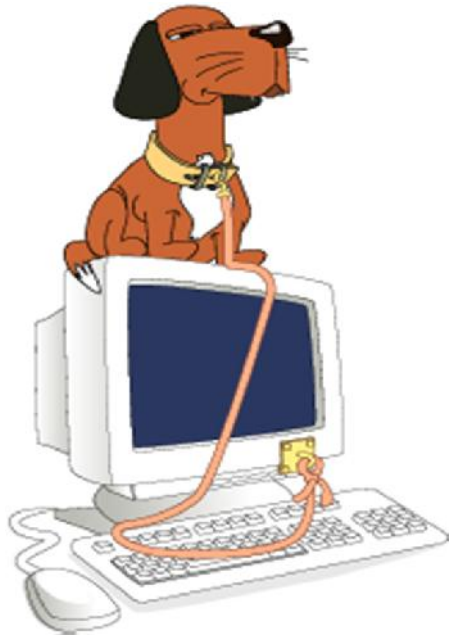
Operating System Security and protection

Outline

- Security definition
- Security features in operating system
- Operating system Security attack types
- Suggestions to secure operating system
- Cryptography
- OS Authentication methods
- Authorization
- Firewall and proxy server
- Intrusion Detection System (IDS)

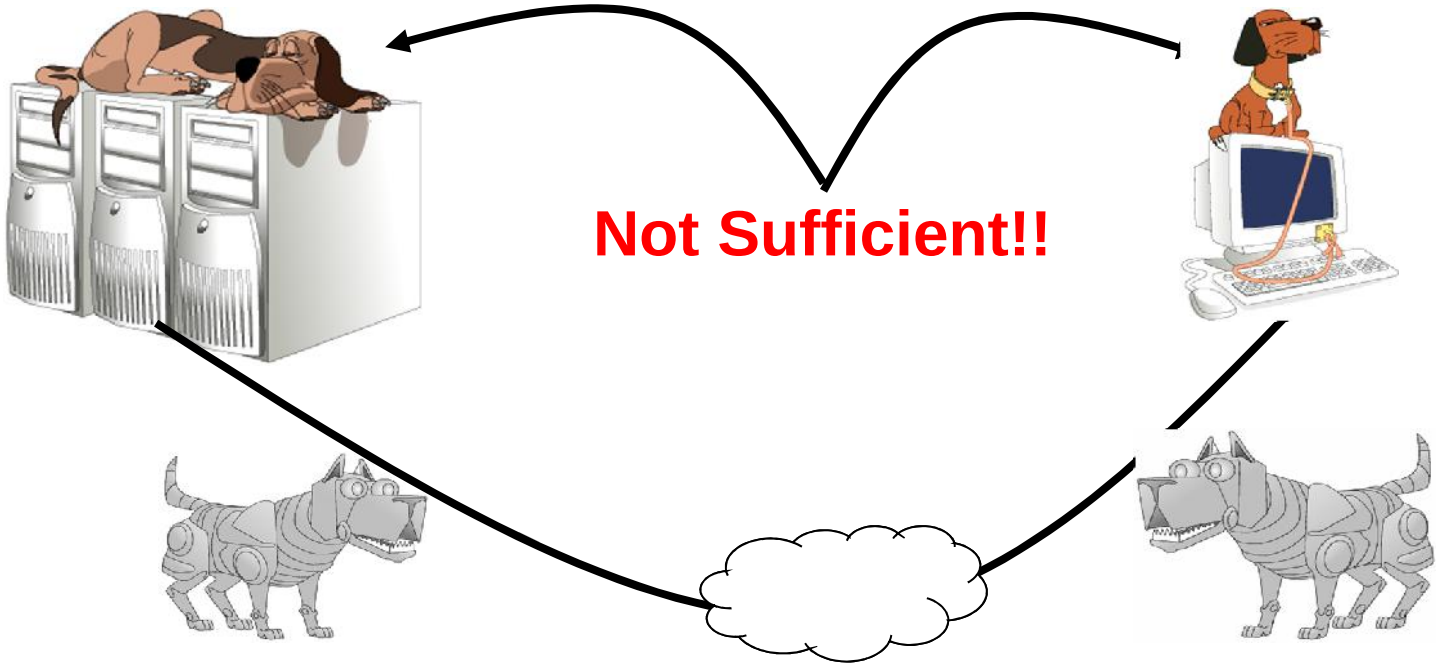
Computer Security

- Computer security is about provisions and policies adopted to protect information and property from theft, corruption, or natural disaster
  - while allowing the information and property to remain accessible and productive to its intended users.
- security of computers against intruders (e.g.,hackers) and malicious software (e.g., viruses).



Network Security

- Network security on the other hand deals with provisions and policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources.



Why need security at the OS level?

- No more standalone computer system environments.
- Any system can be globally accessible through a set of vast inter and intra-network connections.
- Transition motivated by the need to work remotely,
  - convenience in accessing personal records, online shopping etc.
- A single security loophole in the OS design and implementation known to a malicious attacker could do serious damage.

Security in Operating System

- Security refers to providing a protection system to computer system resources such as:
  - CPU, memory, disk
  - software programs and
  - most importantly data/information stored in the computer system.
- So a computer system must be protected against
  - unauthorized access by users and
  - malicious access to system including viruses, worms etc...

Who are the attackers?

- Vandals (Hackers, crackers) driven by intellectual challenge.
- Insiders: employees or customers seeking revenge or gain informal benefits
- Natural disasters: flooding, fire, storms, earthquake...
- Criminals seeking financial gain.
- Organized crime seeking gain or hiding criminal activities.
- Organized terrorist groups or nation states trying to influence national policy.
- Foreign agents seeking information (spying) for economic, political, or military purposes.
- Tactical countermeasures intended to disrupt military capability.
- Large organized terrorist groups
- Cyber attacks

What are the vulnerabilities?

- Physical vulnerabilities (Eg. Computer can be stolen)
- Natural vulnerabilities (Eg. Earthquake)
- Hardware and Software vulnerabilities (Eg. Failures)
- Media vulnerabilities (Eg. Hard disks can be stolen)
- Communication vulnerabilities (Ex. Wires can be tapped)
- Human vulnerabilities (Eg. Insiders)
- Poorly chosen passwords
- Software bugs (non reliability of software)
  - buffer overflow attacks

What are the vulnerabilities?...

- Automatically running active content: active-x, scripts, Java programs (applet)
- Open ports: telnet, mail
- Incorrect configuration
  - file permissions
  - administrative privileges
- Untrained users/system administrators
- Trap doors (intentional security holes)
- Unencrypted communication
- Limited Resources (i.e. TCP connections)

Security features in Operating System

- An operating system manages and controls access to hardware components
- Older operating systems focused on ensuring data confidentiality
- Modern operating systems support four basic functions
  - Positively identify a user
  - Restrict access to authorized resources
  - Record user activity
  - Ensure proper communications with other computers and devices (sending and receiving data)

Security features in ordinary OS

- Authentication of users
  - password comparison
- Protection of memory
  - user space, paging, segmentations
- File and I/O device access control
  - access control matrix
- Allocation & access control to general objects
  - table lookup

Security features in ordinary OS...

- Enforcement of sharing resources
  - To preserve integrity, consistency (critical section)
- Fair service
  - no starvation and deadlock
- Inter-process communication & synchronization
  - Shared variable (e.g, using semaphores)
- Protection of data
  - encryption, isolation

Security features of Trusted OS

- Identification and Authentication
- Mandatory (enforce multilevel security by classifying the data and users into various security classes) and
- Discretionary Access Control (grant privileges to users)
- Object use and reuse protection (Subject and object)
- Anti-virus scan
- Accountability and Audit (security log)
- Firewall
- Intrusion detection (patterns of normal system usages, anomalies)

Hardening the OS

- Default OS configurations are for ease of use
- Measures have to be done at all stages
  - Installing and patching
  - Configuring
    - Remove unnecessary applications, services and protocols
    - Users, groups, controls and privileges
  - Install additional software (anti-virus, firewall, intrusion detection system, etc.)
  - Test security

Operating system Security attack types

Malware Attack:

- A generic term for software that has malicious purpose
- is software that is intentionally included or inserted in a system for a harmful purpose.

- Different forms of malicious software (malware)
- Intended to
  - Cause distress to a user
  - Damage files or systems
  - Disrupt normal computer and network functions
  - Examples
    - Viruses, worms
    - Logic bomb
    - Trojan horses
    - Spy-wares
    - New ones: Spam/scam, Slammer, Nimda, e-payment frauds, etc.

Name	Description
Virus	Attaches itself to a program and propagates copies of itself to other programs
Worm	Program that propagates copies of itself to other computers
Logic bomb	Triggers action when condition occurs
Trojan horse	Program that contains unexpected additional functionality
Backdoor (trapdoor)	is a secret entry point into a program that allows someone that is aware of the backdoor to gain access without going through the usual security access procedures.
Auto-rooter	Malicious hacker tools used to break into new machines remotely
Kit (virus generator)	Set of tools for generating new viruses automatically
Spammer programs	Used to send large volumes of unwanted e-mail
Flooders	Used to attack networked computer systems with a large volume of traffic to carry out a denial of service (DoS) attack
Keyloggers	Captures keystrokes on a compromised system
Zombie	Program activated on an infected machine that is activated to launch attacks on other machines
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access

Malware Attack...

- Malicious software can be divided into two categories:
- those that need a host program
  - fragments of programs that cannot exist independently of some actual application program, utility, or system program.
  - Viruses and logic bombs are examples.
- those that are independent
  - are self-contained programs that can be scheduled and run by the operating system.
  - Worms and zombie programs are examples.

Malware Attack...

- Malicious software can also be divided into two categories:
  - software threats that do not replicate
    - are programs or fragments of programs that are activated by a trigger.
    - Examples are logic bombs and zombie programs.
  - those that replicate
    - consist of either a program fragment or an independent program that, when executed, may produce one or more copies of itself to be activated later on the same system or some other system.
    - Viruses and worms are examples.

Malware Attack...

- Viruses
  - A malicious code that replicates and hides itself inside other programs usually without your knowledge.
  - A virus is a piece of software that can "infect" other programs by modifying them.
  - Similar to biological virus: Replicates and Spreads
  - Can do serious damage such as erasing file...

- Worms
  - A worm is a program that can replicate itself and send copies from computer to computer across network connections.

More on Virus

During its lifetime, a typical virus goes through the following four phases:

- Dormant phase: The virus is idle.
  - The virus will eventually be activated by some event, such as a date, the presence of another program or file, or the capacity of the disk exceeding some limit.
- Propagation phase: The virus places an identical copy of itself into other programs or into certain system areas on the disk.
  - Each infected program will now contain a clone of the virus, which will itself enter a propagation phase.
- Triggering phase: The virus is activated to perform the function for which it was intended.
  - As with the dormant phase, the triggering phase can be caused by a variety of system events
- Execution phase: The function is performed.
  - The function may be harmless, such as a message on the screen, or
  - damaging, such as the destruction of programs and data files.

More on Virus...

Types of viruses

- Parasitic virus: The traditional and still most common form of virus.
  - A parasitic virus attaches itself to executable files and replicates
- Memory-resident virus: resides in main memory as part of a resident system program.
  - From that point on, the virus infects every program that executes.
- Boot sector virus: Infects a master boot record or boot record and spreads when a system is booted from the disk containing the virus.
- Stealth virus: A form of virus explicitly designed to hide itself from detection by antivirus software.
  - a virus that uses compression so that the infected program is exactly the same length as an uninfected version.

More on Virus...

Types of viruses...

- Polymorphic virus: A virus that mutates with every infection, making detection by the "signature" of the virus impossible.

- Metamorphic virus: As with a polymorphic virus, a metamorphic virus mutates with every infection.
  - The difference is that:
  - a metamorphic virus rewrites itself completely at each iteration, increasing the difficulty of detection.
  - Metamorphic viruses my change their behavior as well as their appearance.

Malware Attack...

- Logic bomb
  - The logic bomb is code embedded in some legitimate program that is set to "explode" when certain conditions are met.
  - Examples of conditions that can be used as triggers for a logic bomb are:
    - the presence or absence of certain files,
    - a particular day of the week or date, or
    - a particular user running the application.
  - Once triggered, a bomb may:
    - alter or delete data or entire files,
    - cause a machine halt, or
    - Do some other damage

Malware attack...

Trojan Horse

- Any malicious program which misinterprets itself as useful, or interesting in order to convince a victim to install it.
- The program claims to do one thing
  - (it may claim to be a game) but instead does damage when you run it (it may erase your Hard Disk).
- Trojan horse programs do not replicate themselves like a virus,
- Such program traps user login credentials and stores them to send to malicious user

Spyware

- Software placed on a computer
  - typically without user's knowledge
  - reports back information about user's activities
- Some operate through monitoring cookies

- A software that literally spies on what you do on your computer.
  - Example: Simple Cookies, mobile codes , web crawlers, Xerox
  - Types of information that is gathered includes the Websites visited, browser and system information, and your computer IP address.

Spam (junk mail)

- Filling e-mail inboxes with unwanted junk mail.
- Anyone using e-mail is essentially guaranteed to receive spam
- How spammers get your mail.
  - Web search
  - Sending test emails
  - Exchange or buy from other spammers

Malware attacks...

- Infection mechanisms
  - First, the virus should search for and detect objects to infect
  - Installation into the infectable object
    - Writing on the boot sector
    - Add some code to executable programs
    - Add some code to initialization/auto-executable programs
- Trigger mechanism
  - Date
  - Number of infections
  - First use
- Effects: It can be anything
  - A message
  - Deleting files
  - Formatting disk
  - Overloading processor/memory
  - Etc.

Suggestions to secure your computer/OS

- Use anti-virus software.
- Depending on the vendor, the antivirus software may also contain anti-spyware tools, anti-spam filtering, a personal firewall, and more.
- Update your computer regularly.
- Be careful with the email attachments
  - Safe: .jpg .bmp .pdf .txt ....
  - Unsafe: .exe .doc .xls .ppt ...
- Use firewall to protect you from malware attack.
- Use IDS...

Threat Monitoring

- Check for suspicious patterns of activity – i.e., several incorrect password attempts may signal password guessing.
- Audit log – records the time, user, and type of all accesses to an object; useful for recovery from a violation and developing better security measures.
- Scan the system periodically for security holes; done when the computer is relatively unused.

Threat Monitoring (Cont.)

- Check for:
  - Short or easy-to-guess passwords
  - Unauthorized set-uid programs
  - Unauthorized programs in system directories
  - Unexpected long-running processes
  - Improper directory protections
  - Improper protections on system data files
  - Dangerous entries in the program search path (Trojan horse)
  - Changes to system programs: monitor checksum values

Protecting an OS from Malicious Software

- Install updates
- Use malicious software scanners
- Back up systems and create repair disks
- Create and implement organizational policies

Installing Updates for Windows

- Windows Update
  - Provides access to patches that are regularly issued/released
- Service packs
  - Address security issues and problems affecting stability, performance, or operation of features included with the OS

- Patch This fixes something small and is usually quick to download and install.
- Rollup This might include a group of patches for a program.
- Update Updates might add or fix features in your program or fix an earlier patch.
- Service Pack This is the biggie; the one you read about in the news when Microsoft releases some big service pack.

Protecting an OS from Malicious Software

- Install updates
- Use malicious software scanners
- Back up systems and create repair disks
- Create and implement organizational policies

Using Malicious Software Scanners

- Effective way to protect operating system
- Scan systems for virus, worms, and Trojan horses
- Often Called Virus Scanners
- Functions of anti-viruses
  - Identification of known viruses
  - Detection of suspected viruses
  - Blocking of possible viruses
  - Disinfection of infected objects
  - Deletion and overwriting of infected objects

Suggestions to fight spam

- Never reply junk emails
- Do not open any files or executable attachments
- Immediately DELETE the malicious email
- Don’t post your actual email address in the website.
- Norton, McAfee, and many more include spam as one of the threats that they protect against.
- Can use spam filtering applications

Virus Scanning Software...

OS Security Services

- Control panel: main component of operating system security environment
- Used to gain access to the OS and its features
- Include
  - User authentication
  - Remote access
  - Administration tasks
  - Password policies

Cryptography

- Purpose of Cryptography:
  - Secure stored information - regardless if access obtained
  - Secure transmitted information - regardless if transmission has been monitored

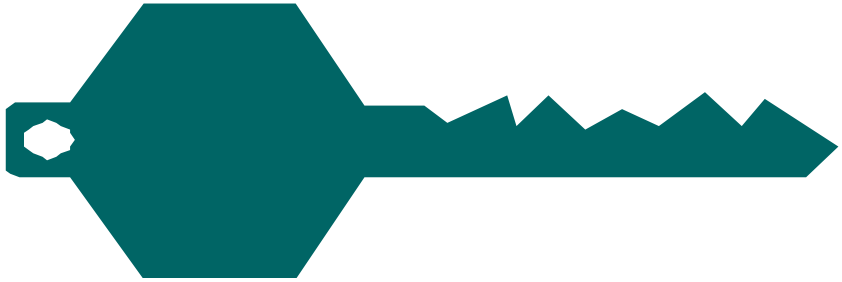
Cryptography

- Cryptography has five components:
  - Plaintext: This is what you want to encrypt.
  - Ciphertext: The encrypted output.
  - Enciphering or encryption: The process by which plaintext is converted into ciphertext.
  - Encryption algorithm: The sequence of data processing steps that go into transforming plaintext into ciphertext.
  - Secret Key: is used to set some or all of the various parameters used by the encryption algorithm.
  - Deciphering or decryption: Recovering plaintext from ciphertext.
  - Decryption algorithm: The sequence of data processing steps that go into transforming ciphertext back into plaintext.

Keys

- A key can be thought of as simply a collection of bits
- The more bits, the stronger the key
- Keys are tied to specific encryption algorithms
- Lengths vary depending on the encryption algorithm
  - e.g. 128 bits is long for some algorithms, but short for others

1 0 1 1 1 1 0 1 1
1 0 1 1 0 0 1 0 1

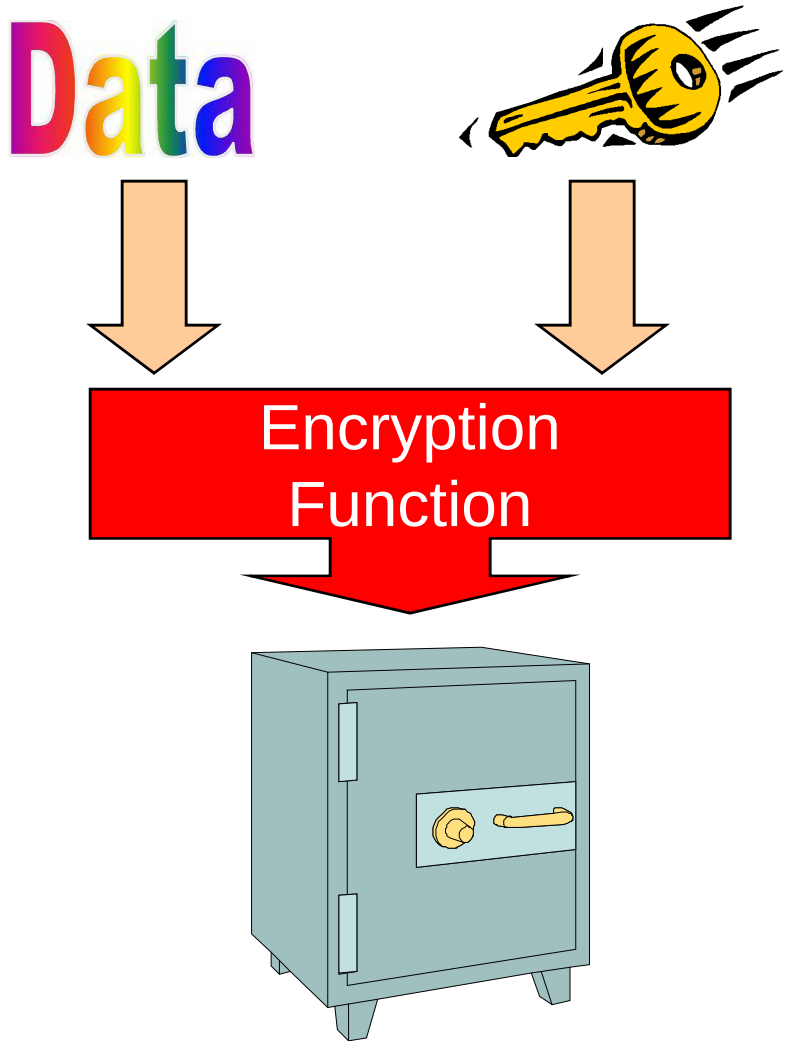


Cryptography

- Encryption Overview
  - Plain text is converted to cipher text by use of an algorithm and key.
    - Algorithm is publicly known
    - Key is held private
  - Three Main Categories
    - Secret Key
      - single key is used to encrypt and decrypt information
    - Public/Private Key
      - two keys are used: one for encryption (public key) and one for decryption (private key)
    - One-way Function
      - information is encrypted to produce a “digest” of the original information that can be used later to prove its authenticity

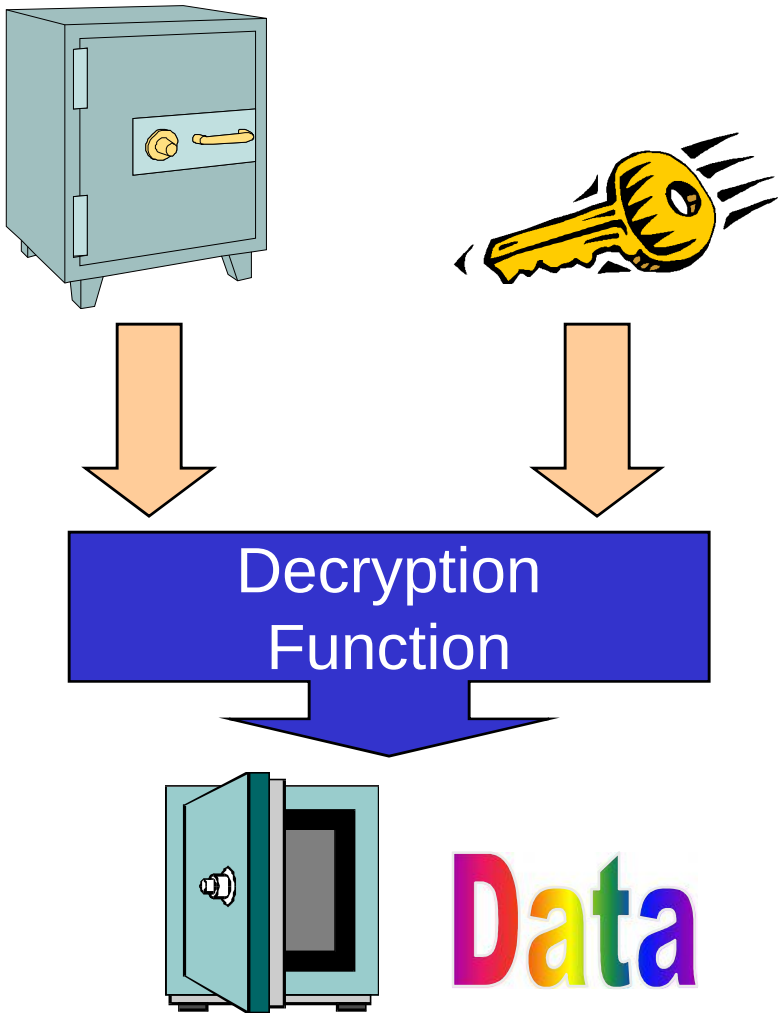
Encryption

- Encryption is the process of taking some data and a key and feeding it into a function and getting encrypted data out
- Encrypted data is, in principle, unreadable unless decrypted



Decryption

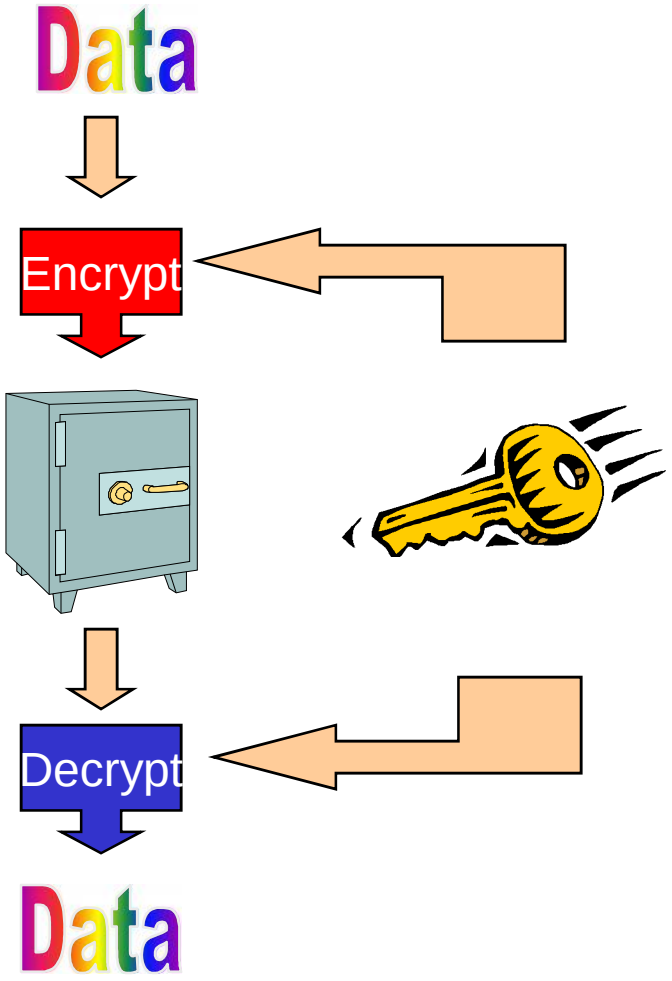
- Decryption is the process of taking encrypted data and a key and feeding it into a function and getting out the original data
  - Encryption and decryption functions are linked



Encryption Techniques

Symmetric Encryption

- Encryption and decryption algorithms that use the same key are called symmetric
  - In this case everyone wanting to read encrypted data must share the same key
- Sender and receive have the same secret key that will encrypt and decrypt plain text.
- Strength of encryption technique depends on key length



Encryption Techniques...

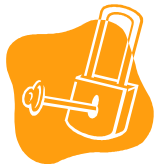
- Secret Key (Symmetric)
  - Known symmetrical algorithms
    - Data Encryption Standard (DES)
      - 56 bit key
    - Triple DES, Double DES
      - 168 bit key
    - Advanced Encryption Standard (AES)
      - 128, 192,256
    - RC2, RC4, RC5
      - variable length up to 2048 bits
    - IDEA - basis of PGP
      - 128 bit key
    - Blowfish
      - variable length up to 448 bits

Encryption Techniques...

Asymmetric Encryption

- Encryption and decryption algorithms that use a key pair are called asymmetric
  - Keys are mathematically linked
- Most common algorithm is the RSA (Rivest Shamir Adelman) algorithm with key lengths from 512 to 1024 bits. Diffie-Hellman (DH)

ENCRYPTION



Message 1

Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment.

Encrypted Message 1

9a46894[illegible]5be49f0b9cab28d755aaa9cd985
71b275bbb0a[illegible]5e6931e856ca3e5e569[illegible]
dd135285482

Same Key
SYMMETRIC

Message 2

The Internet knows no geo[illegible]
It has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.

Encrypted Message 2

a5[illegible]61a770f947ca856cd675463f1c95a
9a2b[illegible]f80830c87f5715f5f59334[illegible]
dd7e9[illegible]
7c[illegible]

Different Keys
[Keys of a pair – Public and Private]
ASYMMETRIC
[PKI]

DECRYPTION

Encrypted Message 1

9a46894335be49f0b9cab28d755aaa9cd98571b
275bbb0adb405e6931e856ca3e5e569edd13528
5482

Message 1

Central to the growth of e-commerce and e-governance is the issue of trust in electronic environment.

Encrypted Message 2

a520eecb61a770f947ca856cd675463f1c95a9a2b
8d4e6a71f80830c87f5715f5f59334978dd7e97da
0707b48a1138d77ced56feba2b467c398683c7db
eb86b854f120606a7ae1ed934f5703672adab0d7
be66dccde1a763c736cb9001d0731d541106f50b
b7e54240c40ba780b7a553bea570b99c9ab3df13
d75f8ccfdddeaaf3a749fd1411

Message 2

The Internet knows no geographical boundaries. It has redefined time and space. Advances in computer and telecommunication technologies have led to the explosive growth of the Internet. This in turn is affecting the methods of communication, work, study, education, interaction, leisure, health, governance, trade and commerce.

Encryption Techniques...

- One-Way Function
  - non-reversible “quick” encryption
  - produces a fixed length value called a hash or message digest
  - used to authenticate contents of a message
  - Common message digest functions
    - MD4 and MD5
      - produces 128 bit hashes
    - SHA
      - produces 160 bit hashes

Cryptographic Services Allow

- Digital Signatures
  - sign messages to validate source and integrity of the contents
- Digital Envelopes (combination of symmetric/asymetric)
  - secure delivery of secret keys
- Message Digests
  - short bit string hash of message
- Digital Certificates
  - used to authenticate: users, web sites, public keys of public/private pair, and information in general
- Secure Channels
  - Encryption can be used to create secure channels over private or public networks

Cryptography using openSSL

1. Presentation of OpenSSL

Protocol SSL

- The SSL protocol (Secure Socket Layer) was developed by Netscape to allow client/server applications to communicate safely.

- TLS (Transport Layer Security) is an evolution of SSL proposed by the IETF.

- SSL is a protocol placed between TCP/IP and applications using the TCP protocol (it is basically at the “session layer” of the OSI).

Cryptography using openSSL...

1. Presentation of OpenSSL

openSSL

- openSSL is a toolbox for cryptographic material implementing SSL and TLS. It gives:

1. A library to program in C allowing to construct client/server applications using SSL/TLS
2. A command line (openssl) allowing
   - Creation of RSA, DSA keys
   - Creation of X509 certificates
   - Digest computation (MD5, SHA, ...)
   - Ciphering and Deciphering (DES, IDEA, RC2, RC4, Blowfish ...)
   - Tests of client/server SSL/TLS
   - Signature and ciphering of mails (S/MIME) Secure Multi-Purpose Internet Mail Extension

Cryptography using openSSL...

1. Presentation of OpenSSL

openSSL

- To know everything about OpenSSL: **`man openssl`**
- The general syntax of openssl is:

  `openssl> <command> <options>`

Cryptography using openSSL...

2. Symmetric encryption with openSSL

Basic commands

- To encrypt a file with openssl using a DES encryption:

```
openssl> enc -des3 -in file -out file2
```

- The result is in the file **file2**.
- To decrypt the same file:

```
openssl> enc -des3 -d -in file2 -out filedecrypted
```

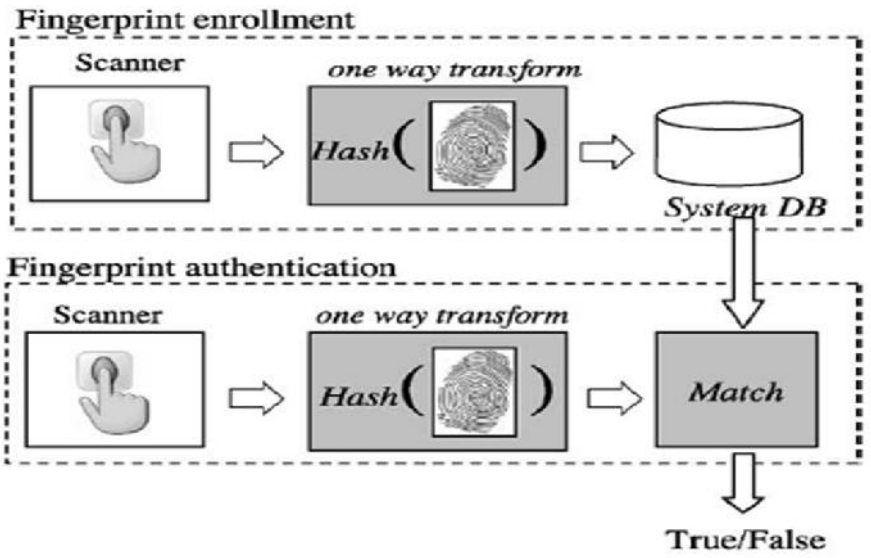
(here, **file** and **filedecrypted** should contain the same content)

OS Authentication Methods

- Authentication:
  - Verifies user identity; something a person is, has, or does.
  - Permits access to the operating system
  - Use of biometrics, passwords, passphrase, token, or other private information.
  - Strong Authentication is important
- Physical authentication:
  - Allows physical entrance to company property
  - Magnetic cards and biometric measures
- Digital authentication:
  - verifies user identity by digital means

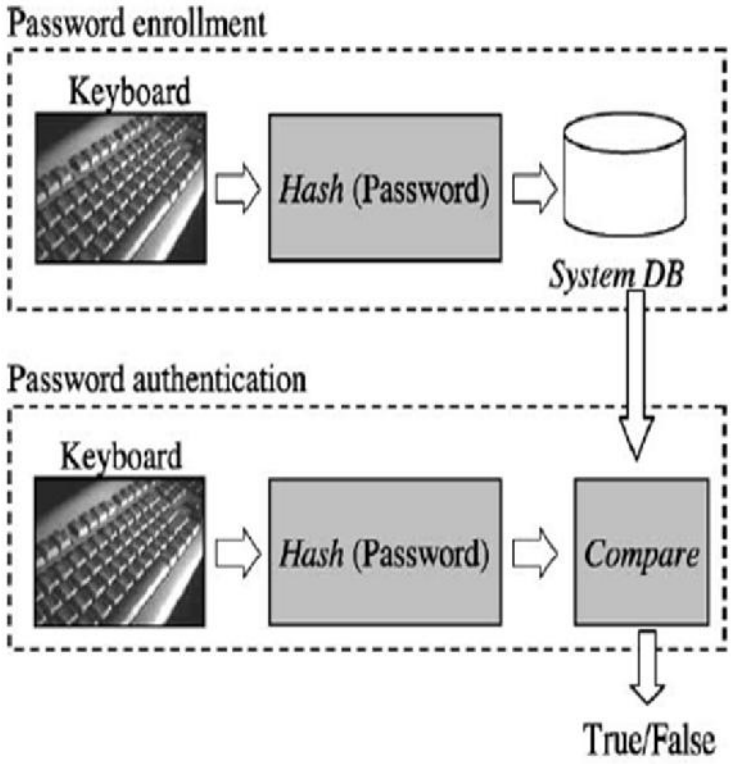
OS Authentication Methods...

- Biometrics
- Verifies an identity by analyzing a unique person attribute or behavior (e.g., what a person “is”).
- Most expensive way to prove identity, also has difficulties with user acceptance.
- Most common biometric systems:
  - Fingerprint
  - Palm Scan
  - Hand Geometry
  - Iris Scan
  - Voice Print
  - Facial Scan



OS Authentication Methods...

- Passwords
  - User name + password most common identification, authentication scheme.
  - Weak security mechanism, must implement strong password protections
- Passphrase
  - Is a sequence of characters that is longer than a password.
  - Takes the place of a password.
  - Can be more secure than a password because it is more complex.



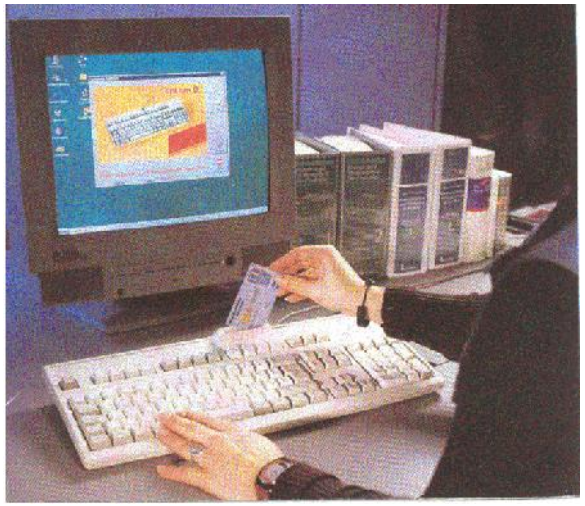
OS Authentication Methods...

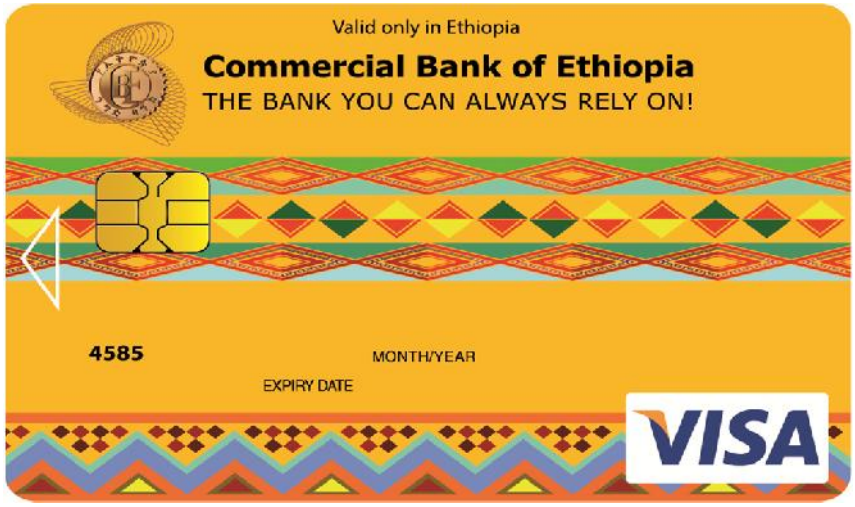
- Digital certificates: digital passport that identifies and verifies holder of certificate

- Kerberos:
  - Developed by MIT
  - Uses tickets for authentication purposes

OS Authentication Methods...

- Digital card:
  - Also known as a security card or smart card
  - Similar to a credit card; uses an electronic circuit instead of a magnetic strip
  - Stores user identification information





OS Authentication Methods...

Digital token (security token)

- Small electronic device
- Displays a number unique to the token holder; used with the holder's PIN as a password

- They are similar to smart cards in functionality as
  - Key is generated inside the token.
  - Key is highly secured as it doesn't leave the token.
  - Highly portable.
  - Machine Independent.
- iKEY is one of the most commonly used token as it doesn't need a special reader and can be connected to the system using USB port.

Biometrics – adds another level of security to these tokens/cards

OS Authentication Methods...

- Secure Socket Layer (SSL):
  - authentication information is transmitted over the network in an encrypted form
- Public Key Infrastructures (PKI):
  - User keeps a private key
  - Authentication firm holds a public key
  - Encrypt and decrypt data using both keys

Authorization

- Process that decides whether users are permitted to perform the functions they request
- Authorization is not performed until the user is authenticated
- Deals with privileges and rights (User administration)
- Create user accounts
- Grant privileges to users...

Maintenance

- Maintenance involves:
  - Monitoring and analyzing logging information
  - Performing regular backups
  - Recovering from security compromises
  - Restoring systems to its previous point
  - Regular testing of security
  - Patch, update, and revise critical software

Data Backup

- Backup is the act of creating copies of information such that it may be recovered
- Archive is to keep these backups for a long period of time
- Data may be lost accidentally (hardware failures, human mistake) or intentionally

Restore

- Restoring the computer system to an earlier point in time
- System restore can resolve many system problems
- It is the best recovery methods to try first
- It undo recent system changes, but leave files such as documents, pictures... unchanged
- System restore remove recently installed programs and drives

Creating and Implementing Organizational Policies

- Provide users with training in security techniques
- Train users about common malicious software
- Require users to scan flush disks and CDs before use
- Establish policies about types of media that can be brought in from outside and how they can be used
- Establish policies that discourage/prevent users from installing their own software

Creating and Implementing Organizational Policies

- Define policies that minimize/prevent downloading files;
- require users to use a virus scanner on any downloaded files
- Create quarantine areas for files of uncertain origin
- Use virus scanning on e-mail and attachments
- Discard e-mail attachments from unknown or untrusted sources

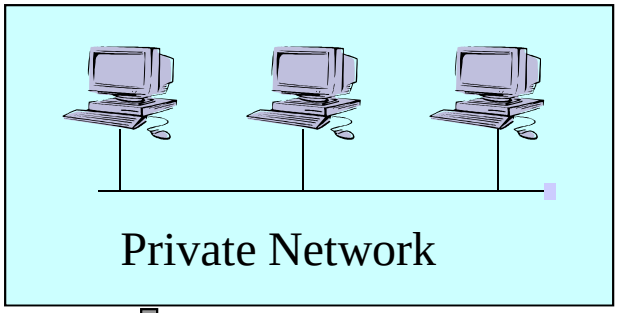
Overview of Firewall

- Firewall is a router or other communications device which filters access to a protected network.
- Firewall is also a program that screens all incoming traffic and protects the network from unwelcome intruders.
- It is a means of protection a local system or network of systems from network-based security threats,
  - while affording access to the outside world via WANs or the Internet

Overview of Firewall...

Firewall Objectives

- Keep intruders, malicious code and unwanted traffic or information out
- Keep private and sensitive information in



Private data

External attacks

security wall between private (protected) network and outside word

Overview of Firewall...

- Two primary types of firewalls are:
  - Packet filtering firewalls
  - Proxy-server firewalls
- Sometimes both are employed to protect a network.
- Firewalls can be designed to operate at any of the following three layers in the TCP/IP protocol stacks:

  - The application layer (eg: HTTP proxy)
  - The network and transport layer (eg: packet filtering)
  - The layer b/n the application layer and the transport layer (eg: SOCKS proxy)

Firewall features

- General Firewall Features
  - Port Control
  - Network Address Translation
  - Application Monitoring
  - Packet Filtering
  - Access control

- Additional features
  - Data encryption
  - Authentication
  - Connection relay (hide internal network)
  - reporting/logging
  - e-mail virus protection
  - spy ware protection

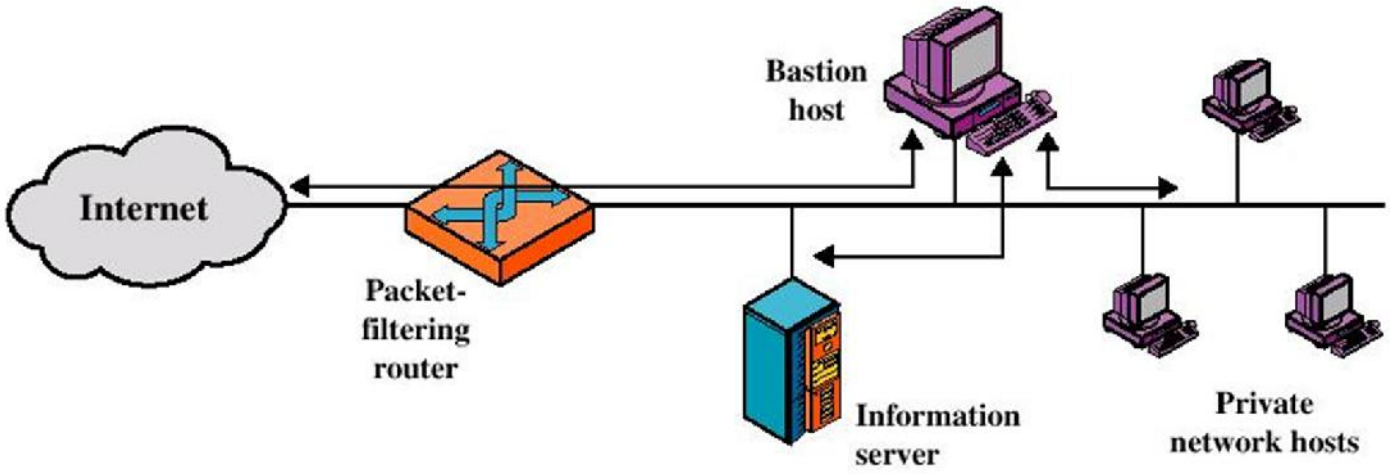
Screened host firewall system

- Also called single homed bastion host

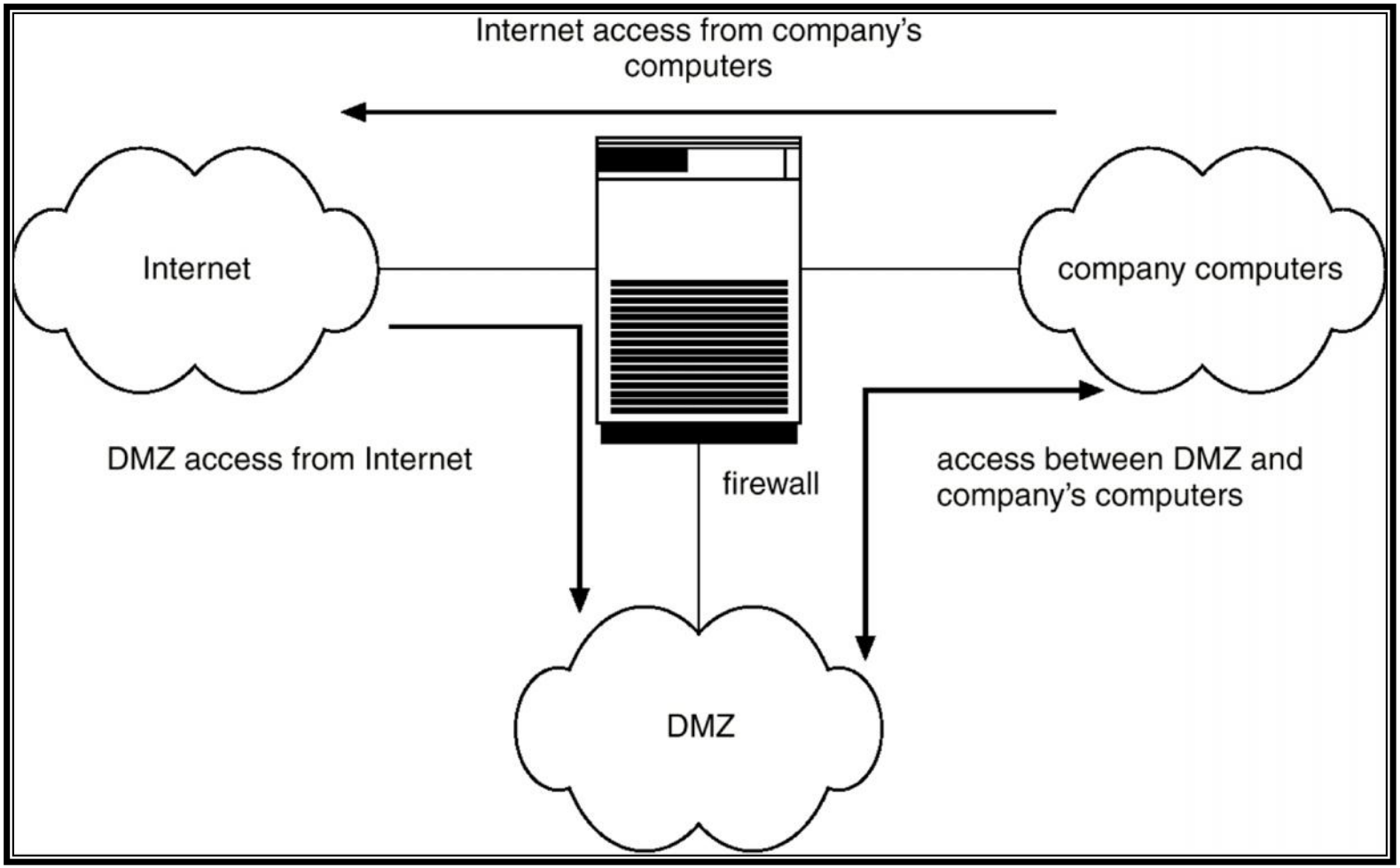
Configuration:

- The firewall consists of two systems:

1. Packet filtering router: The router is configured so that:
   a. For traffic from the Internet, only IP packets destined for the bastion host are allowed in.
   b. For traffic from the internal network, only IP packets from the bastion host are allowed out.
2. Bastion Host
   - performs authentication and Proxy functions.



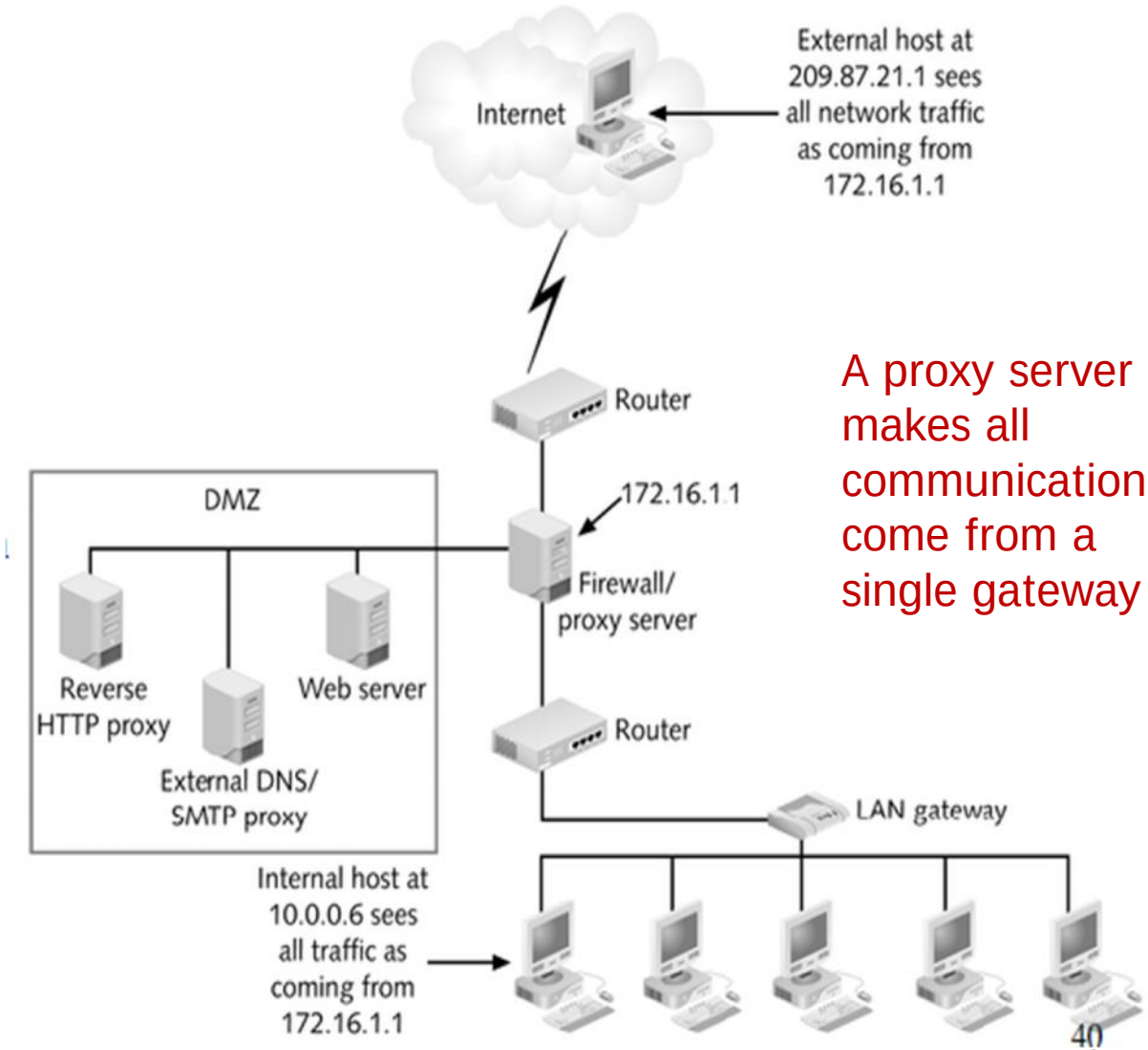
Network Security Through Domain Separation Via Firewall



Proxy Server

Demilitarized zone

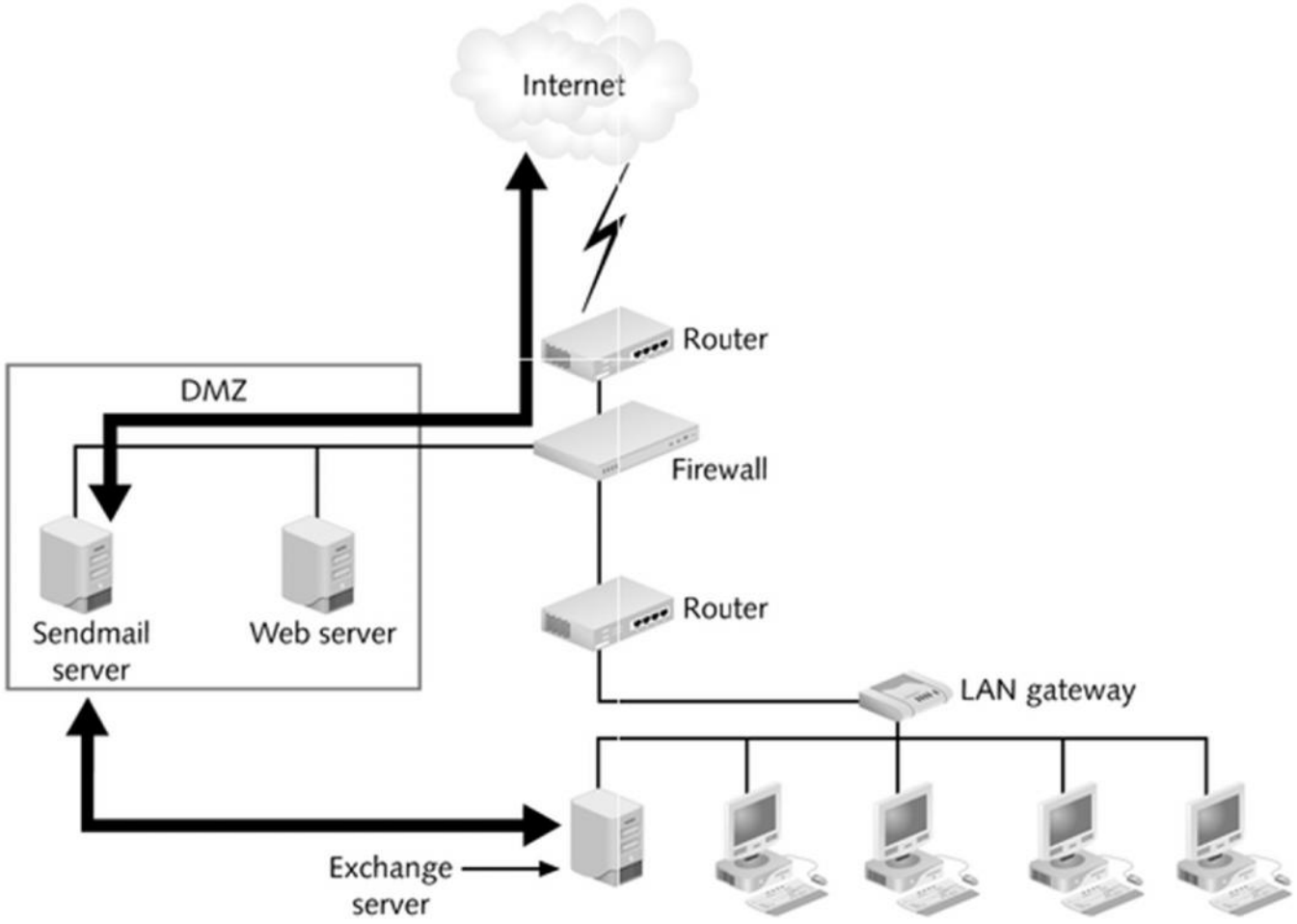
- A DMZ is part of a network on which you place servers that must be accessible by sources both outside and inside your network.
- However, the DMZ is not connected directly to either network, and it must always be accessed through the firewall.
- By using a DMZ, you can create an additional step that makes it more difficult for an intruder to gain access to the internal network.



A proxy server makes all communication come from a single gateway

Example: E-Mail Proxy Protection

- External e-mail users never interact directly with internal hosts



E-mail protection with a proxy SMTP server

Goals of Proxy Servers

- Conceal internal clients
- Block URLs
- Block and filter content
- Protect e-mail proxy
- Improve performance
- Ensure security
- Provide user authentication
- Redirect URLs

Misuse Prevention

- Prevention techniques: first line of defense
- Secure local and network resources
- Techniques: cryptography, identification, authentication, authorization, access control, security filters, etc.

Problem: Still losses can occur!

Contributing Factors for Misuse

- Many security flaws in systems
- Secure systems are expensive
- Secure systems are not user-friendly
- “Secure systems” still have flaws
- Insider Threat
- Hackers’ skills and tools improve

Need:

- Intrusion Prevention: protect system resources
- Intrusion Detection: (second line of defense) discriminate intrusion attempts from normal system usage
- Intrusion Recovery: cost effective recovery models

Intrusion Detection

- Detect attempts to intruder into computer systems.

- Detection methods:
  - Auditing and logging.
  - Tripwire (UNIX software that checks if certain files and directories have been altered – I.e. password files)

- System call monitoring

Why Intrusion Detection?

- Second line of defense
- Deter intruders
- Catch intruders
- Prevent threats to occur (real-time IDS)
- Improve prevention/detection techniques

Terminology

- Audit: activity of looking at user/system behavior, its effects, or the collected data
- Profiling: looking at users or systems to determine what they usually do
- Anomaly: abnormal behavior
- Misuse: activity that violates the security policy
- Outsider: someone without access right to the system
- Insider: someone with access right to the system
- Intrusion: misuse by outsiders and insiders

Phases of Intrusion

- Intelligence gathering: attacker observes the system to determine vulnerabilities
- Planning: attacker decide what resource to attack (usually least defended component)
- Attack: attacker carries out the plan
- Hiding: attacker covers tracks of attack
- Future attacks: attacker installs backdoors for future entry points

Times of Intrusion Detection

- Real-time intrusion detection
  - Advantages:
    - May detect intrusions in early stages
    - May limit damage
  - Disadvantages:
    - May slow down system performance
    - Trade off between speed of processing and accuracy
    - Hard to detect partial attacks

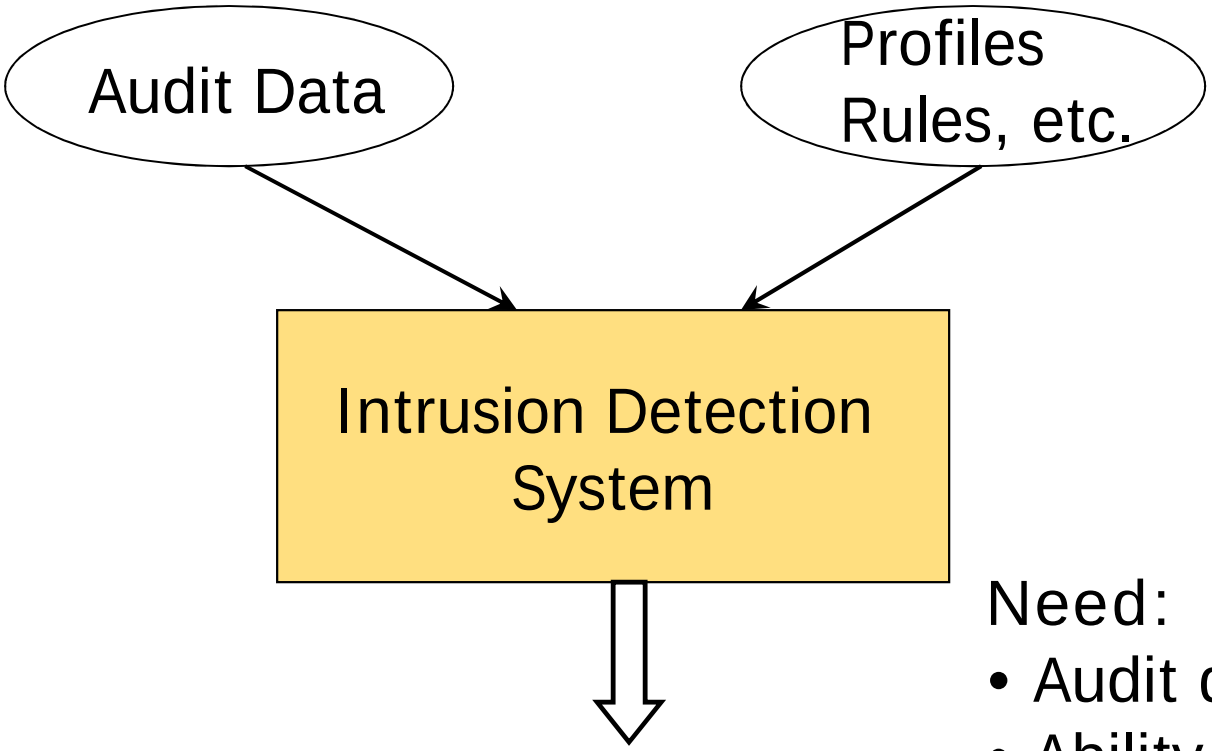
Times of Intrusion Detection

- Off-the-line intrusion detection
  - Advantages:
    - Able to analyze large amount of data
    - Higher accuracy than real-time ID
  - Disadvantages:
    - Mostly detect intrusions after they occurred

Audit Data

- Format, granularity and completeness depend on the collecting tool
- Examples
  - System tools collect data (login, mail)
  - Additional collection of low system level
  - “Sniffers” as network probes
  - Application auditing
- Needed for
  - Establishing guilt of attackers
  - Detecting subversive user activity

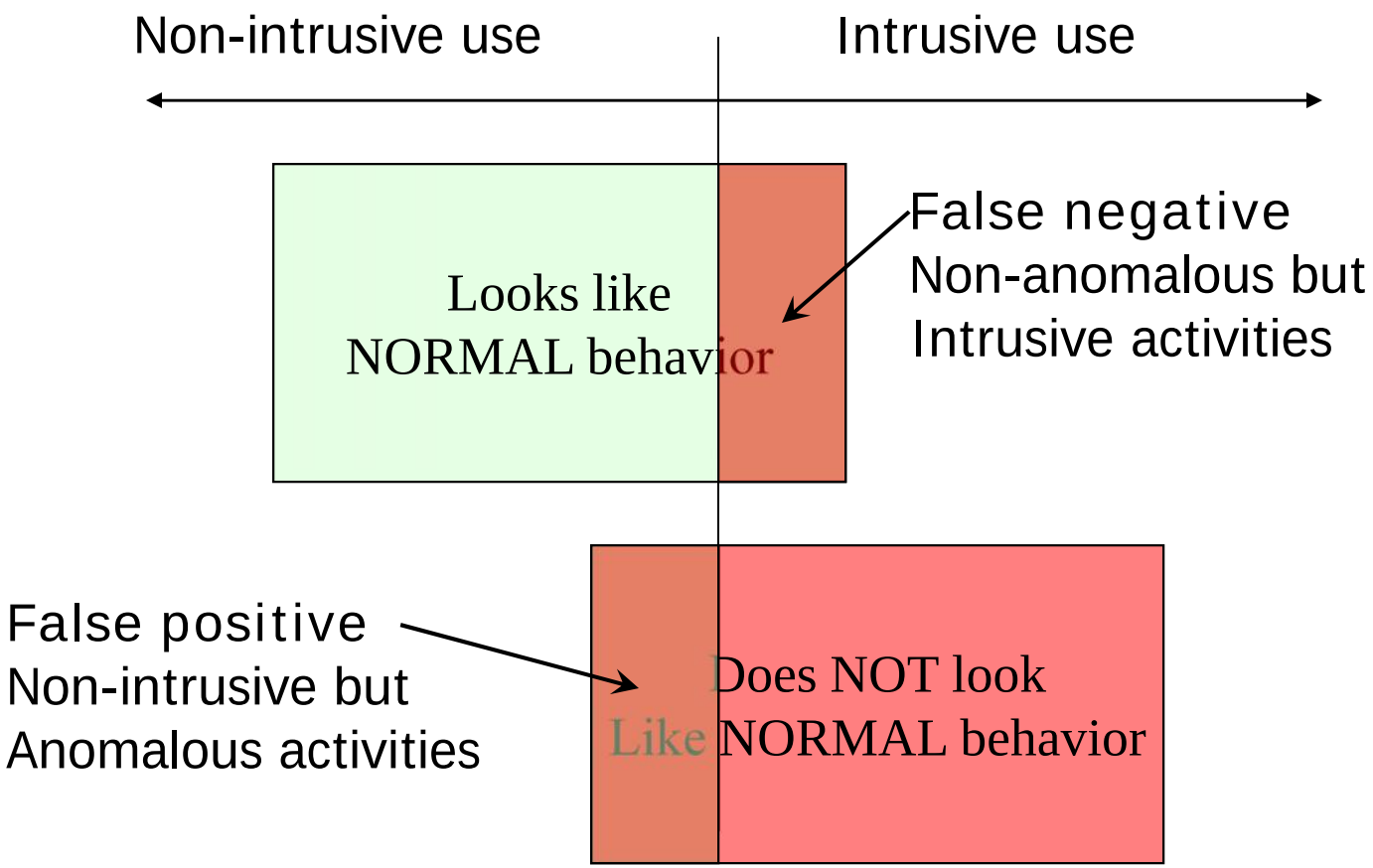
Audit-Based Intrusion Detection



Need:

- Audit data
- Ability to characterize behavior

Anomaly versus Misuse



False Positive v.s. False Negative

- False positive: non-intrusive but anomalous activity
  - Security policy is not violated
  - Cause unnecessary interruption
  - May cause users to become unsatisfied
- False negative: non-anomalous but intrusive activity
  - Security policy is violated
  - Undetected intrusion

Intrusion Detection Techniques

1. Anomaly Detection
2. Misuse Detection
3. Hybrid Misuse/Anomaly Detection
4. Immune System Based IDS

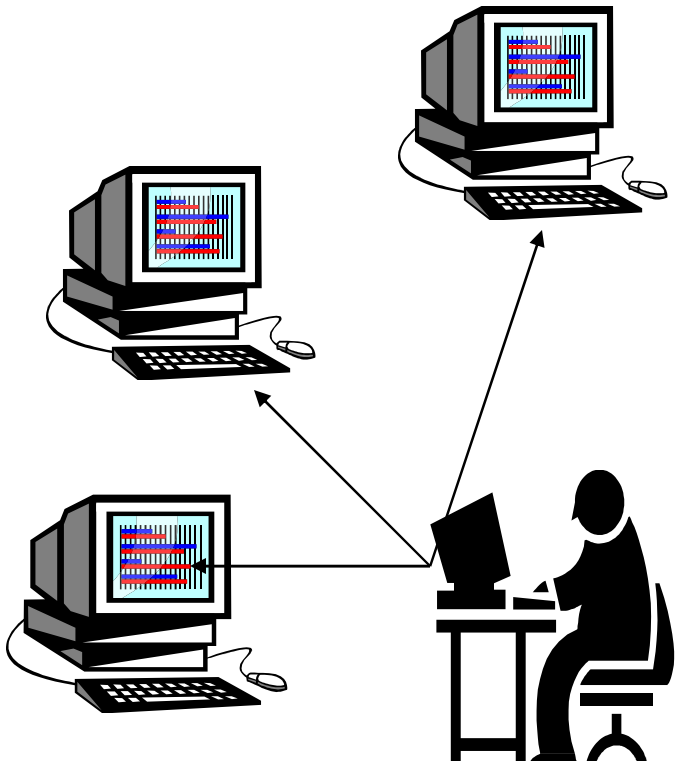
Intrusion Types

- Doorknob rattling
- Masquerade attacks
- Diversionary Attack
- Coordinated attacks
- Chaining
- Loop-back

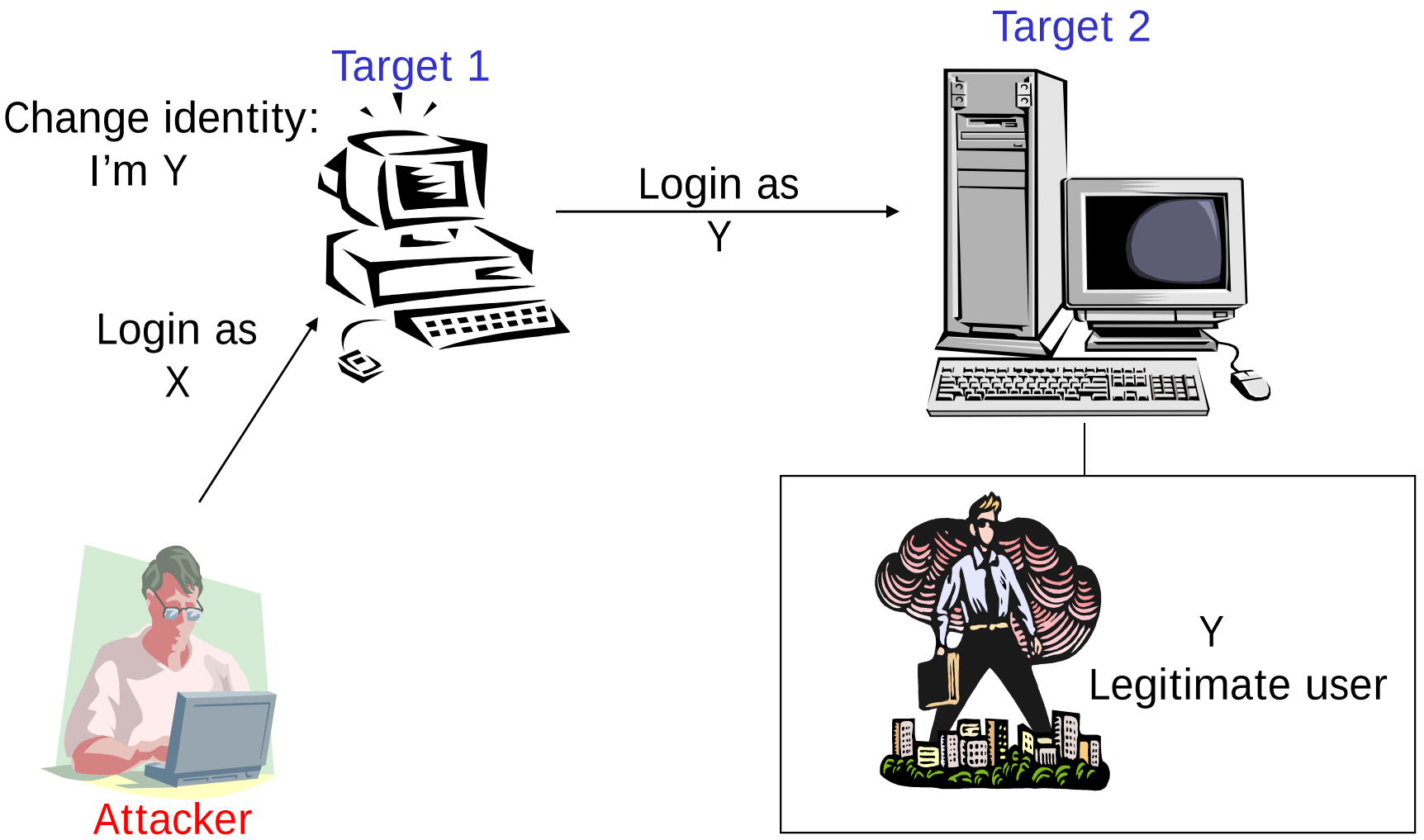
Doorknob Rattling

- Attack on activity that can be audited by the system (e.g., password guessing)
- Number of attempts is lower than threshold
- Attacks continue until
  - All targets are covered

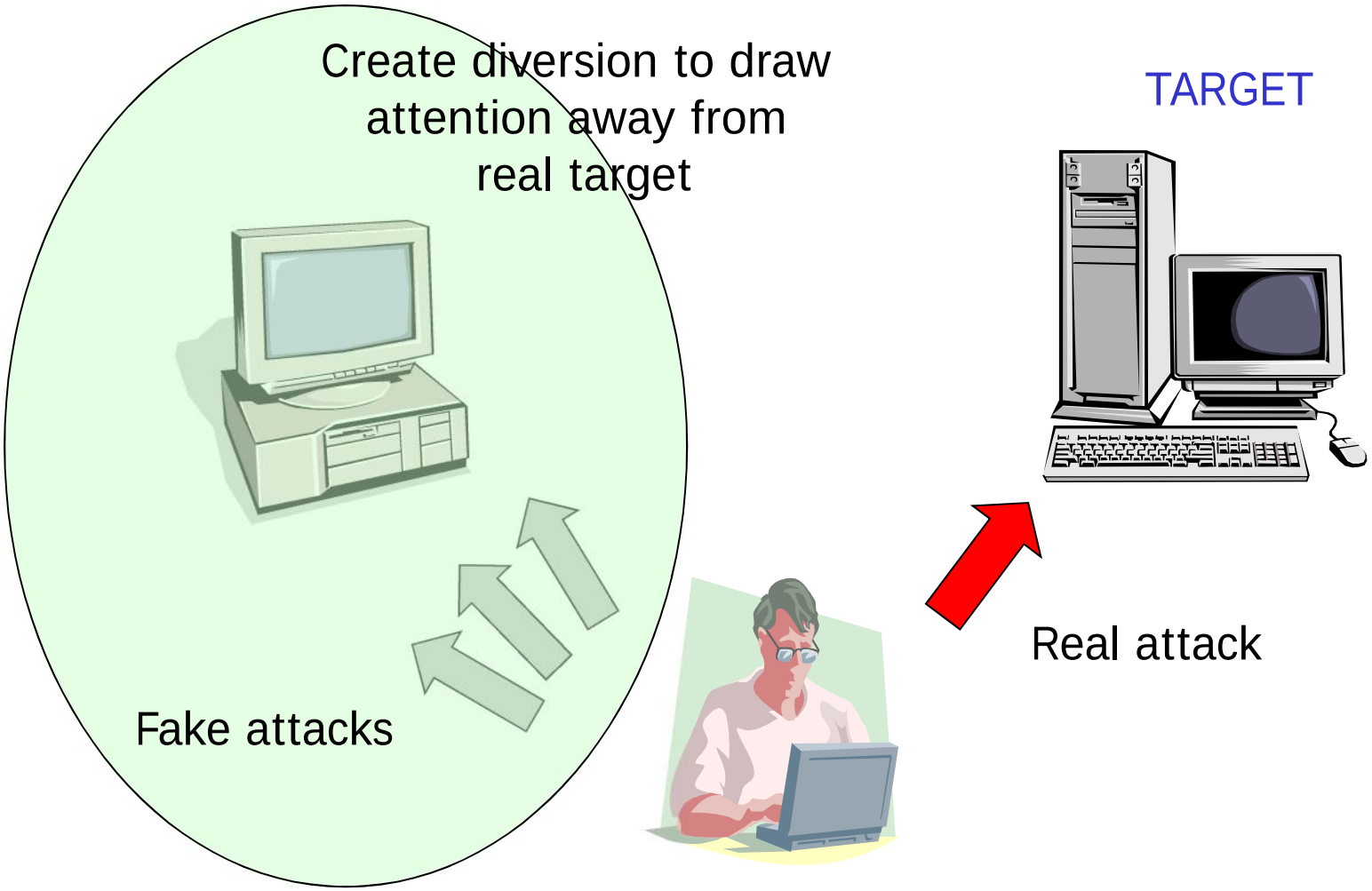
  or
  - Access is gained



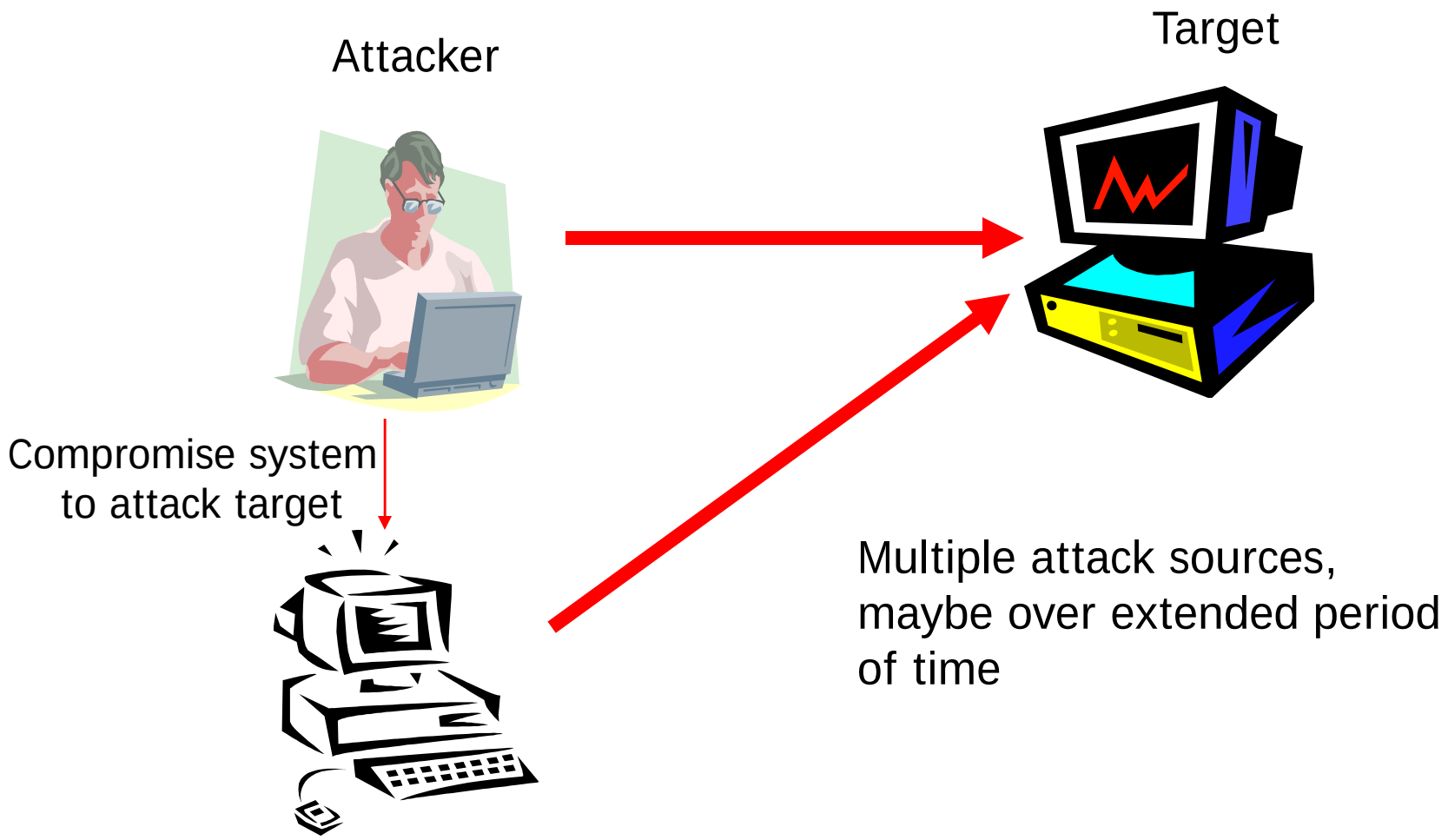
Masquerading



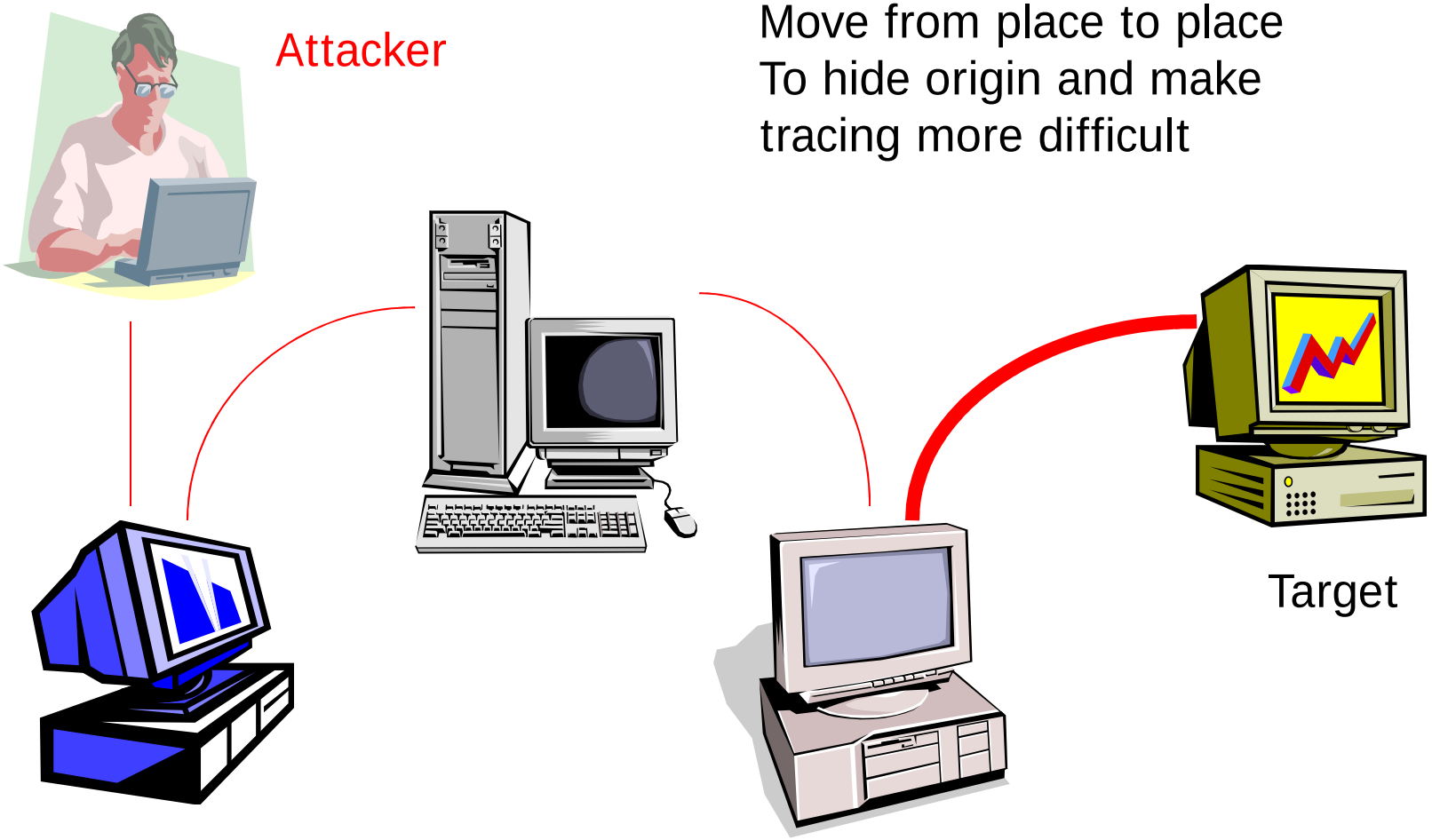
Diversionary Attack



Coordinated attacks



Chaining


Attacker
Move from place to place
To hide origin and make
tracing more difficult
Target

Intrusion Recovery

- Actions to avoid further loss from intrusion.
- Terminate intrusion and protect against reoccurrence.

- Reconstructive methods based on:
  - Time period of intrusion
  - Changes made by legitimate users during the effected period
  - Regular backups, audit trail based detection of effected components, semantic based recovery, minimal roll-back for recovery.

Eight Security requirements Address the Breadth of computer and Network Vulnerabilities