Unit –IV

Introduction to Web Servers

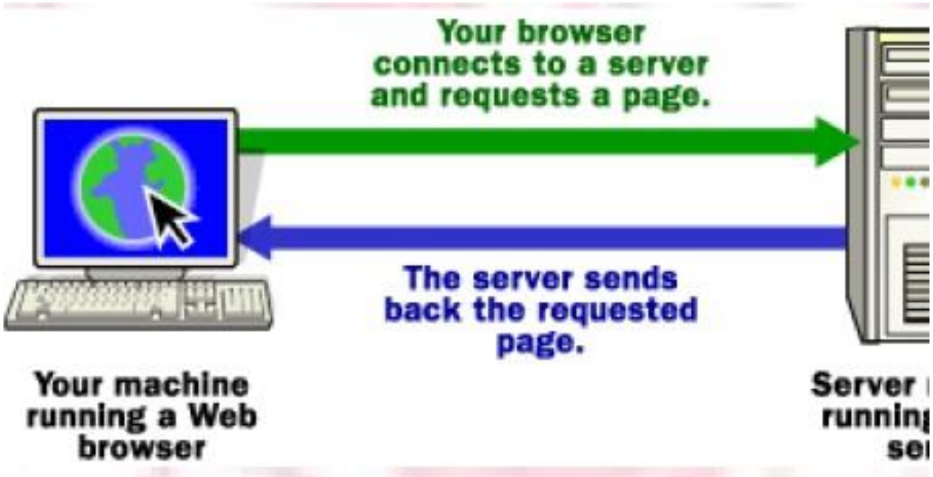
Introduction to Web Servers: A web server can be referred to as either the hardware (the computer) or the software (the computer application) that helps to deliver content that can be accessed through the Internet. A web server is what makes it possible to be able to access content like web pages or other data from anywhere as long as it is connected to the internet. The hardware houses the content, while the software makes the content accessible through the internet.

The most common use of web servers is to host websites but there are other uses like data storage or for running enterprise applications. There are also different ways to request content from a web server. The most common request is the Hypertext Transfer Protocol (HTTP), but there are also other requests like the Internet Message Access Protocol (IMAP) or the File Transfer Protocol (FTP).

How Web Servers Work

The Basic Process

Let's say that you are sitting at your computer, surfing the Web, and you get a call from a friend who says, "I Just read a great article! Type in this URL and check it out. It’s at http:/www.howstuffworks.com/web-server.htm." So you type that URL into your browser and press return. And magically, no matter where in the world that URL lives, the page pops up on your screen. At the most basic level possible, the following diagram shows the steps that brought that page to your screen:


Your browser connects to a server and requests a page.
The server sends back the requested page.
Your machine running a Web browser
Server running se

Your browser formed a connection to a Web server, requested a page and received it. Behind the Scenes If you want to get into a bit more detail on the process of getting a Web page onto your computer screen, here are the basic steps that occurred behind the scenes:

The browser broke the URL into three parts:

1. The protocol ("http")

2. The server name ("www.howstuffworks.com")

3. The file name ("web-server.htm")

- The browser communicated with a name server to translate the server name "www.howstuffworks.com" into an IP Address, which it uses to connect to the server machine.
- The browser then formed a connection to the server at that IP address on port 80.

Note: Any server machine makes its services available to the Internet using numbered ports, one for each service that is available on the server. For example, if a server machine is running a Web server and an FTP Server, the web server would typically be available on port 21. Clients connect to a service at a specific IP address and on a specific port.

- Following the HTTP protocol, the browser sent a GET request to the server, asking for the file "http://www.howstuffworks.com/web-server.htm."
- The server then sent the HTML text for the Web page to the browser.
- The browser reads the HTML tags and displays the page onto your screen.

Internet Information Server (IIS)

Internet Information Server (IIS)

Internet Information Server – is a web server application and set of feature extension modules created by Microsoft for use with Microsoft Windows. It is the most used web server after Apache HTTP Server. IIS 7.5 supports HTTP, HTTPS, FTP, FTPS, SMTP and NNTP.
It is an integral part of Windows Server family of products, as well as all editions of Windows

Vista and Windows 7, although some features are not supported on client versions of Windows. IIS is not turned on by default when Windows is installed.

Versions

- IIS 1.0, Windows NT 3.51 available as a free add- on
- IIS 2.0, Windows NT 4.0
- IIS 3.0, Windows NT 4.0 Service Pack 3 IIS 4.0, Windows NT 4.0 Option Pack IIS 5.0, Windows 2000
- IIS 5.1, Windows XP Professional and Windows XP Media Center Edition (requires retail CD)
- IIS 6.0, Windows Server 2003 and Windows XP Professional x64 Edition
- IIS 7.0, windows server 2008 and windows Vista(Home premium, Business, Enterprise and Ultimate editions
- IIS 7.5, Windows Server 2008 R2 and Windows 7

Features

The architecture of IIS 7 is modular. Modules, also called extensions, can be added or removed individually so that only modules required for specific functionality have to be installed. IIS 7 includes native modules as part of the full installation. These modules are individual features that the server uses to process requests and include the following:

- **HTTP modules –** Used to perform tasks specific to HTTP in the request-processing pipeline, such as responding to information and inquiries sent in client headers, returning HTTP errors, and redirecting requests.
- **Security modules –** Used to perform tasks related to security in the request-processing pipeline, such as specifying authentication schemes, performing URL authorization, and filtering requests.
- **Content modules –** Used to perform tasks related to content in the request-processing pipeline, such as processing requests for static files, returning a default page when a client does not specify a resource in a request, and listing the contents of a directory.
- **Compression modules –** Used to perform tasks related to compression in the requestprocessing pipeline, such as compressing responses, applying Gzip compression transfer coding to responses, and performing pre-compression of static content.

- **Caching modules –** Used to perform tasks related to caching in the request-processing pipeline, such as storing processed information in
- **Logging and Diagnostics modules –** Used to perform tasks related to logging and diagnostics in the request-processing pipeline, such as passing information and processing status to HTTP.sys for logging, reporting events, and tracking requests currently executing in worker processes.

IIS 5.0 and higher support the following authentication mechanisms:

- Basic access authentication
- Digest access authentication
- Integrated Windows Authentication
- NET Passport Authentication (not supported in Windows Server 2008 and above) IIS 7.5 includes the following additional security features:
- Client Certificate Mapping
- IP Security
- Request Filtering
- URL Authorization

Authentication changed slightly between IIS 6.0 and IIS 7, most notably in that the anonymous user which was named "IUSR_{machinename}" is a built-in account in Vista and future operating systems and named "IUSR". Notably, in IIS 7, each authentication mechanism is isolated into its own module and can be installed or uninstalled.

Personal Web Server

Personal Web Server: PWS, an abbreviation for Personal Web Server, is Microsoft's version of a Web server program for individual PC users who want to share Web pages and other files from their hard drive. PWS is a scaled-down version of Microsoft's more robust Web server, Internet Information Server IIS.

PWS can be used with a full-time Internet connection to serve Web pages for a Web site with limited traffic. It can also be used for testing a Web site offline or from a "staging" site before putting it on a main Web site that is exposed to larger traffic.

PWS can be used together with Microsoft's FrontPage, a Web site design product, to upload Web pages from a remote location or to the local hard drive; to check for dead links; to create directories; and to set permissions. PWS is frequently used as part of the trend toward peer-to-peer exchange and publishing.

How to Install Personal Web Server Starting the Installation

There are two places you can get PWS, both of which are free. The Windows 98 CD includes it, and you can download it from the Microsoft web site. Downloading from Microsoft.com

If you don’t have the windows 98 CD, you can download the NT4 option Pack which, believe it or not , contains personal Web Server for Windows 95 and 98. Be Aware that the download is 34mb, which will take nearly 3 hours to download with a 28.8 modem.

To start the download, follow these steps:

1. Go to the microsoft.com web site.
2. Follow the instructions on the web site, choosing Windows 95 as the operating system even if you're running on Windows 98.
3. After the download, the installation starts.

Installing from Windows 98 CD: To install Microsoft Personal Web Server:

1. Insert your Windows 98 CD-ROM in your CD- ROM drive.
2. Click Start, and then click Run.
3. In the Open box, type the following path to the Setup.exe file, where x is the letter of your CD- ROM drive: **x:\add-ons\pws\setup.exe**
4. Click OK.
5. Follow the instructions in Personal Web Server Setup.

Apache Web Server

Apache Web Server

- Apache is generally recognized as the world's most popular Web server (HTTP server). Originally designed for Unix servers, the Apache Web server has been ported to Windows and other network operating systems (NOS). The name "Apache" derives from the word "patchy" that the Apache developers used to describe early versions of their software.
- The Apache Web server provides a full range of Web server features, including CGI, SSL, and virtual domains. Apache also supports plug-in modules for extensibility. Apache is reliable, free, and relatively easy to configure.
- Apache is free software distributed by the Apache Software Foundation. The Apache Software Foundation promotes various free and open source advanced Web technologies.

Features

- Apache supports a variety of features, many implemented as compiled modules which extend the core functionality. These can range from server-side programming language support to Authentication schemes. Some common language interfaces support perl, Python ,Tcl, and PHP. Popular authentication modules include mod_access, mod_auth, mod_digest, and mod_auth_digest, the successor to mod_digest. A sample of other features include SSL and TLS support (mod_ssl), a proxy module (mod_proxy), a URL rewriter (also known as a rewrite engine, implemented under mod_rewrite), custom log files (mod_log_config), and filtering support (mod_include and mod_ext_filter).
- Popular compression methods on Apache include the external extension module, mod_gzip, implemented to help with reduction of the size (weight) of web pages served over HTTP. ModSecurity is an open source intrusion detection and prevention engine for web applications. Apache logs can be analyzed through a web browser using free scripts such as AWStats/W3Perl or Visitors.
- Virtual hosting allows one Apache installation to serve many different actual

websites. For example, one machine with one Apache installation could simultaneously serve www.example.com, www.test.com, test47.test-server.test.com, etc. Apache features configurable error messages, DBMS-based authentication databases, and content negotiation. It is also supported by several graphical user interfaces (GUIs).

Performance

- Although the main design goal of Apache is not to be the "fastest" web server, Apache does have performance comparable to other "high-performance" web servers. Instead of implementing a single architecture, Apache provides a variety of MultiProcessing Modules(MPMs) which allow pache to run in a process-based, hybrid(process and thread) or event -hybrid mode, to better match the demands of each particular infrastructure. This implies that the choice of correct MPM and the correct configuration is important. Where compromises in performance need to be made, the design of Apache is to reduce latency and increase throughput, relative to simply handling more requests, thus ensuring consistent and reliable processing of requests within reasonable time- frames.
- The Apache version considered by the Apache Foundation as providing high-performances is the multi-threaded version which mixes the use of several processes and several threads per process.
- While this architecture works faster than the previous multi-process based topology (because threads have a lower overhead than processes), it does not match the performances of the event- based architecture provided by other servers, especially when they process events with several worker threads.
- This difference can be easily explained by the overhead that one thread per connection brings (as opposed to a couple of worker threads per CPU, each processing many connection events). Each thread needs to maintain its own stack, environment, and switching from one thread to another is also an expensive task for CPUs.

Installing

- Apache can be installed in a variety of ways depending on your operating system and how much control you want over the installation process. If you are installing the server on a Windows machine, you can download the latest Binaries from the apache website. If you are using aUNIX or Linux operating system. You have more options. The Apache website has the source code available to download and compile, as well as OS-specific binaries. You can also install the Web server through the package manager of many Linux and UNIX systems.

Configuring

- Once installed, there are two main configuration files that should be edited. These files are plain text files that can be opened in any text editor. The files contain one directive per line and are case insensitive. Lines starting with the # character are considered comments and are ignored by the server.
- The main configuration file is the httpd.conf file. Linux/Unix users will usually find this file at /etc/httpd/httpd.conf. However, the Debian-based Linux distributions place the file at /etc/apache2/apache2.conf. The default location in the Windows OS is C:\Program Files\Apache Group\Apache2\conf\httpd.conf.
- The httpd.conf file holds the system information such as the server root directory, the listening port, the maximum number of clients who can simultaneously connect and the number of server instances the software can start at one time. Apache can also be configured for virtual hosting, which allows one server to serve many different clients at one time. The virtual host directives are also held in the httpd.conf file.
- The .htaccess file is a way to make changes to the main configuration on a directory level. This file must be created on a per-directory basis, and the configuration changes are applicable only for the directory it resides in and any subdirectories. The .htaccess file allows you to require Authentication before allowing site access provide redirection, specify cgi handling and much more. The entire list of directives can be found in the Apache Documentation.

Starting

- The Apache Web server runs as a service on all operating systems. A service is a software application that runs in the background with no user intervention. This allows outside users to access the Web pages any time the physical server is turned on, regardless of whether a user is logged in or not.
- In Windows, you start the service under the "Services" option of the Control Panel. There will be a list of every service available to the users. You will choose the "Apache" service and click "Start" next to it. To stop the service, you simply click "Stop."
- Starting a service is different for Linux/Unix users. You must open a terminal window, which is found under "System Tools" or "Utilities" in the main "Applications" or "Start" menu. The service must be started by the root user. You can either switch to root using the "su" command or place the word "sudo" before the commands.

The command to start the service is: /etc/init.d/apache2 start The command to stop the service is: /etc/init.d/apache2 stop Once the service is started, you can test your configuration by typing "http://localhost" in a Web browser address bar.

Software Complexity

Software Complexity Contributing Factors

- **Program Size –** A browser may consist of as many as 75000 lines of source code. The executable file for a browser is usually on the order of 5 to 7 mega bytes. It is very difficult to eliminate all errors in such an immense program.
- **Software Interfaces –** The need for the browsers to interface with other software creates an even larger code base and more potential problem areas.
- **Market Forces –** Products must be hurried to market in order to maintain a competitive edge. It is often challenging to test all parts of them thoroughly before release. One reason why new versions of large software systems come out so frequently is that bugs are addressed in newer releases.
- **Team Development –** Large teams of programmers are often used to develop complicated programs such as browsers. Very few individuals can handle such a

task alone. Inconsistent styles, or even just carelessness on the Part of a single programmer can result in bugs that are very difficult to find and correct.

Encryption

There's a whole lot of information that we don't want other people to see, such as:

- Credit-card information
- Social Security numbers
- Private correspondence
- Personal details
- Sensitive company information
- Bank-account information

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood.

The use of encryption/decryption is as old as the art of communication. In wartime, a cipher, often incorrectly called a code, can be employed to keep the enemy from obtaining the contents of transmissions. (Technically, a code is a means of representing a signal without the intent of keeping it secret; examples are Morse code and ASCII.) Simple ciphers include the substitution of letters for numbers, the rotation of letters in the alphabet, and the "scrambling" of voice signals by inverting the sideband frequencies. More complex ciphers work according to sophisticated computer algorithms that rearrange the data bits in digital signals.

In order to easily recover the contents of an encrypted signal, the correct decryption key is required. The key is an algorithm that undoes the work of the encryption algorithm. Alternatively, a computer can be used in an attempt to break the cipher. The more complex the

the key.

Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to tap than their hard-wired counterparts. Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase online, or the discussion of a company secret between different departments in the organization. The stronger the cipher -- that is, the harder it is for unauthorized people to break it -- the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

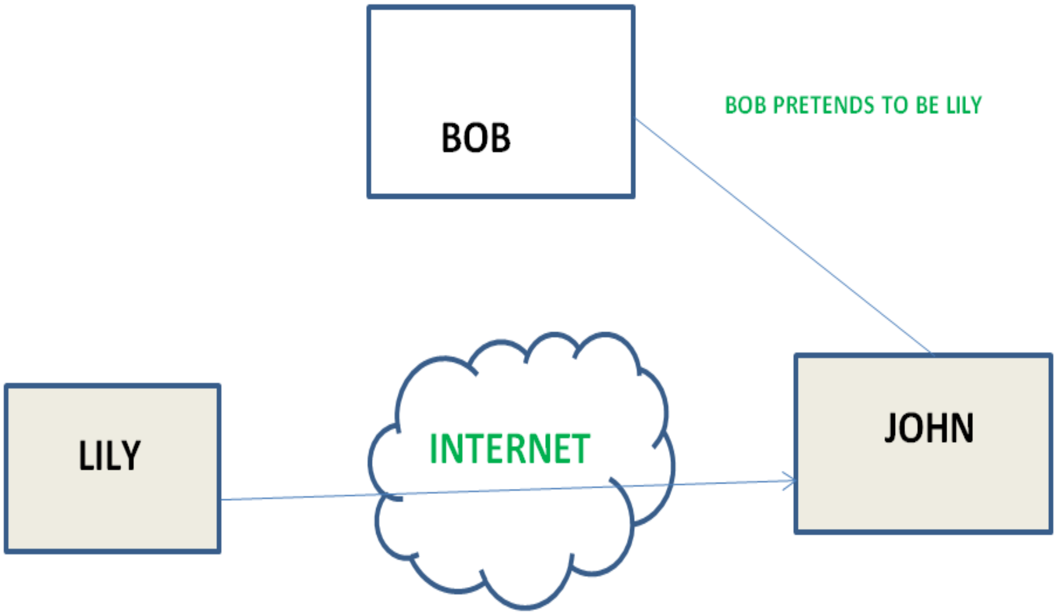
In recent years, a controversy has arisen over so-called strong encryption. This refers to ciphers that are essentially unbreakable without the decryption keys. While most companies and their customers view it as a means of keeping secrets and minimizing fraud, some governments view strong encryption as a potential vehicle by which terrorists might evade authorities. These governments, including that of the United States, want to set up a key-escrow arrangement. This means everyone who uses a cipher would be required to provide the government with a copy of the key. Decryption keys would be stored in a supposedly secure place, used only by authorities, and used only if backed up by a court order. Opponents of this scheme argue that criminals could hack into the key-escrow database and illegally obtain, steal, or alter the keys. Supporters claim that while this is a possibility, implementing the key escrow scheme would be better than doing nothing to prevent criminals from freely using encryption/decryption.

Active and Passive attacks in Information Security

Active attacks: An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:

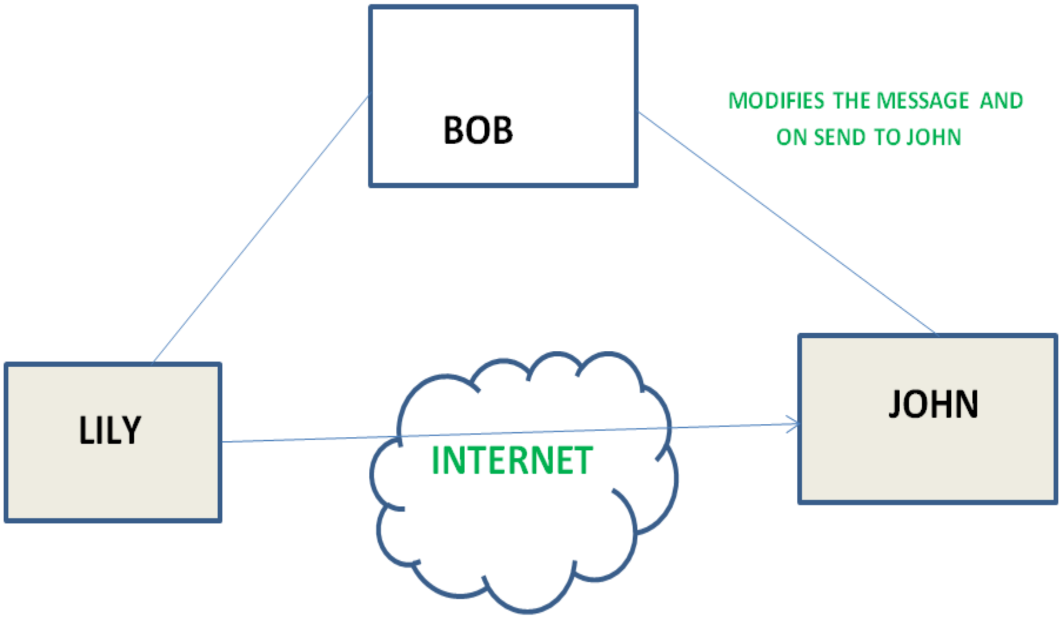
1. **Masquerade –**

   Masquerade attack takes place when one entity pretends to be different entity. A Masquerade attack involves one of the other form of active attacks.



2. **Modification of messages –**

   It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.

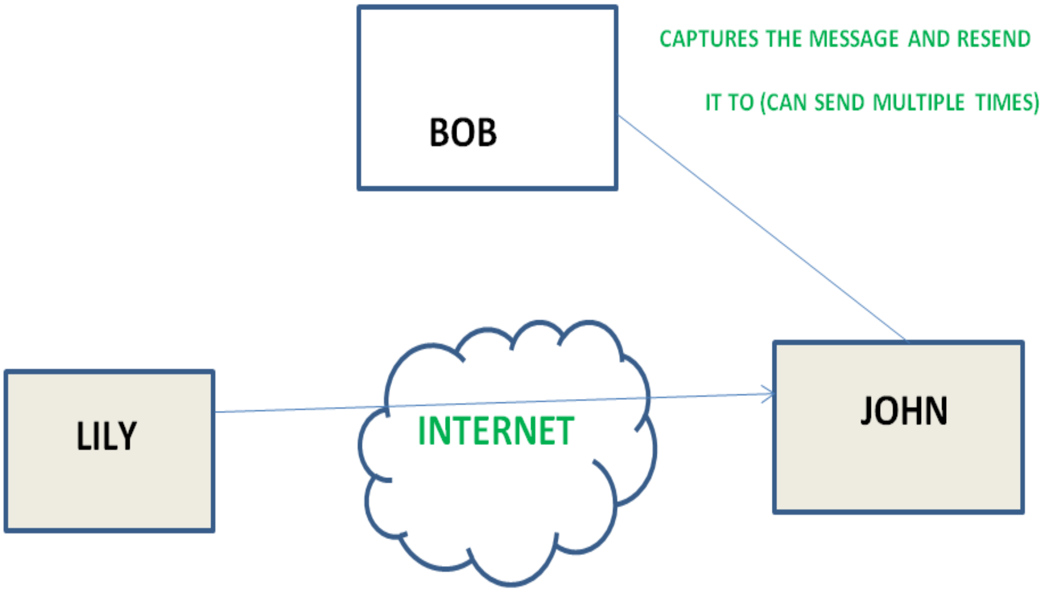


3. **Repudiation –**

   This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask his Bank “To transfer an amount to someone" and later on the sender(customer) deny that he had made such a request. This is repudiation.

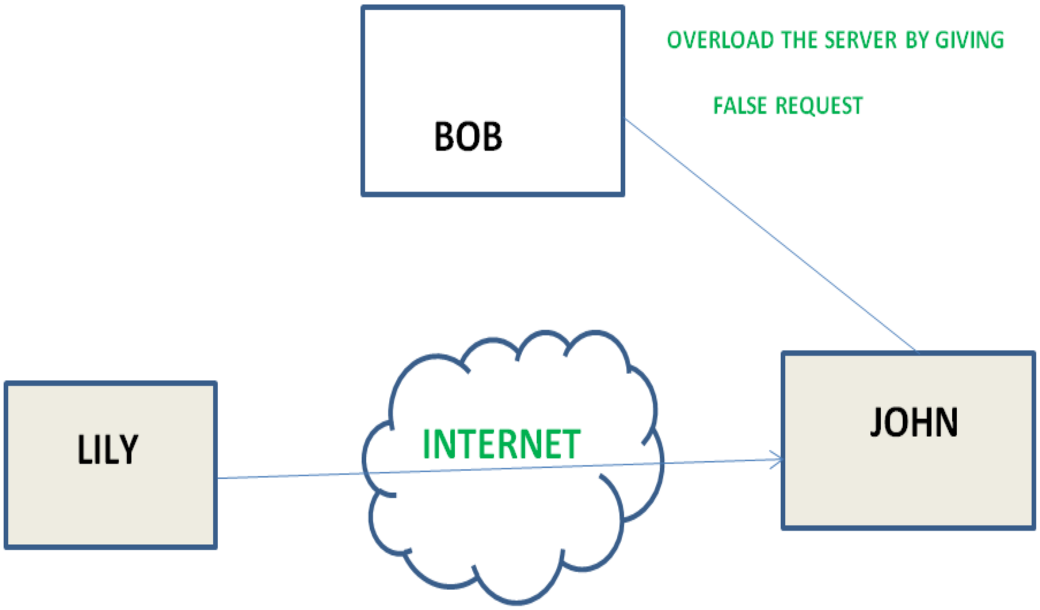
4. **Replay –**

   It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.


BOB
CAPTURES THE MESSAGE AND RESEND
IT TO (CAN SEND MULTIPLE TIMES)
LILY
INTERNET
JOHN

5. **Denial of Service –**

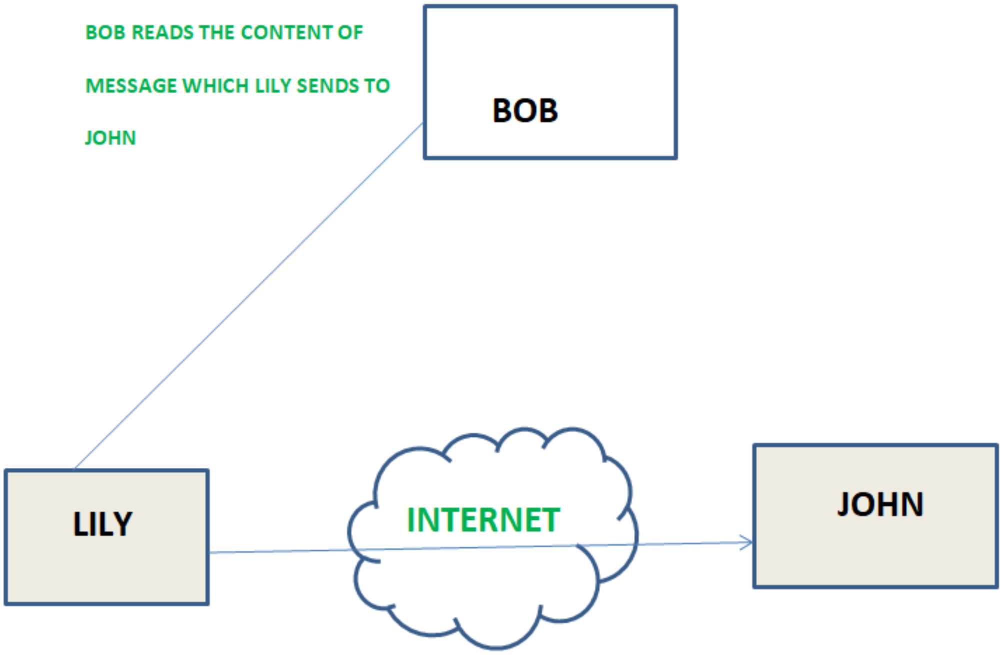
   It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination. Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



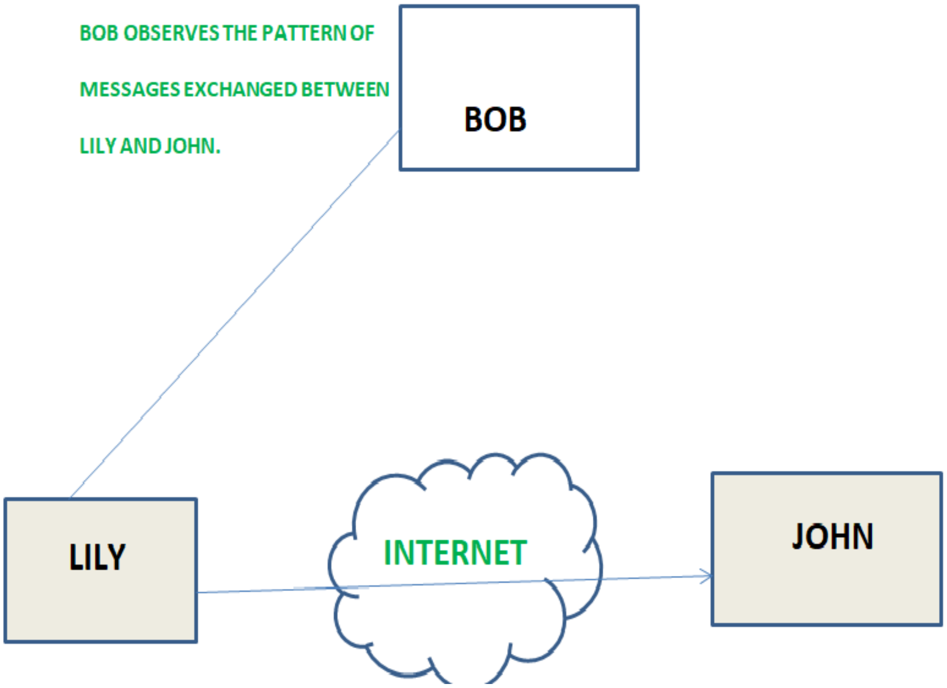
Passive attacks: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:

1. **The release of message content –**

   Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



2. **Traffic analysis –**
   Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.
   The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place.



System Security

Prerequisite – Basic Network Attacks, Types of Viruses
Security of a computer system is a crucial task. It is a process of ensuring confidentiality and integrity of the OS.
A system is said to be secure if its resources are used and accessed as intended under all the circumstances, but no system can guarantee absolute security from several of the various malicious threats and unauthorized access.
Security of a system can be threatened via two violations:

- **Threat:** A program which has the potential to cause serious damage to the system.

- **Attack:** An attempt to break security and make unauthorized use of an asset.

Security violations affecting the system can be categorized as malicious and accidental. **Malicious threats**, as the name suggests are a kind of harmful computer code or web script designed to create system vulnerabilities leading to back doors and security breaches. **Accidental Threats**, on the other hand, are comparatively easier to be protected against. Example: Denial of Service DDoS attack.

Security can be compromised via any of the breaches mentioned:

- **Breach of confidentiality:** This type of violation involves the unauthorized reading of data.
- **Breach of integrity:** This violation involves unauthorized modification of data.
- **Breach of availability:** It involves an unauthorized destruction of data.
- **Theft of service:** It involves an unauthorized use of resources.
- **Denial of service:** It involves preventing legitimate use of the system. As mentioned before, such attacks can be accidental in nature.

Security System Goals –

Henceforth, based on the above breaches, the following security goals are aimed:

1. **Integrity:**
   The objects in the system mustn't be accessed by any unauthorized user & any user not having sufficient rights should not be allowed to modify the important system files and resources.
2. **Secrecy:**
   The objects of the system must be accessible only to a limited number of authorized users. Not everyone should be able to view the system files.
3. **Availability:**
   All the resources of the system must be accessible to all the authorized users i.e only one user/process should not have the right to hog all the system resources. If such kind of situation occurs, denial of service could happen. In this kind of situation, a malware might hog the resources for itself & thus preventing the legitimate processes from accessing the system resources.

Threats can be classified into the following two categories:

1. **Program Threats:**
   A program written by a cracker to hijack the security or to change the behaviour of a normal process.
2. **System Threats:**
   These threats involve the abuse of system services. They strive to create a situation in which operating-system resources and user files are misused. They are also used as a medium to launch program threats.

Types of Program Threats –

1. **Virus:**

   An infamous threat, known most widely. It is a self-replicating and a malicious thread which attaches itself to a system file and then rapidly replicates itself, modifying and destroying essential files leading to a system breakdown.

   Further, Types of computer viruses can be described briefly as follows:

   – file/parasitic – appends itself to a file

   – boot/memory – infects the boot sector

   – macro – written in a high-level language like VB and affects MS Office files

   – source code – searches and modifies source codes

   – polymorphic – changes in copying each time

   – encrypted – encrypted virus + decrypting code

   – stealth – avoids detection by modifying parts of the system that can be used to detect it, like the read system

   call

   – tunneling – installs itself in the interrupt service routines and device drivers

   – multipartite – infects multiple parts of the system

2. **Trojan Horse:**

   A code segment that misuses its environment is called a Trojan Horse. They seem to be attractive and harmless cover program but are a really harmful hidden program which can be used as the virus carrier. In one of the versions of Trojan, User is fooled to enter its confidential login details on an application. Those details are stolen by a login emulator and can be further used as a way of information breaches.

   Another variance is Spyware, Spyware accompanies a program that the user has chosen to install and downloads ads to display on the user's system, thereby creating pop-up browser windows and when certain sites are visited by the user, it captures essential information and sends it over to the remote server. Such attacks are also known as **Covert Channels**.

3. **Trap Door:**

   The designer of a program or system might leave a hole in the software that only he is capable of using, the Trap Door works on the similar principles. Trap Doors are quite difficult to detect as to analyze them, one needs to go through the source code of all the components of the system.

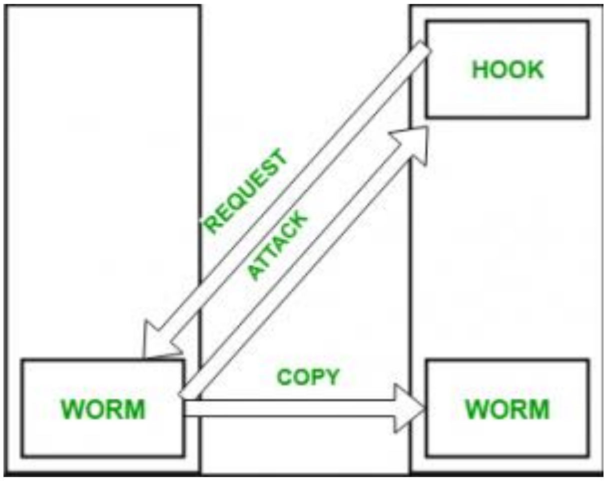
4. **Logic Bomb:**

   A program that initiates a security attack only under a specific situation.

Types of System Threats –

Aside from the program threats, various system threats are also endangering the security of our system:

1. **Worm:**
   An infection program which spreads through networks. Unlike a virus, they target mainly LANs. A computer affected by a worm attacks the target system and writes a small program “hook” on it. This hook is further used to copy the worm to the target computer. This process repeats recursively, and soon enough all the systems of the LAN are affected. It uses the spawn mechanism to duplicate itself. The worm spawns copies of itself, using up a majority of system resources and also locking out all other processes.
   The basic functionality of a the worm can be represented as:



2. **Port Scanning:**
   It is a means by which the cracker identifies the vulnerabilities of the system to attack. It is an automated process which involves creating a TCP/IP connection to a specific port. To protect the identity of the attacker, port scanning attacks are launched from **Zombie Systems**, that is systems which were previously independent systems that are also serving their owners while being used for such notorious purposes.
3. **Denial of Service:**
   Such attacks aren’t aimed for the purpose of collecting information or destroying system files. Rather, they are used for disrupting the legitimate use of a system or facility.
   These attacks are generally network based. They fall into two categories:
   – Attacks in this first category use so many system resources that no useful work can be performed. For example, downloading a file from a website that proceeds to use all available CPU time.
   – Attacks in the second category involves disrupting the network of the facility. These attacks are a result of the abuse of some fundamental TCP/IP principles.
   fundamental functionality of TCP/IP.

Security Measures Taken –

To protect the system, Security measures can be taken at the following levels:

- **Physical:**
  The sites containing computer systems must be physically secured against armed and malicious intruders. The workstations must be carefully protected.
- **Human:**
  Only appropriate users must have the authorization to access the system. Phishing(collecting confidential information) and Dumpster Diving(collecting basic information so as to gain unauthorized access) must be avoided.
- **Operating system:**
  The system must protect itself from accidental or purposeful security breaches.
- **Networking System:**
  Almost all of the information is shared between different systems via a network. Intercepting these data could be just as harmful as breaking into a computer. Henceforth, Network should be properly secured against such attacks.

Usually, Anti Malware programs are used to periodically detect and remove such viruses and threats. Additionally, to protect the system from the Network Threats, Firewall is also be used.

Principle of Information System Security

Information System Security or **INFOSEC** refers to the process of providing protection to the computers, networks and the associated data. With the advent of technology, the more the information is stored over wide networks, the more crucial it gets to protect it from the unauthorized which might misuse the same. Every organisation has the data sets that contain confidential information about its activities. The major reason of providing security to the information systems is not just one fold but 3 fold:

```
1. Confidentiality
2. Integrity
3. Availability
```

Together, these tiers form the **CIA triangle** that happened to be known as the foremost necessity of securing the information system. These three levels justify the **principle of information system security**.

Let us go through the same one by one:

1. **Confidentiality:**
   The main essence of this feature lies in the fact that only the authorized personnel should be allowed the access to the data and system. The unauthorised individuals must be kept away from

the information. This is ensured by checking the **authorisation** of every individual who tries to access the database.
For eg. An organisation's administration must not be allowed to access the private information of the employees.

2. **Integrity:**
   Integrity is ensured when the presented data is untouched or rather, is not altered by any unauthorized power. The information thus can be referred with the eyes closed. The integrity of the information can be altered in either unintentional or intentional ways. Intentionally, information can be passed through malicious content by any individual. Rather, unintentionally, any authorized individual might himself hamper the information for example, he might delete any specific important part of information.
3. **Availability:**
   This feature means that the information can be accessed and modified by any authorized personnel within a given **time frame.** The point here to be noted is that the accessibility of the information in limited. The time frame within which it can be accessed is different for every organisation.

Balancing Information Security and Access:

It is the sole purpose of the organisation to **protect the interests** of the users and to provide them with appropriate amount of information whenever necessary. Also, at the same time, it is necessary to provide **adequate security** to the information so that not anyone can access it. The need for maintaining the perfect balance of information security and accessibility arises from the fact that information security can never be absolute.

It would be harmful to provide free access to a piece of information and it would be hard to restrict any accessibility. So, one needs to make sure that the exact required balance is maintained so that both the users and the security professionals are happy.

Tools of Information Security:

There are various tools which are or which can be used by various organisations in order to ensure the maximum information system security. These tools however, do not guarantee the absolute security, but as stated above, helps in forming the crucial balance of information access and security.

Let us study these tools one by one:

1. **Authentication:**
   This is the foremost important tool that needs to be kept in mind before starting the crucial process of ensuring security. The process of authentication is when the system identifies someone with one or more than one factors. These factors must be unique for most of the users. For example, ID and password combinations, face recognition, thumb impression etc.

These factors can not always be trusted as one could lose them or it might be accessed by any outsider. For these circumstances, one can use **multi factor authorisation** which is done by combining any two or more of the above factors.

2. **Access Control:**

   After ensuring that the right individual gets the access to information, one has to make sure that only the appropriate information reaches him or her. By using the tool of access control, the system judges that which user must be able to re4ad or write or modify certain piece of information. For this it generally maintains a list of all the users. One could find two type of lists :

   - **Access Control List (ACL)** – This is just the list of individuals who are eligible to access the information
   - **Role- Based access Control List (RBAC)** – This list comprises of the names of authorized personnel and their respective actions they are authorized to perform over the information.

3. **Encryption:**

   Sometimes the information is transmitted over the internet so the risk of anyone accessing it increases and now the tools have to be strong to avoid it. In this scenario, the information can be easily accessed and modified by anyone. To avoid this, a new tool is put to work, Encryption. Using encryption, one can put the confidential information into bits of unreadable characters that are difficult to decrypt and only the authorised receivers of the information can read it easily.

Digital Signature

Digital Signature

A digital signature (not to be confused with a digital certificate) is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and possibly to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. The ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

How It Works: Assume you were going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was Unchanged from what you sent and that it is really you.

1. You copy-and-paste the contract (it's a short one!) into an e-mail note.
2. Using special software, you obtain a message hash (mathematical summary) of the contract.
3. You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
4. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.)

At the other end, your lawyer receives the message.

1. To make sure it's intact and from you, your lawyer makes a hash of the received message.
2. Your lawyer then uses your public key to decrypt the message hash or summary.
3. If the hashes match, the received message is valid.

Firewalls

Firewalls

A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices that is configured to permit or deny network transmissions based upon a set of rules and other criteria. Firewalls can be implemented in either hardware or software, or a combination of both.

Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which inspects each message and blocks those that do not meet the specified security criteria.

The Nature of Today’s Attackers

Who are these “hackers” who are trying to break into your computer? Most people imagine someone at a keyboard late at night, guessing passwords to steal confidential data from a computer system. This type of attack does happen, but it makes up a very small portion of the total network attacks that occur. Today, worms and viruses initiate the vast majority of attacks. Worms and viruses generally find their targets randomly. As a result, even organizations with little or no confidential information need firewalls to protect their networks from these automated attackers.

If a worm or a virus does find security vulnerability and compromises your system, it can do one of several things. To begin with, it will almost always start looking for other systems to attack so that it can spread itself further. In this case, you become one of the bad guys— because the worm or virus is using your computer to attack other systems on your internal network and the Internet, wasting your computing resources and bandwidth. Even though the worm or virus won’t know what to do with your confidential data, chances are good that it will open a new back door into your system to allow someone else to further abuse your computer and compromise your privacy. Worms and viruses have dramatically increased the need for network security of all kinds—especially the need for host-based firewalls.

Individuals still launch some attacks, though, and these are generally the most dangerous. The least worrisome attackers focus on crashing computers and networks by using Denial of Service (DoS) attacks. Others might be looking for confidential data that they can abuse for profit, such as sales contacts, financial data, or customer account information. Still others might be amassing hundreds or thousands of computers from which to launch a distributed attack against a single network on the Internet.

The Firewall to the Rescue

In the physical world, businesses rely on several layers of security. First, they rely on their country’s government and military forces to keep order. Then, they trust their local police to patrol the streets and respond to any

windows, employee badges, and security systems. If all these defenses fail and a business is a victim of a crime, the business’s insurance agency absorbs part of the impact by compensating the business for a portion of the loss. Just as you lock your car and home, you need to protect your computers and networks.

Firewalls are these locks, and just like in the physical world, they come in different shapes and sizes to suit different needs. The famous Jargon Dictionary has a great definition for firewall: “a dedicated gateway machine with special security precautions on it, used to service outside network connections and dial-in lines.”

Firewalls serve two useful purposes:

- they filter what traffic comes into your network from the outside world, and
- they control what computers on your network may send there.

It’s important to understand one thing, however. No firewall—whether a small, free hostbased firewall or a multiple-thousand-dollar enterprise firewall array—will make your computers impervious to attack. Firewalls, like locks and walls and moats and dragons, create barriers to attack—they get in the way of someone trying to take control. By making it difficult for attackers to get into your computer, by making them invest lots of time, you become less attractive.

Firewalls very effectively block most bad guys from compromising an individual computer. But it’s impossible to fully prevent every intrusion: All software has bugs, and someone might find an obscure bug in your firewall that allows them to pass through. In a nutshell, there’s no such thing as absolute security.

Types of Firewalls: there are two main types of firewalls:

1. Network firewalls and
2. Host-based firewalls.

Network firewalls, such as the software-based Microsoft’s Internet Security and Acceleration (ISA) Server or the hardware-based Nortel Networks Alteon Switched Firewall System, protect the perimeter of a network by watching traffic that enters and leaves.

Host-based firewalls, such as Internet Connection Firewall (ICF—included with Windows XP and Windows Server 2003), protect an individual computer regardless of the network it’s connected to. You might need one or the other—but most businesses require a combination of both to meet their security requirements.

Secure Web Documents

Secure Web Documents

If you notice a broken skeleton or an unlocked padlock displayed in the lower left corner of the browser window, you are looking at icons that indicate that the document is not secure. Most documents on the Web are not secure. When the skeleton key is whole or the padlock is locked, you are looking at a secure document. Secure documents require a secure server, which is a server that uses encryption schemes. The URL of a secure document usually begins with https, rather than http, where the s means secure.

When a client requests a secure document, the server must first determine if they have the permission required to retrieve the document. The authentication process may require the user to submit a password. The server and the client must agree on an encryption scheme, so that all messages (including password) can be transmitted securely. Users may have to obtain a private key via some other mechanism (such as s-mail) before they can authenticate themselves to a secure server and decrypt messages. A high level of security can thus be achieved on the web, using the encryption schemes currently available.

Intrusion Detection System (IDS)

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.

Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once sends the warning notifications.

Classification of Intrusion Detection System:

IDS are classified into 5 types:

1. **Network Intrusion Detection System (NIDS):**
   Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks. Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.
2. **Host Intrusion Detection System (HIDS):**
   Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot. If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.
3. **Protocol-based Intrusion Detection System (PIDS):**
   Protocol-based intrusion detection system (PIDS) comprises of a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server. It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.
4. **Application Protocol-based Intrusion Detection System (APIDS):**
   Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers. It identifies the intrusions by monitoring and interpreting the communication on application specific protocols. For example, this would

monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

5. **Hybrid Intrusion Detection System :**

   Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system. Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS:

1. **Signature-based Method:**

   Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1's or number of 0's in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

   Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. **Anomaly-based Method:**

   Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

Comparison of IDS with Firewalls:

IDS and firewall both are related to the network security but an IDS differs from a firewall as a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls restrict access between networks to prevent intrusion and if an attack is from inside the network it don't signal. An IDS describes a suspected intrusion once it has happened and then signals an alarm.

Risk analysis

The risk management steps include:

- Assign and track corrective actions, as necessary, to reduce residual risk to an acceptable level.
- Continuously monitor the security posture

A security risk analysis is a procedure for estimating the risk to computer related **assets** and loss because of manifested **threats**. The procedure first determines an asset's level of **vulnerability** by identifying and evaluating the effect of in-place **countermeasures**. *An asset's level of vulnerability to the threat population is determined solely by countermeasures [controls/safeguards] that are in-place at the time the risk analysis is done.*

Next, detailed information about the asset is used to determine the significance of the asset's vulnerabilities. This includes how the asset is (or will be) used, data sensitivity levels, mission criticality, inter-connectivity, etc. Finally, the negative impact [**expected loss**] to the asset is estimated by examining various combinations of threats and vulnerability areas.

The highlighted words in the above paragraphs point out the more important terms associated with security risk analysis. That is, assets, threats, vulnerability, counter- measures, and expected loss. *If you understand how these various "things" relate to each other you will understand the rationale behind a security risk analysis.*

How do we know what our potential losses will be if we do not do an analysis? Should we spend the time and money to implement one or more countermeasures if manifested threats are unlikely? Is the status quo acceptable?

A *security risk analysis* defines the current environment and makes recommended corrective actions if the residual risk is unacceptable. Risk analysis is a vital part of any ongoing security and risk management program. The risk analysis process should be conducted with sufficient regularity to ensure that each agency's approach to risk management is a realistic response to the current risks associated with its information assets. Management must then decide on whether to accept the residual risk or to implement the recommended actions.

Believe it or not, YOU do one or more risk analyses every day of your life! Every time you cross the street or pull out onto the highway you do an analysis of the threats, vulnerabilities, and in-place countermeasures, and decide if the risk of asset loss is acceptable. If it is, you proceed. If not, you may put one or more additional countermeasures in-place and analyze the risk again.

In order to discuss security risk analysis concepts we must first establish a baseline of the related terms. Then, we must define how the terms relate to each other and how they are used to analyze risk.

Risk Analysis Terminology

Asset - Anything with value and in need of protection.

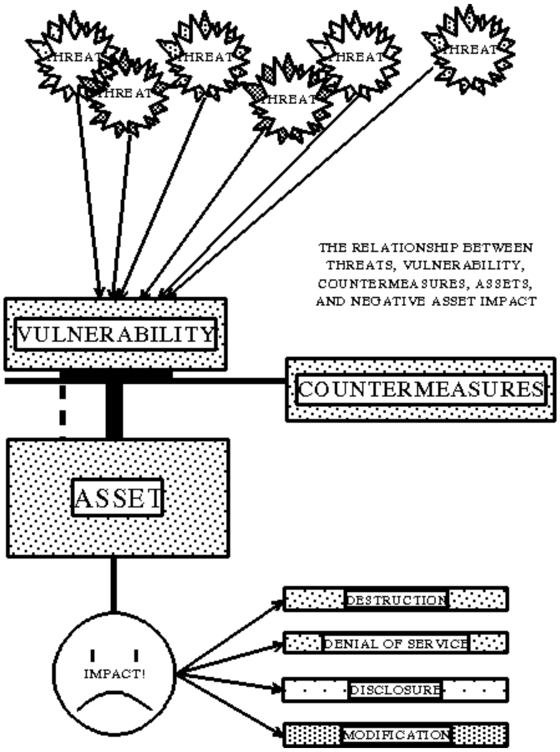
Threat - An action or potential action with the propensity to cause damage.

Vulnerability - A condition of weakness. *If there were no vulnerabilities, there would be no concern for threat activity.*

Countermeasure - Any device or action with the ability to reduce vulnerability.

Expected Loss - The anticipated negative impact to assets due to threat manifestation.

Impact - Losses as a result of threat activity are normally expressed in one or more impact areas. Four areas are commonly used; Destruction, Denial of Service, Disclosure, and Modification.



THE RELATIONSHIP BETWEEN THREATS, VULNERABILITY, COUNTERMEASURES, ASSETS, AND NEGATIVE ASSET IMPACT

How "Things" Work Together

A security risk analysis is an examination of the interrelationships between assets, threats, vulnerabilities, and countermeasures to determine the **current** level of risk. The level of risk that remains after consideration of all in-place countermeasures, vulnerability levels, and related threats is called **residual risk.** Ultimately, it is the residual risk that must be accepted [as is] or reduced to a point where it can be accepted.

The relationship between the elements of a risk analysis is illustrated in the graph at left. Any given threat in the population of threats is poised to take advantage of system vulnerabilities, countermeasures reduce the level of vulnerability, the asset is what needs to be protected, and the impacts are the result of threat activity through residual risk.

Doing The Analysis

Although the same "things" are involved in a security risk analysis, many variations in the procedure for determining residual risk are possible. Likewise, the metric for expressing residual risk can vary from good/bad or high/low to a statement that a certain amount of money will be lost. But, in the end, any security risk analysis should indicate (1) the current level of risk, (2) the likely consequences, and (3) what to do about it if the residual risk is too high.

What risk analysis methodology is best? Which one will produce the desired results with the least cost and time? Should the procedure be qualitative?, quantitative? automated? manual?, or some combination of these?

All risk analysis methodologies enable system users to compare possible losses to their agency with the cost of countermeasures (a.k.a. safeguards or controls) designed to protect against those losses.

To be useful, a risk analysis methodology should produce a quantitative statement of the impact of a risk or the effect of specific security problems. The three key elements in risk analysis are; (1) A statement of impact or the cost of a specific difficulty if it happens, (2) A measure of the effectiveness of in-place countermeasures, and (3) A series of recommendations to correct or minimize identified problems.

How many people will be needed? For how long? How much experience must they have, what type, and what impact will their experience [or lack thereof] have? Will the results suffer from inaccuracies, inconsistencies in the information obtained? What are the advantages of automation?

Planning for information security and risk management begins with identifying the information assets, data sensitivity, values, in-place countermeasures, applicable threats and their frequency of occurrence, system (project) configuration. This information is later used to calculate vulnerabilities and risks. The computer or network risk assessment process consists of nine separate, but interrelated steps. The following paragraphs provide a description of what's involved in these 9 steps.

Identify and Valuate Assets

The first step for all risk assessments is to identify and assign a value to the assets in need of protection. The value of assets is a significant factor in the decision to make operational tradeoffs to increase asset protection. The essential point is to list all things that could be affected by a security problem. These include: *hardware, software, data, people, documentation, and supplies.*

An assets' value is based on its cost, sensitivity, mission criticality, or a combination of these. When the value is based on something other than cost, it is usually converted to money using a standard equivalency table. The asset value will be used later in the assessment process to determine the magnitude of loss when threats occur.

Identify Applicable Threats

After identifying the assets that require protection, the threats to those assets must be identified and examined to determine for loss. This step involves the identification and description of threats in the threat population that seem appropriate for the system or network being assessed, and estimating how often they are likely to occur. These include: *unauthorized access, disclosure of information, denial of service, access points, misconfigured systems, software bugs, insider threats, as a minimum.*

<u>Threat Definition</u>

A threat is a potential force that could degrade the confidentiality (compromise), accuracy (integrity), or avail-ability (denial of service) of the system or network. Threats can be human (intentional or unintentional) or environmental (natural or fabricated). Two axioms apply for threats:

Axiom 1: The same population of threats exist for all systems and networks. <u>Postulation:</u> The population of threats is infinite in number and variety. Any given threat in the population will occur at an undetermined and uncontrolled frequency. Only the likelihood of threat occurrence varies between systems and locations. For example, the threat of an earthquake exists for both a system located inside Cheyenne Mountain, Colorado and one located in Oakland, California, but the likelihood of an earthquake occurrence varies greatly.

Axiom 2: The frequency of occurrence of a threat cannot be altered.

Postulation: Apparent alteration to the frequency of occurrence of a threat is, in reality, altering the *impact* of threat occurrence through countermeasures. Countermeasures reduce the level of vulnerability to the manifested threat, not how often the threat occurs. To say that countermeasure implementation alters threat frequency is to say that using an umbrella will alter how often it rains.

Applicable Threats

Determining which threats apply is an involved process that entails research of historical records, mathematical formulas, and empirical conclusions. In the end, however, both if and when a threat will occur is always an educated guess.

Threat identification, usually on a form, includes a title, a brief definition, and written rational for the inclusion of the threat in the assessment process. A written justification for the estimated frequency of occurrence must also be provided.

Identify/ Describe Vulnerabilities

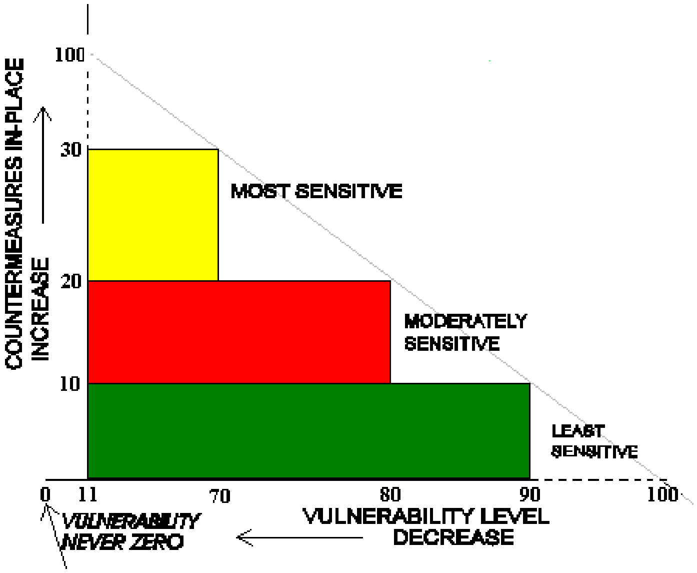
The level of risk is determined by analyzing the interrelationship of threats and vulnerabilities. A risk exists when a threat has a corresponding vulnerability, but even high vulnerability areas are of no consequence if no threats occur.

Vulnerability Definition

A vulnerability is a condition of weakness. A condition of weakness creates an opportunity for exploitation by one or more threats. The following axiom applies for vulnerabilities:

Axiom 3: The level of vulnerability decreases as countermeasures increase. Postulation: The level of vulnerability to threats is reduced by the implementation of countermeasures. Some countermeasures have a greater propensity to offset vulnerability than others. The level of vulnerability and the relative value of each counter-measure said to reduce it can be expressed numerically.

Axiom 3 is illustrated in the following graph:



Determine the Impact of Threat Occurrence

Pair Threats and Vulnerabilities

A threat is any action with the potential to cause a negative impact. If there were no threats to computer systems, there would be no need to be concerned about computer system vulnerabilities. By linking or pairing threats with vulnerabilities the potential for threat occurrence evaluation is tailored to any particular environment.

When the exploitation of a vulnerability occurs, the asset suffers an impact (loss). The losses are categorized in impact areas titled Disclosure, Modification, Destruction, and Denial of Service.

Disclosure

This is a confidentiality issue. Greater emphasis is placed on this impact area when sensitive or classified information is being processed.

Modification

When an asset is changed from its original state by the effect of threat manifestation it is called Modification. This is of special concern when a threat might modify the content of a database, say, in a computer aboard one of NASA's Shuttles.

Destruction

In this case the asset is damaged beyond practical use by threat activity. Emphasis is placed on this impact area when the complete loss of an asset is a more important concern than its modification or temporary non-availability.

Denial of Service

This impact is emphasized when threats are more likely to cause a temporary loss of capability than total destruction of modification.

By emphasizing one or more impact areas in the evaluation process, management can focus their resources on reducing the impact in the area that concerns them most. In-Place Countermeasures

Credit must be given for **all** in-place countermeasures. Identifying in-place countermeasures is part of the up front data gathering process in any risk analysis process. Countermeasures can be categorized as *Technical* or *Administrative* with sub categories of each type as follows:

Preventive

This type countermeasure is designed to prevent damage or impact from an action or event from occurring.

Detective

These countermeasures provide some type of notification that something has gone wrong.

Corrective

Some countermeasures have the ability to correct identified problems, such as the loss of a bit in a word.

Countermeasure Definition

Countermeasures are the protection measures that reduce the level of vulnerability to threats. For recommendation purposes, they come in two flavors; required and discretionary. Both types of in-place countermeasures are identified as part of the initial data gathering activity. The following axiom applies to countermeasures:

Axiom 4: All countermeasures have inherent vulnerabilities.

Postulation: A vulnerability level of ZERO can never be obtained since all countermeasures have vulnerabilities themselves. For this reason, vulnerability can never be zero, and thus risk can never be totally eliminated.

Required Countermeasures

All countermeasures in this category can be traced to one or more written rules or regulations. The sensitivity of data being stored and/or processed on a system or network, and its mode of operation, determine which regulations apply. This, in turn, determines the required countermeasures.

Discretionary Countermeasures

This type of countermeasure is elective in nature. In many cases the required countermeasures will not reduce the level of vulnerability to a level acceptable to the Designated Accreditation Authority (DAA). In such cases, managers may choose to implement this type of countermeasure to adjust the level of vulnerability to an acceptable level.

Determine Residual Risks (Conclusions)

Residual risk refers to the level of risk that remains after giving credit for the in-place countermeasures. Based on the nature of countermeasures, as defined in Axiom 4 above, there will always be residual risk. The issue becomes one of determining whether or not the residual risk acceptable.

The residual risk takes the form of conclusions reached from the assessment process. The conclusions must identify:

(1) Areas which have a high vulnerability coupled with a likelihood of threat occurrence, and

(2) All required countermeasures that are not in-place.

The results of these steps provide the input needed to begin the selection of additional countermeasures.

Identify Additional Countermeasures (Recommendations)

Once the residual risk has been determined the next step is to identify the most effective and least costly way to reduce risk to an acceptable level. *An* *operational trade-off must be made any time additional countermeasures are implemented*.

Tradeoffs can take the form of cost, convenience, time, or a mix of these. The following axiom applies to reducing risk:

Axiom #5: An acceptable level of vulnerability can be obtained through the implementation of countermeasures.
Postulation: There exists a mix of countermeasures that can achieve any arbitrary level of vulnerability. By adding countermeasures, the vulnerability level can be adjusted to

a level commensurate with the sensitivity level of the information being processed or importance of the Project.

For discretionary countermeasures, this step also includes an assessment of the value of one countermeasure over others. This usually takes the form of a Return on Investment (ROI) calculation but may also be based on which is quickest and easiest to implement.

Required Countermeasure Recommendation

Required or mandated countermeasures that are not in-place are the first recommendation.

Discretionary Countermeasure Recommendation

The second recommendation usually identifies the discretionary countermeasures needed to further reduce the risk level.

Prepare a Risk Analysis Report

The risk analysis process helps to identify the information assets at risk and attach a value to the risks. Additionally, it identifies protective measures that minimize the effects of risk and assigns a cost to each countermeasure. The risk analysis process also determines whether the countermeasures are effective. After the analysis is complete, a report documenting the risk assessment must be prepared.

The biggest challenge in writing a security risk analysis report is to bridge the gap between risk analysis jargon and information management can understand and use for decision making. As a rule, management will focus on summary information and only use technical details if they are needed to support a decision or make a choice between recommendations.

The risk analysis report serves as the vehicle for presenting to management the findings of the risk analysis process and recommendations for information security. It provides company or agency management with the information needed to make intelligent and well-informed decisions related to security issues. The report should be forwarded to the agency or company head for prompt review, approval, and action.

The report should include only summary information. The working papers and detailed analyses that support the findings and Recommendations outlined in the report should

be maintained for reference purposes and as a resource for future risk analyses. The report and its related documentation should be considered sensitive information and be protected accordingly. They are not intended for general distribution. An acceptable risk analysis report outline is provided as Attachment (1).

The amount of effort involved with each of the above steps will vary greatly based on the size and complexity of the "Project" being analyzed. The first step is often critical in that the **scope** of the Project needs to be accurately defined. In other words, where does the Project start and end?; what components (individual computer systems, networks, etc.) are included in the definition of the "Project?"

The report’s technical details should include, as a minimum:

- Vulnerability levels

- Applicable threats and their frequency
- The use environment
- System connectivity
- Data sensitivity level(s)
- Residual risk, expressed on an individual vulnerability basis
- Detailed Annual Loss Expectancy calculations

So, which methodology for security risk analysis is best; qualitative?, quantitative?, or hybrid? Should the process be manual or automated? The most basic function of any security risk analysis process is to determine, as accurately as possible, the risk to assets. Of course, the procedure for determining the risk can be complex or simple, depending on the asset and on the analysis methodology used. The amount of risk can be expressed as good/bad; high/low (qualitative), as a calculated metric (quantitative), or a combination of the two (hybrid).

The process of data collection, analysis, and preparing a security risk analysis report involves many steps. It is time consuming, expensive, and more often than not, a collateral duty for the person(s) charged with getting it done. Moreover, the requirement to do a security risk analysis is cyclic in nature, e.g., initially, then once every one to three years.

There is little doubt that an automated risk analysis methodology is less demanding on the user in terms of time and experience. The concepts and implementation of most commercial automated methodologies contain the expertise and have undergone the scrutiny of both government and commercial users.

In contrast, manual methods are often less formal and require the user to interpret and execute numerous, and sometimes complicated, steps. This increases the likelihood of error or omission and makes repeatable results difficult to obtain.

After establishing what is to be protected and assessing the risks these assets face, it is necessary to decide how to implement the controls that protect these assets. The controls and protection mechanisms should be selected to adequately counter the vulnerabilities found during risk assessment and to implement those controls cost effectively.

The controls that are selected represent the physical embodiment of the security policy. Because these controls are the first and primary line of defense in the protection of assets, they must be selected wisely. If the major threat to the system is outside penetrations, implementation of biometric devices to authenticate regular system users would be unnecessary. On the other hand, if the major threat is unauthorized use of computing resources by regular system users, rigorous automated accounting procedures should be established. Another method of protecting assets is to use multiple strategies. In this way, if one strategy fails or is circumvented, another strategy comes into play to continue protecting the asset. Using several simpler strategies can often be more effective than one very sophisticated method. For example, dial-back modems can be used in conjunction with traditional logon mechanisms. Many similar approaches can be devised to provide several levels of protection for assets. However, those planning security strategies must keep in mind exactly what needs to be protected and cautiously avoid unneeded mechanisms and methods.