Application Security:

Application Security, the protection of an application against security threats, is a difficult task. Application Security must now extend beyond traditional network and data security to incorporate the need for Software Protection. The approach to Application Security must also be driven by a clear and thorough understanding of the potential threats at each point in the system or network. Application Security is comprised of Network Security, Data Security and Software Protection: Introduction to Application Security

• Network Security addresses external attacks generally against resources inside the firewall providing a service across a network. Network security has traditionally been addressed using firewalls, intrusion detection systems and virus scanners .

• Data Security is the protection of data used locally by an application or transmitted between users and servers. Cryptography is the main solution here as it is highly effective at protecting data during transmission and storage by ensuring its integrity and confidentiality.

• Software Protection is the protection of the software, or services rendered by the software, from attacks, thereby preventing theft of intellectual property and licensed content and ensuring that the software continues to function as intended. Typically these attacks include reverse engineering, tampering, copying, and automated forms of these attacks that can be launched across the network or on a desktop by relatively unsophisticated attackers.

Database security:- concerns the use of a broad range of information security controls to protect databases (potentially including the data, the database applications or stored functions, the database systems, the database servers and the associated network links) against compromises of their confidentiality, integrity and availability. It involves various types or categories of controls, such as technical, procedural/administrative and physical. Database security is a specialist topic within the broader realms of computer security, information security and risk management.

Security risks to database systems include, for example:

- Unauthorized or unintended activity or misuse by authorized database users, database administrators, or network/systems managers, or by unauthorized users or hackers (e.g. inappropriate access to sensitive data, metadata or functions within databases, or inappropriate changes to the database programs, structures or security configurations).
- Malware infections causing incidents such as unauthorized access, leakage or disclosure of personal or proprietary data, deletion of or damage to the data or programs, interruption or denial of authorized access to the database, attacks on other systems and the unanticipated failure of database services.
- Overloads, performance constraints and capacity issues resulting in the inability of authorized users to use databases as intended
- Physical damage to database servers caused by computer room fires or floods, overheating, lightning, accidental liquid spills, static discharge, electronic breakdowns/equipment failures and obsolescence
- Design flaws and programming bugs in databases and the associated programs and systems, creating various security vulnerabilities (e.g. unauthorized), data loss/corruption, performance degradation etc.
- Data corruption and/or loss caused by the entry of invalid data or commands, mistakes in database or system administration processes, sabotage/criminal damage etc.

Email Security:- Email security is the broad topic dealing with issues of unauthorized access and inspection of electronic mail. This unauthorized access can happen while an email is in transit, as well as when it is stored on email servers or on a user computer. In countries with a constitutional guarantee of the secrecy of correspondence, whether email can be equated with letters and get legal protection from all forms of eavesdropping comes under question because of the very nature of email. This is especially important as more and more communication occurs via email compared to postal mail.

- Email has to go through potentially untrusted intermediate computers (email servers, ISPs) before reaching its destination, and there is no way to tell if it was accessed by an unauthorized entity. This is different from a letter sealed in an envelope, where by close inspection of the envelope, it might be possible to tell if someone opened it. In that sense, an email is much like a postcard whose contents are visible to everyone who handles it.
- There are certain technological workarounds that make unauthorized access to email hard, if not impossible. However, since email messages frequently cross nation boundaries, and different countries have different rules and regulations governing who can access an email, email privacy is a complicated issue.

Internet security:- is a branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet.The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption.

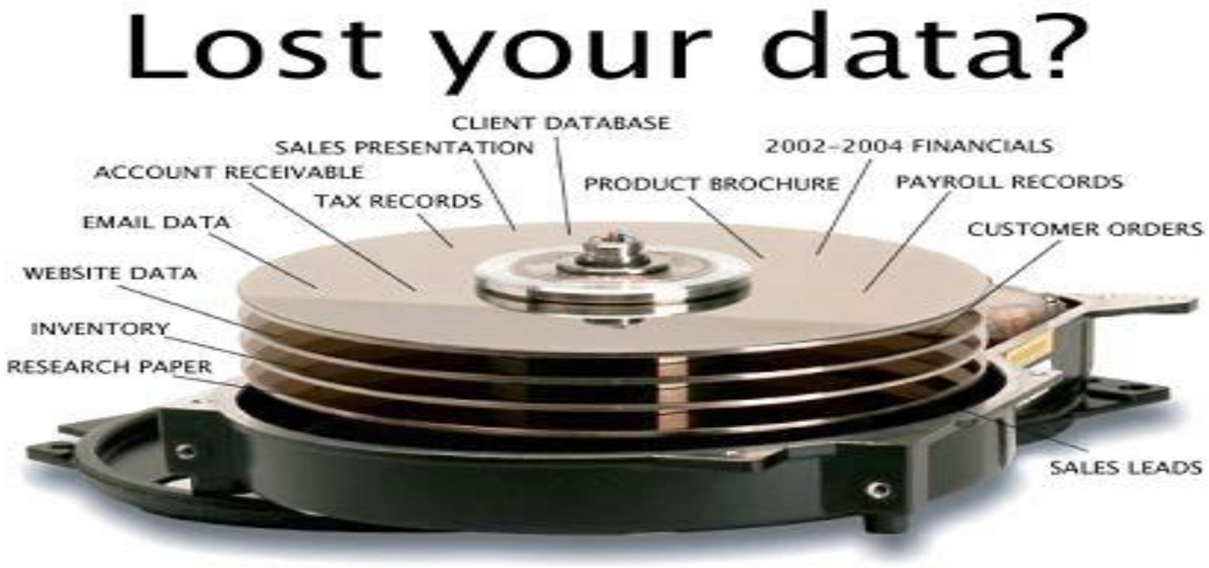
Data Security Considerations:-

To maintain the CIA(Confidentiality-Integrity-Availability) properties which require certain points to be considered.These data security consideration are related to data backup, archival and disposal.

Data Backup:-

Data is the most important aspect of your computer. The operating system can be reinstalled and so can applications, but it may be difficult or impossible to recreate your original data.

It is essential that you always back up your important information and have a plan for recovering from a system failure. An attacker could crash a computer's operating system or data may be corrupted or wiped out by a hardware problem. Computers can be lost, stolen, or destroyed in a fire.You should back up your personal or critical work data on a regular basis. This means copying your files over to a protected system that you can access when those files are needed.



Suggestions for backups

- Encrypt backups that contain sensitive data
- Keep extra backups off-site in a secure location (in case of property damage)
- Verify your backups to make sure files are retrievable
- Sanitize or destroy your backups (e.g., tapes, CDs) before discarding them

Data Archival:-

Data archiving is the process of moving data that is no longer actively used to a separate storage device for long-term retention. Archive data consists of older data that is still important to the organization and may be needed for future reference, as well as data that must be retained for regulatory compliance. Data archives are indexed and have search capabilities so files and parts of files can be easily located and retrieved.

Data archives are often confused with data backups, which are copies of data. Data backups are used as a data recovery mechanism that can be used to restore data in the event it is corrupted or destroyed. In contrast, data archives protect older information that is not needed for daily operations but may have to be accessed occasionally.

Data Disposal:-

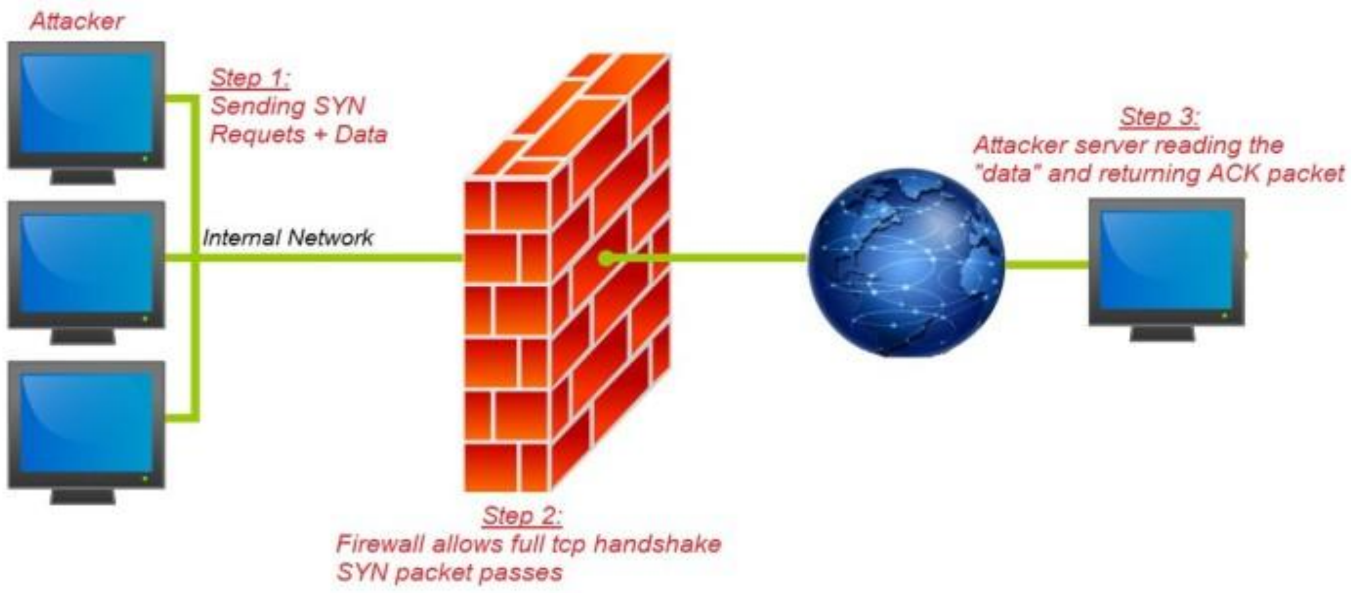
Data destruction is the process of destroying data stored on tapes, hard disks and other forms of electronic media so that it is completely unreadable and cannot be accessed or used for unauthorized purposes. When data is deleted, it is no longer readily accessible by the operating system or application that created it.

Security Technology

Firewall:-

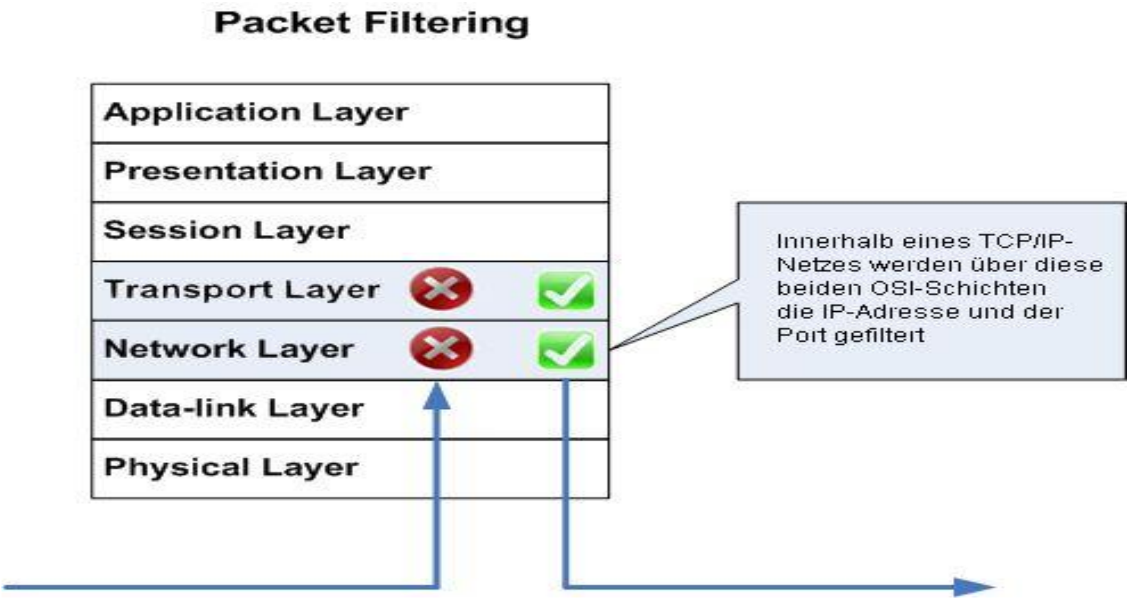
A firewall is a network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules.

A firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network defined in the firewall policy is; all other traffic is denied.

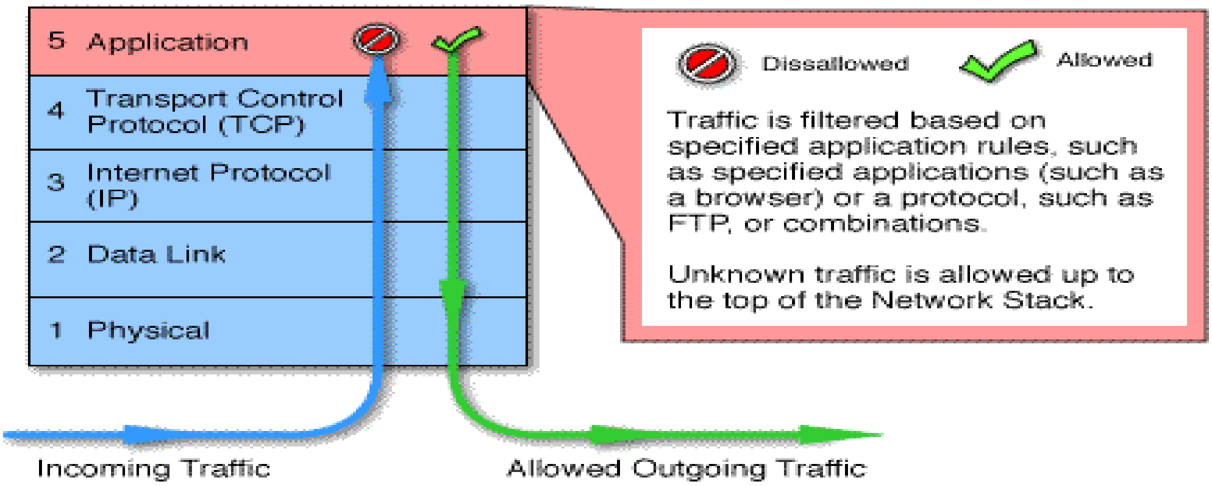

Attacker
Step 1:
Sending SYN
Requets + Data
Internal Network
Step 3:
Attacker server reading the
"data" and returning ACK packet
Step 2:
Firewall allows full tcp handshake
SYN packet passes

Types of Firewall:-

- **Packet filtering**
  Data flow consists of packets of information and firewalls analyze these packets to sniff out offensive or unwanted packets depending on what you have defined as unwanted packets.



- **Proxy server**
  Firewalls in this case assume the role of a recipient & in turn sends it to the node that has requested the information & vice versa.
- **Application level firewall**
  Application layer firewalls function in one of two modes: passive or active. Active application firewalls actively inspect all incoming requests -- including the actual message being exchanged -- against known vulnerabilities such as SQL injection, parameter and cookie tampering, and cross-site scripting. Only requests that are deemed "clean" are passed to the application. Passive application layer firewalls act in a manner similar to an IDS (Intrusion Detection System) in that they also inspect all incoming requests against known vulnerabilities, but they do not actively reject or deny those requests if a potential attack is discovered.

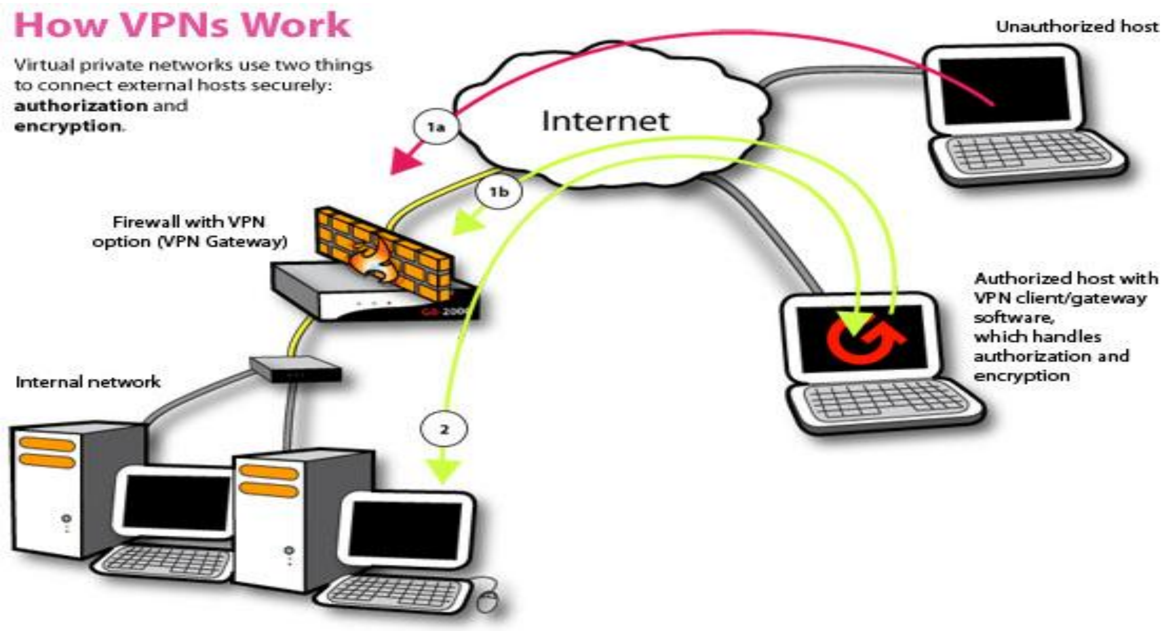

5 Application
4 Transport Control Protocol (TCP)
3 Internet Protocol (IP)
2 Data Link
1 Physical
Dissallowed
Allowed
Traffic is filtered based on specified application rules, such as specified applications (such as a browser) or a protocol, such as FTP, or combinations.
Unknown traffic is allowed up to the top of the Network Stack.
Incoming Traffic
Allowed Outgoing Traffic

Circuit-level gateway:-

A circuit-level gateway is a firewall that provides User Datagram Protocol (UDP) and Transmission Control Protocol (TCP) connection security, and works between an Open Systems Interconnection (OSI) network model's transport and application layers such as the session layer. Unlike application gateways, circuit-level gateways monitor TCP data packet handshaking and session fulfillment of firewall rules and policies.

VPN (Virtual Private Network):-

A VPN (Virtual Private Network) is a way of creating a secure connection 'to' and 'from' a network or a computer. The VPN uses strong encryption and restricted, private data access which keeps the data secure from the other users of the underlying network which could often be a public network like the Internet. VPNs have been used for years, but they have become more robust . They are more affordable & also much faster.


How VPNs Work
Virtual private networks use two things to connect external hosts securely: authorization and encryption.
Unauthorized host
Internet
1a
1b
Firewall with VPN option (VPN Gateway)
Authorized host with VPN client/gateway software, which handles authorization and encryption
Internal network
2

Types of VPN

There are many different types of VPNs available. Let's take a look at most common types.

1. PPTP VPN

This is the most common and widely used VPN protocol. They enable authorized remote users to connect to the VPN network using their existing Internet connection and then log on to the VPN using password authentication. They don't need extra hardware and the features are often available as inexpensive add-on software. PPTP stands for Point-to-Point Tunneling Protocol. The disadvantage of PPTP is that it does not provide encryption and it relies on the PPP (Point-to-Point Protocol) to implement security measures.

2. Site-to-Site VPN

Site-to-site is much the same thing as PPTP except there is no "dedicated" line in use. It allows different sites of the same organization, each with its own real network, to connect together to form a VPN. Unlike PPTP, the routing, encryption and decryption is done by the routers on both ends, which could be hardware-based or software-based.

3. L2TP VPN

L2TP or Layer to Tunneling Protocol is similar to PPTP, since it also doesn't provide encryption and it relies on PPP protocol to do this. The difference between PPTP and L2TP is that the latter provides not only data confidentiality but also data integrity. L2TP was developed by Microsoft and Cisco.

4. IPsec

Tried and trusted protocol which sets up a tunnel from the remote site into your central site. As the name suggests, it's designed for IP traffic. IPSec requires expensive, time consuming client installations and this can be considered an important disadvantage.

5. SSL

SSL or Secure Socket Layer is a VPN accessible via https over web browser. SSL creates a secure session from your PC browser to the application server you're accessing. The major advantage of SSL is that it doesn't need any software installed because it uses the web browser as the client application.

6. MPLS VPN

MPLS (Multi-Protocol Label Switching) are no good for remote access for individual users, but for site-to-site connectivity, they're the most flexible and scalable option. These systems are essentially ISP-tuned VPNs, where two or more sites are connected to form a VPN using the same ISP. An MPLS network isn't as easy to set up or add to as the others, and hence bound to be more expensive.

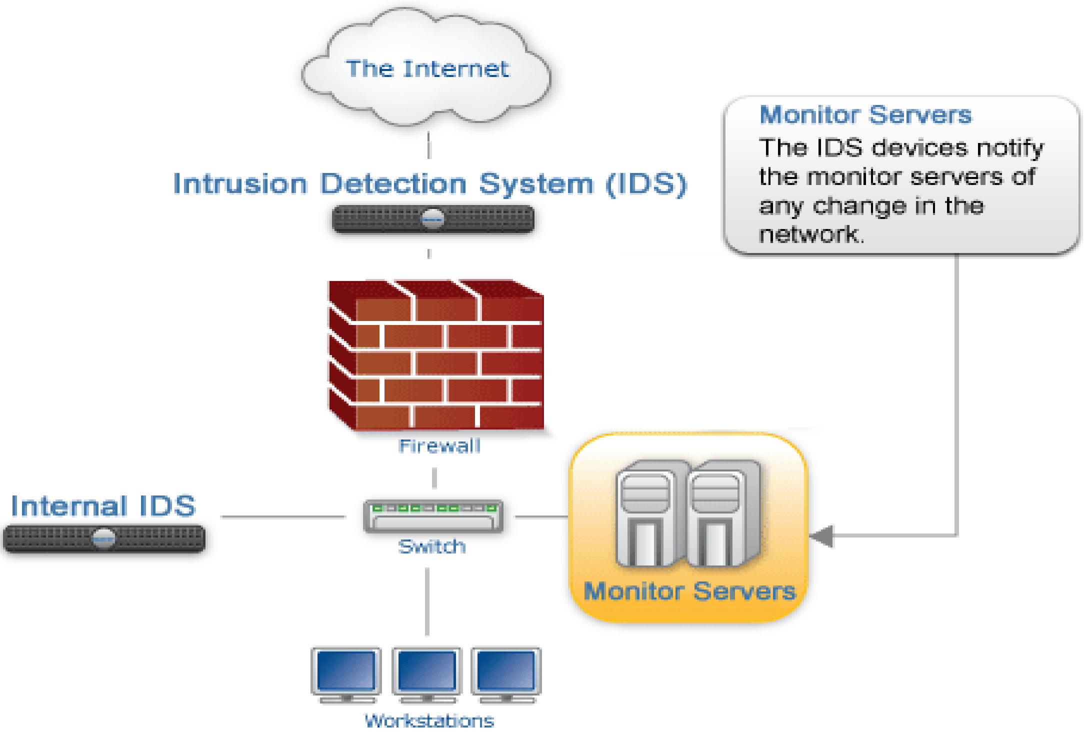
7. Hybrid VPN

A few companies have managed to combine features of SSL and IPSec & also other types of VPN types. Hybrid VPN servers are able to accept connections from multiple types of VPN clients. They offer higher flexibility at both client and server levels and bound to be expensive.

IDS(Intrusion detection system):-

An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.

Intrusion Detection System is any hardware, software, or a combination of both that monitors a system or network of systems against any malicious activity. This is mainly used for detecting break-ins or misuse of the network.


The Internet
Intrusion Detection System (IDS)
Monitor Servers
The IDS devices notify the monitor servers of any change in the network.
Firewall
Internal IDS
Switch
Monitor Servers
Workstations

Types of IDS

There are three main types of Intrusion Detection Systems:

- Host Based
- Network Based
- Stack Based
- Signature Based
- Anomaly Based

Host Based IDS

Intrusion Detection System is installed on a host in the network. HIDS collects and analyzes the traffic that is originated or is intended to that host. HIDS leverages their privileged access to monitor specific components of a host that are not readily accessible to other systems. Specific components of the operating system such as password files in UNIX and the Registry in Windows can be watched for misuse. There is great risk in making these types of components available to NIDS to monitor.

Although HIDS is far better than NIDS in detecting malicious activities for a particular host, they have limited view of entire network topology and they cannot detect attack that is targeted for a host in a network which does not have HIDS installed.

Network Based IDS

Network IDSs (NIDS) are placed in key areas of network infrastructure and monitors the traffic as it flows to other host. Unlike HIDS, NIDS have the capability of monitoring the network and detecting the malicious activities intended for that network. Monitoring criteria for a specific host in the network can be increased or decreased with relative ease.

NIDS should be capable of standing against large amount number of network traffic to remain effective. As network traffic increases exponentially NIDS must grab all the traffic and analyze in a timely manner.

Stack Based IDS

Stack based IDS is latest technology, which works by integrating closely with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers. Watching the packet in this way allows the IDS to pull the packet from the stack before the OS or application has a chance to process the packets.

Signature Based IDS

Signature-Based IDS use a rule set to identify intrusions by watching for patterns of events specific to known and documented attacks. It is typically connected to a large database which houses attack signatures. It compares the information it gathers against those attack signatures to detect a match. Also signature based IDS's may affect performance in cases when intrusion patterns match several attack signatures. In cases such as these, there is a noticeable performance lag. Signature definitions stored in the database need to be specific so that variations on known attacks are not missed. This sometimes leads to building up of huge databases which eat up a chunk of space.

Anomaly Based IDS

Anomaly Based IDS examines ongoing traffic, activity, transactions and behavior in order to identify intrusions by detecting anomalies.

It works on the notion that "attack behavior" differs enough from "normal user behavior" such that it can be detected by cataloging and identifying the differences involved.

Anomaly detectors monitor network segments to compare their state to the normal baseline and look for current behavior which deviate statistically from the normal. This capability theoretically gives anomaly based IDSs abilities to detect new attacks that are neither known nor for which signatures have been created.

Access Control:

Access Control is any mechanism by which a system grants or revokes the right to access some data, or perform some action. Normally, a user must first Login to a system, using some Authentication system. Next, the Access Control mechanism controls what operations the user may or may not make by comparing the User ID to an Access Control database.

Access Control systems include:

- File permissions, such as create, read, edit or delete on a file server.
- Program permissions, such as the right to execute a program on an application server.
- Data rights, such as the right to retrieve or update information in a database.

Security Threats

There are numerous threats to security of applications and data. With the increasing use of internet and the advancing IT, applications are becoming increasingly vulnerable to threats that could be a malicious code, viruses, worms, etc.

Some of the security threats are as follows:-

Virus Attack

A computer virus is a man-made program or piece of code that is loaded onto one‘s computer without the victims‘ knowledge and runs against his/her wishes.

Viruses can also replicate themselves over and over again and is relatively easy to produce. Even a simple virus is dangerous because it corrupts the system.

An even more dangerous type of virus is the one capable of transmitting itself across networks and bypassing security systems.

Viruses can be transmitted as attachments to an e-mail note or in a downloaded file, or be present on a diskette or CD.

E-mail viruses:

An e-mail virus travels as an attachment to e- mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. Some e-mail viruses don't even require a double-click they launch when you view the infected message in the preview pane of your e-mail software.

The different damages a virus can cause:

- An annoying message appearing on the computer screen.
- Reduce memory or disk space.
- Modify existing data.
- Overwrite or Damage files.
- Erase hard drive.

PROTECTION TIPS:

- Use anti-virus from good brands like Mc-Afee or Kaspersky.
- Turn on _auto update option for your browser and plug-ins.
- Install Anti- malware.
- For extra security, run anti-malwares by different brands.
- Set a strong password for your FTP.
- Configure FTP client settings. Activate the option to ―Always use SFTP‖.
- Avoid sites that do not look trustworthy.
- Avoid sites in which _https‘ is clearly striked out.
- Quick Scan pen drives and flash drives when you insert them into your systems.
- Scan your systems frequently.

Worm

Computer worms are standalone malware programs that will use your computer network to replicate themselves in order to spread to other computers. Unlike a computer virus, it does not need to attach itself to any program, file or document.

In some ways worms are more deadly than viruses because they don‘t need to lodge themselves into programs to replicate. Worms can replicate independently through your system. Once in your system, worms will look scan your network for other machines that may have similar security holes. If the worm finds one, it will copy itself into the new computer and start the process all over again.

Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their uncontrolled replication consumes system resources, slowing or halting other tasks. Worms can perform a variety of operations according to how it has been designed.

- It can cause a denial of service attack
- It gets attached to Microsoft outlook or any such mailing facility and sends mails to everybody on the address list (replicates itself and passes on the worm to everyone in the address list),
- overwrites your files and documents, and
- Makes your computer slow and dis-functional.

Illustration:

The ILOVEYOU virus comes in an e-mail note with "I LOVE YOU" in the subject line and contains an attachment that, when opened, results in the message being re-sent to everyone in the recipient's Microsoft Outlook address book and, perhaps more seriously, the loss of every JPEG, MP3, and certain other files on the recipient's hard disk.

As Microsoft Outlook is widely installed as the e-mail handler in corporate networks, the ILOVEYOU virus can spread rapidly from user to user within a corporation. On May 4, 2000, the virus spread so quickly that e-mail had to be shut down in a number of major enterprises such as the Ford Motor Company. The virus reached an estimated 45 million users in a single day.

Trojan

A Trojan horse program is a program that appears to have some useful or benign purpose, but really masks some hidden malicious functionality.

Today‘s Trojan horses try to sneak past computer security fortifications (such as firewalls), by employing like-minded trickery. By looking like normal software, Trojan horse programs are used for the following goals:

- Duping a user or system administrator into installing the Trojan horse in the first place. In this case, the Trojan horse and the unsuspecting user becomes the entry vehicle for the malicious software on the system.

- Blending in with the normal programs running on a machine. The Trojan horse camouflages itself to appear to belong on the system so users and administrators continue their activity, unaware of the malicious code‘s presence.

Attackers have devised a myriad of methods for hiding malicious capabilities inside their wares on your computer. These techniques include

- employing simple, yet highly effective naming games.
- using executable wrappers.
- attacking software distribution sites.
- manipulating source code.
- co-opting software installed on your system.
- disguising items using polymorphic coding techniques.

As we discuss each of these elements, we must bear in mind that the attackers‘ main goal is to disguise the malicious code so that the victims do not realize what the attacker is up to.

Types of Trojans

The most common types of Trojans found today are:

1. Remote Administration Trojans (RATs)

These are the most popular Trojans. They let a hacker access the victim's hard disk, and also perform many functions on his computer (shut down his computer, open and shut his CD-ROM drive etc.).

Modern RATs are very simple to use. They come packaged with two files - the server file and the client file. The hacker tricks someone into running the server file, gets his IP address and gets full control over the victim computer.

Most RATs are used for malicious purposes - to irritate or scare people or harm computers. There are many programs that detect common Trojans. Firewalls and anti-virus software can be useful in tracing RATs.

RATs open a port on your computer and bind themselves to it (make the server file listen to incoming connections and data going through these ports). Then, once someone runs his client program and enters the victim's IP address, the Trojan starts receiving commands from the attacker and runs them on the victim's computer.

2. Password Trojans

Password Trojans search the victim‘s computer for passwords and then send them to the attacker or the author of the Trojan. Whether it's an Internet password or an email password there is a Trojan for every password. These Trojans usually send the information back to the attacker via email.

3. Privileges-Elevating Trojans

These Trojans are usually used to fool system administrators. They can either be bound into a common system utility or pretend to be something harmless and even quite useful and appealing. Once the administrator runs it, the Trojan will give the attacker more privileges on the system. These Trojans can also be sent to less-privileged users and give the attacker access to their account.

4. Key loggers

These Trojans are very simple. They log all of the victim‘s keystrokes on the keyboard (including passwords), and then either save them on a file or email them to the attacker once in a while. Key loggers usually don't take much disk space and can masquerade as important utilities, thus becoming very hard to detect.

5. Joke Programs

Joke programs are not harmful. They can either pretend to be formatting your hard drive, sending all of your passwords to some hacker, turning in all information about illegal and pirated software you might have on your computer to the police etc. In reality, these programs do not do anything.

6. Destructive Trojans

These Trojans can destroy the victim‘s entire hard drive, encrypt or just scramble important files. Some might seem like joke programs, while they are actually destroying every file they encounter. In an unreported case in India, a Trojan almost led to the death of a reporter!

Logic Bomb

A logic bomb is a piece of code intentionally inserted into a software system which when triggered will set off a malicious task such as reformatting, and/or deleting, altering or corrupting data on a hard drive. It's secretly inserted into the code of a computer's existing software, where it lies dormant until that event occurs.

A program in which damage is delivered when a particular logical condition occurs.
e.g.- not having the author's name in the payroll file. Logic bombs are a kind of Trojan Horse and most viruses are logic bombs.

PROTECTION TIPS:

- Always change passwords frequently. They save users from a lot of trouble.
- Use security measures to detect insider threats in your system. Basic anti-viruses are not efficient enough.

Phishing & Spoofing attacks

In the 19th century, British comedian Arthur Roberts invented a game called Spoof, which involved trickery and nonsense. This gave the English speaking world a new word that today symbolizes a gamut of hacking technologies.

Spoofing attacks primarily include e-mail spoofing, SMS spoofing, IP spoofing, and web spoofing. Spoofing attacks are used to trick people into divulging confidential information (e.g. credit card data) or doing something that they would usually not do (e.g. installing malicious software on their own computers).

Such use of spoofing attacks is commonly referred to as Phishing.

Sending an e-mail from somebody else‛s e-mail ID is the simplest form of **Email spoofing**. Innumerable tools exist on the Internet which can easily be used to send e-mails appearing to have been sent by somebody else. The effects are intense.

Case: Many customers received an email from their bank asking them to verify their usernames and passwords for the bank records. The emails were spoofed, but thousands of customers clicked on the link in the email and submitted the information at the webpage that opened up. On investigation, it is found that the emails were sent by a disgruntled employee.

Case: Thousands of employees of a global IT company ended up installing viruses on their computers when they executed an attachment appearing to have been sent out by their officers. The employees even disabled the anti-virus software because the email said that the attachment may be incorrectly detected as a virus!‖ On investigation, it was found that the emails had been sent out by a rival company.

SMS spoofing is very similar to e-mail spoofing. The major difference being that instead of an email ID, a cell phone number is spoofed and instead of a spoofed e-mail, a spoofed SMS is sent.

Case: A young lady received an SMS from her husband‛s cell phone informing her that he had had an accident and was at the hospital and urgently needed money. On receiving the SMS, she rushed out of the house with the money. She was attacked and robbed by the person who had sent her the spoofed SMS.

An IP address (e.g. 192.168.10.85) is the primary identification of a computer connected to a network (e.g. the Internet). A criminal usually uses IP spoofing to bypass IP based authentication or to mislead investigators by leaving a trail of false evidence. IP spoofing can be accomplished using proxy servers and simple PHP scripts that are readily and freely available online.

Case: Internet users in many countries use proxy servers to bypass Government imposed Internet censorship. (We are not passing any comment on whether is it right or wrong to impose Internet censorship or bypass it, as the case may be.)

DNS spoofing involves manipulating the domain name system to take unsuspecting victims to fake websites (that look identical to the original ones). Sitting at the computer you may type in www.asianlaws.org but the site that opens up may be a fake site!

This can and has been done at the local organizational level (e.g. by host file rewriting or by a network administrator with malicious intentions) or at the national or international level (by hackers exploiting vulnerabilities in the BIND software that runs most of the world‛s domain name servers).

Case: Hundreds of employees at a global financial services company received emails from a popular online store about a huge discount on some popular books and DVDs. On clicking the link in the email, users were taken to what appeared to the website of the online store. Most of the recipients of the emails placed orders using their credit cards. No one got the books or the DVDs.

PROTECTION TIPS:

- Enable authentication based on the key exchange on your network. IPsec will significantly reduce the risk of spoofing.

- Ensure you use access control to deny private IP addresses on your downstream interface.
- Filter inbound and outbound traffic.
- Preferably, in cases of suspicion, always ensure if the sender actually sent the mail or

Malware (Malicious Software)

Malware, short for malicious software, is software used or created by hackers to infiltrate or damage or disrupt computer operation, gather sensitive information, or gain access to private computer systems. While it is often software, it can also appear in the form of scripts or code. 'Malware' is a general term used to refer to a variety of forms of hostile, intrusive, or annoying software.

Malware includes computer, worms, trojan horses, spyware, adware, most root kits, and other malicious programs. In law, malware is sometimes known as a computer contaminant, as in the legal codes of several U.S. states. Some malware is disguised as genuine software, and may come from an official company website.

Malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others. It can also hijack your browser, redirect your search attempts, serve up nasty pop-up ads, track what web sites you visit etc. Malware is sometimes used broadly against corporations to gather guarded information, but also to disrupt their operation in general. Many malwares will reinstall themselves even after you think you have removed them, or hide themselves deep within Windows, making them very difficult to clean.

Left un-guarded, personal and networked computers can be at considerable risk against malware threats.

As per an analysis done in the Kaspersky lab, the following is the result.

PROTECTION TIPS:

- Use a firewall.
- Keep track and control your emails.
- Use up-to date antivirus software.
- Scan your computer frequently to detect unknown malicious programs running.
- Secure your browser.

Trap doors

Trap doors, also referred to as **backdoors**, are bits of code embedded in programs by the programmer(s) to quickly gain access at a later time, often during the testing or debugging phase. If an unscrupulous programmer purposely leaves this code in or simply forgets to remove it, a potential security hole is introduced. Hackers often plant a backdoor on previously compromised systems to gain later access. Trap doors can be almost impossible to remove in a reliable manner. Often, reformatting the system is the only sure way.

Macro virus

A macro virus is a computer virus that alters or replaces a macro, which is a set of commands used by programs to perform common actions. For example, the "open document" action in many word-processing programs relies on a macro to function, since there are several discrete steps in the process. Macro viruses change this command set, allowing them to execute whenever the macro is run. A macro virus is a computer virus that "infects" a Microsoft Word or similar application and causes a sequence of actions to be performed automatically when the application is started or something else triggers it. Macro viruses tend to be surprising but relatively harmless.

Network Attack

A Network attack is usually defined as an intrusion on your network infrastructure that will first analyze your environment and collect information in order to exploit the existing open ports or vulnerabilities - this may include as well unauthorized access to your resources. In such cases where the purpose of attack is only to learn and get some information from your system but the system resources are not altered or disabled in any way.

Types of Network Attacks

- Data Modification
- Identity Spoofing (IP Address Spoofing)
- Password-Based Attacks
- Denial-of-Service Attack
- Man-in-the-Middle Attack

Denial of Service (DoS):-

A denial of service (DoS) attack involves an attempt to disrupt the normal functioning of a website or web service. In a typical DoS attack, the attacker will overload a site's server with requests for access far above the capacity of the site, meaning that legitimate requests cannot be processed. Other examples include: disrupting service to a specific person or system, flooding a network with traffic to prevent legitimate traffic from flowing, preventing a person from accessing a particular service and disrupting the connection between two specific machines, there by interrupting a service. An e-mail bomb is another type of DoS attack wherein a large number of spam emails are sent in order to disable a mail server. In a distributed denial of service attack, the attacker uses several host computers to attack another computer or network.

SECURITY THREATS TO E-COMMERCE:-

Internet, being a public domain, is open to all. Each and every transaction that occurs on the internet can be tracked, monitored logged, and stored. The information is shared over the internet or carrying out transactions is constantly under security threats. These threats may originate from internal or external sources. Thus, it becomes imperative for businesses to understand these security threats well before making their presence online. Some of the top security threats from internal and external sources are as follows:-

1. Unauthorized internal users who may access confidential information by using stolen passwords for committing fraud or theft.
2. Former employees of an organization who have maintained access to the information sources directly by creating alternative passwords, back doors into the computer system, or indirectly through former co-workers.
3. Weak access points in information infrastructure and security that can expose company information and trade secrets.
4. Management that undermines security may be the greatest risk to e-commerce.
5. Contractors, partners, consultants, etc. who take benefit of even limited access to important systems.

An increase in the sale of various anti-virus software and subscription to e-mail virus protection indicate that people are increasingly becoming aware of these threats. Businesses can make it mandatory for their service providers and merchants to have firewalls, encryption, as well as testing and access policies as a condition of doing business with them.

E-CASH AND ELECTRONIC PAYMENT SYSTEM

Electronic payments are the central part of E-Commerce activities as it deals with the strategies for the payment of goods and services by online customers. Electronic payments also refer to the activity of account settlement where the prompt settlement of payments is crucial. If the debit and credit to the bank account, customer and the company are not settled immediately or suffers due to conventional processing delays, then the entire business chain may be interrupted. Payment and settlement of the business chain may be interrupted. Payment and settlement of the business account are the bottleneck in all E-Commerce activities. Conventional instruments for payments such as demand draft, credit notes, and cheques are not suited to E-Commerce. The electronic version of this instrument also may not work well particularly when small payments are to be made. The supplier as well as the customer would like to settle the payment online when the amount to be paid is small. Conventional instruments are too slow to be processed and the overheads in processing such instruments may be high.

Electronic Payment is defined as Electronic Payment is a financial exchange that takes place online between buyers and sellers. The content of this exchange is usually some form of digital financial instrument (such as encrypted credit card numbers, electronic cheques or digital cash) that is backed by a bank or an intermediary by a legal tender.

Various instruments which may used to make payment on the Internet are Credit/Debit cards, Smart Cards, Electronic Cash, Electronic Walled etc. Important issues related to the Electronic payment system include the methods, form and characteristic of payment instrument such as credit/debit cards, how to minimize the financial risk such as leakage of information, mistakes and frauds and finally devising methods for the completion of electronic payment cycle.

Several protocols have been devised and deployed to provide the necessary security to payment transactions. The Netscape Navigator and MS Internet Explorer have promoted their payment protocols for safe payment transaction and these have been implemented in their web browsers. Some of the commonly used protocols for secured transaction are as follows:

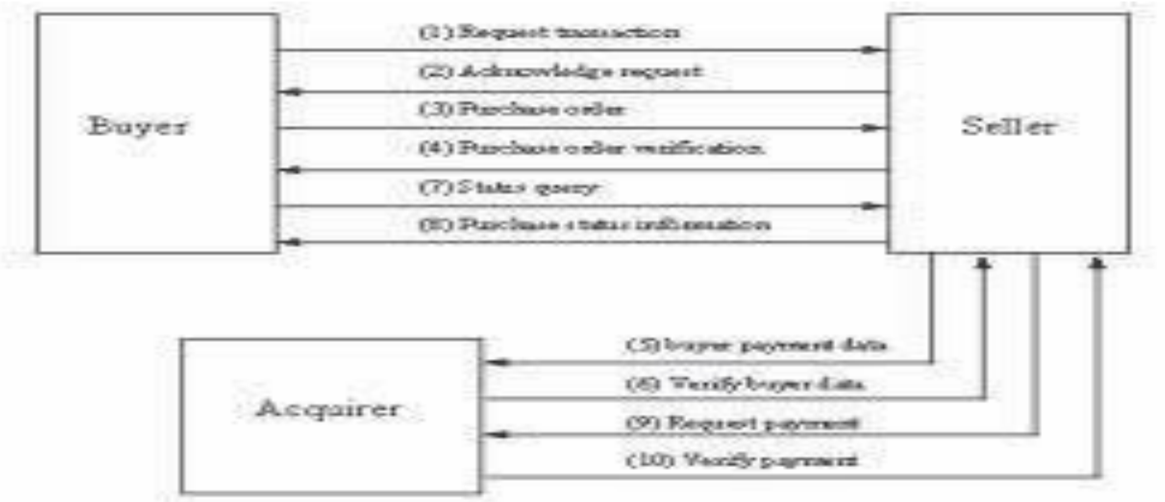
1. Secure Electronic Payment Protocol (SEPP)
2. Secure Electronic Transaction Protocol (SETP)

Secure Electronic Payment Protocol (SEPP)

SEPP has been developed by Master Card and Netscape. It has been implemented in the Netscape web browsers. Secure Electronic Transaction Protocol it a new E-Commerce industry Standard. Many companies are implementing SET protocol and is has many features in common with SEPP. SET is also one of the popular protocols for safe electronic transaction. It was developed by Microsoft and VISA. SET uses the cryptographic standard and digital signatures to secure the authentication and verification is done using digital signatures.

Electronic Payments through SEPP Protocol:

This protocol was developed jointly by Master Cards, e-Cash, Netscape and IBM. SEPP is open vendor free and license free specification for online payment transactions. SEPP works on the simple conventional process of signing and submission. This protocol involves three way communications involving to customer, company and the bank. The process is shown in the fig.



Electronic Payment System

As shown in the figure, the customer is a person who buys the product or services from a company. He does it by visiting the web site of the company. The customer is also a holder of a credit card and intends to pay for the purchased product and services through his credit card.

The company‘s web site displays and sells the items such as goods and services. It also accepts the payment from the customer against the purchased items and services.

Company‘s Banker is essentially a bank that services the company‘s account and processes credit card based transaction for the company.

Certificate management system represents the agent or broker who creates and distributes the digital certificate to customers and other financial institutions. The agent works on behalf of the credit card issuer bank. The whole process of purchase is done in the following steps:

The customer sends an initial message to the company web site.

1. Company response by sending the invoice message, enabling the customer to validate goods and services of the company.
2. The customer then prepares the purchase order the credit cards details. The credit card details are so encrypted that can only be decrypted by the Bank.
3. The company receives the purchase order. The company then sends the encrypted credit card details to its banker.
4. The banker decrypts the credit card details and may verify from the credit issuer bank.
5. When the company‘s banker verifies the authenticity of the credit card, is send an authorization response essentially contains the verification results of credit card.

1. Banking and financial payments

- Large-scale or wholesale payments (e.g.: Bank-to-Bank transfer)
- Small-scale or retail payments (e.g.: Automated teller machines and cash-dispensers)
- Home banking (e.g.: Bill payment)

2. Retailing payments

- Credit cards (e.g.: VISA or Master cards)
- Private label credit/debit cards
- Change cards

3. On-line electronic commerce payments

- Token- based payment system
    - Electronic cash (e.g.: Digicash)
    - Electronic checks (e.g.: Netcheque)

  - Smart cards or debit cards
- **Credit card-based payment system**
  - Encrypted credit cards (eg.: www from-based encryption)
  - Third-party authorization numbers

CREDIT CARDS

Credit card is working on the postpaid mechanism. Credit cards are another payment instrument which has now become very common. Credit cards are issued by a financial institution which allows you to make purchases up to a certain limit on credit. Most of the credit card companies recognize the organization or shop etc. from where you may purchase the item. Payment of these items is made by the credit card company or your behalf. The credit card companies regularly send the bill to the customer for the customers for the shopping they have done. In E-Commerce, use of credit card is very common. If consumers want to purchase a product or service, they simply send their credit card details to the service provider involved and the credit card organization will handle this payment like any other transaction.

The processing of the credit card when an item is purchased from a company or the web. When the customer wishes to purchase items from a web site, he places the purchase order electronically and sends encrypted credit card number. This information will be sent to the customer bank through the credit card processor. After checking the authenticity of the credit card, the banks allow the company to go ahead with the purchase. The bank will issue an electronic token to the company. The customer bank will realize the payment through monthly or fortnightly bill sent to the customer.

ADVANTAGES AND DISADVANTAGES TO CREDIT CARDS

ADVANTAGES:

• **Purchase Power and Ease of Purchase -** Credit cards can make it easier to buy things. If you don't like to carry large amounts of cash with you or if a company doesn't accept cash purchases (for example most airlines, hotels, and car rental agencies), putting purchases on a credit card can make buying things easier.

• **Protection of Purchases -** Credit cards may also offer you additional protection if something you have bought is lost, damaged, or stolen. Both your credit card statement (and the credit card company) can vouch for the fact that you have made a purchase if the original receipt is lost or stolen. In addition, some credit card companies offer insurance on large purchases.

• **Building a Credit Line -** Having a good credit history is often important, not only when applying for credit cards, but also when applying for things such as loans, rental applications, or even some jobs. Having a credit card and using it wisely (making payments on time and in full each month) will help you build a good credit history.

• **Emergencies -** Credit cards can also be useful in times of emergency. While you should avoid spending outside your budget (or money you don't have!), sometimes emergencies (such as your car breaking down or flood or fire) may lead to a large purchase (like the need for a rental car or a motel room for several nights.)

• **Credit Card Benefits -** In addition to the benefits listed above, some credit cards offer additional benefits, such as discounts from particular stores or companies, bonuses such as free airline miles or travel discounts, and special insurances (like travel or life insurance.)
While most of these benefits are meant to encourage you to charge more money on your credit

card (remember, credit card companies start making their money when you can't afford to pay off your charges!) the benefits are real and can be helpful as long as you remember your spending limits.

DISADVANTAGES:

• **Blowing Your Budget --** The biggest disadvantage of credit cards is that they encourage people to spend money that they don't have. Most credit cards do not require you to pay off your balance each month, so even if you only have $100, you may be able to spend up to $500 or $1,000 on your credit card. While this may seem like 'free money' at the time, you will have to pay it off -- and the longer you wait, the more money you will owe since credit card companies charge you interest each month on the money you have borrowed.

• **High Interest Rates and Increased Debt:** Credit card companies charge you an enormous amount of interest on each balance that you don't pay off at the end of each month.

• **Credit Card Fraud:** Like cash, sometimes credit cards can be stolen. They may be physically stolen (if you lose your wallet) or someone may steal your credit card number (from a receipt, over the phone, or from a Web site) and use your card to rack up debts.

DEBIT CARD

A debit card (also known as a bank card or check card) is a plastic card that provides an alternative payment method to cash when making purchases. Functionally, it can be called an electronic check, as the funds are withdrawn directly from either the bank account or from the remaining balance on the card. Debit cards may also allow for instant withdrawal of cash, acting as the ATM card for withdrawing cash and as a check guarantee card.

ADVANTAGES OF DEBIT CARDS:

• A consumer who is not credit worthy and may find it difficult or impossible to obtain a credit card can more easily obtain a debit card, allowing him/her to make plastic transactions. For example, legislation often prevents minors from taking out debt, which includes the use of a credit card, but not online debit card transactions.

• For most transactions, a check card can be used to avoid check writing altogether. Check cards debit funds from the user's account on the spot, thereby finalizing the transaction at the time of purchase, and bypassing the requirement to pay a credit card bill at a later date, or to write an insecure check containing the account holder's personal information.

• Like credit cards, debit cards are accepted by merchants with less identification and scrutiny than personal checks, thereby making transactions quicker and less intrusive. Unlike personal checks, merchants generally do not believe that a payment via a debit card may be later dishonored.

• Unlike a credit card, which charges higher fees and interest rates when a cash advance is obtained, a debit card may be used to obtain cash from an ATM or a PIN-based transaction at no extra charge, other than a foreign ATM fee.

DISADVANTAGES OF DEBIT CARDS:

• Use of a debit card is not usually limited to the existing funds in the account to which it is linked, most banks allow a certain threshold over the available bank balance which can cause overdraft fees if the users transaction does not reflect available balance.

• Many banks are now charging over-limit fees or non-sufficient funds fees based upon pre-authorizations, and even attempted but refused transactions by the merchant

• Many merchants mistakenly believe that amounts owed can be "taken" from a customer's account after a debit card (or number) has been presented, without agreement as to date, payee name, amount and currency, thus causing penalty fees for overdrafts, over-the-limit, amounts not available causing further rejections or overdrafts, and rejected transactions by some banks.

• In some countries debit cards offer lower levels of security protection than credit cards. Theft of the users PIN using skimming devices can be accomplished much easier with a PIN input than with a signature-based credit transaction. However, theft of users' PIN codes using skimming devices can be equally easily accomplished with a debit transaction PIN input, as with a credit transaction PIN input, and theft using a signature-based credit transaction is equally easy as theft using a signature-based debit transaction.

• In many places, laws protect the consumer from fraud much less than with a credit card. While the holder of a credit card is legally responsible for only a minimal amount of a fraudulent transaction made with a credit card, which is often waived by the bank, the consumer may be held liable for hundreds of dollars, or even the entire value of fraudulent debit transactions. The consumer also has a shorter time (usually just two days) to report such fraud to the bank in order to be eligible for such a waiver with a debit card, whereas with a credit card, this time may be up to 60 days. A thief who obtains or clones a debit card along with its PIN may be able to clean out the consumer's bank account and the consumer will have no recourse.

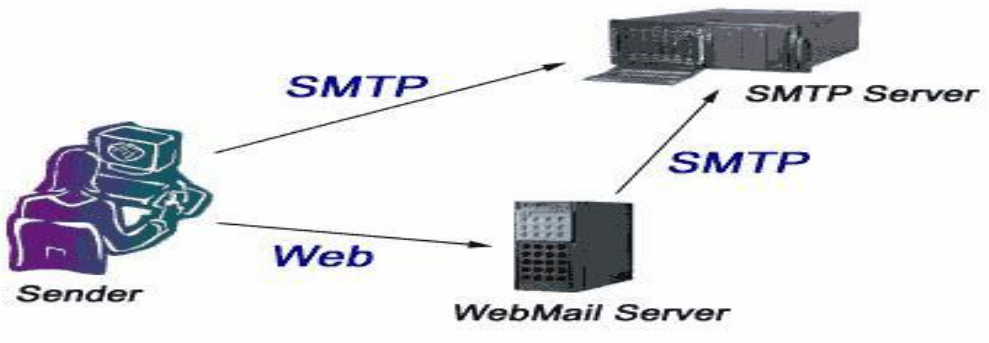
Introduction to Email Security How Email Works

This section describes the general mechanisms and paths taken by an email message on its route from sender to recipient. This should give you an overview of the different protocols (languages) involved, the different types of servers involved, and the distributed nature of email networks. The examples I present are representative of many common email solutions, but are by no means exhaustive.

Sending an Email Message

Sending an email message is like sending a postal letter. When sending a letter, you drop it off at your local post office. The local post office looks at the address and figures out which regional post office the letter should be forwarded to. Then the regional post office looks at the address and figures out which local post office is closest to your recipient.

Finally, the recipient‘s local post office delivers your letter to its recipient. Computers are like post offices, and the Simple Mail Transport Protocol (SMTP) is the procedure which an email post office uses to figure out where to send the letter next. Any program that sends an email message uses SMTP to deliver that message to the next post office‖ for relaying it to its final destination.



When you send a message with an email program on your personal computer (or your mobile phone or tablet), you have to specify an SMTP server so that your email program knows where to send the message. This SMTP server is like your local post office. Your email program talks directly to the server using the computer protocol known as SMTP. This is like dropping off a letter at the local post office.

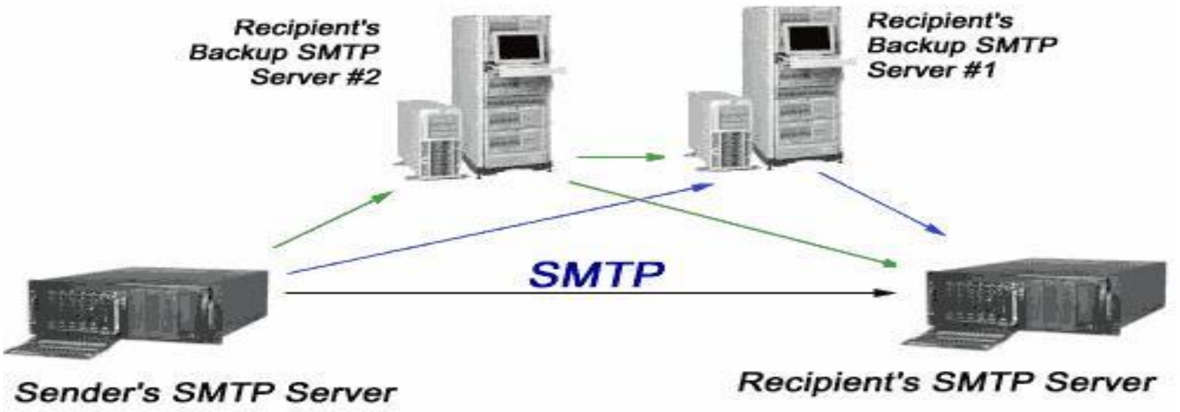
When you use WebMail, your personal computer uses an Internet connection to communicate with a web server. The language that the internet connection uses is HTTP HyperText Transfer Protocol When you send your message with WebMail, the web server itself takes care of contacting an SMTP server and delivering your message to it.

Delivery of email from your SMTP Server to your recipient's SMTP Server:

When an SMTP Server receives an email message, it first checks if an account for the message recipient is configured on the server itself. If there is such an account, the server will drop the message in that person‗s Inbox (or follow other more complex user defined rules). If there is no local account for that recipient, the server must relay the email message to another SMTP server closer to the recipient. This is analogous to how your local post office forwards your letter to a regional post office unless it is for someone served by the post office itself. (Post offices don‗t actually work this way in general, but the concept is easily understood with this analogy.) This process is known as SMTP relaying‖.

How does your SMTP Server know where to relay the message to?

If the recipient‗s email address is bob@luxsci.net‖, then the recipient‗s domain name is luxsci.net‖. Part of the DNS settings‖ for the recipient‗s domain (these are the mail exchange or MX records for the domain; see also Understanding Domain Name Service (DNS)) includes an ordered list of SMTP Servers that expect to receive email for this recipient. The highest priority SMTP Server listed (the one with the smallest numerically priority number in the DNS settings) is the recipient‗s actual inbound SMTP Server; the others are ―backup inbound SMTP Servers‖. These backup servers merely may either queue email for later delivery to the recipient‗s actual SMTP Server or may perform the same real-time delivery actions as the main SMTP server


Recipient's Backup SMTP Server #2
Recipient's Backup SMTP Server #1
SMTP
Sender's SMTP Server
Recipient's SMTP Server

There are many scenarios that govern the path an email message may take from the sender‗s to the recipient‗s SMTP Server. Some of these include:

1. The sender‗s server successfully contacts the recipient‗s server and sends the email message directly.
2. The sender‗s server cannot contact the recipient‗s actual SMTP server (maybe the recipient‗s server is busy, down, or has some other connection problem). In this case the sender‗s server tries to contact and deliver the message to the recipient‗s first backup server.

3. The sender‘s server cannot contact the recipient‘s actual SMTP server or its first backup server. In this case the sender‘s server tries to contact and deliver the message the recipient‘s second backup server.
4. The sender‘s server cannot contact any of the recipient‘s servers. In this case it will queue the message and try to send it later. It will keep retrying periodically for several days until it succeeds in sending or gives up.

Any message delivered to the backup servers which queue email goes through the same process of trying to contact the recipient‘s main SMTP Server, or a higher priority backup servers. Backup servers may also queue email for later sending.

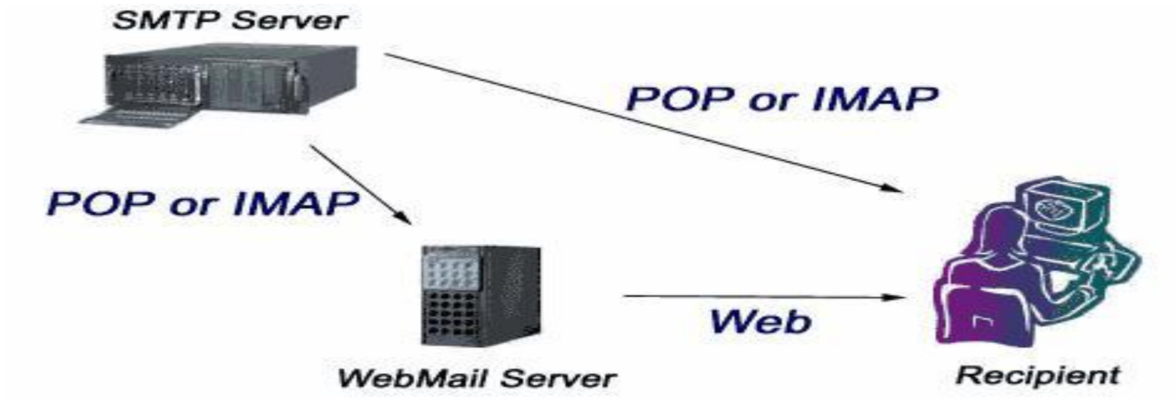
Once the email message arrives at the recipient‘s SMTP Server and is finally delivered to the recipient‘s email box, the recipient may pick up the message and read it whenever chooses .

Each server that receives your message adds its own Received stamp to the message headers. This stamp identifies what server received the message, at what time, and from what other server.Information allows the recipient to trace a message‘s entire journey.

1. Most email servers communicate with each other using SMTP
2. You never know how long it will take an email message to get from sender to recipient because you don‘t know how busy the servers are, how much traffic there is on the Internet, what machines are down for maintenance, etc.
3. Your messages may sit in queues on any number of servers for any amount of time. Some of these servers may belong to third parties.
4. Your recipients can determine the Internet address and name of the computer from which you are sending your messages, even in the case of your email being spoofed by a spammer.

Retrieving Email From an SMTP Server

When you receive an email message it sits in a file (or database) in your email server. If you wish to view this email message you must access this content. Any computer wishing to access your email must speak one of the languages the email Server does. With some exceptions (like MS Exchange), there are really only main 2 languages that email servers understand (for email retrieval, as opposed to email sending, for which they use SMTP), one is called the Internet Message Access Protocol (IMAP) and one is called the Post Office Protocol (POP).



As a recipient, you can generally retrieve your email by either using a web based interface known as WebMail, or via an email client program, such as Microsoft Outlook or iPhone Mail, running on your personal computer or device. The email client programs will talk directly to your email server and speak IMAP or POP or something similar. With WebMail, your computer will talk to a WebMail server using a web connection WebMail server will, in turn, talk to your email server using POP or IMAP or something similar (like a direct database connection).

The Lack of Security in Email

Email is inherently insecure. In the following sections, we will see just how insecure it is. At this stage, it is important to point out the insecurity in the email delivery pathway just discussed

- **WebMail**: If the connection to your WebMail server is insecure then all information including your username and password is not encrypted as it passes between the WebMail server and your computer.
- **SMTP**: SMTP does not encrypt messages. Communications between SMTP servers may send your messages in plain text for any eavesdropper to see. Additionally, if your email server requests that you send your username and password to ―login‖ to the SMTP server in order to relay messages to other servers, then these are also sent in plain text, subject to eavesdropping. Finally, messages sent via SMTP include information about which computer they were sent from and what email program was used. This information, available to all recipients, may be a privacy concern.
- **POP** and **IMAP**: The POP and IMAP protocols require that you send your username and password to login; these credentials are not encrypted. So, your messages and credentials can be read by any eavesdropper listening to the flow of information between your personal computer and your email service provider‗s computer.
- **BACKUPS**: Email messages are generally stored on SMTP servers in plain, unencrypted text. Backups of the data on these servers may be made at any time and administrators can read any of the data on these machines. The email messages you send may be saved unexpectedly and indefinitely and may be read by unknown persons as a result.

These are just a few of the security problems inherent in email. In the next section, we will talk about communications security problems in general so we can see what else can go wrong.

Security Threats to Your Email Communications

Eavesdropping: The Internet is a big place with a lot of people on it. It is very easy for someone who has access to the computers or networks through which your information is traveling to capture this information and read it. Just like someone in the next room listening in on your phone conversation, people using computers near the path your email takes through the Internet can potentially read and copy your messages.

Identity Theft: If someone can obtain the username and password that you use to access your email servers, they can read your email and send false email messages as you. Very often, these credentials can be obtained by eavesdropping on SMTP, POP, IMAP or Webmail connections, by reading email messages in which you include this information, or through other means.

Invasion of Privacy: If you are very concerned about your privacy, then you should consider the possibility of unprotected backups, listed below. You may also be concerned about letting your recipients know the IP address of your computer. This information may be used to tell in what city you are located or even to find out what your address is in some cases. This is not usually an issue with Web Mail, POP, or IMAP, but is an issue with the transport of email, securely or insecurely, from any email client over SMTP.

Message Modification: Anyone who has system administrator permission on any of the SMTP Servers that your message visit, can not only read your message, but they can delete or change the message before it continues on to its destination. Your recipient has no way to tell if the email message that you sent has been altered! If the message was merely deleted they wouldn’t even know it had been sent.

False Messages: It is very easy to construct messages that appear to be sent by someone else. Many viruses take advantage of this situation to propagate themselves. In general, there is no way to be sure that the apparent sender of a message is the true sender the sender‘s name could have been easily fabricated.

Message Replay: Just as a message can be modified, messages can be saved, modified, and re-sent later! You could receive a valid original message, but then receive subsequent faked messages that appear to be valid.

Unprotected Backups: Messages are usually stored in plain text on SMTP Servers. Thus, backups of these servers‘ disks usually contains plain text copies of your messages. As backups may be kept for years and can be read by anyone with access to them, your messages could still be exposed in insecure places even after you think that all copies have been deleted.

Repudiation: Because normal email messages can be forged, there is no way for you to prove that someone sent you a particular message. This means that even if someone DID send you a message, they can successfully deny it. This has implications with regards to using email for contracts, business communications, electronic commerce.

Symmetric and Asymmetric Encryption in a Nutshell

A basic knowledge of the two main types of encryption will be very useful. This section presents these concepts in a simple, straightforward form.

Symmetric Encryption

In symmetric encryption, you and your friend share a secret key. Using this key, you can encrypt a message into cipher text. Cipher text looks like a random sequence of characters and is completely meaningless to anyone unless they also have the secret key, in which case they can decrypt the cipher text back into the original message and read it.

Using symmetric key encryption, eavesdropping and unwanted backups of your messages no longer are a problem It also becomes harder for someone to modify your messages in transit in any kind of a meaningful way.

The problem with symmetric key encryption is precisely the fact that you and your friend must share the same secret key. Unless you meet in person, how do you communicate this key in a way that is secure? What if you want to send a secure message to someone on the other side of the world? How do you get them the secret key quickly in a way that eavesdroppers can‘t detect?

Message Digests / Authentication Codes

A Message Digest or Message Authentication Code is really a very simple concept.

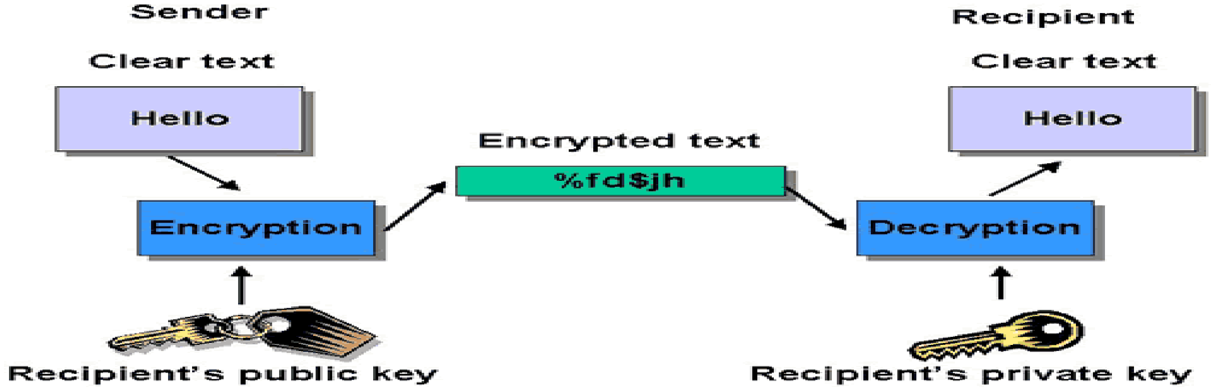
You take your message and pass it through an algorithm that spits out a relatively short sequence of characters (maybe 128 or 256 or so of them). This sequence of characters is a fingerprint of the message. Any minute change in the message would produce a significantly different fingerprint. There is no way to reverse engineer the original message from its fingerprint and it is almost impossible to find two messages that yield the same fingerprint (just like trying to find two complete strangers who have the same fingerprint). Message Digests are quick ways to check to see if a message has been altered. If you have a digest of the original message and compare it with a digest of the message you just received and they match, then you know that the message has been unaltered.

Public key Cryptography (Asymmetric Encryption)

In asymmetric encryption, also known as public key encryption, each person has TWO keys. Any cipher text created using one of the keys can ONLY be decrypted using the other key. For example, say you have keys K1″ and K2″. If you encrypt your message with K1, then ONLY K2 can be used to decrypt it. Similarly, if you encrypt using K2, ONLY K1 can be used to decrypt it. This is distinctly different from symmetric key encryption where you only have one key that performs both functions on the same message.

In asymmetric key encryption, the two keys that each person possesses are commonly named the private‖ and public keys because the public one is published or given out freely to anyone who wants a copy and the private one is kept secret. The security of asymmetric key encryption depends only on whether you can keep your private key secret. Asymmetric key encryption allows you to do many clever things:

- **Send an Encrypted Message:** To send a secure message to someone, all you have to do is encrypt it with their public key. Only the intended recipient who has the matching private key will be able to decrypt and read the message. This solves the problem of eavesdropping and the problem of sending secret keys that is inherent in symmetric key encryption.
- **Prove You Sent A Message:** To prove to someone that you sent a message, you can encrypt the message with your private key. Then, anyone can decrypt it with your public key and read the contents. The fact that your public key decrypts the message proves that only you could have sent it (or someone who has your private key).
- **Sign a Message:** A message signature proves that you sent the message AND allows the recipient to determine if the message was altered in transit. This is done by using your private key to encrypt a digest of a message at the time of sending. The recipient can decrypt this digest and compare it to a digest of the received message. If they match, then the message is unaltered and was sent by you.
- **Encrypted, Signed Messages:** The most secure form of communication is to first add a signature to the message and then to encrypt the message plus signature with the recipient‘s public key. This combines all of the benefits of all of the techniques: security against eavesdropping and unexpected storage, proof of sender, and proof on message integrity.



The ultimate solution is to use asymmetric key encryption to provide message signatures and/or encryption. This completely solves the issues of-

- Eavesdropping (everything is always encrypted)
- Message modification (message digests are used)
- Message replay (you can include a timestamp in the signature)
- Repudiation (signatures allow proof of who sent the message)
- Unprotected backups (everything is always encrypted)

Asymmetric key encryption should be used in combination with SSL so that your username and password are also protected.

Fortunately (or unfortunately), there are two widely used forms of asymmetric key encryption for email: S/MIME and PGP. Both allow you to add signatures and/or encryption to your messages. PGP can be obtained from PGP.com and is compatible with standard email clients. S/MIME is built into many email clients like Microsoft.

Conclusion

Email is, in general, Completely Insecure The security issues include:

1. Eavesdropping
2. Identity Theft
3. Invasion of Privacy
4. Message Modification
5. False Messages
6. Message Replay
7. Unprotected Backups
8. Repudiation (Sender denies that s/he sent it)

SSL: It is simple and easy to use SSL (and TLS) to secure the communications between your computers and your email service provider‘s computers. This works no matter who your recipients are. SSL improves security in these ways:

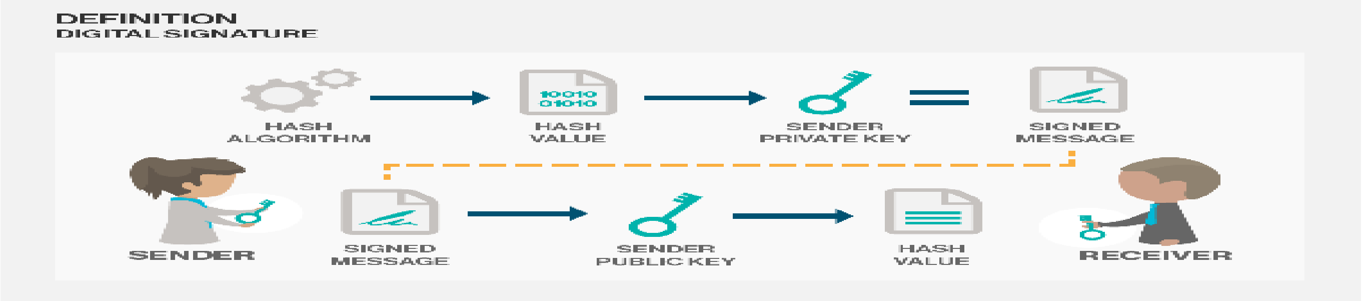
1. It establishes that you are contacting your service provider‘s computers.
2. It encrypts the username and password that you use to login to these servers. This mitigates identity theft and other issues.
3. It protects your message from eavesdroppers between your computer and your SMTP server.

PGP and S/MIME: PGP and S/MIME keys use asymmetric key encryption to protect the contents of your messages throughout their complete journeys. They provide:

1. Protection against eavesdropping and unwanted backups
2. Message Digests to detect whether messages have been altered in transit
3. Signatures to prove sender authenticity.

Digital Signature:-

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software or digital document.

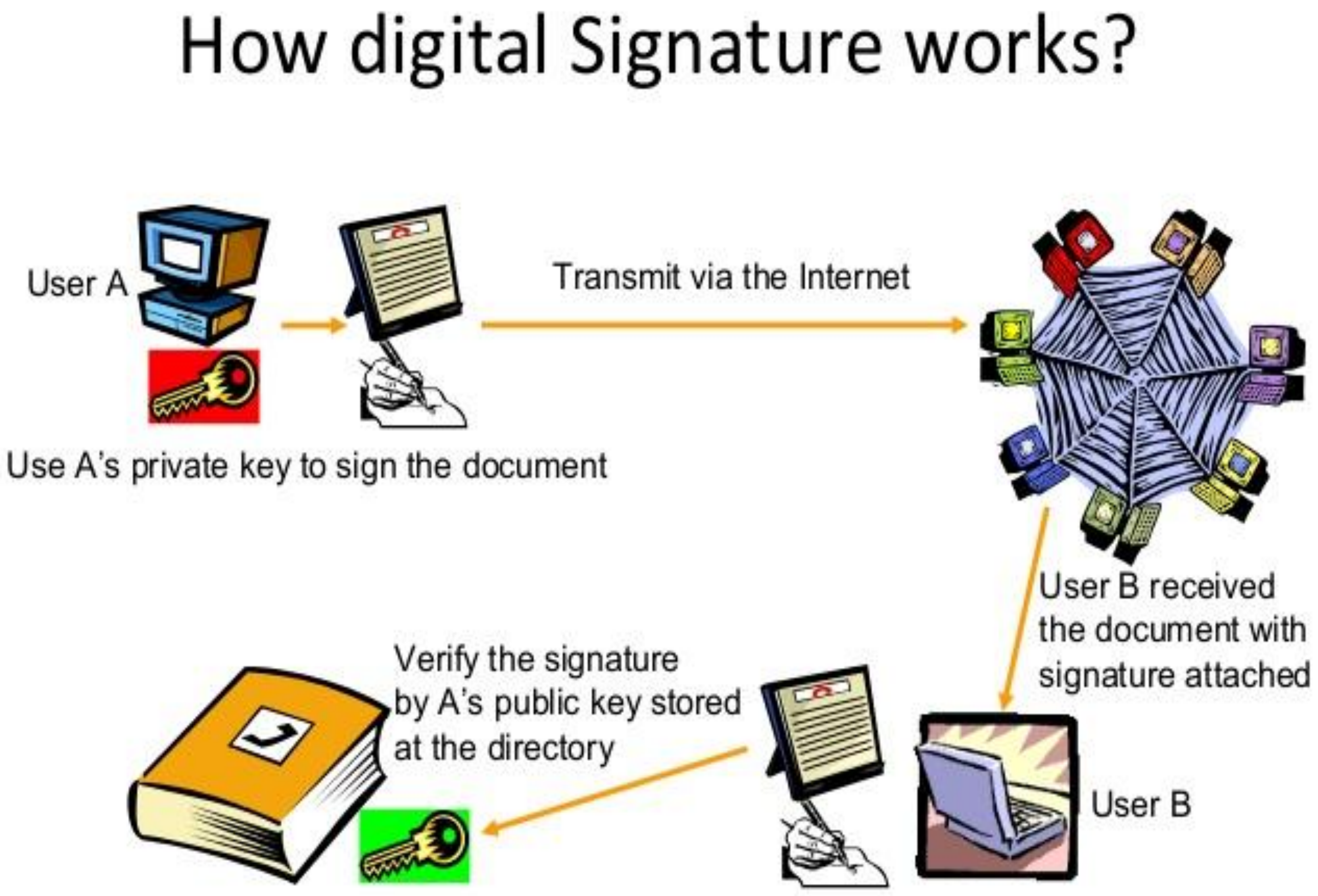


The digital equivalent of a handwritten signature or stamped seal, but offering far more inherent security, a digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide the added assurances of evidence to origin, identity and status of an electronic document, transaction or message, as well as acknowledging informed consent by the signer.

How digital signatures work

Digital signatures are based on public key cryptography, also known as asymmetric cryptography. Using a public key algorithm such as RSA, one can generate two keys that are mathematically linked: one private and one public. To create a digital signature, signing software (such as an email program) creates a one way hash of the electronic data to be signed. The private key is then used to encrypt the hash. The encrypted hash along with other information, such as the hashing algorithm is the digital signature. The reason for encrypting the hash instead of the entire message or document is that a hash function can convert an arbitrary input into a fixed length value, which is usually much shorter. This saves time since hashing is much faster than signing.

A digital signature can be used with any kind of message whether it is encrypted or not simply so the receiver can be sure of the sender's identity and that the message arrived intact. Digital signatures make it difficult for the signer to deny having signed something (non-repudiation) assuming their private key has not been compromised as the digital signature is unique to both the document and the signer, and it binds them together. A digital certificate, an electronic document that contains the digital signature of the certificate-issuing authority, binds together a public key with an identity and can be used to verify a public key belongs to a particular person.


How digital Signature works?
User A
Transmit via the Internet
Use A's private key to sign the document
User B received the document with signature attached
Verify the signature by A's public key stored at the directory
User B