

Subject Notes

Unit -1

Introduction of Cyber Crime:

Cyber crime, or computer oriented crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cybercrimes can be defined as: Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS) Cybercrime may threaten a person or a nation's security and financial health.

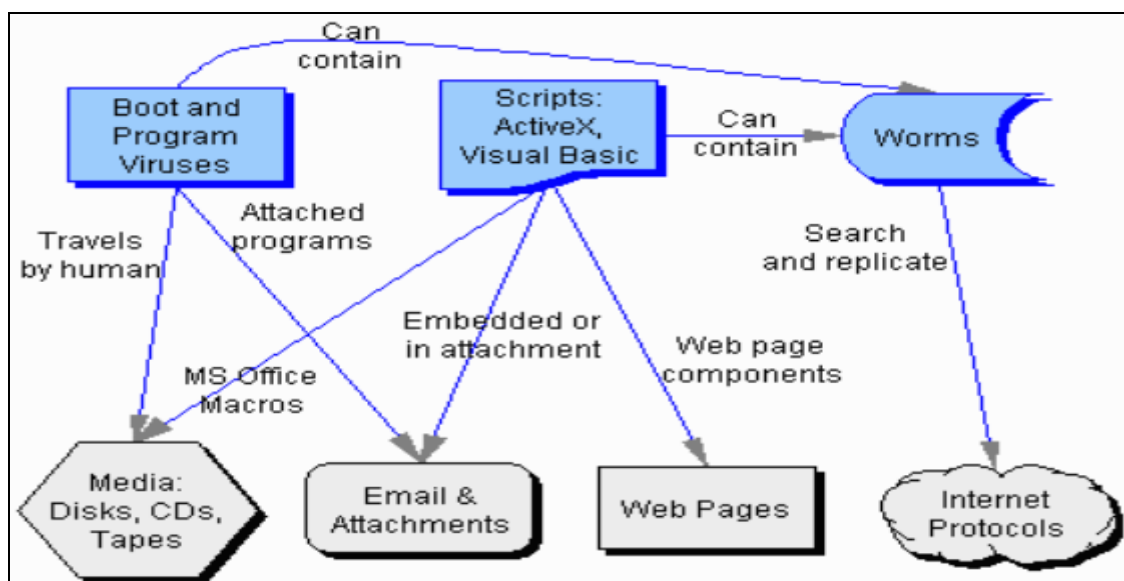


Fig.1 Web attacks

Challenges of cyber crime-There are many challenges in front of us to fight against the cyber crime. Some of them here are discussed below:

- Lack of awareness and the culture of cyber security, at individual as well as organizational level.
- Lack of trained and qualified manpower to implement the counter measures.
- No e-mail account policy especially for the defense forces, police and the security agency personnel.
- Cyber attacks have come not only from terrorists but also from neighboring countries contrary to our National interests.
- The minimum necessary eligibility to join the police doesn't include any knowledge of computers sector so that they are almost illiterate to cyber-crime.
- The speed of cyber technology changes always beats the progress of govt. sector so that they are not able to identify the origin of these cyber-crimes.
- Promotion of Research & Development in ICTs is not up to the mark.
- Security forces and Law enforcement personnel are not equipped to address high-tech crimes.
- Present protocols are not self sufficient, which identifies the investigative responsibility for crimes that stretch internationally.
- Budgets for security purpose by the government especially for the training of law enforcement, security personnel's and investigators in ICT are less as compare to other crimes

Classifications of Cybercrimes: Given below are the types of cybercrime:

- **Hacking-** A hacker is an unauthorized user who attempts to or gains an access to an information system. Hacking is a crime even if there is no visible damage to the system, since it is an intrusion in to the privacy of someone's data. There are classes of Hackers.
 - **White Hat Hackers** - They believe that information sharing is good, and that it's their responsibility to share their expertise by facilitating access to information.
 - **Black Hat Hackers** - They cause damage after intrusion. They may steal or modify information or insert viruses or worms which may damage the system. They are also called „crackers“.
 - **Grey Hat Hackers** - Occasionally violates hacker ethics. Hackers will hack into networks, stand-alone computers and software. Network hackers try to gain unauthorized access to private networks for curiosity, challenge and distributing information. Crackers perform unauthorized intrusion with damage like stealing or changing of information or inserting viruses or worms.
- **Cyber Stalking-** This involves use of internet to harass someone. The behavior in this crime includes false accusations, threats etc. This involves following a person's movements across the Internet by posting messages (sometimes threatening) on bulletin boards frequented by the victim, entering chat-rooms frequented by the victim, constantly sending emails to the victim etc.
- **Spamming** -Spamming is sending of unsolicited bulk and commercial messages over the internet. Although irritating to most email users, it is not illegal unless it causes damage such as overloading network and disrupting service to subscribers or creates .negative impact on consumer's attitudes for Internet Service Provider.
- **Cyber Pornography-** Women and children are victims of sexual exploitation through internet. Pedophiles use the internet to send photos of illegal child pornography to targeted children so as to attract children to such funs.
- **Phishing-** It is a criminally fraudulent process of acquiring sensitive information such as username, passwords and credit card details by disguising as a trustworthy entity in an electronic communication.
- **Software Piracy-** It is an illegal reproduction and distribution of software for business or personal use. This is considered to be a type of infringement of copy right and a violation of a license agreement. Since the unauthorized user is not a party to the license agreement it is difficult to find out remedies.
- **Corporate Espionage-** It means theft of trade secrets through illegal means such as wire taps or illegal intrusions.
- **Money Laundering-** It means moving of illegally acquired cash through financial and other systems so that it appears to be legally acquired. eg. Transport cash to a country having less stringent banking regulations and move it back by way of loans the interest of which can be deducted from his taxes.
- **Embezzlement-** Unlawful misappropriation of money, property or any other thing of value that has been entrusted to the offender's care, custody or control is called embezzlement. This crime is done by misusing the Internet facilities.
- **Password Sniffers-** Password sniffers are programs that monitor and record the name and password of network users as they log in, putting in danger the security at a site. Any person, who installs the sniffer, can act as an authorized user and log in to access on restricted documents.
- **Spoofing-** It is the act of disguising one computer to, electronically "look" like another computer, in order to gain access to a system that would be normally is restricted.
- **Credit Card Fraud-** in U.S.A. half a billion dollars have been lost annually by consumers who have credit cards and calling card numbers. These are stolen from on-line databases.
- **Web Jacking-** The term refers to forceful taking of control of a web site by cracking the password. This occurs when someone forcefully takes control of a website (by cracking the

password and later changing it). Like terrorism, 'e-terrorism' utilizes hacking to cause violence against people or property, or least, it causes enough harm to generate fear.

- **Cyber terrorism-** The use of computer resources to intimidate or coerce government, the population or any segment, thereof in furtherance of political or social objectives is called cyber terrorism. Individuals and groups quite often try to exploit anonymous character of the internet to threaten governments and terrorize the citizens of the country.
- **IP Crimes-** Software Piracy, Copyright Infringement, Trademarks Violations, Theft of Computer Source Code. Email Spoofing a spoofed email is one that appears to originate from one source but actually has been sent from another source.
- **Cyber Defamation-** This occurs when defamation takes place with the help of computers and/or the Internet. E.g. a person publishes defamatory matter about another on a website.
- **Unauthorized Access** -Also known as Hacking, involves gaining access illegally to a computer system or network and in some cases making unauthorized use of this access. Hacking is also an act by which other forms of cyber-crime (e.g., fraud, terrorism) are committed. Theft of any information contained in electronic form such as that stored in hard disks of computers, removable storage media, etc.
- **Email Bombing-** This refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing.
- **Virtual crime-** Virtual crime or in-game crime refers to a virtual criminal act that takes place in a massively multiplayer online game (MMOG).
- **Email spoofing-**spoofed email is one that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage. In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.
- **Virus Attacks-** Viruses are the programs that have the capability to infect other programs and make copies of it and spread into other program. Programs that multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attaches them to other software. Virus, worms, Trojan horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Viruses usually affect the data on a computer, either by altering or deleting it.
- **Salami Attacks-** These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bank employee inserts a program, into the bank servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.
- **Data diddling-** Data diddling involves changing data prior or during input into a computer. The information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also includes automatic changing the financial information for some time before processing and then restoring original information.
- **Software Piracy** - Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.
- **Denial of service Attack-** This is an attack in which the criminal floods the bandwidth of the victim network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic.

- **Sale of illegal articles-** This category of cybercrimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.
- **Cyber Defamation-** When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person friends, it is termed as cyber defamation.
- **Forgery -** Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high quality scanners and printers.
- **Theft of information contained in electronic form-** This includes theft of information stored in computer hard disks, removable storage media etc.
- **Internet time theft -** Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.
- **Theft of computer system -** This type of offence involves the theft of a computer, some part(s) of a computer or a peripheral attached to the computer.
- **Physically damaging a computer system-** This crime is committed by physically damaging a computer or its peripherals.
- **Breach of Privacy and Confidentiality -** Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information. Confidentiality means non-disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.
- **E-commerce/ Investment Frauds -** An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.
- **Cyber Terrorism -** Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.

Intrusion Detection System – An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. While anomaly detection and reporting is the primary function, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious IP addresses.

Different types of intrusion detection systems-Intrusion detection systems come in different flavors and detect suspicious activities using different methods, including the following:

- **Network intrusion detection system-** (NIDS) is deployed at a strategic point or points within the network, where it can monitor inbound and outbound traffic to and from all the devices on the network.
- **Host intrusion detection systems-** (HIDS) run on all computers or devices in the network with direct Access to both the internet and the enterprise internal network. HIDS have an advantage over NIDS in That they may be able to detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to detect. HIDS may also be able to identify malicious traffic that Originates from the host itself, as when the host has been infected with malware and is attempting to spread to other systems.

- **Signature-based intrusion detection systems** – It monitors all the packets traversing the network and compares them against a database of signatures or attributes of known malicious threats, much like antivirus software.
- **Anomaly-based intrusion detection systems** - It monitors network traffic and compares it against an established baseline, to determine what is considered normal for the network with respect to bandwidth, protocols, ports and other devices. This type of IDS alerts administrators to potentially malicious activity.

Virtual Crime- Virtual crime or in-game crime refers to a virtual criminal act that takes place in a massively multiplayer online game (MMOG), usually an MMORPG. The huge time and effort invested into such games can lead online "crime" to spill over into real world crime, and even blur the distinctions between the two.

Perception of cyber criminals: Hackers, insurgents and extremist group-

Hacker and attackers groups are any skilled computer expert that uses their technical knowledge to overcome a problem. While hacker can refer to any skilled computer programmer, the term has become associated in popular culture with a security hacker, someone who, with their technical knowledge, uses bugs or exploits to break into computer systems.

Four primary motives have been proposed as possibilities for why hackers attempt to break into computers and networks.

- There is a criminal financial gain to be had when hacking systems with the specific purpose of stealing credit card numbers or manipulating banking systems.
- Many hackers thrive off of increasing their reputation within the hacker subculture and will leave their handles on websites they defaced or leave some other evidence as proof that they were involved in a specific hack.
- Corporate espionage (Spy) allows companies to acquire information on products or services that can be stolen or used as leverage within the marketplace.
- state-sponsored attacks provide nation states with both wartime and intelligence collection options conducted on, in, or through cyberspace

Web servers hacking

A web server is a program that stores files (usually web pages) and makes them accessible via the network or the internet. A web server requires both hardware and software. Attackers usually target the exploits in the software to gain authorized entry to the server. Let's look at some of the common vulnerabilities that attackers take advantage of.

- **Default settings**– These settings such as default user id and passwords can be easily guessed by the attackers. Default settings might also allow performing certain tasks such as running commands on the server which can be exploited.
- **Misconfiguration operating systems and networks** – certain configuration such as allowing users to execute commands on the server can be dangerous if the user does not have a good password.
- **Bugs in the operating system and web servers**– discovered bugs in the operating system or web server software can also be exploited to gain unauthorized access to the system.
- **Lack of security policy and procedures**– lack of a security policy and procedures such as updating antivirus software, patching the operating system and web server software can create security loop holes for attackers.

Types of Web Servers-The following is a list of the common web servers.

- **Apache**– This is the commonly used web server on the internet. It is cross platform but is usually installed on Linux. Most PHP websites are hosted on Apache servers.

- **Internet Information Services (IIS)**– It is developed by Microsoft. It runs on Windows and is the second most used web server on the internet. Most asp and aspx websites are hosted on IIS servers.
- **Apache Tomcat** – Most Java server pages (JSP) websites are hosted on this type of web server.
- **Other web servers** – These include Novell's Web Server and IBM's Lotus Domino servers.
- Types of Attacks against Web Servers
- **Directory traversal attacks**– This type of attacks exploits bugs in the web server to gain unauthorized access to files and folders that are not in the public domain. Once the attacker has gained access, they can download sensitive information, execute commands on the server or install malicious software.
- **Denial of Service Attacks**– With this type of attack, the web server may crash or become unavailable to the legitimate users.
- **Domain Name System Hijacking** – With this type of attacker, the DNS setting are changed to point to the attacker's web server. All traffic that was supposed to be sent to the web server is redirected to the wrong one.
- **Sniffing**– Unencrypted data sent over the network may be intercepted and used to gain unauthorized access to the web server.
- **Phishing**– With this type of attack, the attack impersonates the websites and directs traffic to the fake website. Unsuspecting users may be tricked into submitting sensitive data such as login details, credit card numbers, etc.
- **Pharming**– With this type of attack, the attacker compromises the Domain Name System (DNS) servers or on the user computer so that traffic is directed to a malicious site.
- **Defacement**– With this type of attack, the attacker replaces the organization's website with a different page that contains the hacker's name, images and may include background music and messages.

Effects of successful attacks

- An organization's reputation can be ruined if the attacker edits the website content and includes malicious information or links to a porn website
- The web server can be used to install malicious software on users who visit the compromised website. The malicious software downloaded onto the visitor's computer can be a virus, Trojan or Botnet Software, etc.
- Compromised user data may be used for fraudulent activities which may lead to business loss or lawsuits from the users who entrusted their details with the organization.

Session hijacking

Session hijacking, sometimes also known as cookie hijacking is the exploitation of a valid computer session—sometimes also called a session key—to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer.

In other words, The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token. Because http communication uses many different TCP connections, the web server needs a method to recognize every user's connections. The most useful method depends on a token that the Web Server sends to the client browser after a successful client authentication. A session token is normally composed of a string of variable width and it could be used in different ways, like in the URL, in the header of the http requisition as a cookie, in other parts of the header of the http request, or yet in the body of the http requisition.

Unit -2

Cybercrime on Mobile and Wireless Device: It is defined as crime done via mobile device, Common Cyber Crimes Associated With Cell Phones:

- **Bluebugging:** As the name suggests this is the attack on the mobile cell phone through Bluetooth. Bluetooth is not a stranger term today. Almost every mobile cell phone is embedded with Bluetooth technology. We use Bluetooth for sharing photos, audio or video files. Bluebugging allows the hacker to take over complete control over your mobile phone. The victim cannot even realize that his mobile cell phone is attacked, because even if the Bluetooth device is disabled or turned off the mobile cell phone can be victim of this attack.
- **Vishing:** This is a tool for committing financial crime by using mobile. Use of mobile making is increased on the mobile phones. Mobile phones are now used for online shopping and managing banking transactions. This has made mobile cell phone an easy victim of Vishing. Motive of the hacker is to get easy money.
- **Malware:** This is one of the biggest threats to mobile cell phones. It is a program (software) designed to perform malicious activities in the device infected. Malware enters the mobile cell phone of victim through SMS, file transfer, downloading programs from internet.
- **Smishing:** In this E-age the term SMS do not need any introduction. It signifies Short Message Service. It is a common term for sharing messages on mobile phone. This service is the one of the most used service on mobile phones. Hence criminals are targeting it as a tool to satisfy their greed. Smishing is an security attack in which the user is sent an SMS posing as a lucrative service that indulges them into exposing their personal information which is later misused.

Proliferation of Mobile and Wireless Devices (wireless threats)

Wireless local area networks (WLAN) allow people to sever the Ethernet cable and connect to their local network or the Internet anytime they are in range of a wireless access point (AP). Wireless APs are often referred to as “hot spots” and their number is growing daily. Hot spots are appearing anywhere that people spend time and might want to connect to the Internet to check e-mail or surf the Web. Typical locations include restaurants, hotels and airports.

Attackers have easy access to mobile devices because they are not bound to the physical environment and can compromise the cornerstones of Information Security; Confidentiality, Integrity and Availability. A thorough analysis of IT threats that can affect corporate data is therefore critical before the use of mobile devices can be accepted. WLAN has an open nature and can introduce a number of new and unknown threats compared to the more traditional wired LAN's. Information stored on mobile devices is therefore also open to attacks and new threats. Risk and threat can be analyzed in two forms, passive and active attacks.

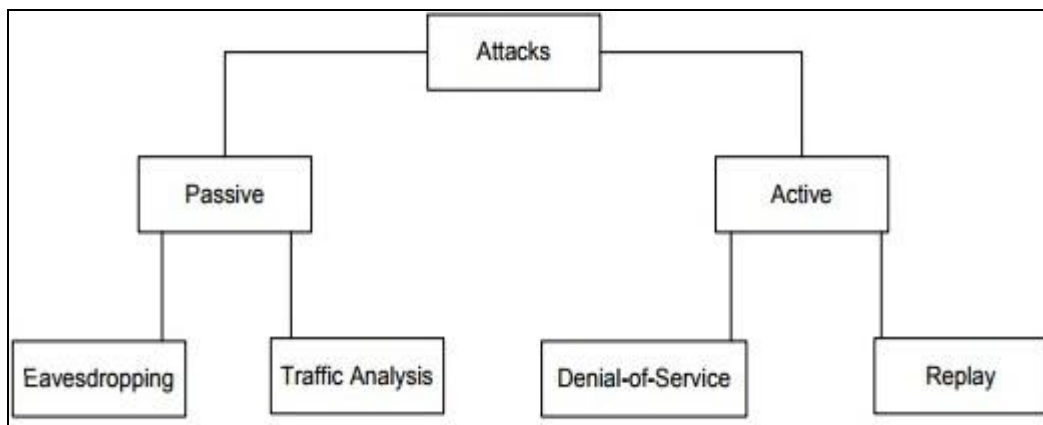


Figure 1: Types of Attacks in Wireless Networks

Passive Attacks- Passive attacks occur when unauthorized users gain entry into a system and do not alter the information or the original content. There are numerous forms of attacks which can occur on a passive basis, such as eavesdropping and traffic analysis.

- **Eavesdropping-** Eavesdropping involves the process of users intercepting data over the air while being a distance away from the physical location. This form of attack may cost an organization both financial loss and corporate identity, as it attacks the confidentiality of the information. This form of attack can be executed with minimal effort or equipment and without detection. The primary goal of the attacker is to understand:

- Who uses the network?
- What information is accessible?
- What the capabilities of the equipment on the network are;
- General usage of the equipment;
- What the coverage area of the equipment is.

The encryption standard, WEP (Wired Equivalent Privacy is a security protocol), was introduced to secure information against this form of attack. This standard should be used as a minimum when securing corporate or personal data. A determined attacker can still log information being transmitted even with WEP turned on.

- **Traffic Analysis-** Traffic analysis is a technique whereby the attacker can determine the load on the network by the number of packets being transmitted. This form of attack is frequently used by attackers to gain access to the network before launching a malicious attack. The attacker first determines the amount of activity across the network. If there is a substantial amount of network activity, it is a clear indication of a large event taking place with large amounts of data being transferred. The attacker may find the physical locations of Access Points (AP's) in the surrounding area. The final goal of traffic analysis is to determine the type of protocol being used in the transmission of data and can therefore be used in attacks against the identified protocol.

Active Attacks -Active attacks are attacks in which attackers gain access to the network and modify the stored data or disrupt network services and attack the network in real time.

- **Denial of Service Attacks (DoS)**-Wireless networks are extremely vulnerable to DoS attacks. A DoS attack can force the speeds of the network to slow dramatically, or worse, disable the network all together therefore compromising the Availability of the information. The protection of the network against this attack can be a costly exercise. The only effective way to safeguard information is to isolate the network with heavy security. This solution is not practical unless the information stored on the network is of a highly sensitive nature . A viable solution to protect data against DoS attacks is to design, implement and maintain a strong Intrusion Detection Systems (IDS) to monitor the network activity and enforce a predefined security policy.

Different types:

- Ping-of-Death
- Teardrop
- Smurf
- SYN

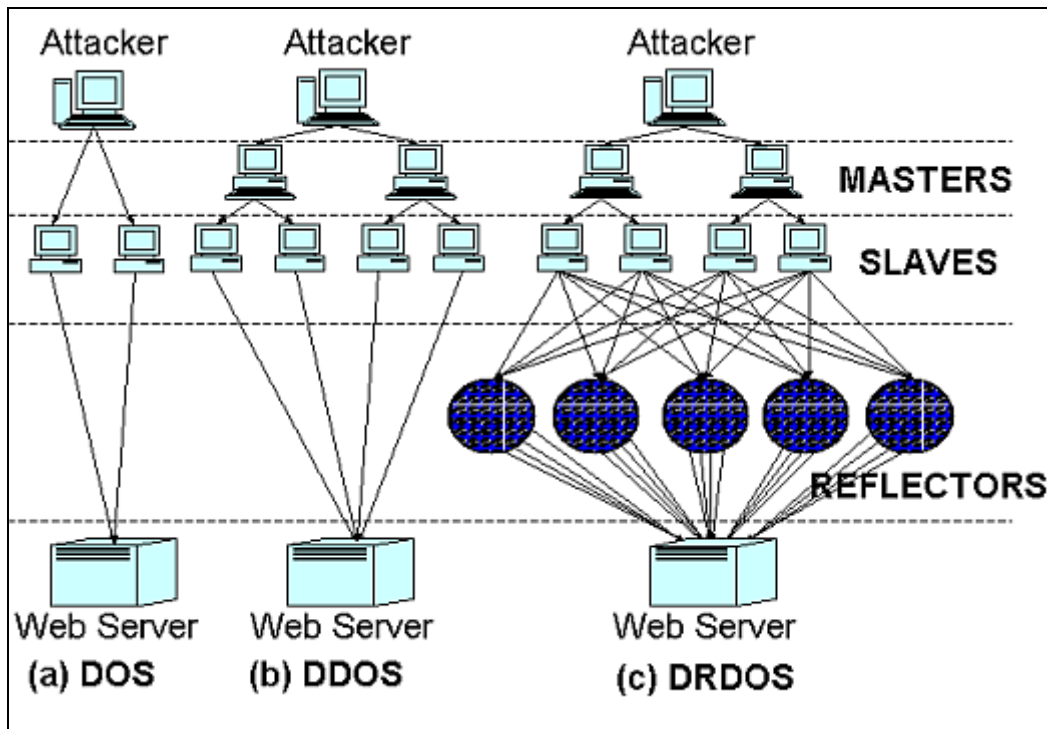


Fig. 2 DOS Attack

- **Replay Attacks**-This form of attack is used to gain access to the network by convincing the host that a valid client needs to associate within the network. This attack is not executed in real time, which makes detection difficult. The original information obtained in a session is not altered or interfered in any way, but the attacker will have access to the network at a later stage. Replay attacks target the integrity of information by injecting incorrect data into the system. Network administrators need to identify the threats associated with wireless networks and mobile devices to the organizations' information assets and resources. Securing wireless access requires securing the confidentiality; integrity and availability of information, only then can an organization gather the benefits of a wireless network.

Wireless Security-Many organizations are spending large amounts of money on implementing security for wired technologies by means of various firewall technologies and other security solutions. All wired and wireless networks cannot be kept secure against attacks especially when adding Wireless technology.

It is crucial that the organizations develop a Wireless Security policy as part of an overall security policy. A security policy should be developed before a wireless network is initiated. Management can reduce costs that may incur later through developing a security policy at an early stage, followed by the implementation of stronger security mechanisms. A security policy will not eliminate wireless threats but will help create a proactive environment to combat these threats effectively. When developing a security policy, the desired security should be reached by following the characteristics:

- **Confidentiality** - The assurance that all information is kept secret and made only available to users who have access to the information;
- **Integrity** - The assurance that information is kept in its true form whether the data is in transit or at rest;
- **Authenticity** - The assurance that the information originates from the claimed entity.
- Wireless Equivalency Protocol was introduced as a countermeasure to attacks to maintain the confidentiality and integrity of information. The initial intent for WEP was to prevent passive

attacks such as eavesdropping from occurring. WEP ensures that only authorized users have access to the information.

Trends in Mobility Credit Card Frauds in Wireless Computing-The rising importance of electronic gadgets , which became an integral part of business, providing connectivity with the internet outside the office , brings many challenges to secure these devices from being a victim of cyber crime. These Credit card frauds and all are the new trends in cybercrime that are coming up with mobile computing – mobile commerce (M- COMMERCE) and mobile banking (M-Banking).

Elements of Credit Card Fraud-Debit/credit card fraud is thus committed when a person.

- fraudulently obtains, takes, signs, uses, sells, buys, or forges someone else's credit or debit card or card information;
- Uses his or her own card with the knowledge that it is revoked or expired or that the account lacks enough money to pay for the items charged; and
- Sells goods or services to someone else with knowledge that the credit or debit card being used was illegally obtained or is being used without authorization.

Theft, the most obvious form of credit card fraud, can happen in a variety of ways, from low tech dumpster diving to high tech hacking. A thief might go through the trash to find discarded billing statements and then use your account information to buy things. A retail or bank website might get hacked, and your card number could be stolen and shared. Perhaps a dishonest clerk or waiter takes a photo of your credit card and uses your account to buy items or create another account. Or maybe you get a call offering a free trip or discounted travel package. But to be eligible, you have to join a club and give your account number, say, to guarantee your place. The next thing you know, charges you didn't make are on your bill, and the trip promoters who called you are nowhere to be found.

Types and techniques of Credit Card Frauds:

- The first category, lost or stolen cards, is a relatively common one, and should be reported immediately to minimize any damages.
- The second is called "account takeover" — when a cardholder unwittingly gives personal information (such as home address, mother's maiden name, etc.) to a fraudster, who then contacts the cardholder's bank, reports a lost card and change of address, and obtains a new card in the soon-to-be victim's name.
- The third is counterfeit cards — when a card is "cloned" from another and then used to make purchases. In Asia Pacific, 10% to 15% of fraud results from malpractices such as card skimming but this number has significantly dropped from what it was a couple of years prior, largely due to the many safety features put in place for payment cards, such as EMV chip.
- The fourth is called "never received" — when a new or replacement card is stolen from the email, never reaching its rightful owner.
- The fifth is fraudulent application— when a fraudster uses another person's name and information to apply for and obtain a credit card.
- The sixth is called "multiple imprint" — when a single transaction is recorded multiple times on old-fashioned credit card imprint machines known as "knuckle busters".
- The seventh is collusive merchants — when merchant employees work with fraudsters to defraud banks.
- The eighth is email order/telephone order (MO/TO) fraud, which now includes e-commerce, and is the largest category of total payment card fraud in Asia-Pacific, amounting to nearly three-quarters of all fraud cases. The payments industry is working tirelessly to improve card verification and security programs to prevent fraud in so-called "card-not-present" transactions online or via email order and telephone transactions.

Techniques of Credit Card Frauds:

Skimmers

Unfortunately for consumers and banks alike, skimmers are versatile and can be installed almost anywhere credit cards are accepted, given the opportunity.

These are devices that read and store credit card information as a customer attempts to make a purchase. They allow the purchase to go through, but keep the information in onboard memory. When the thief collects the skimmer, they simply need to plug it into a computer to collect the stolen information.

The most common types of skimmers are those installed in public places, like on ATMs and gas pumps. These skimmers are typically designed to go over the existing credit card reader and give the appearance that they are part of the whole unit. Before using your card at these places, grab the reader and shake it a bit. Skimmers installed in this way usually aren't securely attached, so it should come off right away.

Phishing

Some fraudsters trick customers into giving them their information. This process is called phishing and most commonly occurs over phone or email. A criminal will contact you pretending to be your bank or some other official entity and convinces them to relay their credit card information. If this happens, never respond directly. Instead, call the number on the back of your credit card. That is the only definite way you can guarantee you are talking with someone from your bank. If the call was from them, you will quickly be routed to the correct department. If it wasn't, you can report the suspicious activity to your bank.

Duplicate websites

Some websites try to pass themselves off as reputable storefronts but are actually only there to steal your credit card information. If you have any doubts, type in the website directly rather than clicking a link from another source. Also, check the site's URL. If it begins with HTTPS that means it's a secure site and it should be alright to proceed.

Attacks on Mobiles: Mobile Viruses

A mobile phone virus is a malicious computer program that targets cellular phones and other wireless PDAs. Once infected, a mobile phone can become a source for spreading the virus by sending texts and emails to other vulnerable devices. These texts and emails can lead other users to open or download the virus. Mobile phone viruses can also come in the form of malware that spreads through downloaded apps. Some notable mobile phone viruses include:

- **Cabir:** The first verifiable example of a mobile phone virus, Cabir was created by the 29A, a group of hackers from the Czech Republic and Slovakia. Cabir uses Bluetooth technology to infect mobile users within a range of 30 meters while disguised as a security file. Each time a mobile device is powered on, the virus launches and scans the area for other vulnerable devices. Because the virus cannot actually destroy data, Cabir is not considered dangerous. However, it causes reduced battery life resulting from a frequent searching for other Bluetooth devices.
- **Commwarrior:** In March 2005, Commwarrior infected Symbian Series 60 mobile phones. Using the multimedia messaging system, it sends a replication to all of the numbers stored in the phone's contacts, generating high bills for the phone's owner.
- **Trojan-SMS.AndroidOS.FakePlayer.a:** In August 2010, the first Trojan horse virus for mobile phones was detected on Smartphones using Google's Android OS. This virus initially showcases like a media player, but when installed, it starts to send messages in mass numbers, resulting in huge bills for the user.

Pharming, Vishing, Smishing:

Pharming

Pharming is a tactic used by criminals to redirect a legitimate web site to a fraudulent site. Unlike phishing and its variations, Pharming does not try to trick you into clicking a URL or talk you into providing sensitive information. Instead, it uses malicious code to redirect you to the criminal's site without your consent or knowledge, making it more difficult to detect. To help avoid Pharming, follow the guidelines in Protect Your Computer. Also, be careful when entering financial information on a web site. Look for the key or lock symbol at the bottom of the browser. If the Web site looks different than when you last visited, be suspicious and don't click unless you are absolutely certain the site is safe.

Vishing

Unfortunately, phishing emails are not the only way people can try to fool you into providing personal information in an effort to steal your identity or commit fraud. Criminals also use the phone to solicit your personal information. This telephone version of phishing is sometimes called vishing. Vishing relies on "social engineering" techniques to trick you into providing information that others can use to access and use your important accounts. People can also use this information to pretend to be you and open new lines of credit. To avoid being fooled by a vishing attempt:

- If you receive an email or phone call asking you to call and you suspect it might be a fraudulent request, look up the organization's customer service number and call that number rather than the number provided in the solicitation email or phone call.
- Forward the solicitation email to the customer service or security email address of the organization, asking whether the email is legitimate. Though vishing and its relative, phishing, are troublesome crimes and sometimes hard to identify, there are things that you can do to protect your identity.

Smishing

Just like phishing, smishing uses cell phone text messages to lure consumers in. Often the text will contain an URL or phone number. The phone number often has an automated voice response system. And again just like phishing, the smishing message usually asks for your immediate attention. In many cases, the smishing message will come from a "5000" number instead of displaying an actual phone number. This usually indicates the SMS message was sent via email to the cell phone, and not sent from another cell phone.

Hacking Bluetooth (Wireless Device):

Bluetooth is peer-to-peer based network technology. Due to this, the technology lacks management over security issues. This could eventually cause you grief. The fact that this technology is now standard on many electronic devices, from speakers to Smartphone's, paired with the lack of security functions, makes Bluetooth an easy entrance point for hackers. Some of the techniques of hacking are as follows:

- **Bluejacking**-Bluejacking is probably the most common form of Bluetooth hacking. This happens when a hacker searches for discoverable devices in the area and then sends spam in the form of text messages to the devices. This form of hacking is rather childish and harmless. It was once used mainly to prank people in the past when mobile devices came with Bluetooth that was automatically set to discoverable. Bluejacking is used today for spam messaging and the hackers who use this do it just to frustrate others. The method does not give hackers access to your phone or the information on it. or open Wi-Fi area. This will prevent Bluejacking and the next two popular forms of hacks.
- **Bluesnarfing**-This form of hack is more serious than Bluejacking and can leave open some of the private information stored on your Smartphone. This is made possible through software. A hacker may purchase software that allows them to request information from your device. Even though this form of hacking is capable of happening while your device is set to "invisible" or "non-discoverable", it is unlikely to happen due to the time, effort, and money needed to complete it. The information stolen may seem important to you, but it might not be as precious as banking information. That data can be accessed by hacking your device through Bluebugging.

- **Bluebugging**-If a hacker Bluebugs your phone, they gain total access and control of your device. This makes it capable for them to access all info including photos, apps. Contacts, etc. Bluebugging can happen when your device is left in the discoverable state. From here hackers gain access to your phone at the same point they do when performing Bluejacks. This is a much harder form of hacking than Bluesnarfing and Bluejacking. Although this is only feasible on older phones with outdated firmware. Newer Smartphone's and their owners are less likely to have this happen to them because of the constant updates mobile operating systems perform.
-

Unit -3

Proxy Servers

A proxy server is a server (a computer system or an application) that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource available from a different server and the proxy server evaluates the request as a way to simplify and control its complexity. Proxies were invented to add structure and encapsulation to distributed systems. Today, most proxies are web proxies, facilitating access to content on the World Wide Web, providing anonymity and may be used to bypass IP address blocking.

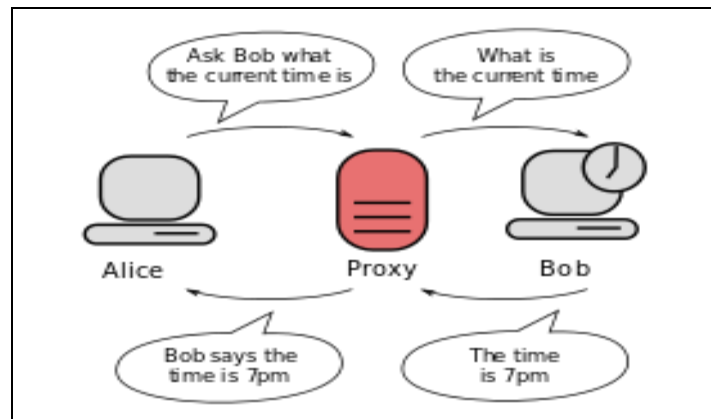


Fig. 1: Communication between two computers connected through a third computer acting as a proxy. Bob does not know to whom the information is going, which is why proxies can be used to protect privacy.

Anonymizer

An anonymizer or an anonymous proxy is a tool that attempts to make activity on the Internet untraceable. It is a proxy server computer that acts as an intermediary and privacy shield between a client computer and the rest of the Internet. It accesses the Internet on the user's behalf, protecting personal information by hiding the client computer's identifying information. There are many reasons for using anonymizer. Anonymizer help minimize risk. They can be used to prevent identity theft, or to protect search histories from public disclosure.

Some countries apply heavy censorship on the internet. Anonymizer can help in allowing free access to all of the internet content, but cannot help against persecution for accessing the Anonymizer website itself.

Password Cracking

- Password cracking is the process of recovering passwords from data that have been stored in or transmitted by a computer system. A common approach (brute-force attack) is to try guesses repeatedly for the password and check them against an available cryptographic hash of the password.
- The purpose of password cracking might be to help a user recover a forgotten password (installing an entirely new password is less of a security risk, but it involves System Administration privileges), to gain unauthorized access to a system, or as a preventive measure by system administrators to check for easily crackable passwords. On a file-by-file basis, password cracking is utilized to gain access to digital evidence for which a judge has allowed access but the particular file's access is restricted.
- Password cracking refers to various measures used to discover computer passwords. This is usually accomplished by recovering passwords from data stored in, or transported from, a computer system. Password cracking is done by either repeatedly guessing the password, usually through a

computer algorithm in which the computer tries numerous combinations until the password is successfully discovered.

- Password cracking can be done for several reasons, but the most malicious reason is in order to gain unauthorized access to a computer without the computer owner's awareness. This results in cybercrime such as stealing passwords for the purpose of accessing banking information.

Keyloggers

- A Keyloggers is a piece of software — or, even scarier, a hardware device — that logs every key you press on your keyboard. It can capture personal messages, passwords, credit card numbers, and everything else you type.
- Keyloggers are generally installed by malware, but they may also be installed by protective parents, jealous spouses, or employers who want to monitor their employees. Hardware Keyloggers are perfect for corporate espionage.
- Keyloggers can pose a serious threat to users, as they can be used to intercept passwords and other confidential information entered via the keyboard. As a result, cybercriminals can get PIN codes and account numbers for your financial accounts, passwords to your email and social networking accounts and then uses this information to take your money, steal your identity and possibly extort information and money from your friends and family.

Spyware

- Spyware is the term given to a category of software which aims to steal personal or organizational information. It is done by performing a set of operations without appropriate user permissions, sometimes even covertly. General actions a spyware performs include advertising, collection of personal information and changing user configuration settings of the computer.
- A Spyware is generally classified into adware, tracking cookies, system monitors and Trojans. The most common way for a spyware to get into the computer is through freeware and shareware as a bundled hidden component. Once a spyware gets successfully installed, it starts sending the data from that computer in the background to some other place.
- These days' spywares are usually used to give popup advertisements based on user habits and search history. But when a spyware is used maliciously, it is hidden in the system files of the computer and difficult to differentiate.
- One of the simplest and most popular, yet dangerous is Keyloggers. It is used to record the keystrokes which could be fatal as it can record passwords, credit card information etc. In some shared networks and corporate computers, it is also intentionally installed to track user activities.
- Presence of spyware in a computer can create a lot of other troubles as spyware intended to monitor the computer can change user preferences, permissions and also administrative rights, resulting in users being locked out of their own computer and in some cases, can also result in full data losses. Spyware running in the background can also amount to increased number of processes and result in frequent crashes. It also often slows down a computer.

Virus

A computer virus is malicious code that replicates by copying itself to another program, computer boot sector or document and changes how a computer works. The virus requires someone to knowingly or unknowingly spread the infection without the knowledge or permission of a user or system administrator.

A virus can be spread by opening an email attachment, clicking on an executable file, visiting an infected website or viewing an infected website advertisement. It can also be spread through infected removable storage devices, such USB drives. Once a virus has infected the host, it can infect other system software or resources modify or disable core functions or applications, as well as copy, delete or encrypt data. Some viruses begin replicating as soon as they infect the host, while other viruses will lie dormant until a specific trigger causes malicious code to be executed by the device or system.

Types of viruses

- **File infectors-** Some file infector viruses attach themselves to program files, usually selected .com or .exe files. Some can infect any program for which execution is requested, including .sys, .ovl, .prg, and .mnu files. When the program is loaded, the virus is loaded as well. Other file infector viruses arrive as wholly contained programs or scripts sent as an attachment to an email note.
- **Macro viruses-** These viruses specifically target macro language commands in applications like Microsoft Word and other programs. In Word, macros are saved sequences for commands or keystrokes that are embedded in the documents. Macro viruses can add their malicious code to the legitimate macro sequences in a Word file. Microsoft disabled macros by default in more recent versions of Word; as a result, hackers have used social engineering schemes to convince targeted users to enable macros and launch the virus. As macro viruses have seen a resurgence in recent years, Microsoft added a new feature in Office 2016 that allows security managers to selectively enable macro use for trusted workflows only, as well as block macros across an organization.
- **Overwrite viruses-** Some viruses are designed specifically to destroy a file or application's data. After infecting a system, an overwrite virus begins overwriting files with its own code. These viruses can target specific files or applications or systematically overwrite all files on an infected device. An overwrite virus can install new code in files and applications that programs them to spread the virus to additional files, applications and systems.
- **Polymorphic viruses-**A polymorphic virus is a type of malware that has the ability to change or mutate its underlying code without changing its basic functions or features. This process helps a virus evade detection from many antimalware and threat detection products that rely on identifying signatures of malware; once a polymorphic virus' signature is identified by a security product, the virus can then alter itself so that it will no longer be detected using that signature.
- **Resident viruses-**This type of virus embeds itself in the memory of a system. The original virus program isn't needed to infect new files or applications; even if the original virus is deleted, the version stored in memory can be activated when the operating system loads a specific application or function. Resident viruses are problematic because they can evade antivirus and antimalware software by hiding in the system's RAM.
- **Rootkit viruses-**A Rootkit virus is a type of malware that installs an unauthorized rootkit on an infected system, giving attackers full control of the system with the ability to fundamentally modify or disable functions and programs. Rootkit viruses were designed to bypass antivirus software, which typically scanned only applications and files. More recent versions of major antivirus and antimalware programs include rootkit scanning to identify and mitigate these types of viruses.
- **System or boot record infectors-**These viruses infect executable code found in certain system areas on a disk. They attach to the DOS boot sector on diskettes and USB thumb drives or the Master Boot Record on hard disks. In a typical attack scenario, the victim receives storage device that contains a boot disk virus. When the victim's operating system is running, files on the external storage device can infect the system; rebooting the system will trigger the boot disk virus. An infected storage device connected to a computer can modify or even replace the existing boot code on the infected system so that when the system is booted next, the virus will be loaded and run immediately as part of the master boot record. Boot viruses are less common now as today's devices rely less on physical storage media.

Worms

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

Trojan Horses

A Trojan horse or Trojan is a type of malware that is often disguised as legitimate software. Trojans can be employed by cyber-thieves and hackers trying to gain access to users' systems. Users are typically tricked by some form of social engineering into loading and executing Trojans on their systems. Once activated, Trojans can enable cyber-criminals to spy on you, steal your sensitive data, and gain backdoor access to your system. These actions can include:

- Deleting data
 - Blocking data
 - Modifying data
 - Copying data
 - Disrupting the performance of computers or computer networks.
- Unlike computer viruses and worms , Trojans are not able to self-replicate.

Backdoors

A backdoor is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware. Backdoor installation is achieved by taking advantage of vulnerable components in a web application. Once installed, detection is difficult as files tend to be highly obfuscated. Webserver backdoors are used for a number of malicious activities, including:

- Data theft
- Website defacing
- Server hijacking
- The launching of distributed denial of service (DDoS) attacks
- Infecting website visitors (watering hole attacks)

DoS Attack

A denial-of-service (DoS) is any type of attack where the attackers (hackers) attempt to prevent legitimate users from accessing the service. In a DoS attack, the attacker usually sends excessive messages asking the network or server to authenticate requests that have invalid return addresses. The network or server will not be able to find the return address of the attacker when sending the authentication approval, causing the server to wait before closing the connection. When the server closes the connection, the attacker sends more authentication messages with invalid return addresses. Hence, the process of authentication and server wait will begin again, keeping the network or server busy.

DDoS Attack

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. They target a wide variety of important resources, from banks to news websites, and present a major challenge to making sure people can publish and access important information.

Buffer Overflow

A buffer overflow, or buffer overrun, is a common software coding mistake that an attacker could exploit to gain access to your system. To effectively mitigate buffer overflow vulnerabilities, it is important to understand what buffer overflows are, what dangers they pose to your applications, and what techniques attackers use to successfully exploit these vulnerabilities.

Key Concepts of Buffer Overflow

- This error occurs when there is more data in a buffer than it can handle, causing data to overflow into adjacent storage.
- This vulnerability can cause a system crash or, worse, create an entry point for a cyber attack.
- C and C++ are more susceptible to buffer overflow.
- Secure development practices should include regular testing to detect and fix buffer overflows. These practices include automatic protection at the language level and bounds-checking at run-time.

Attack on Wireless Networks

Wireless attacks have become a very common security issue when it comes to networks. This is because such attacks can really get a lot of information that is being sent across a network and use it to commit some crimes in other networks. Every wireless network is very vulnerable to such kinds of attacks and it is therefore very important that all the necessary security measures are taken so as to prevent the mess that can be caused by such attacks. These attacks are normally carried out to target information that is being shared through the networks. It is therefore very important to know of such attacks so that one is in a position to identify it in case it happens. Some of the common network attacks have been outlined below.

- **Rogue access points**-A rogue access point is basically an access point that has been added to one's network without one's knowledge. One totally has no idea that it is there. This is a kind of scenario that can create a kind of back door especially if one is not conversant with it and have complete management of it. This is an access point that can create some very huge security concerns. One is due to the fact that it can be very easy to plug in a wireless access point in it. If one is not doing any type of network access control protocols on one's network, it becomes very easy for additional workstations and access points to be added onto one's network.
- **Jamming/Interference**-Wireless interference basically means disruption of one's network. This is a very big challenge especially owing to the fact that wireless signals will always get disrupted. Such interference can be created by a Bluetooth headset, a microwave oven and a cordless phone. This makes transmission and receiving of wireless signals very difficult. Wireless interference can also be caused by causing service degradation so as to make sure that one denies complete access to a particular service. Jamming can also be used in conjunction with an evil twin.
- **Evil twin**-A wireless evil twin mainly comes into play when criminals are trying to create rogue access points so as to gain access to the network or access to information that is being put through a network. Coming up with an evil twin is very simple since all one need to do is purchase a wireless access point, plug it into the network and configure it as exactly as the existing network. This is possible in open access points that do not have any passwords associated with them. Once one comes up with one's access point, one plugs it into the network so that it becomes the primary access point thus overpowering other existing access points. With this, one's evil twin will tend to have a stronger network signal and therefore people will choose it. Through this, the individual controlling the access point will be in a position to see all the information being sent around the network.
- **War driving**-War driving is a way that bad guys use so as to find access points wherever they can be. With the availability of free Wi-Fi connection and other GPS functionalities, they can drive around and obtain a very huge amount of information over a very short period of time. One can also use some special type of software to view all the different access points around one. With this information, an individual is in a position to come up with a very large database which he or she can use to determine where he or she can gain access to a wireless signal.
- **Bluejacking**-Blue jacking is a kind of illegal activity that is similar to hacking where one can be able to send unsolicited messages to another device via Bluetooth. This is considered spam for Bluetooth and one might end up seeing some pop-up messages on one's screen. Bluejacking is

possible where a Bluetooth network is present and it is limited to a distance of ten meters which is the distance a Bluetooth device can send a file to another device. It rarely depends on antennae. Bluejacking works on the basis that it takes advantage of what is convenient for us on our mobile devices and the convenience is being able to communicate and send things back and forth between devices. With this, one can easily send messages to other Bluetooth devices since no authentication is required. Some third party software can also be used to carry out Bluejacking.

- **Bluesnarfing**-Bluesnarfing is far much more malicious than Bluejacking since it involves using one's Bluetooth to steal information. This is where a Bluetooth-enabled device is able to use the vulnerability on the Bluetooth network to be able to get into a mobile device to steal information such as contacts and images. This is a vulnerability that exposes the weakness and vulnerability with the Bluetooth network. This is an act that creates some very serious security issues since an individual can steal a file from one if he or she knows it.
- **War chalking**-War chalking is another method that was used so as to determine where one could get a wireless access signal. In this case, if an individual detected a wireless access point, he or she would make a drawing on the wall indicating that a wireless access point has been found. However, this is not currently used.
- **IV attack**-An IV attack is also known as an Initialization Vector attack. This is a kind of wireless network attack that can be quite a threat to one's network. This is because it causes some modification on the Initialization Vector of a wireless packet that is encrypted during transmission. After such an attack, the attacker can obtain much information about the plaintext of a single packet and generate another encryption key which he or she can use to decrypt other packets using the same Initialization Vector. With that kind of decryption key, attackers can use it to come up with a decryption table which they and use to decrypt every packet being sent across the network.
- **Near field communication**-Near field communication is a kind of wireless communication between devices like smart phones where people are able to send information to near filed communication compatible devices without the need to bring the devices in contact. This allows one device to collect information from another device that is in close range.

Phishing Techniques: Popular Phishing Techniques used by Hackers:

- **Deceptive Phishing**-Deceptive phishing is the most common type of social media phishing. In a typical scenario, a phisher creates an account pretending to be the account of the victim. Next, the phisher sends friend requests to the friends of the victim as well as a message such as "I have abandoned my previous Facebook account. From now on, please communicate with me through this account only". Afterwards, the phisher starts sending messages to the friends of the victim that demand the recipient to click on a link. Examples of such messages include:
 - A statement that the receiver of the message has a virus which can be deleted by signing up for a special anti-virus inspection conducted by the social network.
 - A fictitious invoice which can be cancelled by clicking on a link requesting the user to provide her/his personal information.
- **Content Injection based Phishing**-The content-injection social network phishing refers to inserting malicious content in social networks. The malicious content can often be in the form of bogus posts (e.g., tweets, posts in the Facebook feed or in LinkedIn feed) published by users whose accounts were affected with rogue apps. In many cases, the victims are unable to see the bogus posts posted by the malware apps on their behalf. The bogus posts, for example, may contain a photo of the account owner and the text: "I am in the hospital. If you would like to help me, please sign up by clicking on the following link". When the victim clicks on the link, he/she will be requested to provide his/her personal data, which may be used by the phisher for committing identity theft and other scams.
- **Malware Based Phishing**-Malware-based phishing refers to a spread of phishing messages by using malware. For example, the Facebook account of a victim who installed a rogue Facebook app will automatically send messages to all the friends of the victim. Such messages often contain links allowing the receivers of the messages to install the rogue Facebook app on their computers or

mobile devices. The best way to avoid the installation of rogue Facebook apps is to be very selective when installing any third-party Facebook applications. For example, Facebook apps developed by unknown developers that request access to extensive information should be researched thoroughly. One method often used by phishers to “seduce” the Facebook users to install malware to their computer is to promise them that the malware will enable them to see a list of people who visited their Facebook profile page.

- **Men in the Middle Phishing**-A man-in-the-middle social network attack, also known as social network session hijacking attack, is a form of phishing in which the phisher positions himself between the user and a legitimate social network website. Messages intended for the legitimate social network website pass through the phisher who can inspect the messages and acquire valuable information.
-

Unit -4

Cyber Crime-Cyber crime, or computer oriented crime, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Cyber crime is a Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (networks including but not limited to Chat rooms, emails, notice boards and groups) and mobile phones (Bluetooth/SMS/MMS).Cybercrime may threaten a person or a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, unwarranted mass-surveillance, sextortion, child pornography, and child grooming. There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise.

IT Act, 2000-An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

Hacking-Hacking is unauthorized intrusion into a computer or a network. The person engaged in hacking activities is generally referred to as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system.

Teenage Web Vandals-IT defines, vandalism as willful or malicious destruction, injury, disfigurement, or defacement of any public or private property, real or personal, without the consent of the owner or persons having custody or control. Vandalism includes a wide variety of acts, including graffiti, damaging property (smashing mailboxes, trashing empty buildings or school property, breaking windows, etc.), stealing street signs, arson, egging homes or cars, toilet papering homes, and other types of mischief.

Cyber Fraud and Cheating-It means the person who is doing the act of cyber crime i.e. stealing password and data storage has done it with having guilty mind which leads to fraud and cheating.

Defamation-The offense of injuring a person's character, fame, or reputation by false and malicious statements.

Harassment -Harassment is a form of discrimination. It involves any unwanted physical or verbal behavior that offends or humiliates you. Generally, harassment is a behavior that persists over time. Serious one-time incidents can also sometimes be considered harassment.

E-mail Abuse-Email Abuse, also known as junk email, is a type of electronic spam where unsolicited messages are sent by email. Many email spam messages are commercial in nature but may also

contain disguised links that appear to be for familiar websites but in fact lead to phishing web sites or sites that are hosting malware. Spam email may also include malware as scripts or other executable file attachments (Trojans).

Other IT Act Offences-The offences included in the IT Act 2000 are as follows:

- i) Tampering with the computer source documents.
- ii) Hacking with computer system.
- iii) Publishing of information which is obscene in electronic form.
- iv) Power of Controller to give directions
- v) Directions of Controller to a subscriber to extend facilities to decrypt information
- vi) Protected system
- vii) Penalty for misrepresentation
- viii) Penalty for breach of confidentiality and privacy
- ix) Penalty for publishing Digital Signature Certificate false in certain particulars
- x) Publication for fraudulent purpose
- xi) Act to apply for offence or contravention committed outside India
- xii) Confiscation
- xiii) Penalties or confiscation not to interfere with other punishments.
- xiv) Power to investigate offences.

Monetary Penalties-A Monetary Penalty is a civil penalty imposed by a regulator for a contravention of an Act, regulation or by-law. It is issued upon discovery of an unlawful event, and is due and payable subject only to any rights of review that may be available under the AMP's implementing scheme. It is regulatory in nature, rather than criminal, and is intended to secure compliance with a regulatory scheme, and it can be employed with the use of other administrative sanctions, such as demerit points and license suspensions.

Jurisdiction and Cyber Crimes:

Jurisdiction over Internet-The whole trouble with internet jurisdiction is the presence of multiple parties in various parts of the world who have only a virtual nexus with each other. Then, if one party wants to sue the other, where can he sue?

Traditional requirement generally encompass two areas:-

- i) The Place where the defendant reside.
- ii) Where the cause of action arises.

However, in the context of the internet or cyberspace (Cyberspace is the electronic medium of computer networks, in which online communication takes place), both these are difficult to establish with any certainty. Considering the lack of physical boundaries on the internet, is it possible to reach out beyond the court's geographic boundaries to haul a defendant into its court for conduct in "Cyberspace"? Issues of this nature have contributed to the complete confusion and contradictions that plague judicial decisions in the area of internet jurisdiction. Accordingly, in each case, a determination should be made as to where an online presence will subject the user to jurisdiction in a distant state or a foreign company.

As such, a single transaction may involve the laws of at least three jurisdictions:

- i) The laws of the state/nation in which the user resides,
- ii) The laws of the state/nation that apply where the server hosting the transaction is located.

- iii) The laws of the state/nation which apply to the person or business with whom the transaction takes place

Nature of Criminality

- i) Human individuals as considered as the basis of explaining crime as an individual criminality. As compared to the theory of crime as a social construct, the focus of the concept of crime as an individual criminality is already on the individual. Rooting from the person, it looks into the innate or inherent factors that can significantly influence the making of a criminal.
- ii) In the perspective of individual criminality, it can be asserted that a criminal is born or can be made. In the claim that a criminal is born, it can be traced on the studies regarding the importance of heredity. On the other hand, the claim that a criminal is made, it is traced on an individual's environment- one's diet and even the environment. While, the aspect of environment is still included in the theory of individual criminality, it is still geared towards the study of the individual.
- iii) The concept of a born criminal can be traced with the studies that show the importance and power of oneself in the development of one's criminality. Being a born criminal is also equated to being hereditary. A person is more likely to become criminal if it is already in their blood to become one. In heredity, it includes the elements like physical appearance, modern genetics theory as well as learning theory.

Strategies to tackle Cyber Crime and Trends:

- i) **Protect Your Most Visible Asset**-Websites are the most visible and vulnerable part of a company's infrastructure. As hackers scan the Internet nonstop in search of weaknesses, companies should not overlook this vulnerable entry point in their cyber security defense strategy. Products like malware and vulnerability scanners and web-application firewalls can help you guard this important asset that is the face of your brand.
- ii) **Focus on Effects**- it's clear that organizations can't prevent 100 percent of intrusions. A sophisticated and determined adversary will eventually get in. This is why companies should focus on detecting the effects (also called indicators of attack) of malware and adversary activity, and not just look out for known bad signatures (known as indicators of compromise).
- iii) **Remember That People Are Your Weakest Link**-Even the most advanced technology can't prevent a great employee from accidentally opening your doors to cybercrime. Their strong, alphanumeric 32-character password is now exposed in a plaintext email. These unintentional slip-ups happen; combat them by reiterating common sense practices to all of your employees.

The Indian Evidence Act of 1872 v. Information Technology Act, 2000-The Court may presume that an electronic message forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent.

The Information Technology Act was originally passed on 17th October 2000 with one of the aim to provide legal recognition to digital/electronic evidence. Hence, amendments were made in the Indian Evidence Act regarding collection and production of digital evidence in the court of law.

Some of the important provisions of the Indian Evidence Act pertaining to digital/electronic evidence are as follows –

- i) Defining Electronic Record.
- ii) Scope of definition of evidence expanded to include electronic records.
- iii) Admissibility of electronic records
- iv) Presumption as to electronic messages

Status of Electronic Records as Evidence

- i) It is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence it is vital that the determination of its relevance, veracity and authenticity be ascertained by the court and to establish if the fact is hearsay or a copy is preferred to the original.
- ii) Digital Evidence is “information of probative value that is stored or transmitted in binary form”. Evidence is not only limited to that found on computers but may also extend to include evidence on digital devices such as telecommunication or electronic multimedia devices. The e-EVIDENCE can be found in e-mails, digital photographs, ATM transaction logs, word processing, documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories databases, Contents of computer memory, Computer backups, Computer printouts, Global Positioning System tracks, Logs from a hotel’s electronic door locks, Digital video or audio files. Digital Evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available.

Proof and Management of Electronic Records

- i) It Defines Records Management (RM) as the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including the processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. Electronic Records Management (ERM) ensures your organization has the records it needs when they are needed.
- ii) Records management refers to a set of activities required for systematically controlling the creation, distribution, use, maintenance, and disposition of recorded information maintained as evidence of business activities and transactions.

Relevancy-As a quality of evidence, "relevancy" means applicability to the issue joined. Relevancy is that which conduces to the proof of a pertinent hypothesis; a pertinent hypothesis being one which, if sustained, would logically influence the issue.

Admissibility and Probative Value of E-Evidence

- i) Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial. Before accepting digital evidence a court will determine if the evidence is relevant, whether it is authentic, if it is hearsay and whether a copy is acceptable or the original is required.
- ii) The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs, ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning System tracks, logs from a hotel’s electronic door locks, and digital video or audio files.

Proving Digital Signatures-Proving the legality of a digital signature involves a two-step process: having the signature admitted as evidence and then demonstrating its trustworthiness. To admit a signature as evidence, you will need expert testimony describing the record creation process and supporting its accuracy. Once the signed record is admitted, the trustworthiness of the signature must be shown.

Proof of Electronic Agreements:

- i) Section 84A12 provides for the presumption that a contract has been concluded where the parties' digital signatures are affixed to an electronic record that purports to be an agreement.
- ii) Section 85B of the Evidence Act provides that where a security procedure has been applied to an electronic record at a specific time, the record is deemed to be a secure electronic record from such time until the time of verification. Unless the contrary is proved, the court is to presume that a secure electronic record has not been altered since obtaining secure status. The provisions relating to a secure digital signature are set out in Section 15 of the IT Act.
- iii) It is presumed that by affixing a secure digital signature the subscriber intends to sign or approve the electronic record. In respect of digital signature certificates (Section 8 of the Evidence Act) , it is presumed that the information listed in the certificate is correct, with the exception of information specified as subscriber information that was not verified when the subscriber accepted the certificate.

Proving Electronic Messages-Under section 88A, it is presumed that an electronic message forwarded by a sender through an electronic mail server to an addressee corresponds with the message fed into the sender's computer for transmission. However, there is no presumption regarding the person who sent the message.

Concept of Cyber Crime and the IT Act, 2000

Objectives of IT legislation in India:

The Government of India enacted its Information Technology Act 2000 with the objectives stating officially as:

“to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as “electronic commerce”, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers’ Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.”

What does IT Act 2000 legislation deals with?

The Act essentially deals with the following issues:

1. Legal Recognition of Electronic Documents
2. Legal Recognition of Digital Signatures.
3. Offenses and Contraventions
4. Justice Dispensation Systems for cyber crimes.

Why did the need for IT Amendment Act 2008 (ITAA) arise?

The IT Act 2000, being the first legislation on technology, computers, e-commerce and e-communication, was the subject of extensive debates, elaborate reviews with one arm of the industry criticizing some sections of the Act to be draconian and other stating it is too diluted and lenient. There were some obvious omissions too resulting in the investigators relying more and more on the time-tested (one and half century-old) Indian Penal Code even in technology based cases with the IT Act also being referred in the process with the reliance more on IPC rather on the ITA.

Thus the need for an amendment – a detailed one – was felt for the I.T. Act. Major industry bodies were consulted and advisory groups were formed to go into the perceived lacunae in the I.T. Act and comparing it with similar legislations in other nations and to suggest recommendations. Such recommendations were analyzed and subsequently taken up as a comprehensive Amendment Act and after considerable administrative procedures; the consolidated amendment called the Information Technology Amendment Act 2008 was placed in the Parliament and passed at the end of 2008 (just after Mumbai terrorist attack of 26 November 2008 had taken place). The IT Amendment Act 2008 got the President assent on 5 Feb 2009 and was made effective from 27 October 2009.

Notable features of the ITAA 2008 are:

-
- Focusing on data privacy
 - Focusing on Information Security
 - Defining cyber café
 - Making digital signature technology neutral
 - Defining reasonable security practices to be followed by corporate
 - Redefining the role of intermediaries
 - Recognizing the role of Indian Computer Emergency Response Team
 - Inclusion of some additional cyber crimes like child pornography and cyber terrorism
 - Authorizing an Inspector to investigate cyber offenses (as against the DSP earlier)
-

Structure of IT Act

How is IT Act structured?

The Act totally has 13 chapters and 90 sections. Sections 91 to 94 deal with the amendments to the four Acts namely Indian Penal Code 1860, The Indian Evidence Act 1872, The Bankers' Books Evidence Act 1891 and the Reserve Bank of India Act 1934. The Act has chapters that deal with authentication of electronic records, electronic signatures etc.

Elaborate procedures for certifying authorities and electronic signatures have been spelt out. The civil offence of data theft and the process of adjudication and appellate procedures have been described. Then the Act goes on to define and describe some of the well-known cyber crimes and

lays down the punishments therefore. Then the concept of due diligence, role of intermediaries and some miscellaneous provisions have been described.

What is the applicability of IT Act?

The Act extends to the whole of India and except as otherwise provided, it also applies to any offence or contravention there under committed outside India by any person.

Rules and procedures mentioned in the Act have also been laid down in a phased manner, defined as recently as April 2011.

For the sake of simplicity, here we will be only discussing the various penalty and offences defined as per provisions of ITA 2000 and ITAA 2008. Please note that wherever the terms IT Act 2000 or 2008 are used, they refer to same act because the IT Act now includes amendments as per IT 2008 Amendment Act.

Specific exclusion(s) to the Act where it is not applicable are:

-
- Negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;
 - A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882;
 - A trust as defined in section 3 of the Indian Trusts Act, 1882
 - A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition
-

What is a cyber crime?

Cyber Crime is not defined officially in IT Act or in any other legislation. In fact, it cannot be too. Offence or crime has been dealt with elaborately listing various acts and the punishments for each, under the Indian Penal Code, 1860 and related legislations. Hence, the concept of cyber crime is just a “combination of crime and computer”.

Cybercrime in a narrow sense (computer crime): Any illegal behavior directed by means of electronic operations that targets the security of computer systems and the data processed by them.

Cybercrime in a broader sense (computer-related crime): Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

- Any contract for the sale or conveyance of immovable property or any interest in such property;
- Any such class of documents or transactions as may be notified by the Central Government.

Teen Vandalism

IT defines, vandalism as “willful or malicious destruction, injury, disfigurement, or defacement of any public or private property, real or personal, without the consent of the owner or persons having custody or control.” Vandalism includes a wide variety of acts, including graffiti, damaging property (smashing mailboxes, trashing empty buildings or school property, breaking windows, etc.), stealing street signs, arson, egging homes or cars, toilet papering homes, and other types of mischief.

Why do teens engage in vandalism?

There are a number of reasons why a teen might vandalize property. They could be bowing down to peer pressure. Someone dared them to do it, or the girl they like admires someone else who vandalizes, or perhaps it could be part of an initiation in a gang. Sometimes teens make poor decisions when they are bored. For example, a teen might view stealing a street sign as a fun way

to pass time where no one gets hurt. Another reason could be for revenge. A teen is angry at someone and tries to get back at that person by damaging their property. Finally, it is possible in the case of graffiti, that the teen considers their vandalism as a form of self-expression or art.

How does a parent know if their teen is engaging in vandalism?

Unfortunately, vandalism is very easy for a teen to hide. Unless they bring a street sign home as a souvenir, there is no 'evidence' to find, and rarely do they act differently than they normally do. That's why it is important for parents to do two things: (1) simply talk about vandalism with your children and explain why it is not a good idea, and (2) know where your teens are at all times because a teen who knows his parent cares and is involved is more likely to avoid becoming a vandal. We also offer some prevention tips at the end of this article.

How does a parent explain the problems vandalism cause?

It is important that parents explain how to distinguish pranks from vandalism. Often, teens think vandalism is a 'victimless crime'; in other words, they don't believe they're hurting anyone by spray painting graffiti on a brick building, or tossing a few eggs at a neighbor's car. Help them see the ramifications of their actions. Explain to them that vandalism costs taxpayers a lot of money because the property must be repaired and the crime must be investigated. That takes money away from other important things that your teen may care about. For example, because the school has to use money to cover up graffiti, they may have to cut out art programs. Besides repairing damage, there are other high costs to teen vandalism. Publicly viewable vandalism changes the atmosphere of a place. It may give the impression that the people in the area do not value their space and that the area is not well-protected and perhaps unsafe.

If you find out your child has vandalized something, the best consequence is to make them clean it up and/or pay for repairs. When they have to scrape off the gross, dried egg and they see that it takes off paint, the message will be loud and clear. If you happen to have a graffiti artist on your hands, then it's important to provide them with a sanctioned place to stage his art or opportunities to put the talent to a positive use.

Finally, it's important that parents communicate that vandalism is a crime. If they are caught, they can be charged with a crime and that will stain their permanent record as they try to go to college and start a career.

Offences & Penalties under the Information Technology Act, 2000:

Introduction:

The introduction of the internet has brought the tremendous changes in our lives. People of all fields are increasingly using the computers to create, transmit and store information in the electronic form instead of the traditional papers, documents. Information stored in electronic forms has many advantages, it is cheaper, easier to store, easier to retrieve and for speedier to connection. Though it has many advantages, it has been misused by many people in order to gain themselves or for sake or otherwise to harm others. The high and speedier connectivity to the world from any place has developed many crimes and these increased offences led to the need of law for protection. Some countries have been rather been vigilant and formed some laws governing the net. In order to keep in pace with the changing generation, the Indian Parliament passed the law --- Information Technology Act 2000. The IT Act 2000 has been conceptualized on the United Nations Commissions on International Trade Law (UNCITRAL) Model Law.

The increase rate of technology in computers has led to enactment of Information Technology Act 2000. The converting of the paper work into electronic records, the storage of the electronic data, has led tremendous changed the scenario of the country. The Act further amends the Indian Penal Code, 1860, The Evidence Act, 1872, The Banker's Book's Evidence Act, 1891 and The Reserve Bank of India Act, 1934.

Offences:

Cyber offences are the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both. Cyber crime usually includes:

- (a) Unauthorized access of the computers
- (b) Data diddling
- (c) Virus/worms attack
- (d) Theft of computer system
- (e) Hacking
- (f) Denial of attacks
- (g) Logic bombs
- (h) Trojan attacks
- (i) Internet time theft
- (j) Web jacking
- (k) Email bombing
- (l) Salami attacks
- (m) Physically damaging computer system.

The offences included in the IT Act 2000 are as follows:

1. Tampering with the computer source documents.
2. Hacking with computer system.
3. Publishing of information which is obscene in electronic form.
4. Power of Controller to give directions
5. Directions of Controller to a subscriber to extend facilities to decrypt information
6. Protected system
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offence or contravention committed outside India
12. Confiscation
13. Penalties or confiscation not to interfere with other punishments.
14. Power to investigate offences.

Offences under the IT Act 2000:**Tampering with computer source documents:**

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer Programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation: For the purpose of this section "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Object: The object of the section is to protect the "intellectual property" invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law.

Essential ingredients of the section:

1. Knowingly or intentionally concealing,
2. Knowingly or intentionally destroying,
3. Knowingly or intentionally altering,
4. Knowingly or intentionally causing others to conceal,
5. Knowingly or intentionally causing another to destroy,
6. Knowingly or intentionally causing another to alter.

This section extends towards the Copyright Act and helps the companies to protect their source code of their programmes.

Penalties: Section 65 is tried by any magistrate.

This is cognizable and non-bailable offence.

Penalties: Imprisonment up to 3 years and / or

Fine: Two lakh rupees.

Hacking with the computer system:

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation: The section tells about the hacking activity.

Essential ingredients of the section:

1. Whoever with intention or knowledge.
2. Causing wrongful loss or damage to the public or any person.
3. Destroying or altering any information residing in a computer resource.
4. Or diminishes its value or utility or.
5. Affects it injuriously by any means.

Penalties: Punishment: Imprisoned up to three years and

Fine: which may extend up to two lakh rupees. Or with both?

Publishing of obscene information in electronic form:

Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of

either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

Power of controller to give directions:

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made there under.

(2) Any person who fails to comply with any order shall be guilty of an offence and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

Explanation: Any person, who fails to comply with any order of the above section, shall be guilty of an offence and shall be convicted for a term not less than three years or to a fine exceeding two lakh rupees or to both.

The under this section is non-bailable & cognizable.

Penalties: Punishment: imprisonment up to a term not exceeding three years

Fine: not exceeding two lakh rupees.

Directions of Controller to a subscriber to extend facilities to decrypt information:

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence; for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed, extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to shall be punished with an imprisonment for a term which may extend to seven years.

Penalties: Punishment: imprisonment for a term which may extend to seven years.

The offence is cognizable and non- bailable.

Protected System:

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified.

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provision of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

Explanation: This section grants the power to the appropriate government to declare any computer, computer system or computer network, to be a protected system. Only authorized person has the right to access to protected system.

Penalties: Punishment: the imprisonment which may extend to ten years and fine.

Penalty for misrepresentation:

(1) Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Penalties: Punishment: imprisonment which may extend to two years

Fine: may extend to one lakh rupees or with both.

Penalty for breach of confidentiality and privacy:

Save as otherwise provide in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulation made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Explanation: This section relates to any to any person who in pursuance of any of the powers conferred by the Act or it allied rules and regulations has secured access to any: Electronic record, books, register, correspondence, information, document, or other material.

If such person discloses such information, he will be punished with punished. It would not apply to disclosure of personal information of a person by a website, by his email service provider.

Penalties: Punishment: term which may extend to two years.

Fine: one lakh rupees or with both.

Penalty for publishing Digital Signature Certificate false in certain particulars:

(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that-

(a) The Certifying Authority listed in the certificate has not issued it; or

(b) The subscriber listed in the certificate has not accepted it; or

(c) The certificate has been revoked or suspended, unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Explanation: The Certifying Authority listed in the certificate has not issued it or, The subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended.

The Certifying authority may also suspend the Digital Signature Certificate if it is of the opinion that the digital signature certificate should be suspended in public interest.

A digital signature may not be revoked unless the subscriber has been given opportunity of being heard in the matter. On revocation the Certifying Authority need to communicate the same with the subscriber. Such publication is not an offence it is the purpose of verifying a digital signature created prior to such suspension or revocation.

Penalties: Punishment imprisonment of a term of which may extend to two years.

Fine: fine may extend to 1 lakh rupees or with both.

Act to apply for offence or contravention committed outside India:

(1) Subject to the provisions of, the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality.

(2) For the purposes of, this Act shall apply to an offence or Contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Explanation: This section has broader perspective including cyber crime, committed by cyber criminals, of any nationality, any territoriality.

Confiscation:

Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provisions of this Act, rules, orders or regulations made there under has been or is being contravened, shall be liable to confiscation :

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

Explanation: The aforesaid section highlights that all devices whether computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device which helped in the contravention of any provision of this Act, rules, orders, or regulations made under there under liable to be confiscated.

Penalties or confiscation not to interfere with other punishments:

No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

Explanation: The aforesaid section lays down a mandatory condition, which states the Penalties or confiscation not to interfere with other punishments to which the person affected thereby is liable under any other law for the time being in force.

Power to investigate offences:

Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offence under this Act.

Indian Evidence Act

The Indian Evidence Act, originally passed in India by the Imperial Legislative Council in 1872, during the British Raj, contains a set of rules and allied issues governing admissibility of evidence in the Indian courts of law.

Importance

The enactment and adoption of the Indian Evidence Act was a path-breaking judicial measure introduced in India, which changed the entire system of concepts pertaining to admissibility of

evidences in the Indian courts of law. Until then, the rules of evidences were based on the traditional legal systems of different social groups and communities of India and were different for different people depending on caste, community, faith and social position. The Indian Evidence Act introduced a standard set of law applicable to all Indians.

The Act

The Indian Evidence Act, identified as Act no. 1 of 1872, and called the Indian Evidence Act, 1872, has eleven chapters and 167 sections, and came into force 1 September 1872. At that time, India was a part of the British Empire. Over a period of more than 125 years since its enactment, the Indian Evidence Act has basically retained its original form except certain amendments from time to time.

Amendments: The Criminal Law Amendment Act, 2005

Applicability

When India gained independence on 15 August 1947, the Act continued to be in force throughout the Republic of India and Pakistan, except the state of Jammu and Kashmir. Then, the Act continues in force in India, but it was repealed in Pakistan in 1984 by the Evidence Order 1984 (also known as the "Qanun-e-Shahadat"). It also applies to all judicial proceedings in the court, including the court martial. However, it does not apply on affidavits and arbitration.

Contents

This Act is divided into three parts and there are 11 chapters in total under this Act.[2]

Part 1

Part 1 deals with relevancy of the facts. There are two chapters under this part: the first chapter is a preliminary chapter which introduces to the Evidence Act and the second chapter specifically deals with the relevancy of the facts.

Part 2

Part 2 consists of chapters from 3 to 6. Chapter 3 deals with facts which need not be proved, chapter 4 deals with oral evidence, chapter 5 deals with documentary evidence and chapter 6 deals with circumstances when documentary evidence has been given preference over the oral evidence.

Part 3

The last part, that is part 3, consists of chapter 7 to chapter 11. Chapter 7 talks about the burden of proof. Chapter 8 talks about estoppels, chapter 9 talks about witnesses, chapter 10 talks about examination of witnesses, and last chapter which is chapter 11 talks about improper admission and rejection of evidence.

Indian Evidence Act Classic Classification

This section does not cite any sources. Please help improve this section by adding citations to reliable sources. Unsourced material may be challenged and removed. (July 2016) (Learn how and when to remove this template message)

In the Evidence Act All the Provisions can be divided into two Categories (1) Taking the Evidence (By Court) (2) Evaluation

In Taking the Evidence Court take the Evidence for the Facts (Either "Issue of Facts" or "Relevant Facts"); The Facts means the things which is said before the court in connection with the matter, The main thing, which is Crime in Criminal and Right etc. in Civil matters are main Issues, So main

Issues are known as "Issue of Facts", and the other facts which are Relevant to it are "Relevant Facts".

For those Facts Evidence is Given to the Court by two ways, One is orally and Second is Documentary (includes Electronic Documents), Oral Evidence mostly suggest the Verbal deposition before the Court (and not otherwise), and which includes oral statement regarding materials too, Documentary Evidence suggest the Documents. So The Evidence Regarding Matter which have number of Facts, for which Evidence by way of oral or Documentary produced before the court for its Evaluation for either one factor facts. Court by going through those Documentary Evidence and Oral Evidence decide that particular fact and all facts are proved or not, or whether the fact or facts can be presumed to be proved?

In Evaluation as above said by looking into the Oral and Documentary Evidence Court decide whether particular fact is proved or not, or facts are proved or not, In Evaluation there are two concepts to prove facts; One is Prove (Prove, Disprove or Not prove) and Other is Presumption (that fact is proved) (may Presume, Shall presume and Conclusive proof) After going to Oral and Documentary Evidence Court see that whether any fact or facts are proved by looking to such evidence or not? If at all no evidence is given or enough evidence is given for the fact it's said fact is 'Not proved'; The second Concept for evaluation is "Presumption" In Evidence many Section suggest these presumptions, Where there is said Facts 'may presume', Court is extremely free to believe it or not and may ask to prove the fact, In 'shall presume' there is more weight given to believe facts but in that too court may ask to give more evidence to prove the facts, Where in any provision it is said that particular fact, or particular fact in particular circumstances must be concluded as "conclusive proof" Court has no liberty then to believe it to be proved.

Classification of Evidence Act in Four Questions

Evidence Act may be divided in four questions. Question 1 Evidence is Given of What Answer 1 of Facts ("Issue of Facts" or "Relevant Facts") Question 2 How the Evidence of such Facts are Given Answer 2 The Evidence of Such Facts is Given Either by way of "Oral Evidence" or "Documentary Evidence" Question 3 On whom the Burden to Prove Facts lies Answer 3 "Burden of Proof"(of particular fact) or "Onus of proof" (to prove whole case) lies on the Prosecution in charge Question 4 What are the Evaluation of the Facts. Answer 4 the Evaluation is "Prove" or "Presumption"(of prove); the fact is either 'proved', 'disproved', or 'Not proved'; or there may be presumption that proof of facts "may presume", 'shall presume', or 'conclusive proof'.

Electronic Evidence/ Digital Evidence & Cyber Law in India

The proliferation of computers and the influence of information technology on society as whole, coupled with the ability to store and amass information in digital form have all necessitated amendments in Indian law, to incorporate the provisions on the appreciation of digital evidence. The Information Technology Act, 2000 and its amendment is based on the United Nations Commission on International Trade Law (UNCITRAL) model Law on Electronic Commerce. The Information Technology (IT) Act 2000 was amended to allow for the admissibility of digital evidence. An amendment to the Indian Evidence Act 1872, the Indian Penal Code 1860 and the Banker's Book Evidence Act 1891 provides the legislative framework for transactions in electronic world. *Digital evidence or electronic evidence* is any probative information stored or transmitted in

digital form that a party to a court case may use at trial. Before accepting digital evidence it is vital that the determination of its relevance, veracity and authenticity be ascertained by the court and to establish if the fact is hearsay or a copy is preferred to the original. Digital Evidence is “information of probative value that is stored or transmitted in binary form”. Evidence is not only limited to that found on computers but may also extend to include evidence on digital devices such as telecommunication or electronic multimedia devices. The e-EVIDENCE can be found in e-mails, digital photographs, ATM transaction logs, word processing, documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories databases, Contents of computer memory, Computer backups, Computer printouts, Global Positioning System tracks, Logs from a hotel’s electronic door locks, Digital video or audio files.

Digital Evidence tends to be more voluminous, more difficult to destroy, easily modified, easily duplicated, potentially more expressive and more readily available.

Electronic Evidences: Considerations, Care and Caution

It is very important to understand the nature of electronic evidences. Unlike any other form of evidences, it is quite easy to tutor electronic evidence, much less for an expert who deals with them on regular basis. Therefore, special care and caution must be attributed to handling such sensitive pieces of evidence. Primary threats to electronic evidence include virus, electromagnetic or mechanical damages.

Such tools and methods must be adopted that are tested and tried, confirmed my experts are precise enough to get to the thin roots of nuances of complex evidence. As far as possible the tools must be subject to mock examination every time before use in order to avoid any sort of error at the time of collection/examination of evidence. As far as possible sensitive information must be analyzed by experts and amateur should not be allowed to fiddle with the data. These are some of the basics, which, if followed religiously, can bring about unprecedented change in successful culmination of the prosecution.

Position in India

Information and Technology Act, 2000 was enacted to cater to the growing demand of legislation in cyber space. For the first time it introduced the concept of ‘digital signatures’, ‘encryption’, ‘electronic evidences’ etc. These terms were foreign to the then law of evidence. No provision was there to adduce them as evidences in courts of law. Inevitably, certain changes were made in the Indian Evidence Act, 1872 to make it more contemporary and in tune with the changing times. The Indian Evidence Act, 1872 and Information Technology Act, 2000 grants legal recognition to electronic records and evidence submitted in form of electronic records. According to section 2(t) of the Information Technology Act, 2000 “electronic record” means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. The Information Technology Amendment Act, 2008 has recognized various forms of communication devices and defines a “communication device” under section 2 (ha) of the Act “communication device” means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.

The second schedule of The Information Technology Act 2000 is India’s only act dealing with computer crime, with an intension to introduce the concept of electronic evidence has added to the

provisions of Indian Evidence Act, 1872 which had been drafted earlier keeping in mind only the physical world. These amendments can be summed up as following:

1. In section 3,—

(a) In the definition of "Evidence", for the words "all documents produced for the inspection of the Court", the words "all documents including electronic records produced for the inspection of the Court" have been substituted;

(b) after the definition of "India", the following have been inserted, namely:— 'the expressions "Certifying Authority", "digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber" with the meanings respectively assigned to them in the Information Technology Act, 2000. '

2. In section 17, for the words "oral or documentary,", the words "oral or documentary or contained in electronic form" have been substituted.

3. After section 22, section 22A has been inserted which says that "Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question."

4. In section 34, for the words "Entries in the books of account", the words "Entries in the books of account, including those maintained in an electronic form" have been substituted.

5. In section 35, for the word "record", in both the places where it occurs, the words "record or an electronic record" have been substituted.

6. For section 39, the following section has been substituted, namely: —

What evidence to be given when statement forms part of a conversation, document, electronic record, book or series of letters or papers.

When any statement of which evidence is given forms part of a longer statement, or of a conversation or part of an isolated document, or is contained in a document which forms part of a book, or is contained in part of electronic record or of a connected series of letters or papers, evidence shall be given of so much and no more of the statement, conversation, document, electronic record, book or series of letters or papers as the Court considers necessary in that particular case to the full understanding of the nature and effect of the statement, and of the circumstances under which it was made."

7. After section 47, section 47A has been inserted, which talks about, Opinion as to digital signature where relevant.

8. In section 59, for the words "contents of documents" the words "contents of documents or electronic records" have been substituted.

9. After section 65, section 65A and 65B have been added laying down the provisions about Admissibility of electronic records.

10. After section 67, section 67A has been inserted, which talks about Proof as to digital signature.
11. After section 73, section 73A has been added which talks about Proof as to verification of digital signature.
12. After section 81, section 81A has been added which talks about Presumption as to Gazettes in electronic forms.
13. After section 85, the following sections have been inserted, namely: —
 - i) 85A which talks about Presumption as to electronic agreements
 - ii) 85B which talks about Presumption as to electronic records and digital signatures.
 - iii) 85C which talks about Presumption as to Digital Signature Certificates.
14. After section 88, section 88A has been inserted which talks about Presumption as to electronic messages.
15. After section 90, section 90A has been added which talks about Presumption as to electronic records five years old.
16. For section 131, the following section has been substituted, namely: — Production of documents or electronic records which another person, having possession, could refuse to produce.

No one shall be compelled to produce documents in his possession or electronic records under his control, which any other person would be entitled to refuse to produce if they were in his possession or control, unless such last-mentioned person consents to their production."

Prior to enforcement of this schedule, judiciary did not witness any evidence involving computer records. With the growth of the use of electronic evidence in courts of law, it has left opened a very pertinent question that whether the judiciary is well equipped to appreciate these highly technical evidences. It goes without saying that the judges will need to know the finer aspects of this branch. However, we have seen that the courts of India have very well encountered such electronic evidence in accordance with the newly introduced laws. They have been frequently assisted by cyber forensic expert and the cyber lawyer. The next question which strikes our mind is that whether such computer records are as good evidence as paper based documentary evidence. The nature of such electronic evidence is a complex one as it demands extra caution and care during collection of evidence. Moreover, the concept of electronic evidence fails to identify the kinds of documentary evidence namely the primary and the secondary evidence as every electronic record is an original as well as in duplicate. However, the provisions of section 65A and 65B help to overcome this complex situation.

Unit- 5

Computer forensics:

- i) Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law. The goal of computer forensics is to perform a structured investigation while maintaining a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.
- ii) Forensic investigators typically follow a standard set of procedures: After physically isolating the device in question to make sure it cannot be accidentally contaminated, investigators make a digital copy of the device's storage media. Once the original media has been copied, it is locked in a safe or other secure facility to maintain its pristine condition. All investigation is done on the digital copy. Below Fig. shows the various domains of Forensic Science.

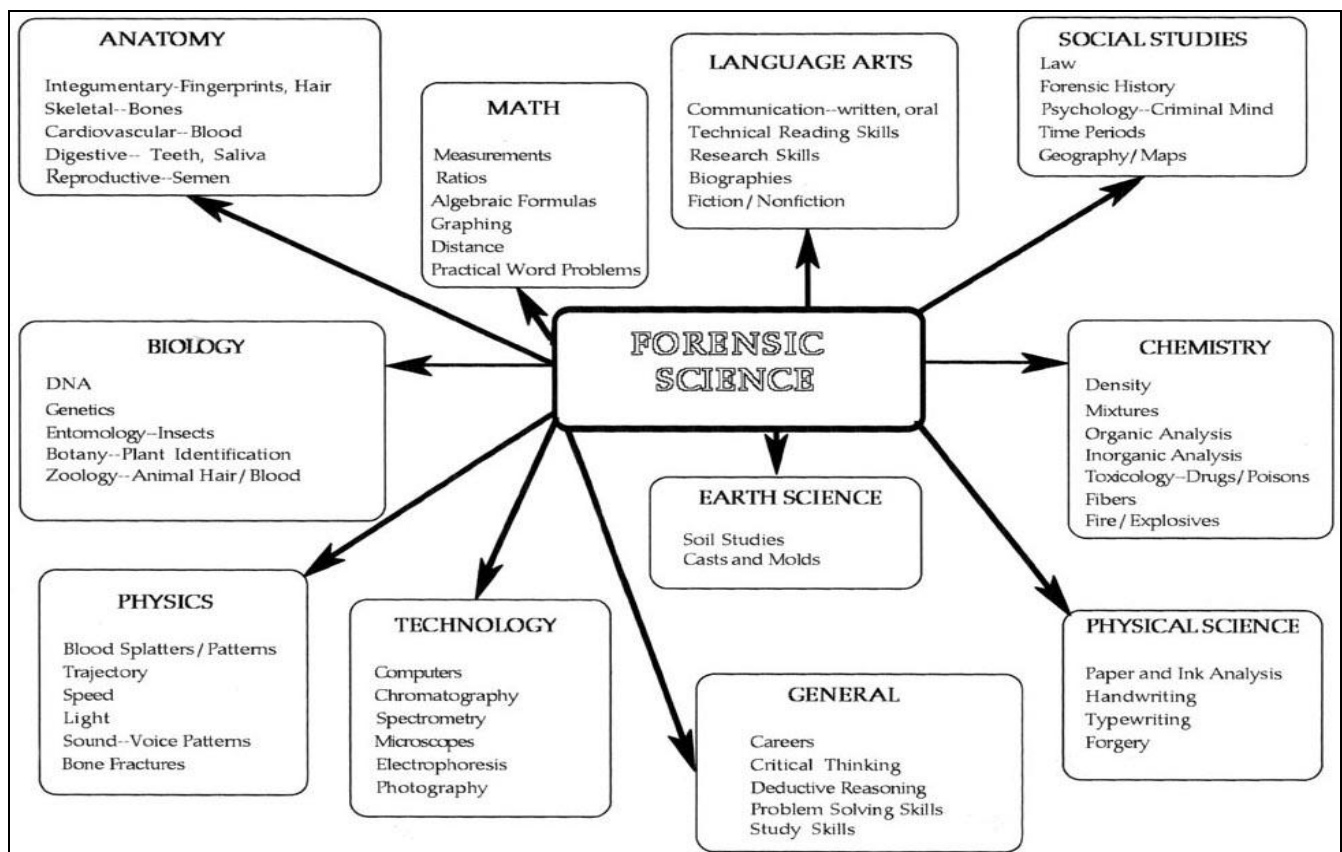


Fig. 5.1 domains of Forensic Science

Information Security Investigations-Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. Any evidence found on the digital copy is carefully documented in a "finding report" and verified with the original in preparation for legal proceedings that involve discovery, depositions, or actual litigation. Below Fig defines Digital Investigation Process.

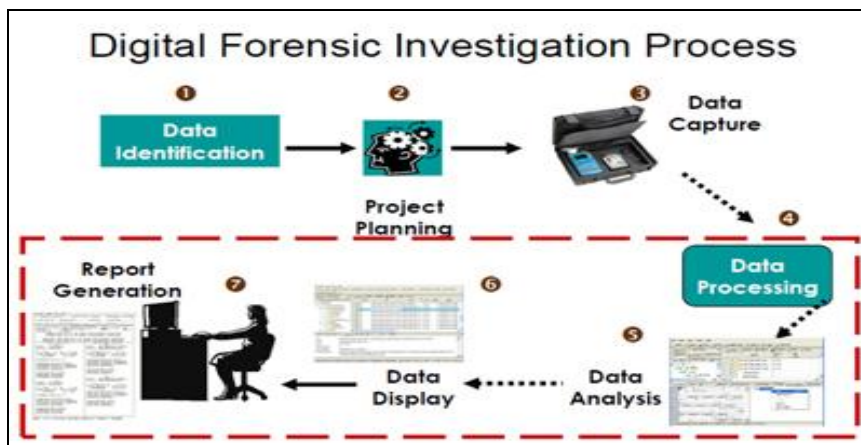


Fig. 5.2 Investigation Process

Scientific Method in Forensic analysis

- iii) The procedure by which scientists, communally and over periods, attempt to assemble a precise interpretation of the world, is referred to as the scientific method. The desired result is that of an unswerving, non-capricious and consistent portrayal. Perceptions and interpretations of natural phenomena can be influenced by personal and cultural beliefs.
- iv) The application of criteria and standard procedures assists in the minimization of these archetypal persuasions while developing a theory. The scientific method attempts to reduce the presence of prejudice or bias in the assessor when examining theories and hypotheses. Below Figure shows data acquiring Process.



Fig. 5.3 Investigation Process

The scientific method is comprised of four steps:

- i) Observation and description of a phenomenon or group of phenomena.
- ii) Formulation of a hypothesis (or hypotheses) to explain the phenomena.
- iii) Use of the hypothesis to predict the existence of other phenomena, or to predict quantitatively the results of new observations.
- iv) Performance of experimental tests of the predictions by several independent experimenters.

Types of Business Computer Forensic Technology-The following types of business computer forensics technology are:

- i) **Remote monitoring of target computers**-Data Interception by Remote Transmission (DIRT) from Codex Data Systems (CDS), is a powerful remote control monitoring tool that allows stealth monitoring of all activity on one or more target computers simultaneously from a remote command

center. No physical access is necessary. Application also allows agents to remotely seize and secure digital evidence prior to physically entering suspect premises.

- ii) **Creating trackable electronic documents**-Binary Audit Identification Transfer (BAIT) is another powerful intrusion detection tool from CDS that allows the user to create trackable electronic documents. Unauthorized intruders who access, download, and view these tagged documents will be identified (including their location) to security personnel. BAIT also allows security personnel to trace the chain of custody and chain of command of all who possess the stolen electronic documents.
- iii) **Theft recovery software for laptops and PCs**-Also, according to Safe ware Insurance, 756,000 PCs and laptops were stolen in 1997 and 1998, costing owners \$2.3 billion dollars. And, according to a recent joint Computer Security Institute/FBI survey, 69% of the Fortune 1000 companies experienced laptop theft.
Nationwide losses of computer component theft cost corporate America over \$8 billion a year. So, if your company experiences computer-related thefts and you do nothing to correct the problem, there is an 89% chance you will be hit again.
- iv) **Basic forensic tools and techniques**-The basic techniques needs to know types of computer crime, cyber law basics, tracing e-mail to source, digital evidence acquisition, cracking passwords, monitoring computers remotely, tracking on-line activity, finding and recovering hidden and deleted data, locating stolen computers, creating trackable files, identifying software pirates.



Fig. 5.4 Forensic Process

The basic methods are shown below:

- i) Lost password and file recovery
- ii) Location & retrieval of deleted and hidden files
- iii) File and e-mail decryption
- iv) E-mail supervision and authentication
- v) Threatening e-mail traced to source
- vi) Identification of Internet activity
- vii) Computer usage policy and supervision
- viii) Remote PC and network monitoring
- ix) Tracking and location of stolen electronic files
- x) Honey pot sting operations
- xi) Location and identity of unauthorized SW users
- xii) Theft recovery software for laptops and PCs
- xiii) Investigative and security software creation
- xiv) Protection from hackers and viruses

Corporate Cyber Forensics-It deals with the tracking of personal user information by monitoring their hardware and software components using different techniques to understand their behavior and create secure platform and infrastructure.

Scientific Method in Forensic analysis:

Identification Phase-The identification phase is the process of identifying evidence material and its probable location. This phase is unlike a traditional crime scene it processes the incident scene and documents every step of the way. Evidence should be handled properly. Basic requirement in evidence collection is evidence must be presented without alteration. This requirement applies to all phases of forensics analysis. At the time of evidence collection, there is a need of thorough check of system logs, time stamps and security monitors.

Acquisition Phase-The acquisition phase saves the state of evidence that can be further analyzed. The goal of this phase is to save all digital values. Here, a copy of hard disk is created, which is commonly called as an image. Different methods of acquiring data and their relative advantages and disadvantages are described in. As per law enforcement community, there are three types of commonly accepted forensics acquisition: mirror image, forensics duplication and live acquisition.

Analysis Phase-Forensic analysis is the process of understanding, recreating and analyzing arbitrary events that have gathered from digital sources. The analysis phase collects the acquired data and examines it to find the pieces of evidences. This phase also identify that the system was tampered or not to avoid identification. Analysis phase examines all the evidence collected during collection and acquisition phases. There are three types of examinations can be applied for the forensics analysis; limited, partial or full examination.

Reporting Phase-The reporting phase comprises of documentation and evidence retention. The scientific method used in this phase is to draw conclusions based on the gathered evidence. This phase is mainly based on the Cyber laws and presents the conclusions for corresponding evidence from the investigation. There is a need of good policy for how long evidence from an incident should be retention. Factors to be considered in this process are prosecution, data retention and cost. To meet the retention requirements there is a need of maintaining log archival. The archived logs must be protected to maintain confidentiality and integrity of logs.



Fig. 5.5 Evidence Processing

Forensics Methodology-The International Association of Computer Investigative Specialists (IACIS) has developed a forensic methodology which can be summarized as follows:

- i) Protect the Crime Scene, power shutdown for the computer and document the hardware configuration and transport the computer system to a secure location.
- ii) Bit Stream backup of digital media, use hash algorithms to authenticate data on all storage devices and document the system date and time.
- iii) Search keywords and check file space management (swap file, file slack evaluation, unallocated space).
- iv) Evaluate program functionality, document findings/results and retain Copies of software.

Investigating large scale Data breach case

- i) A data breach is the intentional or unintentional release of secure or private/confidential information to an un-trusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak and also data spill. Incidents range from concerted attack by black hats associated with organized crime, political activist or national governments to careless disposal of used computer equipment or data storage media.
- ii) A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve financial information such as credit card or bank details, personal health information (PHI), personally identifiable information (PII), trade secrets of corporations or intellectual property. Most data breaches involve overexposed and vulnerable unstructured data – files, documents, and sensitive information.

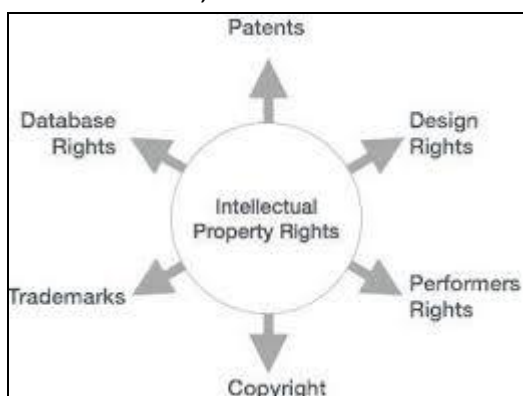


Fig. 5.6 Intellectual Property Rights

Analyzing malicious software-Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor. Malware or malicious software is any computer software intended to harm the host operating system or to steal sensitive data from users, organizations or companies. Malware may include software that gathers user information without permission.

- i) **Computer security incident management:** If an organization discovers or suspects that some malware may have gotten into its systems, a response team may wish to perform malware analysis on any potential samples that are discovered during the investigation process to determine if they are malware and, if so, what impact that malware might have on the systems within the target organizations' environment.
- ii) **Malware research:** Academic or industry malware researchers may perform malware analysis simply to understand how malware behaves and the latest techniques used in its construction.

- iii) **Indicator of compromise extraction:** Vendors of software products and solutions may perform bulk malware analysis in order to determine potential new indicators of compromise, this information may then feed the security product or solution to help organizations better defend themselves against attack by malware.

Types of Computer Forensics Technology:

- i) Move documentary evidence quickly from the printed or typewritten page to computer data stored on floppy diskettes, Zip disks, CDs, and computer hard disk drives.
- ii) Create a new type of virtual evidence for e-commerce transactions and email communications over the Internet.
- iii) Share computer files over the Internet, when tied to the commission of a crime, (creates a new and novel twist to the rules of evidence and legal jurisdiction).
- iv) Keep the venue in mind when criminal activities involve the use of the Internet (venue can be in different cities, counties, states, and/or countries). The evidence needed to prove such computer-related crimes potentially resides on one or more computer hard disk drives in various geographic locations.
- v) Keep in mind that the computer hard disk drives may also be the property of criminals as well as innocent third parties (Internet service providers). Such evidence is commonly referred to as computer evidence, but it is not limited to cases involving computer crimes.
- vi) Rely on computer evidence that is connected to a computer crime (not to traditional crimes that are committed using one or more computers as tools in the commission of a crime). Computer crimes are specifically defined by federal and/or state statutes.
- vii) Make sure computer evidence resides on computer storage media as bytes of data in the form of computer files and ambient data.
- viii) Make sure ambient data (which is usually beyond the awareness of most computer users) provides the computer forensics investigator with the element of surprise when computer users are interviewed. For example, a computer user who believes that he or she destroyed the computer evidence may confess when confronted with part or all of the evidence extracted from ambient data sources.
- ix) Make sure your computer investigations rely on evidence that is stored as data and that the timeline of dates and times of files that were created, modified, and/or last accessed by the computer user are recorded. Timelines of activity can be especially helpful when multiple computers and individuals are involved in the commission of a crime.
- x) Make sure your computer forensics investigator always considers timelines of computer usage in all computer-related investigations. The same is true in computer security reviews concerning potential access to sensitive and/or trade secret information stored in the form of computer files. Computer investigations play an important role in cases involving the theft of company trade secrets.
- xi) Make sure your intellectual property lawyers rely on computer evidence and computer investigations in such cases as stock frauds, financial frauds, and embezzlements. The same is true concerning criminal litigation involving stock frauds, financial frauds, and embezzlements. Much of the evidence related to these types of crimes will be in computer data form. In the past, documentary evidence used to prove these crimes was exclusively in paper form. However, many computer-related communications and transactions are now conducted without paper documents

ever being created. Financial fraud investigators have been forced to change the way they do business.

- xii) Make sure your computer-related investigations involve the review of Internet log files to determine Internet account abuses in businesses or government agencies.
- xiii) Make sure your computer investigations involve the analysis of the Windows swap file.
- xiv) Make sure you use computer forensics procedures, processes and tools, so that the computer forensics specialist can identify passwords, network logons, Internet activity, and fragments of email messages that were dumped from computer memory during past Windows work sessions. When such leads are identified, they can be perfected through the use of computer forensics text search programs.
- xv) Use other computer forensics software tools to document the computer evidence once it has been preserved, identified and extracted.

Types of Business Computer Forensic Technology

- i) Remote monitoring of target computers
- ii) Creating trackable electronic documents
- iii) Theft recovery software for laptops and PCs
- iv) Basic forensic tools and techniques
- v) Forensic services available

Forensic Services Available-Through Forensic Evidence Acquisition Services, CDS forensic experts can provide management with a potent arsenal of digital tools at its disposal. Services include but are not limited to:

- i) Lost password and file recovery
- ii) Location & retrieval of deleted and hidden files
- iii) File and e-mail decryption
- iv) E-mail supervision and authentication
- v) Threatening e-mail traced to source
- vi) Identification of Internet activity
- vii) Computer usage policy and supervision
- viii) Remote PC and network monitoring
- ix) Tracking and location of stolen electronic files
- x) Honey-pot sting operations
- xi) Location and identity of unauthorized SW users
- xii) Theft recovery software for laptops and PCs
- xiii) Investigative and security software creation

Specialized Forensics Techniques:

- i) **Laser Ablation Inductively Coupled Plasma Mass Spectrometry (LA-ICP-MS)** : When broken glass is involved in a crime, putting together even tiny pieces can be key to finding important clues like the direction of bullets, the force of impact or the type of weapon used in a crime. Through its highly sensitive isotopic recognition ability, the LA-ICP-MS machine breaks glass samples of almost any size down to their atomic structure. Then, forensic scientists are able to match even the smallest shard of glass found on clothing to a glass sample from a crime scene. In order to

work with this type of equipment in conjunction with forensic investigation, a Bachelor's Degree in Forensic Science is usually necessary.

- ii) **Alternative Light Photography:** For a forensic nurse, being able to quickly ascertain how much physical damage a patient has suffered can be the difference between life and death. Although they have many tools at their disposal to help make these calls quickly and accurately, Alternative Light Photography is one of the coolest tools to help see damage even before it is visible on the skin. A camera such as the Omni chrome uses blue light and orange filters to clearly show bruising below the skin's surface. In order to use this equipment, you would need a MSN in Forensic Nursing.
- iii) **High-Speed Ballistics Photography:** You might not think of it right away as a tool for forensic scientists, but ballistics specialists often use high-speed cameras in order to understand how bullet holes, gunshot wounds and glass shatters are created. Virtually anyone, from a crime scene investigator to a firearms examiner, can operate a high-speed camera without any additional education or training. Being able to identify and match bullet trajectories, impact marks and exit wounds must be done by someone with at least a Bachelor's of Science in Forensic Science.
- iv) **Video Spectral Comparator 2000:** For crime scene investigators and forensic scientists, this is one of the most valuable forensic technologies available anywhere. With this machine, scientists and investigators can look at a piece of paper and see obscured or hidden writing, determine quality of paper and origin and "lift" indented writing. It is sometimes possible to complete these analyses even after a piece of paper has been so damaged by water or fire that it looks unintelligible to the naked eye. In order to run this equipment, at least a Bachelors degree in Forensic Science or a Master's Degree in Document Analysis is usually required.
- v) **Digital Surveillance for Xbox (XFT Device):** Most people don't consider a gaming system a potential place for hiding illicit data, which is why criminals have come to use them so much. In one of the most ground-breaking forensic technologies for digital forensic specialists, the XFT is being developed to allow authorities visual access to hidden files on the Xbox hard drive. The XFT is also set up to record access sessions to be replayed in real time during court hearings. In order to be able to access and interpret this device, a Bachelor's Degree in Computer Forensics is necessary.
- vi) **3D Forensic Facial Reconstruction:** Although this forensic technology is not considered the most reliable, it is definitely one of the most interesting available to forensic pathologists, forensic anthropologists and forensic scientists. In this technique, 3D facial reconstruction software takes real-life human remains and extrapolates a possible physical appearance. In order to run this type of program, you should have a Bachelor's Degree in Forensic Science, a Master's Degree in Forensic Anthropology or a Medical Degree with an emphasis on Forensic Examination and Pathology.
- vii) **DNA Sequencer:** Most people are familiar with the importance of DNA testing in the forensic science lab. Still, most people don't know exactly what DNA sequences are and how they may be used. Most forensic scientists and crime lab technicians use what's called DNA profiling to identify criminals and victims using trace evidence like hair or skin samples. In cases where those samples are highly degraded, however, they often turn to the more powerful DNA sequence, which allows them to analyze old bones or teeth to determine the specific ordering of a person's DNA nucleobases, and generate a "read" or a unique DNA pattern that can help identify that person as a possible suspect or criminal.

- viii) **Forensic Carbon-14 Dating:** Carbon dating has long been used to identify the age of unknown remains for anthropological and archaeological findings. Since the amount of radiocarbon (which is calculated in a Carbon-14 dating) has increased and decreased to distinct levels over the past 50 years, it is now possible to use this technique to identify forensic remains using this same tool. The only people in the forensic science field that have ready access to Carbon-14 Dating equipment are forensic scientists, usually with a Master's Degree in Forensic Anthropology or Forensic Archaeology.
- ix) **Magnetic Fingerprinting and Automated Fingerprint Identification (AFIS) :** With these forensic technologies, crime scene investigators, forensic scientists and police officers can quickly and easily compare a fingerprint at a crime scene with an extensive virtual database. In addition, the incorporation of magnetic fingerprinting dust and no-touch wandling allows investigators to get a perfect impression of fingerprints at a crime scene without contamination. While using AFIS requires only an Associate's Degree in Law Enforcement, magnetic fingerprinting usually requires a Bachelor's Degree in Forensic Science or Crime Scene Investigation.
- x) **Link Analysis Software for Forensic Accountants:** When a forensic accountant is trying to track illicit funds through a sea of paperwork, link analysis software is an invaluable tool to help highlight strange financial activity. This software combines observations of unusual digital financial transactions, customer profiling and statistics to generate probabilities of illegal behavior. In order to accurately understand and interpret findings with this forensic technology, a Master's Degree in Forensic Accounting is necessary.

Methodology for the Featured Forensic Science Technologies-When deciding which technologies to include on this list, a number of factors were taken into consideration.

- i) **Relevance to the Topic of Forensic Technology:** The said technology must be actively used in the field of Forensic Science and can be taught at the college level. Widely regarded technologies were considered first, while more experimental technologies were included only on the basis of reputable peer-reviewed documentation.
 - ii) **Novelty in the Field of Forensic Science:** More experimental technologies were given higher priority based on whether the technology gave advanced information that is not readily available by using other technologies. These "cutting-edge" technologies were thoroughly vetted to ensure that they have become accepted techniques by leaders in the field.
 - iii) **Reliability of Technology:** Finally, only techniques used with more than 80% reliability were included in this list. Factors that affect reliability included case closure rate, successful conviction rate and correct identification rate.
-

Unit 6

Web Application Introduction

Introduction to Internet:

Internet is a collection of two or more systems, capable of sharing or accessing applications and their features, which are actually located at different places, even at different continents. Internet is identified as www(World Wide Web). Almost 90% business sectors are dependent on Internet and its functionalities, users could purchase, sell, transfer or execute their applications like banking, education, reservation etc. Internet is free or open for every user, some users use it for positive purpose and some use for unauthorized purposes and they are called as attackers or hackers or crackers.

This chapter contains Internet (web application) layered architecture, components of web application like HTTP or HTTPS features, protocols, packet structure etc. It also contains information about Internet user, how user is identified on Internet using IP addresses, how user accesses different applications like mail services, banking, reservation just sitting on a single machine at their chosen location. Here, in this chapter web attack type has been given with malicious code fragments to guide user or researcher, so that the strong design with protective shield could be created by knowing attack names, signatures and their fingerprints. Here, security tips have been given to keep and create safe design, algorithm, architecture, and module.

"It is said that protection or strong analytical or logical understanding is better than cure, so be safe by updating knowledge"

Web Design and Architecture

Web Application architecture contains three layers, which is accessed by user through Web-Browser (may be called as Program or tool or software), consist of three layers Presentation layer, CGI layer (Common Gateway Interface) or Business Logic Layer and Database Layer respectively.

(1) Web Application Architecture(3-Tier)

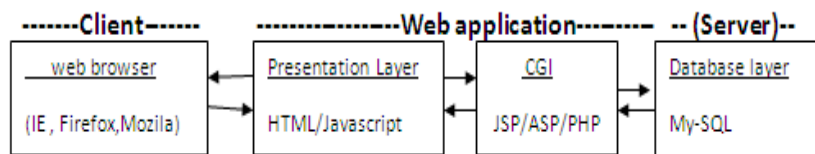


Fig.6.1: web layer architecture

- **Presentation Layer(First Tier)**

It is a graphical representation of Interface, which collects all the data from user or shows the evaluated result by server as a response to the user back. JavaScript, Flash, VBscript and HTML makes the design of this layer called as Client side scripting language, which communicates from user at client machine.

- **CGI Layer(Common gateway interface) or Business logic layer(Middle Tier)**

It acts as interface between presentation layer and database layer and located between middle of architecture design. CGI contains design and codes of JSP(Java Server Page), PHP(Preprocessor Hypertext), ASP(Active Server Page) and are called as server side scripting language. These languages contain logic and concept for execution of data present at Application databases. CGI translates inputted data of user into standard form and saves into database. It also works in reverse order, collects data from database and sends to the presentation layer.

- **Database layer(Third Tier)**

It manages the information of user after processed by CGI layer and also provides requested data to CGI layer back. This layer should be protected from unauthorized and malicious activities from attackers or hackers or crackers to steal, modify, delete Data from database.

Database contains Confidential and secret information of users, which is the main concern in Internet Application. Various secure algorithm, design and cryptographic techniques are needed for protecting database to create secure and trustworthy environment. This layer needs regular

security updation, as new attacks are invented every minute to create fraudulent activities in web application.

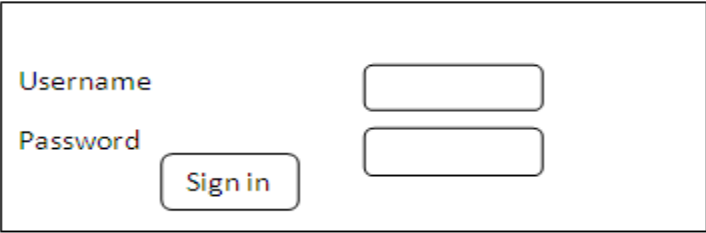
Database layer mainly contains data centers which store huge amount of data using Storage Area Network or Network Area Storage technology and can be placed all over the world. Today most of the mail service provider stores their customers information at various part of the cities and take backup Locally or remotely in case of any hazards.

“According to Law of physics, action and reaction are reverse and interdependent processes, and therefore, Attack and Protection are interrelated too”.

“Basic requirement of any web application is, it must be represented in tiered architecture.”

(2) Working of Web layers

Display Form



The image shows a simple login form within a rectangular border. On the left side, there are two labels: 'Username' and 'Password'. To the right of 'Username' is a single-line text input field. To the right of 'Password' is another single-line text input field. Below the 'Password' label and to the left of the second input field is a button labeled 'Sign in'.

Fig.6.2: Login.jsp

Figure shows above, represents presentation logic can be any html, jsp, or php page through which client sends its request to service provider.

Example: <http://www.college.com/display.jsp?username=abc&password=123>

This example shows the format of client request using GET method.

Here, www.college.com represents domain name,

Display.jsp represents jsp file, contains the logic, responsible for handling and checking of login validation. Username and password represents FORM attributes.

- First of all client sends its username and password through presentation logic i.e. Login.jsp.
- Then it internally sends it to display.jsp running on Apache business logic, contains the logic to validate the username and password.
- It sends its request to business logic, RDBMS application i.e. MySQL
- MySQL sends those parameters in the form of query to Database logic i.e. Login.jsp to validate the login and sends reply to display.jsp and display.jsp sends it to Login.jsp

Here,

- HTTP(Hypertext transfer protocol has port number 80, Susceptible to attack) or HTTPS (Hypertext Transfer protocol With secure channel for providing Cryptography has port number 443) is used to access web application on web browser(Ex- Mozilla, Google chrome, Internet Explorer)
- www.college.com --- It is a domain on internet for indentifying service providers, contains various web servers to fulfill client request. Mapping of various web servers to their domain name is done through DNS server.

username	password	stud_name
abc	123	Sam-Tom

Table 6.3: Student Table

Above is a sample Database table, taken for creating SQL Queries and different examples.

SQL (Structured Query Languages) is used to access tables of database.

Below SQL queries can be used to manage student record:

Query= Select * from Student where username='abs' && password='';

Query= insert into Student values ('xyz', '34566', 'dummy');

Query= Update table Student set stud_name='pqr' where username = 'xyz';

Query=Drop table Student;

(3) HTTP request and HTTP response.

User enters his details into web page and forwards to web server using one of the mentioned methods:

- **GET method and its format.**

http://www.college.com/display.jsp?stud_name=sam%20Tom&password=123

Here, user input is visible and could be manipulated easily by attacker, by modifying the values in the query string generated at the URL. Attacker changes the logic of string and generates his well defined malicious string to by-pass request, or creates any fraudulent activities at the server end. %20 is used for space [Sam%20Tom = Sam Tom].

- **POST methods and its format.**

Here, user information does not appear in the URL. web site data is transmitted within the message body. It should be used when FORM data contains non-ASCII characters, or dataset is large enough.

<http://www.college.com/display.jsp>

“Now a days, various service providers implements XML controllers to hide the file details i.e. display.jsp from display in the query i.e. <http://www.college.com>”

(4) HTTP sessions and cookies.

HTTP is a stateless protocol. It could not store useful information required for communication between client and server. Concept of session and cookies are used for maintaining and managing the state information. User's state information in web application is maintained by session between each and every request during a period of certain time. User is uniquely identified on web application by session unique ID field and its status.

Example- When user successfully logs into any web site, its session is created which is identified by session ID. Every session has some predefined time limit i.e. 15 sec, if user remains idle up to specified time limit, its session gets expired and user again has to login.

Every website pages contains the logic to identify session id, if session is not created, then user cannot access those pages directly.

(5) Session ID's storing Techniques.

Session ID could be stored in any of four ways.

- **URL(Uniform Resource Locator) encryption:**

It contains links of web applications.

http://www.college.com/display.jsp?stud_name=sam%20Tom&password=123

The above URL session will be based on attribute values i.e, stud_name

This can be done using URL encryption technique.

- **HTML hidden Field:**



Fig.6.4: Http Header

Here, header contains host, version of Web Browser, content length and application server fields. This contains the session information. It is basically implemented by hidden field, and other page checks the value of this field to get session information.

- **Cookies:**

Cookies are the amount of web data transmitted between client and server for user profile remembrance and its authentication. *Persist cookies* are the one which last over a period of session and are stored on user's hard drive, while session cookies are deleted, when the user exits or quits from his web browser

Cookies stores account and password or login information, which is very sensitive and contains confidential information (**Example:** ATM pin information, Internet bank account login information, Fund Transfer information etc). It must be protected from malicious activities or modification from its contents. Attacker usually targets data present in cookies for gaining the secure information.

Example-Cookies folder is situated in user's system account folder, when user starts web browser, temporarily file is created which contains Information shown below-

File-

```
GAPS:Etr1hZfh86m-htgk-  
8e743gdfdhhy:76gdhdghdh5gsgsg8taccounts.mail.com/767676785497209730379  
27270*  
0_utma65789767.5643195.98762416.09134684.5accounts.mail.com/647764374  
767436436743760*0_utmb686775.5.7.21.344446.accounts.mail.com/785098453  
0978346734767467*_utmz34267748.6.7.utmcsr=(direct)|utmccn=(direct)|utmc  
md=(none)accounts.mail.com/25453637743645745785478547854*
```

The file so created contains different coding scheme, but it is showing, user is using MAIL account, Attack follows different scheme to access cookies.

- Attacker accesses cookies data.
- Apply different encoding, decoding scheme methods to convert encrypted code to usable form.
- Attackers have great expertise on attack encryption and decryption techniques and have strong knowledge about study of tools and tricks.
- If attacker succeeds, he gain username and password or login information and he will use that account for malicious or unauthenticated purposes.
- All the above techniques are expired and will not be used today by any of the service providers. Now, user sessions are created on server side using Session class and also stored on server side.

Example-Session. SetAttribute ("abc", "user_name");

In above example, abc shows username value and "user_name" shows the session attribute value which is used to store user session information.

So, now hacker cannot access user' session information, since it is maintained by Server.

(6) TCP/IP architecture and implementation

It contains different layers used for communication between client and server.

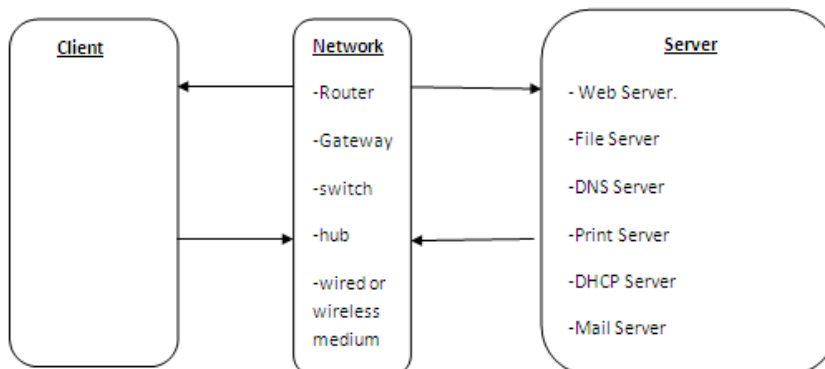


Fig.6.5: Client – Server Architecture

Client Server Interaction:

- Client machine sends http request by URL to the web server. [Client machine contains Operating system and firewall ,antivirus for security]
- The request is converted into HttpServletRequest object by the web-server. The object generated, deals with the web components and generates dynamic contents from database.
- Web component generates HttpServletResponse or can communicate with other web components.
- Web component generates an object of HttpServletResponse.
- The object is converted into HTTP Response by web server and returns to the URL of client machine.

Servers are basically used to provide services to client machines. Server can be one of the following types:

- Web server: responsible for managing web applications.
- File server: responsible for managing file i.e. uploads and downloads.
- Print Server: responsible for providing print service to many clients.
- DNS Server: responsible for mapping of Domain names and Web server IP addresses.

- DHCP Server: responsible for assigning IP addresses to machines dynamically.
- Mail Server: responsible for managing mails locally and globally.

(7) Web Packet architecture

Data is transmitted as per the TCP/IP Model (5 layered model). Which contains layered architecture, user deals with application layer, then data is travelled along other layers, which appends different security checks and design. At-last data is converted into ETHERNET Frame and then into electrical signals, which is then transferred over the network to reach up to receivers address and their TCP/IP layer starts working in reverse order.

Communication over the internet takes place in the form of packets. Packets contains following fields:

- Sender s' IP address
- Receiver's IP address
- Protocol used i.e. TCP, UDP
- User Data
- CRC, Checksum or other error detection mechanisms

If attacker traces this information present in packets, he could easily hack secure system and could use it for performing malicious operations.

Figure below shows mail packet sent by the client using a mail server:

```
Delivered-To: Abhishek.Data
Received: by 10.60.3.161 with SMTP id d1csp139592oed;
    Mon, 13 Aug 2012 02:34:55 -0700 (PDT)
Received: by 10.66.75.133 with SMTP id c5mr16941706paw.24.1344850495005;
    Mon, 13 Aug 2012 02:34:55 -0700 (PDT)
Return-Path: <Sender.DATA@gmail.com>
Received: from dualxeonindia.ns3.999servers.com
    (dualxeonindia.ns3.999servers.com. [182.18.172.61])
    by mx.google.com with ESMTPS id
    gk6si1211946pbc.275.2012.08.13.02.34.53
    (version=TLSv1/SSLv3 cipher=OTHER);
    Mon, 13 Aug 2012 02:34:54 -0700 (PDT)
Received-SPF: neutral (google.com: 182.18.172.61 is neither permitted nor
    denied by best guess record for domain of Sender.DATA@gmail.com) client-
    ip=182.18.172.61;
Authentication-Results: mx.google.com; spf=neutral (google.com:
    182.18.172.61 is neither permitted nor denied by best guess record for
    domain of Sender.DATA@gmail.com) smtp.mail=Sender.DATA@gmail.com
Received: from localhost.localdomain ([127.0.0.1]:60677
    helo=dualxeonindia.ns3.999servers.com)
    by dualxeonindia.ns3.999servers.com with esmtpa (Exim 4.77)
    (envelope-from <Sender.DATA@gmail.com>)
    id 1T0r2x-004NH8-Qb; Mon, 13 Aug 2012 15:04:51 +0530
Received: from localhost ([127.0.0.1] helo=localhost) by
    dualxeonindia.ns3.999servers.com
    with ESMTP (A3SP 1.9); 13 Aug 2012 15:04:51 +0530
Received: from 122.168.101.68 ([122.168.101.68]) by
    dualxeonindia.ns3.999servers.com (Horde Framework) with HTTP; Mon, 13 Aug
    2012 15:04:51 +0530
Message-ID:
    <asp.5572311bc4.20120813150451.33643xxa37c4qq0r@dualxeonindia.ns3.999serv
    ers.com>
Date: Mon, 13 Aug 2012 15:04:51 +0530
```

Fig.6.6: Packet architecture

The packet structure shown above contains confidential information's like:

- Senders email id and IP address
- Receivers email id and IP address
- Type of mail service used
- Time, Date, version information about protocol and application.
- Actual data
- Route information, type of Network information.

Hacker traces the packets to obtain these personalize and confidential information of sender and receiver, to perform malicious and unauthorized activities like.

- Could generate fake packet by altering message content and forward to receiver.
- Could generate fake reply from receiver side.
- Could change the route of packet and divert the path towards unintentional receiver.
- Could generate mails use for terrorist activities.

Several tools and techniques are available to trace packet like packet analyzer, protocol analyzer, network analyzer, port analyzer etc.

The only way to keep safe is to use updated software's and tools and best designed security algorithms.

Attacking and Security Techniques

(8) Basic Needs for performing ethical hacking.

- Knowledge of networking commands (Ipconfig, Net, Traceroot, Tracert ,ping ,Telnet, FTP etc) and networking tools like Remote access-login (Example –RLOGIN –which controls remote machines and performs their illegitimate activities).networking devices knowledge is also require to bypass techniques, like router ,hub , switch etc. they contains routing table(Routing table contains IP address of sender and receiver, routes information, packet information, time to live information) information.
- Knowledge of assembly and binary language or low level language.
- Knowledge of database design, accessing methods, fake login tricks, time & type of response generated by database servers, data storing mechanism.
- Knowledge of firewall, Cryptographic algorithm, Network and tracing tools.
- Network scanner tools like Packet sniffer, protocol analyzer, traffic analyzer, port scanner, URL Scanner, Web contents scanner, tracing software's (Key logger- traces, key pressed and creates log and snapshots for malicious use), These tool and software's are very dangerous, because it creates packet information, which travel along network and contains user information,(port scanner –it searches for open port and try to send vulnerability).
- Knowledge of attack signatures and fingerprints like Virus signatures (i.e. 098474GHJHJ758JH88FG type Folder, Recycler type folder), Packet structure, Hit and trial methods for password guessing (eg. admin,root,rootadmin,weroot,sa, 123456 etc).
- Knowledge of Proxy Servers:

Proxy Server arrangement between client-server model

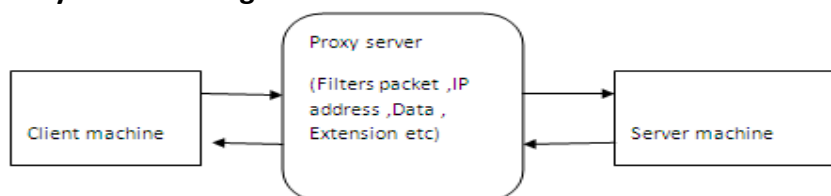


Fig.6.7: Proxy server design

The Proxy server filter, request generated from client side, if request is valid, it bypass towards server, otherwise generates an error message to user screen (You are not authorized to access it).

- It filters Packet Information.
- Extension(.exe , .zar etc as they may contain virus and Trojan horse programs)
- IP address and domains(Social networking sites)
- Data(data types)

(9) Hard code Programs for malicious purposes.

Programs are nothing, they are just a logic created, to access system file, folder, alters their meaning, & misguiding system to perform illegitimate work. Here some simple malicious programs are shown, which helps in understanding, how attacker creates malicious codes and targets system.

- **C program to get the information of network interfaces i.e. IP address, hardware address etc.**

```
#include<stdlib.h>
main ()
{
system ("C:\\Windows\\System32\\ipconfig");
system ("pause");
return 0;
}
```

- **C programming code for O.S. Shutdown**

```
#include<stdio.h>
#include<stdlib.h>
main()
{
char ch;
printf ("Do you want to shut down your computer now (y/n) ");
scanf("%c", &ch);
if ( ch == 'y' || ch == 'Y')
system("C:\\WINDOWS\\System32\\shutdown -s");
return 0;
}
```

- **Infinite loop code. This will hang computer and system busy.**

```
# include<stdio.h>
#include<stdlib.h>
Main()
{
Int i=3;
While(i==3)
Printf ("SYSTEM HACKED");
}
```

The malicious program shown above are written in C language, but the malicious content or code designing is not language dependent, database dependent, platform dependent, specific tool dependent. User could generate the code as per their knowledge of domain and area of interest

(10) **Malicious program categories**

- **Virus:**

It is the self –replicating programs or codes that injects and propagates through files. Virus needs startup programs for activation by means of either process, and scheduled task or occurrence etc. Types of viruses (always performs malicious activities):

➤ **Memory resident:**

Creates their permanent position in RAM, when Operating System loads in kernel area or privilege area or OS area of RAM, its activates and performs, its destruction.

➤ **Boot sector virus:**

Corrupts MBR (Master boot records), run itself every time, when computer is booted up.

➤ **Stealth Virus:**

It works in hidden mode, either by encryption or by changing the extensions to be unnoticed by antivirus or malware programs.

- **Worms:**

Self replicating programs that propagates over network through web channels or applications. Classes of worm are shown below.

- **Network Aware worm:** It targets particular host, captures their control by accessing or updating system files, and then starts his operations from that system to attack or hack other systems present over network (Ex: Backdoor attack).
- **Mass mailing worm:** It spreads through email attachments, email contains malicious codes hidden or attach (hidden in exe file, jar file, zip file, rar file) by a file, when downloaded on client machine starts its working.
- **Spamming:** It occurs by sending identical email to a target address or machine repeatedly to catch its reply for retrieving user's information.
- **Trojans:**
These are program codes or fragments or logic or commands hidden in other program. When they reach their target machine, starts their working.

(11) **Effect of above mention malicious codes or fragments**

- Changes the file extensions. Ex .dll to .doc (Makes system.dll file unavailable for OS process)
- Corrupts and modifies system file, due to which system may shutdown, restart or permanently crashes.
- Crashes or corrupts hardware files, by updating their device driver programs.
- Corrupts system configuration files and makes unwanted file in system folder for controlling targeted machine.

(12) **Security techniques for preventing or protecting system**

- **Intrusion detection system:** These are highly advanced system designed using Artificial Intelligence techniques .Which filters and indentify attacks.
- **Firewall:** filters suspicious IP address, Ports, Packets, Contents, extensions for protecting system from suspicious activity.
- **Cryptographic System:** It uses security algorithms designed for encryption or decryption using cryptographic frameworks. Advanced techniques are implemented to provide secure channel for data transfer and unbreakable or unmodifiable code or packet by attacker. Ex RSA-512 key.
- **IPSec (Internet Protocol security):** It provides secure communication to IP (internet Protocol) by providing algorithms, security services, encryption method and protocols. It protects IP layer from attack by providing various security features.
- **SSL (Secure Socket Layer):** It provides security between web-browser and website by providing different standard of key exchange authentication and encryption. HTTP (Here, data is transferred from client to other client over network without any encryption or certificates and thus it is susceptible to attack) operates on port no 80, and SSL-encrypted (HTTPS-Here data is first encrypted and several levels of key exchange certificate is asked to confirm authenticity of machines communicating over network) on port no 443, and provides safe and secure communications.
- **Antivirus or Antimalware:** It contains fingerprints or signatures of attacking programs or codes, it detects malicious activity and removes or blocks from system.
- **Black Holing and Sink Holing:** Here, attacked IP address and DNS are diverted to black-hole (non existing server).It avoids network traffic and unwanted connection. Sink-holing senses or analyzes and rejects malicious or bad request & reply. Thus, creates only that connection or traffic which is intended or safe for user' machine and provides sufficient bandwidth for network usage.
- **CAPTCHA:** It is abbreviated for Completely Automated Public Turing Test to tell Computers and Human apart. This technique helps to protect sites or web application like Mails from automated software's, which performs malicious operations and degrades the application service performances. This Technique protects web application or sites from internet bots or from automated systems.

- **Clean Pipes:** Here web traffic are passed through various systems like proxies, Tunnels, Logic circuits Artificial Intelligence system to check the authenticity of system & also checks the vulnerability, if present in connection.
- **Teardrop attack:** here, attacker works by sending malicious or disturbed IP packet fragment for creating oversized and overlapping payloads towards target machine.
- **Fraggle attack:** Here, attacker generates large amount of UDP echo traffic to IP broadcast, for creating network flood.
- **Other class attacks:** attacker studies about packets and their structure for creating attacking source by modifying it or by creating same structures as packets have(Ex- IP packers , ICMP packets/Echo request/reply ,TCP/SYN packets etc)

(13) General guideline for internet users. The unknown information may contains malicious codes for attack:

- Do not use internet password like banking, reservations etc, at cyber cafe. Their system may contain key loggers (hardware +software), cameras for tracing user confidential information.
- Don't provide any information to unknown email, which ask for user id and password like in lottery mail, gift mail etc. just delete them without reading.
- Don't save user id, password and any confidential information to the mail draft.
- The web-sites to whom, you are genuine user, does not accepts username and password, just complain to toll free contacts of that site regarding your security issues.

Cyber Attack

Introduction of Web attacks:

The purpose of this chapter is to provide information about attack initiated targeting points, from where attack or malicious activity alters, the behavior of web application. Here different types of attack with their signature and fingerprint have presented, to understand malicious structure or behavior created by attacker. The services, features, application, code fragments, design, protocol, fields, which could be changed and passed through the application to misguide user, the attackers intentional targeting points are shown in this chapter to create strong design for generating best protective shield.

(1) Web Attacking Points

Unauthorized or illegal access of information on a network is called as cyber attack. Purpose of attacker (Hacker or cracker) is to perform malicious or illegitimate activity on a network for the intension of destroying, stealing, or modifying the contents of database application. ATTACK on web application occurs through Programming codes, tools, software's, logics and design frameworks. These attacks are logical and don't need to physically destroy the machine and connecting wires.

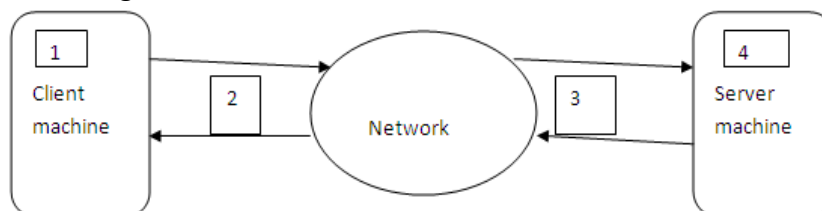


Fig 6.8 Architecture for attacking points

Attackers generally targets, the points specified in fig 2.1, their ultimate target is to get access over server machine to steal or modify information present on database application, lying at server.

- Attacker could target at Points shown in fig, like (1) Client machine for controlling its machine and generating attack towards server machine by hiding its identity in client's machine request packets.
- Attacker could target at the network locations (2) and (3) (position between client machine and server machine) as the packets passes through network for reaching to the target machine. Attacker captures information or packets by using networking tools (Packet sniffer or packet analyzer, port scanner, IP scanners etc) modifies that packet by malicious codes and again sends to his route ,here it uses advance techniques by which attacker misguided server for accepting request and performing operation.
- Again, Attacker capture packet from server side (3) or (4), adds a malicious code and sends to client back to misguide client application(Example - email spam).
- Attacker couldn't target directly server point (4) as server contains various protecting algorithms ,tools ,firewall and filtering approaches, which are very difficult to break, still for getting server access, he needs to access or bypass several application points like(1),(2) (3).

(2) Web application attacks

• URL manipulation:

If using a GET method, attacker inserts malicious code or parameters into the query string presented at the URL filed.

Example: `www.college.com/display.jsp?username=abc&password=123` (Original URL Field)

`www.college.com/display.jsp?username=abc&password=R$%^GHH` (malicious URL Code inserted by attacker)

• Form Field manipulation also called Cross side scripting attacks.

Attacker could change or modify the fields of WEB-FORM like text field, Radio button presented in designing or scripting language code and reload the page to create fraudulent page by altering its security permission and restrictions. Here code executes in a user's web browser and have architecture as shown below:

```
<FORM method="post"> action="Display.jsp"

  <input type="text" name="username">

  <input type="password" name="password">

  <input type="submit" name="submit">
```

Fig.6.9 : Original login.jsp page

```
<FORM method="post"> action="FakeDisplay.jsp"

  <input type="text" name="username">

  <input type="password" name="password">

  <input type="submit" name="submit">
```

Fig.6.10 : Change malicious login.jsp page

Here, attacker access original login.jsp page modifies it and diverts user, towards Fake login page, which contains FakeDisplay.jsp page and it looks exactly same as original, when user enters his username and password, attacker traces it, and then uses for malicious purposes.

- **HTTP Header manipulation:**

Header of HTTP contains combination of name and value, which is separated by a colon character, control information in HTTP header could be manipulated to bypass the mechanism of security.

```
Host :http://www.college.com

User-agent :IE/7.0

Referer: http://www.college.com/display.jsp

Content-length: 26
```

Fig.6.11: Original HTTP Header

```
Host :http://www.college.com

User-agent :IE/7.0

Referer: http://www.school.com/Fakedisplay.jsp

Content-length: 30
```

Fig.6.12: Suspicious HTTP Header

It is checked by some websites to confirm that the request is coming from authenticated page present in their own domain. If fields changes, server or web-page, refuses to load the next page.

- **Cookies Theft /poisoning/hijacking/ forging/session ID attack/session fixation.**

As cookies Stores and maintains session state information and saves on client machine , if altered by attacker using decoding algorithms and patterns matching schemes will create malicious or

unauthorized activities. Attacker's uses fake ID to obtain another's identity. Below is the structure of cookies information.

Ex: Cookies file- [Original File of Cookies]

```
GAPS:Etr1hZfh86m-htgk-  
8e743gdfdhhy:76gdhdghdh5gsgsg8taccounts.mail.com  
/767676785497270* 0_ utma 65767. 56195. 98716.09134684.  
5accounts.mail.  
com/64776760*0_utmb686775.5.7.21.34446.accounts.google.com/785  
098767467*_utmz34267748.6.7.utmcsr=(direct)|utmccn=(direct)|utmc  
md=(none)accounts. mail /254536745785854*
```

Attacker will use decoding techniques to decode the cookies to extract useful information, for performing malicious activities or gaining username and password values.

- **Brute Force Attack:**

Here, attacker uses hit and trial methods to get the password or username values by applying all combinations, or types of values and checks the response of web page error message, if appears & time taken to generate a response from server. Attacker continuously observes the behavior of web page to find the trick of bypassing, (ex: if attacker needs to get access of administrator account, he tries values like-Admin, webmaster, administrator, root, webroot , webpass etc.)

- **Remote File Inclusion(Malicious File Execution):**

Code is designed by attacker, which executes at server side. Here, attacker uses System or shell commands within a code to confuse server for execution. **Example-** shell.txt , ls, las.

- **Local File Inclusion(or Insecure Indirect Direct Object Reference):**

This attack occurs due to bad programming or coding style. When designer does not uses authorization or validation structure and guidelines.

Example: <http://www.college.com/display.jsp?username=7> (Original Query)

http://www.college.com/display.jsp?username=7../../../../data_file (changed)

Due to bad coding attacker can jump to any directory location. (../ is used to jump at different directory location).

- **HTTP response splitting:**

Here, Attacker misguides web server by generating fake Http responses and pretends that web browser contains two different http responses. As described in previous example, HTTP header. Here, Attacker uses trick.

Content-length: 0

Content-length: 30 [with malicious code within]

When Server finds content-length=0 of 1st HTTP Header, it diverts to another header, which divert towards malicious HTTP Header and generates result.

- **DOS attack(Denial-Of-Service attack):**

Here, attacker generates multiple requests towards Server, as a result, server gets overloaded and starts performing undefined things which provides advantage to attacker to bypass its application.

- **Browser Exploitation or cross-site request forgery(CSRF):**

Unauthorized or malicious script could redirect client browser to an attacker's site, from where attacker gets control of client browser for illegitimate purposes.

www.college.com



Username

Password

[www.abc.com](#)

Fig.6.13 Attackers script page

Here original page contains a link, www.abc.com (Attacker's link) when user finds it, he clicks and link is diverted towards attacker's page, where he could exploit input entries.

- **Phishing attack:**

Creating same or similar websites for misguiding user,

www.college.com (Original)

www.collage.com (Phishing attack)

Generally user use search engine to find his web-site and search engine shows all links, if by mistaken user uses www.collage.com, the link is diverted to Attacker's page, which contains same environment of input fields & designing, nobody could predict the fakeness of page, in a single view, User finds the site and start entering his secure login and password information, which in the background is stored by attacker for malicious use. Various Fake web sites are available on internet. *"Use URL to type your website and check its spelling and characters to secure your access"*

- **Buffer Overflow and Underflow:**

Overflow: Attacker's program overrides memory locations or overflows or underflows program logical codes & its size, to generate the overloaded or corrupted memory address, due to which segmentation fault is generated to cause DOS attack.

Underflow: Null values are provided from the input data fields to cause producer-consumer pattern problem and to misbehave by server.

- **SQL-Injection:**

User Inserts vulnerable string from the username and password field, which contains suspicious logic field, which is then executed at the server application server.

- **SYN Flood:**

Attacker sends multiple connection requests to the server, which fills buffer of TCP connection. As server could not bound user or restrict for request, internet is a collection of infinite system users & attackers, generate multi connection request and thus makes server to work abnormally and busy in responding generated requests. Then, attacker bypasses his logic, when server seems busy and forgets to execute attack detection process.

- **Ping of Death:**

More than 65,507 octets of data is send to the machine by Ping Packet (Echo request), which crashes computer Server. Here, attacker uses new trick, he overloaded server by multiple messages or request to fill his buffer size, as a result important process could not gets proper route to enter in server area, due to which server starts malfunctioning.

- **Trojan horse:**

Dangerous and suspicious code is hidden inside a valid request and becomes active after it has been accepted inside the system. Here, attacker sends malicious code inside a packet, which confuses user like `admission.zip`, `job.exe`, as these names appear authentic, when user clicks, internally hidden malicious code starts his function. Here user hides extension from the names, so as to create confidential message.

Example: - Email contains `.exe` file and `.zar` file etc

Attacker converts `-hack.exe`, `data.doc`, `a.mpeg` like files into `data.jar` file, when user find it, he will click on the jar file and the hidden hack code start installing on user's system, and user's system get controlled by attacker logics.

- **DNS Poisoning:** Attacker generates fake DNS (URL or IP Address) to misguide user.
- **ARP poisoning /IP Poisoning:** Attacker generates fake ARP (Address Resolution Protocol) to generate fake IP (Internet Protocol) address. Here, attacker works by generating fake IP, to divert packet to fraudulent recipient
- **Replay attacks:** Attacker creates Delay or generate fake packet to divert user to other malicious sites. Here, attacker generates delay between the connection, in the way of packet route, alters his destination or source and diverts connection towards attacker intended route.

(3) Attack surface parameters representation for analysis

- Degree of Distribution: It describes, different parameters values could suffer from different ways of vulnerability.
- Page Creation Method: Designed code has two types Static and Dynamic, The dynamic code is most susceptible to attack.
- Security Mechanisms: The security validation should be provided at each level of layer to protect from vulnerability
- Input Vectors: The attack occurrence depends upon the counting of input, more input points, more attacking paths.
- Active Content: The supporting applications available at client side to run server application, generates maximum risk of attacks and vulnerabilities.
- Cookies: Cookies contains user authentication and session management information at client side, generates maximum threat of confidentiality and authentication stealing.
- Access Control: The number of access and privileges generates multi point of attack occurrence.

(1) Security tips for designing systems and software's.

- Follow the software development life cycle (SDLC) and phases of engineering to develop a structured secure code.
- Use updated & secured libraries, header, file system, packages and namespaces for algorithm designing to protect against security threats.
- Use latest application and web scanners to test code against vulnerability and designing flaws.
- Always keep updated list of white-list (Secure data lists) and black-list (Unsecure data lists) input parameter for providing training to system.
- Proper interfaces, design, return values of function and calling mechanism should be validated to check errors and exceptions.
- Cookie information should be properly managed, so as to avoid cookie theft attack.
- Never trust on user Input, Use parameterized statement and highly updated algorithms and encryption techniques to design data access functions (Ex- Use RSA 512 keys), Use bind variables for querying sql statement.
- Use and provide limited permission to access database, always use execute only permission.
- Avoid or ban the use of function, tools, software's, designs algorithms, files, which are already been hacked or seems susceptible to attack. Because attacker already knows their loopholes for targeting or launching attack.
- Use latest tested compiler, interpreter and latest tools as they protects against attack. It is very difficult to attacker also, for understanding signatures & patterns of latest security techniques.
- Use version/configuration control to track changes, which occurred in code or the document .It will provide compatibility wizards for moving across the version.
- Use strong cryptographic techniques for encrypting all confidential data.
- Encrypt and encode HTML and scripting languages to protect web browser from XSS attack.
- Study security related magazine, research papers, surf standard and authenticated websites for updated knowledge of secure design.
- Training, workshop and modern development programs should be provided to programmers, coders and designers to guide or educate them by new attacking patterns and techniques for keeping them active.
- Use updated scanners, antivirus for scanning them at regular interval to provide signature authentication about new attacks.
- If DOS window appears in your system, scan all system file extension and window folders. If unwanted or known thing appeared, check and analyze its cause and signature.
- In Email application, never click on unknown mail, always analyze for executable file, they may contain Trojan and virus programs.
- Never feel free when using network, always check about unrecognized activity that happened at system.

SQL Injection attack

Introduction of SQL-Injection:

Web application suffers from different types of attack disease, discussed in previous chapter. Here in this chapter SQL-Injection attack has been discussed, it is the most powerful attack, it occurs due to improper designing, bad coding, bad database designing framework, or by improper flow of information.

Attacker should have strong knowledge about database designing and fingerprinting for firing SQL-Injection attack, as coder generates design, if any loophole exist, attacker enters through it using hit and trial, analysis of web application results, or by error message generated by application.

Here, attacker uses different combinations in URL field or in login field to change the logic of request for generating backend dynamically SQL-Query.

Various input filtration techniques are used by web application to get authorized input combination and filter vulnerable characters or symbols. The rest of chapter is going to describe sql attack types, web scanning techniques to find vulnerable points for attacks.

Structure and Design of SQL-Injection Attack

(1) SQL Injection attack:

Web application is free for user to provide input or feed data to web pages.

Attacker may use malicious or unwanted input to change logic of application by means of input section, needed for processing.

SQL-Injection or SQL-Poisoning is such an attack, which changes the logic's of databases by inserting malicious statement or string. It only occurs due to the lack of input validation, proper coding or designing practices.

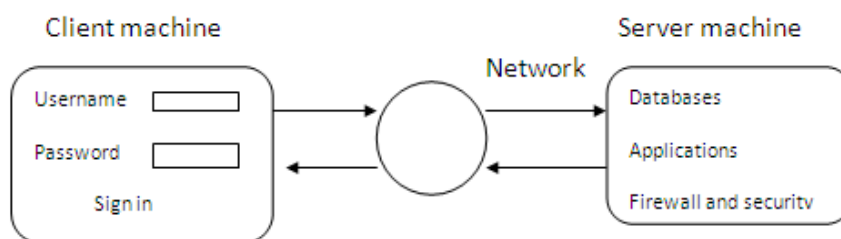


Fig.6.14: Client-Server Design

Original, username=' abc '

Password='123'

The query required for accessing data from the database looks like:

SQL-query- : Select * from student where username= "abc" && password= "123";

But hacker uses some tricks to validate the query and to return as a true statement to fulfill basic conditions to gain access from database.

Hack-sql-query: select * from student where username= ""OR 1=1; -- && password = " ';

Here, attacker used statement "OR 1=1; --", which bypasses towards login page. Attackers query contains closing of double quotes(") OR 1=1 ;-- , which is a tautology, & always returns true and ends with ; (semicolon) and -- (double dashes) & are used for comment variable in sql-query databases and thus misguides database server to provide access and display the fields of tables.

(2) SQL-Injection attack Techniques , basic requirement:

- Strong knowledge of SQL query statement structure (Like SELECT , INSERT, UPDATE, DROP, ALTER and other system execution commands and queries)
- Knowledge of Comment use in databases (Like --(use in Sql server) , # (use in other databases) . every databases has its own comment type declaration.
- Knowledge of database connectivity procedure and coding structure and their fingerprints (Like which database supports Error messages, access mechanism and security algorithms).

- It is the attack, which doesn't need any tool but only requires web application and database fingerprinting strong knowledge.
- Knowledge provided by databases (Input filtering , Validation , type of statements supported by database etc)

(3) Types of SQL-Injection attack:

- **Tautology:**

This attack is used to inject one or more conditional statement, so that they always evaluate to true.

Example: select password from student where username = ""OR 1=1; -

The conditional injected code ("OR 1=1; - -) transform the entire WHERE clause into a tautology and always bypasses authentication.

- **Union Query:**

Here, attacker joins injected query to the safe query by the word union to get the data from the tables present in a application fraudly.

Ex 1: select password from student where username=" "UNION select sub_id from branch where subject="pqr "; - -

The first query will return null set, where as second query will return data from table branch.

- **Illegal /logically incorrect queries:**

When a wrong query is used, an error message is generated from the database application, which contains useful debugging and data type information

The error message generated helps attacker to find vulnerable points and parameters in the application. Attacker intentionally injects SQL tokens of false type, logical errors, type mismatches to make a system, to generate error messages.

Example: Original URL

http://www.student.com/display.jsp?username=abc

Suspicious SQL Injection:

http://www.student.com/display.jsp? Username='abc'

- **Piggy-backed queries(Command Injection or Statement Injection):**

Here, attacker injects malicious query using delimiter to make a server for executing multiple distinct queries.

Example: select * from student where password=" 123 "; Drop table branch;

Database accepts both query and executes them, the second query is illegitimate and can drop branch table from the database.

- **Inference:**

Here, intruder changes the functioning or behaviors of a database application. There are two types of attacking techniques based on inference attack are shown below.

- **Blind Injection:**

If the application developer hides the errors details , which helps the attacker to compromise database.

Here, still in such situation attacker uses trick to find vulnerable points by asking series of True/False question through SQL-Injection statement.

Example: select * from student where password= "123" && 1=0; - -

Select * from student where password=" 123 "&& 1=1; - -

If the application contains input validation mechanism both query result in unsuccessful statement. But if there are input validation ,attacker checks error message , as 1=0 and then the attacker fires seconds statement ,which results true and checks vulnerable point.

- **Timing attack:**

Here, attacker uses timing game to observe, time delays in the database responses, It uses IF-Then statement to behave SQL-Injection to execute a long running query or a time delay statement depending on the logic injected WAITFOR is a keyword use, which causes the database to delay its responses by a specified time.

Example:

Query= declare @ k varchar (7000) select @ k=db_name() if (ascii(substring(@k,1,1)) & power(3,0))>0 WAITFOR delay '0:0:9'

Database will pause for 9 seconds, if the first bit of the first byte of name, of Current database is 1. Then the code is executed to generate a delay in response time, when the condition is true. Here, attacker uses series of operations.

- **Alternate Encoding:**

Here, attacker modifies the SQL query by using alternate encoding such as, hexadecimal, ASCII and Unicode.

Select * from student where password="123 "; exec (char (0X 736875746f776e));

The exec (char (0X 736875746f776e)) coding refers To SHUTDOWN when executed by server will result in server shutdown.

- **Stored Procedure:**

It injects attackers query in stored procedures too.

Example: create procedure DBO.isauthenticated@ Username varchar 2,@ password varchar 2, AS exec ("select * from where username=' " + @ username + " ' and password=' "+@password+" '); GO

Example: select * from student where username = ' abc 'and password = ' '; Shutdown;

It uses stored procedures to fire system commands.

- **LIKE queries:**

Like keyword or percent sign cited in an error message are indication of this situation, LIKE clauses are used in sql query statement for generating result.

Example:

Select password from student where username LIKE '% "& StrUsername & "';

- **%(Percent sign) are wild card,** In This case the where clause will return true in any case, The wild card " %" makes query to be return true and display all records.

(4) Secure framework for designing database query:

- **Never allow multiple query statement.**

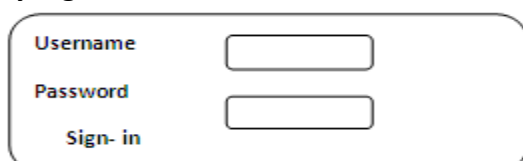
Example: select * from student; shutdown (multiple query statement).

- **Use input filtering to eliminate vulnerability like.**

- Union, %, %5C, tautology (1=0, 1=1), ""(blank double quotes).
- Special character which appears simultaneously (; - - , ' , ").
- Filter encoding schemes like hexadecimal, Unicode (char (0X73689e)) and filter, system commands and special characters like shutdown, wait for, append, and delay, #, @ respectively.

(5) Attacking modes of SQL-Injection.

- **By login:**



The image shows a login form with a rounded rectangular border. Inside, there are two input fields. The first field is labeled 'Username' in blue text and has a white rectangular box next to it. The second field is labeled 'Password' in blue text and also has a white rectangular box next to it. Below these two fields, there is a 'Sign-in' button in blue text.

Fig. 6.15: Login Page

It is the point from where the user deals with web application and communicates from the database applications.

Here, working of input & query generation process is shown below, which works when user enters input and, gets output from server.

User types values in username and password field.

Username = "OR 1=1; - - && Password = 123

The request generated by URL, when user press Sign-in button .Request is taken by server for checking authenticity of client request, here three cases arises.

- If request ID is true (Valid response is generated).
- If request is false (nothing is generated that is server rejects the request).
- Request is false but still positive response is generated, because the SQL-query contains logic, which interprets the result true and provides response from the server by trapping and confusing server to bypass application.
- Response is generated by server that is link of next page (If condition satisfies)

- **By URL:**

URL encoding, percent encoding, UTF encoding, Escape encoding and web encoding are used interchangeably.

Web application usually transfers data between the client and server using the HTTPS and HTTP protocols.

The user input is provided to the server either in the form of HTTP headers (submitted by the cookies field or the post data field) or included in the query portion of the requested URL.

If the data is transferred by a URL, it has to be encoded to follow the authorized syntax rules and structure of URL's.

Example: `http://www.student.com/display.jsp%25id`

It uses escaping characters like % to change the logic of URL (we request).

(6) SQL Injection attacking reasons:

SQL queries always embeds in language code for providing the functioning like display , add , delete or modify data in the database application.

All programming languages(C# dotnet, PHP, JAVA etc) are affected by SQL-Injection attacks, which are connected by databases.

Example: `<form method="post" action="Display.jsp">`

`<input type="text" name="username">`

`<input type="pwd" name="password">`

`</form>`

Here in the example above, if input validation is not used, attacker could easily insert malicious code (Cross site Scripting code) in username and password field, and then resulting query appears as:

Select * from student where username=abc && password= "OR 1=1;

- **Due to insecure direct object reference:**

It occurs when designer or coder does not use secure authorization techniques and exposes a referential link to an internal implementation object such as URL file directory , FORM parameter or database records.

Ex: `http://www.student.com/display.jsp?username=abc` (Original)

The attacker could use directory traversal technique to switch to other location or

Directory (occurs due to poor programming).

Attacker uses `.../.. /` To switch to another location for accessing resource, kept secure at server end.

Example: `http://www.student.com/display.jsp?username=abc. ./ . ./ . ./` (User's trick)

- **Improper error handling and information leakage from database server.**

If the technique of proper error or exception handling is not used they could create fatal attacking problems, Error message will dispose to user's screen, and attacker will use them to get system information shown through error messages.

Example: Error message type or structure.

My-Sql OLE DB Provider error '70040e08'

The multiply or subtraction operation cannot take a varchar data type as an argument.

This error message indicates that data type of username is 'varchar'. The attacker can repeat same process to determine the data type of other columns. Once he knows the data type of all columns & could create different query structures.

Error message revealed by server could lead to system crash, terminate abnormally or restart the program and the fatal result would be of DOS attack (Denial of Service).

- C/C++, ASP and PHP returns Function error values.
- C#, VB .net and Java throw Exception.

- **Insecure storage and improper use of cryptography.**

Use of short keys(DES uses 56-bit key), weak algorithm (MD4 and RC4) and non standard algorithms , weak cryptography , weak random number in a pseudo random number generator(PRNG) , improper key management(Ex: key stored at an insecure location) and hard coding of keys could cause a security breach of sensitive information.

(7) Protection and preventive measures from SQL-Injection Attack:

SQL Injection attack could be eliminated by applying simple programming changes. A single unprotected SQL statement can result in compromising of the application, data or database servers.

- **Use of bind variable:**

Example: select * from student from username=? And password=?

- **Input validation:**

Apply input filtering and validation techniques to protect applications, and securing the servers to bypass unauthorized and tricky queries.

- **Function Security:**

Database contains various functions and all have accesses to PUBLIC .they should be protected by attacker's to perform any malicious activities in a database.

- **Error message:**

Design and test the application, so that they could not generate any error message or exception to user's screen. Protecting from public disposal of database fingerprints.

(8) Injection attack classifications:

- Script Injection: Code is inserted into scripting languages (HTML , JavaScript , VBscript etc)
- Xpath Injection: XML (Extensible markup language) document is executed by Xquery. Here XML code is replaced by a series of Boolean queries and logic to change the clause and reverse its statement meaning.
- Cross site history manipulation (XSHM) Injection: Here, history stored on client computer is modified to cause injection attacks.
- Argument Injection: Here, pseudo code or argument in programming source code is used to change the logic or semantic of code designs.
- Server side Includes (SSI) Injection: Web application contains directives feeded in HTML page with dynamic contents.SSI are used to execute some actions before the current page is loaded, they are similar to CGI.
- Resource Injection: It is use, to change the identity used by an application to perform malicious operations and task in a web application like PORT NAME traversal, FILKE NAME traversal and IP ADDRESS Traversal.
- LDAP Injection or Shell Injection: It is used to exploit or execute arbitrary commands to grant permission in databases or application servers by unauthorized queries and system commands.

- Command injection: Here malicious code or malicious commands are embedded into input scripting and code and is passed to language interpreter, the interpreter then execute it as a sense of commands and results in a malicious or unauthorized activity.
- Email- header Injection: Attacker hijacks email sending web forms and uses them by altering its contents with malicious code to send spam hidden on email packets.
- I frame injection: Attacker hides attacking code or scripts in a picture or frame to bypass its design and structure and misguides server or execution engines.

(9) SQL-Injection scanning applications.

- Why web scanning tools are needed.
It is needed to check or find if any vulnerability present in a application, It also checks the strength of software to protect against malicious activities, various tools and software's are available for web application.
- What these tools contains to protect web application.
They contains secure algorithm, secure guidelines ,updating and protecting mechanism, blacklist(Attack signature), validation features and highly trained algorithms created using machine learning approaches. But still they can't protect present or existing systems, completely from varieties of attacks, as attack have infinite varieties and signatures and daily inventions of these attacks and malicious programs are in progress, so securing tools need to be updated with high-tech algorithms and designs at regular interval of time.
- **Static code checkers(It deals with malicious Programs)**
 - It is used to scan C source code for security vulnerabilities and programming design flaws.
 - Performs security checks in source code and generates possible security weaknesses in code.
 - Scans PHP, C/C++, Python & Perl languages source code files for security weaknesses and flaw present in programming.
 - Use to check Java code for finding errors that are even not detected at runtime.
 - Use to scan software defects like uninitialized variables, NULL pointer reference, Out of bound array indexing etc.
- **Runtime code checker(Deal with program code)**
 - It protects from stack smashing attacks.
 - It protects from buffer overflow coding flaws.
 - It detects memory leaks and problems present in software.
- **Profiling tools (Deals with Operating System)**
 - It screens and prevent malicious event by system users.
 - It profiles and debugs Linux executables.
 - It protects system calling from unauthorized access.
- **Penetration testing tools(Deals with complete networks)**
 - Network port scanner for finding the open port.
 - It finds Vulnerability present in a network.
 - It scans host for vulnerability and protects from unwanted activities.
- **Application scanning tools(Deals with databases)**
 - Checks malicious inputs injected by attacker in a web application.
 - Checks for CGI(Common gateway Interface) flaws.
 - Scans database server applications(My-sql)
 - Checks injection flaws in URL.
 - Performs logic for SQL Operations to detect and exploit SQL Injection Vulnerability.
 - It is a tool for brute forcing data out of databases.
- **Patterns based system techniques**
 - They are used to detect SQL-Injection script injection attack, here, strong algorithm and engines to analyze the input text for the possibility of attacks are used ,after detecting attack, they

generates log for future research based on log information's and blocks them. Here, the levels of security are provided for the analysis of attacking patterns. If any attack is found by the application, it safely handles them without informing user. Thus provides good sense of security frameworks

- In this category, the system monitors attacker's behavior, who hits a page several times for protecting against brute force attack. If any malicious activity is found, the system blocks the page, and diverts the link of attacker to other page (page could be used by security validator).dummy page.

Unit 7

Web Issue: Introduction

Web security problem

As many benefits that there are in doing business online across the borders of the world without too many restrictions, there are as many disadvantages, particularly where security is concerned. Below is an overview of what kinds of website security problems companies face when conducting business online.

Website Security

The internet has revolutionised how many business industries operate and generate revenue. The concept of online business has allowed for many doors to be opened and barriers broken. Anyone from anywhere is able to receive access at any time. This is one factor that makes the internet so incredibly appealing to many businesses the world over. Less restriction can often mean the generation of more profit.

Since the internet operates over structured networks which are programmed, security problems are unavoidable. Loop holes, hacking and viruses are common areas where vulnerabilities will be taken advantage of with disruptive and disastrous results. Website security, otherwise referred to as web application security or webappsec, is imperative for all online business or website owners and requires constant attention and updates. There are always new ways for "internet criminals" or hackers to "beat the system" and cause disruptions, especially where a website offers its internet users interactive convenience facilities.

Website Security Risks

A webmaster is mostly affected by common issues and problems that internet criminals target. From the very minute that a web server is installed, a "window" (of opportunity) into a local network is opened. Anyone, anywhere with online access has the ability to "peer through" this window. Whilst most internet users are content with what they're presented with and aren't likely to "nose around" and peek at things that were never really intended for public consumption, many other individuals are "free" to figure out ways to snoop. This sort of behaviour can be likened to not being able to "look without touching". These individuals will attempt to force their way inside this opened window and cause programming or structural damage by, for instance inserting a "bug".

Surfing the web may, to the general, innocent internet user, be viewed as a safe and anonymous environment. The simple truth is that the internet isn't quite all that safe and anonymous at all. In a sense the internet "has eyes" everywhere. Web browsers can be easily exposed to viruses and malicious software, causing a user's personal system to experience malfunctions and problems. Web browsers also leave an electronic "footprint" whenever websites are visited. This footprint leaves a record of the user's web surfing history, which creates an opportunity for internet criminals to create a profile of individuals' tastes and habits, and potentially cause disruptions and problems. Personal detail confidentiality is one area where hackers can breach security vulnerabilities and allow data to be transmitted across the World Wide Web.

Types of security risks whereby network eavesdropping can occur include:

- Bugs or mis-configuration problems in a web server - this allows confidential documents to be "stolen", commands on the server host machine to be modified and web server host machine vulnerabilities able to be "broken into" etc.
- Browser - side risks - this allows active for content to crash the browser, damage an internet user's system and breach a user's privacy.
- Interception of network data (sent and received) - this allows hackers the ability to operate from any point on the pathway between a web browser and server causing disruptions.

Common Website Security Problems

Website security problems can be divided into two categories:

1. System Security - this ensures that a general internet user cannot change a website, altering content on web pages.
2. Information Security - this ensures that the personal or private details of an internet user are secure and safe from prying eyes.

Guessing - simple passwords such as a mother's maiden name, a pet's name that can be easily guessed Brute force search which allows as many guesses as desired to be entered Social engineering - tricking people into revealing password information Obtaining stored passwords - passwords can be retrieved whereby people have stored them on computer systems etc.

Obtaining shared passwords - the same passwords may be used for more than one system Installing Trojans - "Trojan horse" software programmes may install invisibly on a computer and monitor key strokes made by a user.

Interception - passwords are sent across an unencrypted connection, which can then be intercepted and transmitted.

1. Human Error

Human beings are not by nature, perfect. Mistakes are, one could say, inherently a part of our "general make up". Consequently, most security problems on the internet come down to human error. Human beings programme and run websites. Where mistakes are made, vulnerabilities are created. Website developers need to properly plan and proof test scripts that are coded into website programmes and applications often as hackers and other internet criminals will find ways to extract confidential information and do with it as they please. Particular errors will be exploited where the opportunity presents itself.

2. Privacy Neglect

More often than not, the general internet user will become too comfortable with the notion that internet surfing is "safe" and "anonymous" and openly part with personal details all too easily. Parting with this type of information could seemingly be as innocent as giving away a personal email address on a public forum and others of a more confidential nature such as credit card details. Hackers and internet criminals make use of "crawler bots" (small programmes coded to collect email addresses) who's function it is to locate addresses and add them to mass emailing

lists, for the sole purpose of distributing SPAM to internet users. This isn't necessarily a serious security breach for websites, but when used in the same way to accumulate user names and passwords on sites, damage can be done.

3. Hacking

Hacker's generally have little information or none at all at their disposal about their specific targets and establish a breakthrough almost entirely based on his or her own knowledge. The general internet user is usually not the main target. Internet or website servers of large corporations and organisations generally suffer with regular security breaches and should constantly be updated with newer security software versions.

4. Password Problems

Passwords can be intercepted in the following ways by internet criminals and hackers:

5. Software Flaws

Software that makes up a system can also provide problems whereby a flaw or loop hole becomes apparent. Bugs and security holes allow access even without a password. Flaws provide an opportunity for hackers to access a system and files even if a password isn't requested. Firewalls can be used to prevent server access and help to reduce security breaches. If breaches occur, web pages can be modified or information wiped out completely. Software that is used must always be kept current.

6. Encryption Problems

Website developers make use of encryption to help keep information secure in transit. A "public key" scheme is the usual method this is done and allows a message to be transferred securely between parties who are unknown to one another. This message, even if intercepted by an internet criminal, cannot be easily decrypted. Problems occur whereby this system isn't secure enough and messages can be decrypted (messages may be secure in transit, but not if the web server is hacked).

Penetration Testing

What is Penetration Testing?

A Penetration Test, also known as a Pen Test is a legal attempt at gaining access to your protected computer systems or networks, often conducted by a third party organisation. The purpose of the test is to identify security vulnerabilities and then attempt to successfully exploit them in order to gain some form of access to the network or computer system.

Should a successful compromise take place, the flaw/vulnerability is classified into a threat level for the organisation; typically low, medium or high. Most penetration tests are concluded with a detailed report on the security findings along with remedies for the threats.

What are the most common types of Penetration Tests?

Two of the more common types of penetration tests are black box and white box penetration testing. In a black box test, no prior knowledge of the corporate system is given to the third party tester. This is often the most preferred test as it is an accurate simulation of how an outsider/hacker would see the network and attempt to break into it. A white box test on the other hand is when the third party organisation is given full IP information, network diagrams and source code files to the software, networks and systems, in a bid to find weaknesses from any of the available information.

What is Black Box Penetration Testing

Black box testing is where the penetration tester is given very minimal information about the target systems. This is to mimic the level of information a typical attacker might have and can provide an accurate picture of the security of the client's systems from the perspective of a would-be attacker. Whilst this information is useful, it may not provide a complete picture of the security of the target systems. There may be more security vulnerabilities in the target systems which could have been uncovered if the attacker had been given more information at the outset of the test.

What is White Box Penetration Testing

A penetration test is called white box testing if the consultant is given information about the target systems prior to and during the engagement. With this knowledge the consultant is often able to uncover more vulnerabilities than with the black box testing approach and therefore the systems may be considered more secure if the white box testing approach is used.

What is Network Penetration Testing

There are various different types of networks that can expose security vulnerabilities to attackers including external networks (Internet-facing), internal networks, DMZ networks, private networks, VPN's and wireless networks. Standard network penetration testing assesses these networks for common security vulnerabilities including weak encryption ciphers, weak encryption protocols, default login accounts or weak passwords, buffer overflows and format string attacks, vulnerable web server software, insecure database services, weak remote administration services, unencrypted network services, vulnerable network services and potential Denial of Service attacks

What is Web Application Penetration Testing

Web application penetration testing is the process of assessing the pages and parameters of websites and web applications to test for issues which could be leveraged by an attacker to compromise the confidentiality, integrity or availability of the website. Common web application security flaws include SQL injection, Cross-Site Scripting, broken authentication and session management, insecure encryption implementation and potentially dangerous redirects and forwards amongst others. Testing often involves proxying the HTTP requests to the website and modifying the data to attempt to discover security issues.

What are the advantages of a Penetration Test?

Having a penetration test conducted can be extremely useful to people who wish to get extra reassurance when it comes to critical web facing systems, however they can also be useful in a variety of other ways, such as:

Testing a System Administrator to see if he is keeping systems updated and secured.
Compliance & the Payment Card Industry (PCI), when operating an online payments system.
Risk reduction and risk mitigation factors for insurance or other industries.
Protection of Confidentiality, Integrity and Availability (CIA triad) of data.

Are there alternatives to Penetration Testing?

Yes, there are network scanners available, however if you don't know enough about the security results displayed in a scanner or how to confirm the results are not false positives, it is highly advised you seek out professional help, rather than taking a chance and putting your business at risk.

Penetration Testing compared to Vulnerability Scanning

The advantage of a penetration test compared with an automated vulnerability scan is the involvement of the human element versus automated systems. A human can do several attacks based on skills, creativity. and information about the target system that an automated scanning can not do.

Several techniques like social engineering can usually be done by humans alone since it requires physical techniques that have to be performed by a human and is not covered by an automated system.

The Penetration Test Process

- a) **Discovery:** The SecPoint Penetrator performs information discovery via a wide range of techniques—that is, whois databases, scan utilities, Google data, and more—in order to gain as much information about the target system as possible. These discoveries often reveal sensitive information that can be used to perform specific attacks on a given machine.
- b) **Enumeration:** Once the specific networks and systems are identified through discovery, it is important to gain as much information possible about each system. The difference between enumeration and discovery depends on the state of intrusion. Enumeration is all about actively trying to obtain usernames as well as software and hardware device version information.

- c) **Vulnerability Identification:** The vulnerability identification step is a very important phase in penetration testing. This allows the user to determine the weaknesses of the target system and where to launch the attacks.
- d) **Exploitation and Launching of Attacks:** After the vulnerabilities are identified on the target system, it is then possible to launch the right exploits. The goal of launching exploits is to gain full access of the target system.
- e) **Denial of Service:** A DOS (Denial of Service) test can be performed to test the stability of production systems in order to show if they can be crashed or not. When performing a penetration test of a preproduction system, it is important to test its stability and how easily can it be crashed. By doing this, its stability will be ensured once it is deployed into a real environment. It is important to perform DOS testing to ensure the safeness of certain systems. If an attacker takes down your system during busy or peak hours, both you and your customer can incur a significant financial loss.
- f) **Reporting:** After the completion of the penetration test, it is important to get user-customized reporting suites for a technical and/or management overview. This includes the executive summary, detailed recommendations to solve the identified vulnerabilities, and official security ID numbers for the vulnerabilities. The reports come in different formats such as html, pdf, and xml. Furthermore, all the reports are open to be modified as of the user's choice.

Content Filter

What is a Content Filter?

A Content Filter helps decide which content is acceptable for viewing and access through a given system. Software that controls content, which is also known as web-filtering programs or censorware, is a term used for applications created and developed for managing what information or media is allowed to be seen by the end user (specifically content from the Internet).

Why is a Content Filter needed?

It is important to control the content on your network and know how your resources are being used. Often, employees will tend to do private or illegal things in the work hours, due to boredom or other reasons. This will waste valuable work hours and can possibly put you at risk if your network is being abused for downloading copyrighted materials.

What does the Content Filter consist off?

Included modules in the SecPoint Content Filter are:

- **Anti-Free Mail:** This blocks access to official free email providers such as Hotmail, Yahoo Mail, Google's Gmail, and so on. The use of free email providers can often indicate employees checking their private email during working hours
- **Anti-Game:** It is often a tempting to play network games such as Counterstrike or other addictive games during work hours.

- **Instant Message Recording:** This provides monitoring of the usage of MSN Instant Messaging to see if your employees are communicating with your business customers or with their friends.
- **Anti-Instant Message:** If your security policy disallows all sorts of instant messengers, then this module can be used to block programs such as MSN Instant Messenger, Yahoo Messenger, Google Chat, Skype Chat, and so forth.
- **Anti-VoIP:** This allows the blocking of services like Skype, Yahoo Talk, Google Talk, VoIP usage, and lots more. Employees can be talking to non-work-related contacts during work hours or even leak sensitive information without your knowledge.
- **Anti-P2P:** If your security policy requires you to block all P2P file sharing services like BitTorrent, eDonkey2000, Emule, Kazaa, and Napster, then you should enable this module. Those programs are often used to share copyrighted materials such as music or movies. If this is done in your corporate perimeter, you will become responsible for this dilemma once a raid is started. In some countries, ISPs will outright close down the Internet connection of a guilty business, so such a case can become a very costly affair.
- **File Filter:** This option blocks downloading of specific file formats such as *.exe, *.zip, or *.rar files depending on the supervisor's choice. This applies to emails, web browsing, and other protocols.
- **Protocol Filter:** This allows blocking of specific protocols in your network. In some locations, POP3 traffic is forbidden since this is often used by employees to check their private email in working hours. You can customize which protocols to block as well.
- **Block Websites:** This allows blocking of websites of your choice. Often, employees will spend hours daily to read news sites, gossips, and websites of personal interest during working hours.

Firewalls

A firewall is a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to.

Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain name and Internet Protocol addresses. For mobile users, firewalls allow remote access in to the private network by the use of secure logon procedures and authentication certificates.

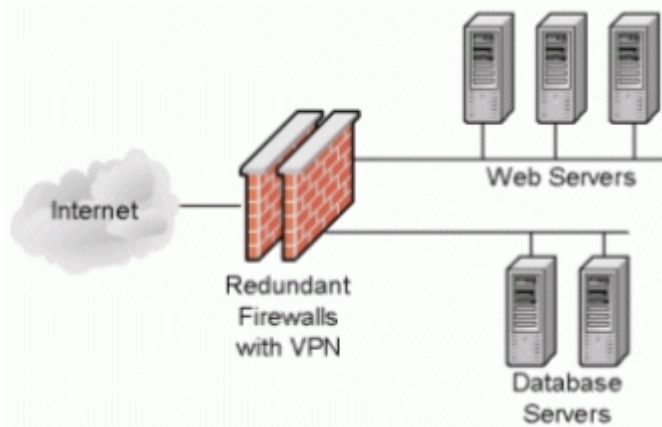


Fig 7.1

Firewalls

A firewall is a hardware and/or software which functions in a networked environment to block unauthorized access while permitting authorized communications. Firewall is a device and/or a software that stands between a local network and the Internet, and filters traffic that might be harmful. Firewalls can be either stand-alone systems or included in other devices such as routers or servers.

Hardware firewalls are separate devices which function as dedicated firewalls (They also contain software but normally stored in ROM to prevent tampering). Cisco and Checkpoint are the two leading companies which make hardware firewalls.

Software firewalls can be installed on servers or workstations and they help to prevent unwanted inbound and outbound traffic. Microsoft ISA Server, Zone Alarm, Comodo etc are some leading software based firewalls. Linux Operating System include an Open Source firewall called iptables.

This article examines the different types of Firewall technologies. The four common types of firewalls are:

1. Packet Filtering Firewalls.
2. Circuit level gateway Firewalls.
3. Application level gateway Firewalls.
4. Stateful multi-layer inspection Firewalls.

1. Packet Filtering Firewalls:

Packet Filtering mechanisms work in the network layer of the OSI model. In packet filtering, each packet passing through a firewall is compared to a set of rules before it is allowed to pass through. Depending on the packet and the rule, the packet can be either dropped, sent through or a message can be forwarded to the originator. The rules which determine which packets to be sent, and which not to be sent can be based on the source and destination IP address, source and destination port number or the protocol used. Packet filtering can also be done at the router level, providing an additional layer of security. For example, if a certain destination IP address is found in a packet, it could be dropped or if the packet conforms to a certain protocol (eg. http), it could be dropped for companies which do not allow internet access to their employees.

2. Circuit level gateway Firewalls:

The circuit level gateway firewalls work at the session layer of the OSI model. They monitor TCP handshaking between the packets to determine if a requested session is legitimate. And the information passed through a circuit level gateway, to the internet, appears to have come from the circuit level gateway. So, there is no way for a remote computer or a host to determine the internal private ip addresses of an organization, for example. This technique is also called Network Address Translation where the private IP addresses originating from the different clients inside the network are all mapped to the public IP address available through the internet service provider and then sent to the outside world (Internet). This way, the packets are tagged with only the Public IP address (Firewall level) and the internal private IP addresses are not exposed to potential intruders.

3. Application level gateway Firewalls:

Application level firewalls decide whether to drop a packet or send them through based on the application information (available in the packet). They do this by setting up various proxies on a single firewall for different applications. Both the client and the server connect to these proxies instead of connecting directly to each other. So, any suspicious data or connections are dropped by these proxies. And since they are application aware, they can handle more complex protocols like H.323, SIP, SQL Net etc.

Application level firewalls ensure protocol conformance. For example, attacks over http that violates the protocol policies like sending Non-ASCII data in the header fields or overly long string along with Non-ASCII characters in the host field would be dropped because they have been tampered with, by the intruders.

Application level firewalls can look in to individual sessions and decide to drop a packet based on information in the application protocol headers or in the application payload. For example, SMTP application proxies can be configured to allow only certain commands like helo, mail from:, rcpt to: etc. to pass through the firewall and block other commands like expn, vrfy etc. which tries to expand a list or verify if that account exists, and are used by attackers and spammers for their vested self interests.

4. Stateful multilayer inspection firewalls:

Stateful multilayer inspection firewalls combine the aspects of the other three types of firewalls. They filter packets at the network layer, transport layer and the application layer. And allow the packets to pass though if they pass all of them, individually. Some of them allows direct connection between the client and the server, as they rely on algorithms to recognize and process application layer data instead of relying on application specific proxies.

FIREWALL DATA (Additional)

1. Security Threats from connecting to the Internet

Most organisations today have an internal network that interconnects their computer systems. There is usually a high degree of trust between the computer systems in the network, particularly if the network is private. However, many organizations now see the benefits of connecting to the Internet. But, the Internet is inherently an insecure network. Some of the threats inherent in the Internet include:

Weak or No Authentication required. Several services e.g. rlogin, require no password to be given when a user logs in. Other services provide information with no or little authentication e.g. anonymous FTP, and WWW. Other services trust the caller at the other end to provide correct identification information e.g. TCP and UDP trust the IP address of the remote station; whilst other services grant access at too large a granularity e.g. NFS grants access to anyone from a particular remote host. Finally many services require passwords to be transmitted in the clear across the network, which make them vulnerable to capture and replay.

Insecure software. Internet software, particularly shareware, free or low cost packages, often have bugs or design flaws in them usually as a result of poor design or insufficient testing of the software. But due to their ready availability and low cost, many people still take the packages. Examples include: the UNIX sendmail program which has had numerous vulnerabilities reported in it, and a freeware FTP product which contained a Trojan Horse that allowed privilege access to the server. Unscrupulous people are always ready to exploit these weaknesses.

Sniffer programs. In 1994 the CERT reported that thousands of systems on the Internet had been compromised by hackers, and sniffer programs installed on them. Sniffer programs monitor network traffic for usernames and passwords, subsequently making these available to the hacker.

Cracker programs. These programs, widely available on the Internet, run in background mode on a machine, encrypting thousands of different words and comparing these to the encrypted passwords stored on the machine. These so called *dictionary* attacks (because the words are held in a dictionary) are often very successful, providing the hacker with up to a third of the passwords on a machine.

Port Scanners. These programs, again available freely from the Internet, will send messages to all the TCP and UDP ports on a remote computer to see if any of them are open and waiting to receive a call. Once an open port has been located, the hacker will then try to get in to the computer through it.

Ease of Masquerade (Spoofing). The above make it relatively easy for the hacker to exploit the trust inherent in the Internet, or to capture passwords and replay them. Other security weaknesses include: the SMTP protocol uses ASCII messages to transfer messages, so a hacker can TELNET into an SMTP port and simply type in a bogus Email message; a feature called IP source routing allows a caller to falsify its IP address, and to provide the recipient with a return path directly back to itself.

So how can an organization securely connect to the Internet? One solution is to use one or more network firewalls.

2. What is a Firewall ?

A firewall is a secure Internet gateway that is used to interconnect a private network to the Internet (see Figure). There are a number of components that make up a firewall:

i) the Internet access security policy of the organisation. This states, at a high level, what degree of security the organisation expects when connecting to the Internet. The security policy is independent of technology and techniques, and should have a lifetime independent of the equipment used. An example of,

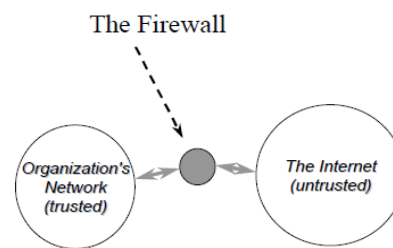


Figure 1

Fig 7.2

Statements from such a security policy might be: external users will not be allowed to access the corporate network without a strong level of authentication; any corporate information not in the public domain must be transferred across the Internet in a confidential manner, and corporate users will only be allowed to send electronic mail to the Internet - all other services will be banned.

ii) the mapping of the security policy onto technical designs and procedures that are to be followed when connecting to the Internet. This information will be updated as new technology is announced, and as system configurations change etc. For example, regarding authentication, the technical design might specify the use of one-time passwords. Technical designs are usually based on one of two security policies, either: permit any service unless it is expressly denied, or deny any service unless it is expressly permitted. The latter is clearly the more secure of the two.

iii) the firewall system, which is the hardware and software which implements the firewall. Typical firewall systems comprise a IP packet filtering router, and a host computer (sometimes called a bastion host or application gateway) running application filtering and authentication software. Each of these firewall components are essential. A firewall system without an Internet access security policy cannot be correctly configured. A policy without enforced procedures is worthless as it is ignored.

3. Advantages of Firewalls

Firewalls have a number of advantages.

They can stop incoming requests to inherently insecure services, e.g. you can disallow rlogin, or RPC services such as NFS. They can control access to other services e.g. bar callers from certain IP addresses, filter the service operations (both incoming and outgoing), e.g. stop FTP writes hide information e.g. by only allowing access to certain directories or systems They are more cost effective than securing each host on the corporate network since there is often only one or a few firewall systems to concentrate on. They are more secure than securing each host due to: the complexity of the software on the host - this makes it easier for security loopholes to appear. In contrast, firewalls usually have simplified operating systems and don't run complex application software, the number of hosts that need to be secured (the security of the whole is only as strong as the weakest link).

4. Disadvantages of Firewalls

Firewalls are not the be all and end all of network security. They do have some disadvantages, such as:

They are a central point for attack, and if an intruder breaks through the firewall they may have unlimited access to the corporate network. They may restrict legitimate users from accessing valuable services, for example, corporate users may not be let out onto the Web, or when working away from home a corporate user may not have full access to the organization's network. They do not protect against back door attacks, and may encourage users to enter and leave via the backdoor, particularly if the service restrictions are severe enough. Examples of backdoor entrance points to the corporate network are:

modems, and importing/exporting floppy discs. The security policy needs to cover these aspects as well. They can be a bottleneck to throughput, since all connections must go via the firewall system. Firewall systems on their own cannot protect the network against smuggling i.e. the importation or exportation of banned material through the firewall e.g. games programs as attachments to Email messages. Smuggling could still be a significant source of virus infection if users download software from external bulletin boards etc. The recent Melissa and Love Bug viruses were smuggled inside Email messages unbeknown to the recipients. This is an area that the security policy needs to address. There are software packages that can help in this e.g. Mimesweeper runs in the firewall and will check Email attachments before letting them pass. It will remove potentially dangerous attachments or stop the Email altogether. The biggest disadvantage of a firewall is that it gives no protection against the inside attacker. Since most corporate computer crime is perpetrated by internal users, a firewall offers little protection against this threat. E.g. an employee may not be able to Email sensitive data from the site, but they may be able to copy it onto a floppy disc and post it. Consequently organizations need to balance the amount of time and money they spend on firewalls with that spent on other aspects of information security.

Firewalls, Layers and Models

ISO 7 Layer Model	Internet 5 Layer Model	Firewalls
Application (7)	Application (5)	Proxy Service
Transport (4)	TCP/UDP (4)	Packet Filtering Router/Packet Screening Router
Network (3)	IP/ICMP (3)	Stateful Inspection
Link (2)	Link (2)	
Physical (1)	System Interface (1)	none

Figure 2

Fig 7.3

5. Models, Layers and Firewalls

ISO uses a 7 layer model for Open Systems Interconnection, whereas the Internet can be regarded as having a 5 layer model. Whereabouts in these models are firewall systems placed?

Firewall systems are usually placed at layers 3, 4 and 5 of the Internet model, (3, 4 and 7 of the ISO model), see Figure 2. Their purpose is to control access to and from a protected network. Note that a firewall can be placed between any two networks, for example between a corporate business network and its R&D network. In general, a firewall is placed between a high security domain and a lower security domain. A firewall system operating at layers 3 and 4 is sometimes called a packet filtering router or a screening router. Its purpose is to filter IP and ICMP packets and TCP/UDP ports. The router will have several ports and be able to route and filter the packets according to the filtering rules. Packet filters can also be built in software and

Run on dual homed PCs, but whilst these can filter packets they are not able to route Them to different networks.

A firewall at layer 5 Internet (7 ISO) is sometimes called a bastion host, application gateway, proxy server or guardian system. Its purpose is to filter the service provided by the application. It is also possible to operate a firewall system at Layer 2 (the link level) e.g. by configuring an Ethernet bridge to only forwards certain packets, but this is not very common. The Inspection Module from Checkpoint's Firewall 1 product operates between the link and network layers and inspects packets before letting them pass through the firewall.

Packet Filtering Firewall

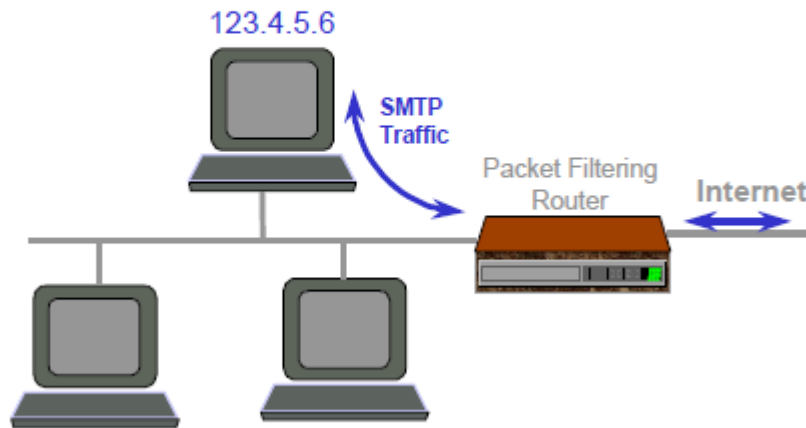


Figure 3

Fig 7.4

6. Packet Filtering Router

Packet filtering routers were the first type of firewall to be invented. A packet filtering Router should be able to filter IP packets based on the following four fields:

- Source IP address.
- Destination IP addresses.
- TCP/UDP source port.
- TCP/UDP destination port.

Filtering is used to:

- Block connections from specific hosts or networks.
- Block connections to specific hosts or networks.
- Block connections to specific ports.
- Block connections from specific ports.

When configuring a router, it is usually possible to specify *all* ports or hosts, as well as specific ones. Packet filtering routers have fast performance, since the IP packets are either forwarded or dropped without inspecting their contents (other than the address and port fields). Packet filtering routers are equivalent to guards who ask someone “where are you from and where are you going to” and if the answer is OK, the person is let into the building. For example, suppose an Internet access security policy stated that the only Internet access allowed was incoming and outgoing Email. Assuming that the organisation's Email server was located on host 123.4.5.6, then the router would be configured in the following way:

Type SourceAddr DestAddr SourcePort DestPort Action

```
tcp * 123.4.5.6 >1023 25 permit
tcp 123.4.5.6 * >1023 25 permit
* * * * * deny.
```

Note. * means any address.

Note. It is conventional for SMTP mail switches to always listen for incoming messages on port 25 (the well known port number), and to send messages on port numbers 1024 upwards. The first rule allows incoming Email from any address to be sent to the Email server, the second rule allows outgoing Email to be sent from the Email server to any address, whereas the last rule forbids any other traffic from passing through the router.

7. Problems with Packet Filtering Routers

Packet filtering routers are a vital component of a firewall system, but they should only be considered as a first line of defence, since they do have a number of deficiencies.

1. They can be complex to configure (the rule set can be large, particularly when many services are supported), and there is no automatic way of checking the correctness of the rules i.e. that the rules correctly implement the security policy. Furthermore, if the router does not support logging of calls, there is no way of knowing if supposedly disallowed packets are actually getting through via a hole in the rules.
2. If some members of staff have special requirements for Internet access, then new rules may have to be added for their machines. This further complicates the rule set, maybe making it too complex to manage. Furthermore this access is at the wrong level of granularity, since the machine rather than the user is being given permission. Users are not authenticated, only the packets are checked.
3. Some basic routers do not allow TCP/UDP filtering, and this makes it impossible to implement certain security policies e.g. the one given in the example above.
4. You cannot filter between different ISO protocols running over TCP/IP. RFC 1006 specifies how ISO applications such as X.500 and X.400 may run over TCP/IP. However, all of the ISO applications must connect to port 102, on which the RFC 1006 service sits.
5. Finally, packet filtering routers are not very secure, since the contents of the packets are not inspected (only their headers) so anything can be being passed through e.g. viruses, unauthorised delete commands etc. Finally, the senders of the packets are not authenticated.

In order to overcome some of these deficiencies, more of the contents of the packets need to be inspected. This led to application level firewalls and more recently to the stateful packet inspection module from Checkpoint.

8. Stateful Packet Inspections

This is a software module that runs in the operating system of a Windows or Unix PC firewall, and inspects the packets that are arriving. The inspection is driven by security rules configured into the machine by the security officer. Headers from all seven layers of the ISO model are inspected, and information about the packets is fed into dynamic state tables that store information about the

connection. The cumulative data in the tables is then used in evaluating subsequent packets on the same connection and subsequent connection attempts.

Whilst this technology is more secure than simple packet filtering routers, it is not as secure as application gateways, as the full application layer data is not inspected. However, it does perform faster than application proxies. Stateful inspection is similar to a security guard that asks who are you, where are you going, and what are you carrying, before he lets you into the building. Note that this technology is patented by Checkpoint, the manufacturers of FireWall-1.

9. Application Level Firewalls

An application level firewall is created by installing a (bastion) host computer running the appropriate application(s), between the packet filtering router and the intranet. The packet filtering router directs all calls from the Internet to the application level firewall. The application(s) running on the host are not usually full blown versions of the application(s), but rather are slimmed down proxy services that simply filter the messages at the application level, letting some messages through, rejecting other messages, and modifying others before accepting them. If the host does not run a particular application proxy service, then calls to this application will not usually pass through the firewall to/from the Internet. In other words, all services **not** running on the firewall are blocked. Common application proxies, supported by most application firewalls suppliers are FTP, SMTP, HTTP and Telnet.

Application proxies are similar to a security guard who asks you why you want to enter the building and what are you carrying, and if he does not like your answer he will refuse you entry, or he may direct you to another person, or even remove some of your items or substitute them before letting you pass through. He may even take things off you before you can leave the building.

FTP poses a security threat because confidential information may be exported from the organisation, or bogus information may be deposited in the organisation's file store. The FTP proxy allows FTP commands to be selectively blocked according to source and destination addresses. For example, if the organisation has information that it wishes to publish on the Internet, the proxy would forbid sending *put* commands (i.e. writing) to the relevant FTP server and directory. If the organisation wishes customers to send files to it, then the FTP proxy can ensure that *dir* and *get* commands are blocked, and that the FTP connection is sent to the correct system and directory.

SMTP poses a security threat because mail servers (often the buggy *sendmail* program on UNIX systems) run with system level permissions in order to deliver incoming mail to users mailboxes. Hackers can initiate an interactive session with a mail server (by hand typing in commands or writing their own programs) and exploit its system level privileges. The SMTP proxy which runs on the firewall isolates the internal Email system from incoming Internet mail, thereby preventing Internet users from directly interfering with a mail server. Incoming mail is spooled in a reserved directory on the firewall host, by the proxy SMTP mail program that runs without system privileges. The remote Email sender is then disconnected before any harm can be done. Another process picks up the mail from the reserved directory and forwards it to the internal Email system.

TELNET allows users to login to remote machines. This can be a security risk if remote users are allowed to login to the organisation's computers with standard username/password pairs, given the inherent weaknesses with password based systems. The Telnet proxy can be configured to state which systems can make calls to it, and which systems it will permit to be called. A typical configuration will be to allow internal users to call the Internet, but not vice versa.

HTTP accesses remote web pages. HTTP proxies can filter the various HTTP commands (methods) such as POST, PUT and DELETE as well as filter the URLs (e.g. forbid connections to .com sites) In addition, all of the application proxies will provide logging of the incoming and outgoing sessions, and will authenticate the users. However, rather than each proxy having its own authentication service, it is beneficial if all proxies can make use of a common authentication module that runs on the firewall. We also want to make sure that the data being transferred is virus free, therefore we need Content Filtering as well.

10. Content Filtering

With content filtering, the application data is handed over to a content filtering server that unpacks the data to see what is inside, and harmful content is then disposed of. For example, zipped files are unzipped first to see what is inside them. If the content contains a virus it will be discarded or disinfected. (Note, this requires that organisations regularly update their virus checking software, as new viruses are found daily.) File types are identified (not from the filename extension but from their content) and undesirable types e.g. executables can be removed, according to the security policy. Alternatively, if imported code is digitally signed, the author/signer can be checked to see if he is on a trusted list of signers and then the file can be accepted. Text files can be scanned for a list of undesirable key words (e.g. swear words or explicit sexual language). Finally, incoming http Java or ActiveX applets can be removed if this is company policy. Content filtering is like the security guard that empties your pockets, and gives you a full body check both on entering and leaving a building. The biggest vendor of content checking software is Checkpoint with its MIMESweeper family of products (that include MAILsweeper and WEBSweeper).

The biggest problem with scanning and filtering all the packet contents as they pass through the firewall, is the amount of processing time this takes, Consequently, large servers are needed if all incoming data is to be screened.

11. Authentication

It has already been noted that simple passwords can not be relied upon to provide authentication information over the Internet. Something stronger is needed. The logical place to site the strong authentication functionality is in the firewall. An increasingly common authentication method is the use of **one-time passwords or hashed passwords**. But digital signatures are also becoming more popular as PKIs get implemented. Digital signatures rely on asymmetric encryption. The sender digitally signs a message, by appending to it a digital summary of the message (called a message digest), encrypted with his private key. The firewall can decipher the digital signature using the

sender's public key. The firewall can also compute the message digest and compare this to the deciphered one. If both digests are the same, the message is authentic (it must have come from the owner of the private key and it has not been tampered with during transfer). SOCKS authentication was one of the first general authentication mechanisms to be placed in a firewall, that allows remote applications to authenticate to the firewall. RADIUS is the Internet draft standard for dial in user authentication to a firewall.

11.1. SOCKS Authentication

SOCKS provides an authentication layer for the firewall that can be used by all application proxies. Calls come into the SOCKS service, are authenticated by it, then a call is opened up to the application proxy which does further application level filtering before making a call to the application on the intranet, see Figure 4.

SOCKS Authentication Service

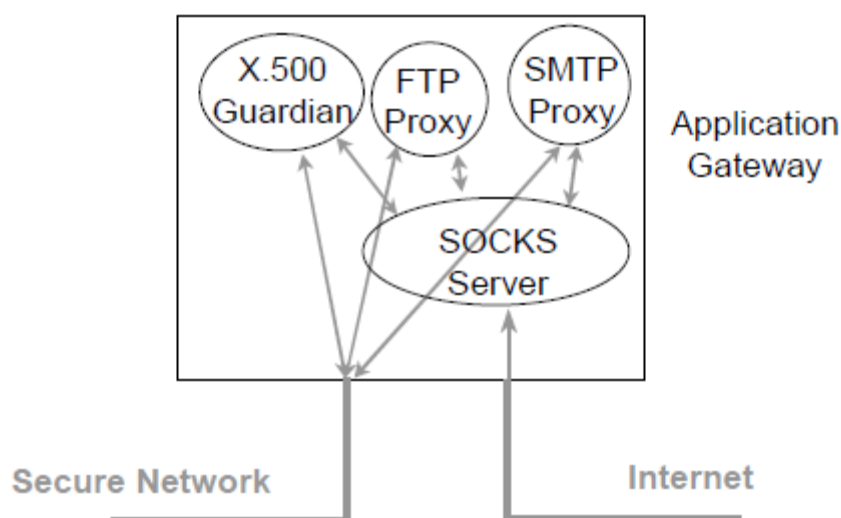


Figure 4

Fig 7.5

SOCKSv5(SOCKet Secure which is an Internet protocol that routes network packets between a client and server through a proxy server.) operates as follows. A TCP client opens up a connection to a SOCKS server at port 1080 in the firewall. The client negotiates an authentication method, then authenticates to the SOCKS server. If successful, the client sends a Relay Request to the SOCKS server. The SOCKS server then either relays the request to the requested server or rejects the request. If accepted, thereafter messages between the application server and the client are relayed via the SOCKS server. A full description of SOCKSv5 can be found in.

A disadvantage of SOCKSv5 is that it requires modified TCP software in the client system. Fortunately this is now widely implemented, and is supported for example in Netscape and Internet Explorer, plus freely available implementations of the SOCKS library and server are available for download from the Internet. Authentication methods primarily supported by SOCKS are username

password and GSS-API. But this is not such a wide range, and the password is sent in the clear so it is open to sniffing attacks.

Security architecture

Intrusion detection system

An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.

IDS come in a variety of “flavors” and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect based on looking for specific signatures of known threats- similar to the way antivirus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat. We’ll cover each of these briefly.

NIDS

Network Intrusion Detection Systems are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. Ideally you would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network.

HIDS

Host Intrusion Detection Systems are run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator of suspicious activity is detected

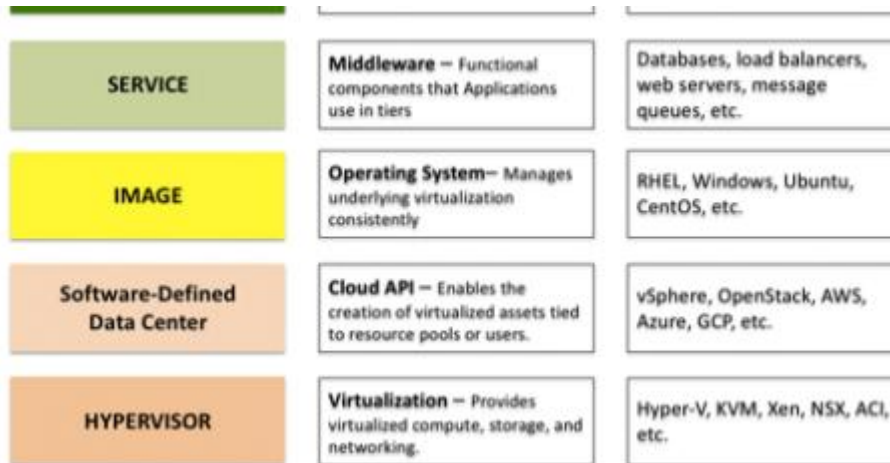
Signature Based

A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most antivirus software detects malware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that lag time your IDS would be unable to detect the new threat.

Anomaly Based

An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is “normal” for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

An OSI Model for Cloud



In 1984, after years of having separate thoughts on networking standards, the International Organization for Standardization (ISO) and the International Telegraph and Telephone Consultative Committee (CCITT) jointly published the Open Systems Interconnection Reference Model, more commonly known as the OSI model. In the more than three decades that have passed since its inception, the OSI model has given millions of technologists a frame of reference to work from when discussing networking, which has worked out pretty well for Cisco.

OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example	Central Device/Protocols	DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	End User layer Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management	User Applications SMTP	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	Syntax layer encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • Character Set Translation	JPEG/ASCII EBDIC/TIFF/GIF PICT	
Session (5) Allows session establishment between processes running on different stations.	Synch & send to ports (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.	Logical Ports RPC/SQL/NFS NetBIOS names	
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	TCP Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING TCP/SPX/UDP Routers IP/IPX/ICMP	Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	Packets ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	Frames ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgement • Frame delimiting • Frame error checking • Media access control	Switch Bridge WAP PPP/SLIP	Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	Physical structure Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique • Baseband or Broadband • Physical medium transmission Bits & Volts	Hub Land Based Layers	

Cloud technologies have progressed in recent years that a similar model is now suitable as different audiences have very different interests in the components that make up a cloud stack and understanding the boundaries of those components with common terminology can go a long way towards more efficient conversations.

Layer 1: Infrastructure

Layer	Description	Examples
INFRASTRUCTURE	Hardware — Physical devices in a data center providing a foundation for the model.	Cisco UCS, HP ConvergedSystem, VCE vBlock, etc.

Analogous to the Physical layer in the OSI model, Layer 1 here refers to the Infrastructure that sits in a data center to provide the foundation for the remainder of the stack. Corporate data centers and colocation providers have been running this Infrastructure layer for years and are experts at “racking and stacking” pieces of hardware within this layer for maximum efficiency of physical space, heating/cooling, power, and networking to the outside world.

Layer 2: Hypervisor

Layer	Description	Examples
HYPERVISOR	Virtualization — Provides virtualized compute, storage, and networking.	Hyper-V, KVM, Xen, NSX, ACI, etc.
INFRASTRUCTURE	Hardware — Physical devices in a data center providing a foundation for the model.	Cisco UCS, HP ConvergedSystem, VCE vBlock, etc.

Commonly installed on top of that Infrastructure layer is some sort of virtualization, commonly provided by a Hypervisor. This enables systems administrators to chunk up use of the physical assets into Virtual Machines (VMs) that can be bin packed onto physical machines for greater efficiency. Prior to the advent of the Hypervisor layer, components higher up the stack had to wait weeks to months for new Infrastructure to become available, but with the virtualization provided at this layer, virtualized assets become available in minutes.

Layer 3: Software-Defined Data Center (SDDC)

Layer	Description	Examples
Software-Defined Data Center	Cloud API — Enables the creation of virtualized assets tied to resource pools or users.	vSphere, OpenStack, AWS, Azure, GCP, etc.
HYPERVISOR	Virtualization — Provides virtualized compute, storage, and networking.	Hyper-V, KVM, Xen, NSX, ACI, etc.
INFRASTRUCTURE	Hardware — Physical devices in a data center providing a foundation for the model.	Cisco UCS, HP ConvergedSystem, VCE vBlock, etc.

Resource pooling, usage tracking, and governance on top of the Hypervisor layer give rise to the Software-Defined Data Center (SDDC). The notion of “infrastructure as code” becomes possible at this layer through the use of REST APIs. Users at this layer are typically agnostic to Infrastructure and Hypervisor specifics below them and have grown accustomed to thinking of compute, network, and storage resources as simply being available whenever they want.

Layer 4: Image

Layer	Description	Examples
IMAGE	Operating System — Manages underlying virtualization consistently	RHEL, Windows, Ubuntu, CentOS, etc.
Software-Defined Data Center	Cloud API — Enables the creation of virtualized assets tied to resource pools or users.	vSphere, OpenStack, AWS, Azure, GCP, etc.
HYPERVISOR	Virtualization — Provides virtualized compute, storage, and networking.	Hyper-V, KVM, Xen, NSX, ACI, etc.
INFRASTRUCTURE	Hardware — Physical devices in a data center providing a foundation for the model.	Cisco UCS, HP ConvergedSystem, VCE vBlock, etc.

Here, a bias towards compute resources (as opposed to network or storage) becomes apparent as Image connotes use of particular operating systems and other pre-installed software components. Format can be an issue here as not all SDDCs support the same types of Images (.OVA vs .AMI, etc.), but most operating systems can be baked into different kinds of Images to run on each popular SDDC. Developers will sometimes get involved at this layer, but not nearly as much as the two layers yet to come.

Layer 5: Services

Layer	Description	Examples
SERVICE	Middleware — Functional components that Applications use in tiers	Databases, load balancers, web servers, message queues, etc.
IMAGE	Operating System — Manages underlying virtualization consistently	RHEL, Windows, Ubuntu, CentOS, etc.
Software-Defined Data Center	Cloud API — Enables the creation of virtualized assets tied to resource pools or users.	vSphere, OpenStack, AWS, Azure, GCP, etc.
HYPERVISOR	Virtualization — Provides virtualized compute, storage, and networking.	Hyper-V, KVM, Xen, NSX, ACI, etc.
INFRASTRUCTURE	Hardware — Physical devices in a data center providing a foundation for the model.	Cisco UCS, HP ConvergedSystem, VCE vBlock, etc.

Application architectures are typically built on top of a set of common middleware components like data bases, load balancers, web servers, message queues, email services, other notification methods, etc. This Service layer is where those are defined, on top of particular Images from the layer below. Sometimes these Services manifest themselves as open source installed on a VM or container, such as MySQL to give a database example. Other times the SDDC may offer an API for accessing components from a pool of Services such as AWS RDS, but underneath that API those components are still built upon an Image and the other layers that precede it.

Layer 6: Applications

Layer	Description	Examples
APPLICATION	End User Layer — Provides measurable business value to a set of constituents.	Blogs, Wikis, CRMs, HPCs, etc
SERVICE	Middleware — Functional components that Applications use in tiers	Databases, load balancers, web servers, message queues, etc.
IMAGE	Operating System — Manages underlying virtualization consistently	RHEL, Windows, Ubuntu, CentOS, etc.
Software-Defined Data Center	Cloud API — Enables the creation of virtualized assets tied to resource pools or users.	vSphere, OpenStack, AWS, Azure, GCP, etc.
HYPERVISOR	Virtualization — Provides virtualized compute, storage, and networking.	Hyper-V, KVM, Xen, NSX, ACI, etc.
INFRASTRUCTURE	Hardware — Physical devices in a data center providing a foundation for the model.	Cisco UCS, HP ConvergedSystem, VCE vBlock, etc.

The final layer is where end users interact with the stack through deployed Applications that are comprised of custom code that makes use of various Services defined below it.

Now What?

Whether in a technical conversation or a sales engagement, understanding what layer in this stack a specific person has expertise is important. Someone who implemented a Hypervisor before the SDDC layer became widely available, for example, has a very different view of the world than someone who has never known a world where the SDDC did not exist. Experts at each layer in this stack have bias and often lack of understanding for those working at other layers in the stack. Admitting that and having a framework for all to understand how their part of the world makes up the whole leads to better conversations because everyone understands everyone else's motivations and places of intersection far better.

Attack surface:

The attack surface of a software environment is the sum of the different points (the "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment. Keeping the attack surface as small as possible is a basic security measure.

Understanding an attack surface:

Due to the increase in the countless potential vulnerable points each enterprise has, there has been increasing advantage for hackers and attackers as they only need to find one vulnerable point to succeed in their attack.

There are three steps towards understanding and visualizing an attack surface:

Step 1: Visualize. Visualize the system of an enterprise is the first step, by mapping out all the devices, paths and networks.

Step 2: Find indicators of exposures. The second step is to correspond each indicator of a vulnerability being potentially exposed to the visualized map in the last step. One IOE can be "missing security controls in systems and software".

Step 3: Find indicators of compromise. This is an indicator that an attack has already succeeded.

Surface reduction

The basic strategies of attack surface reduction include the following: reduce the amount of code running, reduce entry points available to untrusted users, and eliminate services requested by relatively few users. One approach to improving information security is to reduce the attack surface of a system or software. By turning off unnecessary functionality, there are fewer security risks. By having less code available to unauthorized actors, there will tend to be fewer failures. Although attack surface reduction helps prevent security failures, it does not mitigate the amount of damage an attacker could inflict once vulnerability is found.

An organization's attack surface can be subdivided into a few categories:

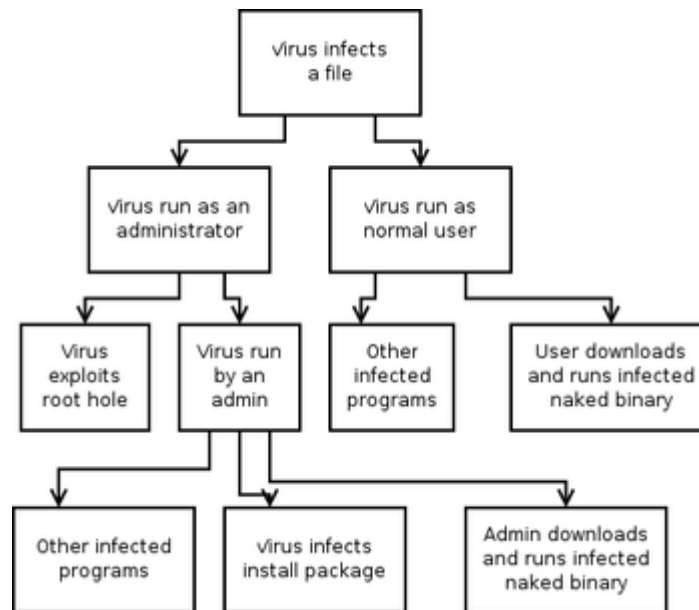
- The network attack surface: the totality of all vulnerabilities in connected hardware and software that are accessible to an unauthenticated user.
- The software attack surface: the complete profile of all functions in any code running in a given system that are available to an unauthenticated user.
- The physical attack surface: all security vulnerabilities in a given hardware system that are accessible to an attacker in the same location as the target.

Attack tree

Attack trees are conceptual diagrams showing how an asset, or target, might be attacked. Attack trees have been used in a variety of applications. In the field of information technology, they have been used to describe threats on computer systems and possible attacks to realize those threats. However, their use is not restricted to the analysis of conventional information systems. They are widely used in the fields of defense and aerospace for the analysis of threats against tamper resistant electronics systems (e.g., avionics on military aircraft). Attack trees are increasingly being applied to computer control systems (especially relating to the electric power grid). Attack trees have also been used to understand threats to physical systems.

Some of the earliest descriptions of attack trees are found in papers and articles by Bruce Schneier, when he was CTO of Counterpane Internet Security. Schneier was clearly involved in the development of attack tree concepts and was instrumental in publicizing them. However, the attributions in some of the early publicly available papers on attack trees also suggest the involvement of the National Security Agency in the initial development.

Design:



Attack tree for computer viruses. Here we assume a system such as Windows NT, where not all users have full system access. All child nodes operate on OR conditions.

Attack trees are multi-levelled diagrams consisting of one root, leaves, and children. From the bottom up, child nodes are conditions which must be satisfied to make the direct parent node true; when the root is satisfied, the attack is complete. Each node may be satisfied only by its direct child nodes.

A node may be the child of another node; in such a case, it becomes logical that multiple steps must be taken to carry out an attack. For example, consider classroom computers which are secured to the desks. To steal one, the securing cable must be cut or the lock unlocked. The lock may be unlocked by picking or by obtaining the key. The key may be obtained by threatening a key holder, bribing a keyholder, or taking it from where it is stored (e.g. under a mousemat). Thus a four level attack tree can be drawn, of which one path is (Bribe Keyholder, Obtain Key, Unlock Lock, Steal Computer).

Note also that an attack described in a node may require one or more of many attacks described in child nodes to be satisfied. Our above condition shows only OR conditions; however, an AND condition can be created, for example, by assuming an electronic alarm which must be disabled if and only if the cable will be cut. Rather than making this task a child node of cutting the lock, both tasks can simply reach a summing junction. Thus the path ((Disable Alarm, Cut Cable), Steal Computer) is created.

Attack trees are related to the established fault tree formalism. Fault tree methodology employs boolean expressions to gate conditions when parent nodes are satisfied by leaf nodes. By including a priori probabilities with each node, it is possible to perform calculate probabilities with higher nodes using Bayes Rule. However, in reality accurate probability estimates are either unavailable or too expensive to gather. With respect to computer security with active participants (i.e., attackers), the probability distribution of events are probably not independent nor uniformly distributed, hence, naive Bayesian analysis is unsuitable.

Since the Bayesian analytic techniques used in fault tree analysis cannot legitimately be applied to attack trees, analysts instead use other techniques to determine which attacks will be preferred by a particular attacker. These may involve comparing the attacker's capabilities (time, money, skill,

equipment) with the resource requirements of the specified attack. Attacks which are near or beyond the attacker's ability to perform are less preferred than attacks that are perceived as cheap and easy. The degree to which an attack satisfies the adversary's objectives also affects the attacker's choices. Attacks that are both within the adversary's capabilities, and which satisfy their goals, are more likely than those that do not.