RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Cyber Security**

Subject Code: **CS-503**

Semester: **5th**

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

Subject Notes
CS-503(C)-Cyber Security
Unit-1

Topics to be covered

UNIT 1

Introduction of Cyber Crime, Challenges of cyber crime, Classifications of Cybercrimes: Email Spoofing, Spamming, Internet Time Theft, Salami attack/Salami Technique,

---

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.

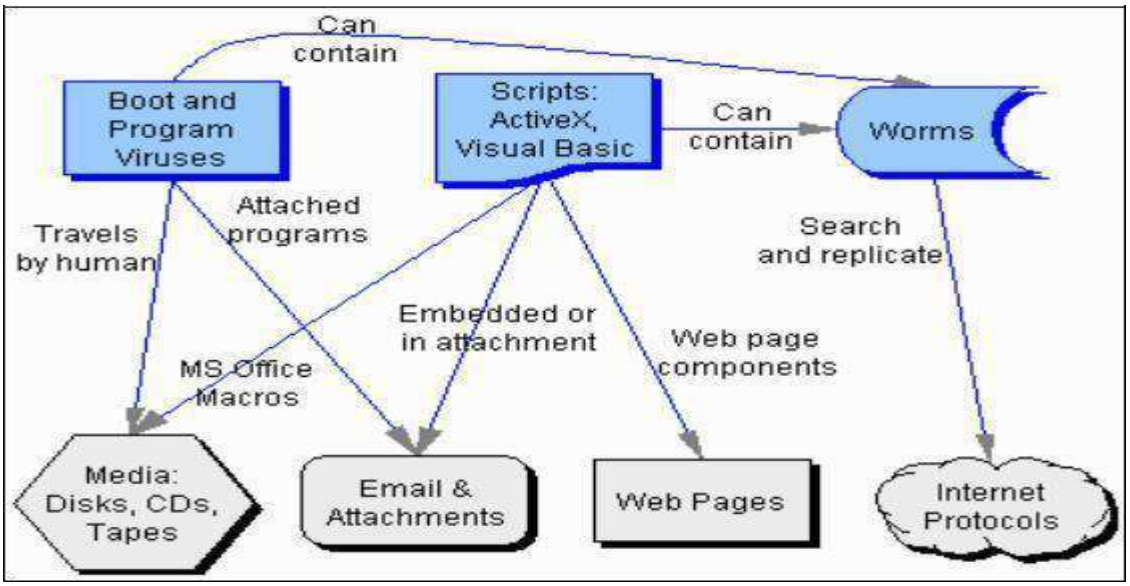

Figure 1.1: Web attacks

Challenges of cyber-crime-There are many challenges in front of us to fight against the cyber-crime. Some of themhere 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

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

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.
- **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.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

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' is utilizes hacking to cause violence against people orproperty, 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 governmentsand terrorize the citizens of the country.

IP Crimes- Software Piracy, Copyright Infringement, Trademarks Violations, Theft of Computer SourceCode. Email Spoofing a spoofed email is one that appears to originate from one source but actually hasbeen sent from another source.

Cyber Defamation- This occurs when defamation takes place with the help of computers and/or theInternet. 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 whichother forms of cyber-crime (e.g., fraud, terrorism) are committed. Theft of any information containedin 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 serviceprovider) 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.
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.

Internet Time Theft: Normally in these kinds of thefts the Internet surfing hours of the victim are used up byanother person. This is done by gaining access to the login ID and the password. E.g. Colonel *Bajwa's case*- theInternet hours were used up by any other person. This was perhaps one of the first reported cases related to cyber-crime in India. However this case made the police infamous as to their lack of understanding of the nature of cyber-crime.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

Email Spoofing: In the context of computers, to spoof one's email address means that the sender is acting as if the email is coming from someone it is not.How someone (or something) sends an email made to look like it comes from somewhere or somewhere it does not, is a little more technical to explain. The spoofing process involves:Spoofing email addresses is rather easy. All a person needs to spoof an email address is an SMTP (Simple Mail Transfer Protocol) server (a server that can send email) and the appropriate email software. Most website hosting services will even provide an SMTP server in their hosting package. It is also possible to send emailfrom your own computer if you load an SMTP server on it, however most ISPs will block port 25 (which is required to send out email).Many of the available free SMTP servers will allow you to show a different "from" address than the actual registered domain that the email is transmitting from. However, to the recipient of said message, they will see that it actually came from the address you specified.

Now, there are special checks in place (and more being put into place) to prevent exactly this problem. One is called SPF or "Sender Policy Framework" which was developed by Meng Weng Wong in 2003. Basically, each time an email is sent, the receiving server compares the IP of the origin with the IP listed in the SPF record with the appropriate domain.

EXAMPLE 1: So, for example, let's say someone tried to spoof Bill Gates (billgates@microsoft.com):

They would send an email on his behalf the recipient server would then talk back to microsoft.com and say"Hey, I have an email that is coming from 123.123.123.123 stating that it was sent frombillgates@microsoft.com."microsoft.com would then tells the recipient server, "No, sorry, it should be comingfrom 111.111.111.111." and the message would never get delivered.

Two basic reasons people (and machines) spoof:

1. Malicious: To cause useless internet traffic - ultimately hoping to bog down servers or bring them to a halt.
2. Because you were unlucky enough to have clicked the wrong thing at the wrong time.

How did they get my email address?

1. People click a link in a phishing email and freely submit their email address (unbeknownst) to the list.
2. People send forwards (such as today's latest funny) to mass groups of people, exposing their email addressand everyone else's. All you need is for one of those receiving email boxes to have a scraper in it (somethingthat pulls all the email addresses it can find and adds it to a list).

Protection against spoofing:

- Use your spam filters. Nearly every free (and paid) email service has spam filters and junk boxes. If somethinggoes to your junk mail, don't simply unblock it. Investigate the email, even if it looks like it's coming fromsomeone you know. Make sure that it really did come from that person and that they intended to send it toyou.
- Never click an unexpected link or download an unfamiliar attachment. Nearly all major companies (such asbanks) have policies in place that require that if they need you to click a link to their site, they will includesome sort of identifying information such as your name or last four digits of an account number. Pay specialattention to that. Too many people see a generic email that simply says "Your account has been compromised,click here to validate." No legitimate bank or institution will ever send that. They would say "Dear Jason, Webelieve your account has been compromised, please call us at XXX-XXX-XXXX."
- Learn to read email message headers and check domain names and IP addresses. Nearly all email programswill let you float your mouse over an email address (or link in an email). What you see pop up should beidentical to what you are floating over. If it is something different, then it is probably spam or phishing forinformation.

Salami Attack/ Salami Slicing: These attacks are used for the commission of financial crimes. The key here isto make the alteration so insignificant that in a single case it would go completely unnoticed. E.g. a bankemployee 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 thebank employee will make a sizable amount of money every month.Salami Attack consists of merging bits of seemingly inconsequential data to produce huge results.A simple example is when an attacker/forger removes Rs. 0.01 (1 paise) from each account of SBI.No one will

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

notice such a tiny mismatch. But when one praise is deducted from all account holdersof India's largest bank; It produces a huge amount Computer computations are many times rounded off to small fractions. It is while doing such corrections many bankers tries to rob money**.**

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 overloadingnetwork and disrupting service to subscribers or creates .negative impact on consumer's attitudesfor Internet Service Provider.

How Does Spamming Take Place?

Although electronic Spam exists within a wide range of settings, the implementation of Spamming isconsidered to exist within the illegal and unlawful sales, solicitation, and marketing within the Commercial industry.

Commercial Spamming:Spamming that includes online, or Internet-based, solicitation can include a vast array of offenses, ranging from unlawful communication tactics to intrusive marketing techniques, which result in the violation of one's privacy. The oversight of the of implied legislation, decorum, legality, and ethics with regard to online advertising efforts considered to be ethical forbid the use of intrusive and unsolicited Spamming endeavors. How to prevent spamming?

In order to deter the transmission of Spamming, many e-mail providers have introduced 'Spam filters' aimed at deterring the deliverance of electronic Spam. Furthermore, Internet browsers have undertaken methodologies utilized in order to limit, if not fully prohibit, the existence of 'pop-up solicitation', as well as the prevention of 'Spyware' and additional intrusive monitoring programs. These types of preventative measures can be accessed both through paid services, as well as free services.

The following legal jurisdictions contribute to the bulk of the oversight of Spamming efforts:

- **Commercial Law:** Existing within the electronic and online sector, Commercial Law focuses on the regulationof legislation, ethics, legality, and stipulations that exist with regard to the operation and facilitation of commercial activity engaging the usage of computer networks, virtual marketplaces, online businesses, andInternet-based business activity.
- **Cyber Law:** Considered one of the most recently developed legal specialties that address the legislation andlegality innate within the expressed legal and lawful decorum required while engaging in the use of acomputer, electronic network, or telecommunications system.

Get real-time updates from RGPV

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in

RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Cyber Security**

Subject Code: **CS-503**

Semester: **5th**

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

Unit-2

Topics to be covered

UNIT 2

Web jacking, Online Frauds, Software Piracy, Computer Network Intrusions, Password Sniffing, Identity Theft, cyber terrorism, Virtual Crime, Perception of cyber criminals: hackers, insurgents and extremist group etc. Web servers were hacking, session hijacking.

Web Jacking- The Web Jacking Attack Vector is another phishing technique that can be used in social engineering engagements. Attackers that are using this method are creating a fake website and when the victim opens the link a page appears with the message that the website has moved and they need to click another link. If the victim clicks the link that looks real he will redirected to a fake page.

Web jacking is same as like web hijacking but the difference between web jacking and hijacking is in web jacking attack methodhackers compromised with the domain name system but in hijacking they take a full control over the website.

Web jacking attack method is another type of social engineering phishing attackwhere an attacker creates a fake web page of victim website and sends it to the victim. And when a victim click on that link, a message display on the browser "the site abc.com has move on another address, click here to go to the new location" and if a victim does click on the link, he/she will redirect on the fake website page where an attacker can ask for any sensitive data such as credit card number, username, password etc. Web jacking attack method is one kind of trap which is speeded by the attacker to steal the sensitive data of any people, and those people got trapped who are not aware about cyber security. And web jacking attack method is very common phishing attack nowadays, so if a people have even a little knowledge about cyber security, those people will never get trap.

The process of web jacking attack method:

- The first step of web jacking attack method is to create a fake page of victim website.
- The second step is to host it either on your local computer or shared hosting.
- The third step is to send the link of a fake page to the victim.

The fourth step victim will open the link and enter their details and submit. And in last step, you will get all the details submitted by victim.

Online Frauds - Fraud that is committed using the internet is "online fraud." Online fraud can involve financial fraud and identity theft. The most common types of online fraud are called phishing and spoofing.

Online Scams-Online scam is an attempt to trap you for obtaining money. There are many types of online scams; this includes obtaining money with fake names, fake photos, fake e-mails, forged documents, fake job offers and many more.

Generally, it happens by sending fake e-Mails for your personal details like online banking details, credit carddetails. Sometimes e-Mails are sent from lottery companies with fake notice, whenever you participate in online auction and e-Mails received for fake gifts.

Phishing scam-Online scammers send you an e-mail and ask your account information or credit card detailsalongwith a link to provide your information. Generally, the links sent will be similar to your bank. So whenever you post your details in the link then the details will be received by scammers and money is misused.

Lottery scam-Sometimes you receive an email like "you won a lottery of million dollars" receiving such a kind of mails is a great thing, and really it's a happiest thing. By responding to such a kind of mails huge

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

amount of money will be lost. Because these e-Mails are not true, scammers try to fool and trap you to obtain money.

Online Auction- If you bid for a product you never get the product promised or don't match the product, and the description given to you may be incomplete, wrong, or fake. The scammer accepts the bid from one person and goes for some other sites where they can get less than the winning bid so scammers may not send the product you wanted.

Forwarding Product or Shipping Scam-Whenever you answer an online advertisement for a letter or e-mail manager like some US based corporation which lacks address or bank details and needs someone to take goods and sent to their address or ship overseas, and you are asked to accept the transfers into your bank. Generally, it happens for products that are purchased using stolen credit cards and shipped to your address and then you will be fooled and asked to reship the product to others they might have deceived, who reship the product overseas. The stolen money will be transferred to your account.

E-mail Scam Like --Congratulations you have won Webcam, Digital Camera, etc.-Sometimes you get an e- mail with a message like -- you have won something special like digital camera webcam , all you need to do is just visit our web site by clicking the link given below and provide your debit or credit card details to cover shipping and managing costs. However the item never arrives but after some days the charges will be shown on your bank account and you will lose money.

By E-mails- Generally, fraudsters send you an e-mail with tempting offers of easy access to a large sum ofmoney and ask you to send scanned copies of personal documents like your address proof, passport details and ask you to deposit an advance fee for a bank account. So once you deposit the funds, they take money and stop further communication, leaving you with nothing in return.

Unscrupulous Websites for Income Tax Refund- Generally, websites feel like official websites and seek the details of credit card, CVV PIN of ATM and other personal details of the taxpayers in the name of crediting income tax refund through electronic mode.

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.

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.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

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 unauthorizeduse 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.

Computer Network Intrusions- A network intrusion is any unauthorized activity on a computer network. In most cases, such unwanted activity absorbs network resources intended for other uses, and nearly always threatens the security of the network and/or its data.

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 monitor network traffic and compare 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.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

Password Sniffing- A password sniffer is a software application that scans and records passwords that are used or broadcasted on a computer or network interface. It listens to all incoming and outgoing network traffic and records any instance of a data packet that contains a password. A password sniffer installs on a host machine and scans all incoming and outgoing network traffic.

Identity Theft- Identity theft is the unauthorized collection of personal information and its subsequent use for criminal reasons such as to open credit cards and bank accounts, redirect mail, set up cell phone service, rent vehicles and even get a job. These actions can mean severe consequences for the victim, who will be left with bills, charges and a damaged credit score.

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.At this juncture a necessity may be felt that what is the need to distinguish between cyber terrorism and cyber-crime. Both are criminal acts. However there is a compelling need to distinguish between both these crimes. A cyber-crime is generally a domestic issue, which may have international consequences; however cyber terrorism is a global concern, which has domestic as well as international consequences. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks, etc. Technology savvy terrorists are using 512-bit encryption, which is next to impossible to decrypt. The recent example may be cited of – Osama Bin Laden, the LTTE, and attack on America's army deployment system during Iraq war.

Cyber terrorism may be defined to be " the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives" (4). Another definition may be attempted to cover within its ambit every act of cyber terrorism.

A terrorist means a person who indulges in wanton killing of persons or in violence or in disruption of servicesor means of communications essential to the community or in damaging property with the view to –

- Putting the public or any section of the public in fear; or
- Affecting adversely the harmony between different religious, racial, language or regional groups or castesor communities; or
- Coercing or overawing the government established by law; or
- Endangering the sovereignty and integrity of the nation and a cyber-terrorist is the person who uses thecomputer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof isan act of cyber terrorism.

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.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

- 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.

Prevention of Cyber Crime:

Prevention is always better than cure. It is always better to take certain precaution while operating the net. Ashould make them his part of cyber life. Saileshkumar Zarkar, technical advisor and network securityconsultant to the Mumbai Police Cyber-crime Cell, advocates the 5P mantra for online security: Precaution,Prevention, Protection, Preservation and Perseverance. A netizen should keep in mind the following things-

- To prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.
- Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
- Always use latest and update antivirus software to guard against virus attacks.
- Always keep back up volumes so that one may not suffer data loss in case of virus contamination
- Never send your credit card number to any site that is not secured, to guard against frauds.
- Always keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children.
- It is better to use a security program that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
- Website owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
- Use of firewalls may be beneficial.
- Web servers running public sites must be physically separate protected from internal corporate network.

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 securityloop 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 it'susually installed on Linux. Most PHP websites are hosted on Apache servers.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

- **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 becomeunavailable to the legitimate users. One of the ways to deploy denial of service attack is to flood syn request to server we will discuss this attack thoroughly in next unit.

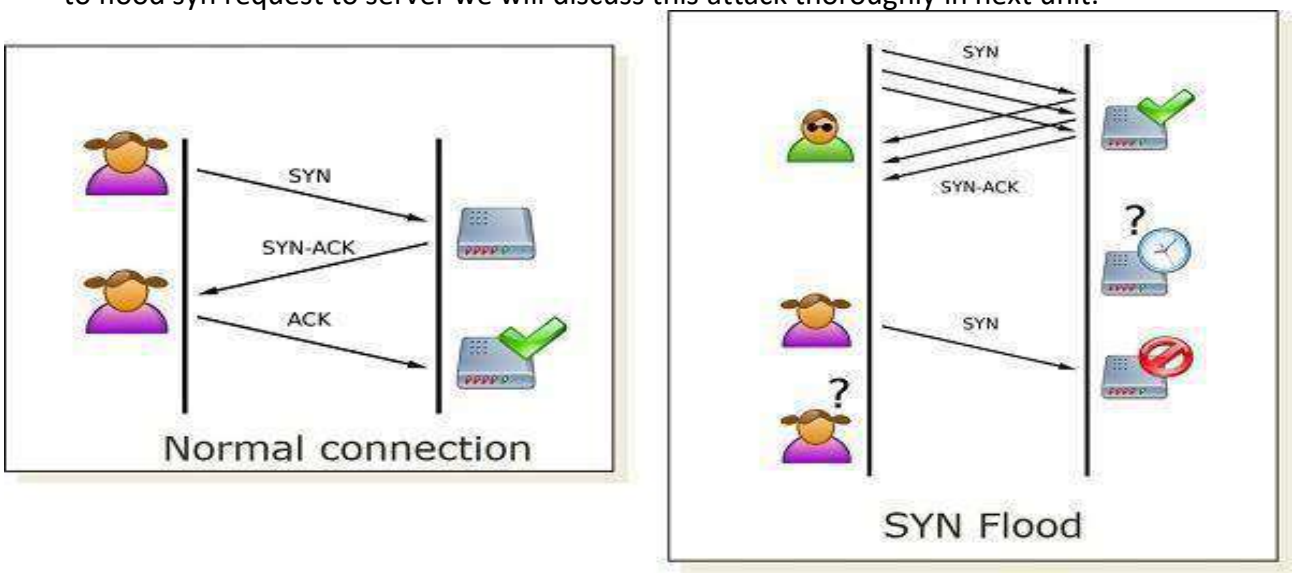

Figure 2.1: Denial of Service Attacks

- **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 datasent overthe network may be intercepted and used to gainunauthorized 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 BotnetSoftware, etc.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

- 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 controlmechanism, 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.

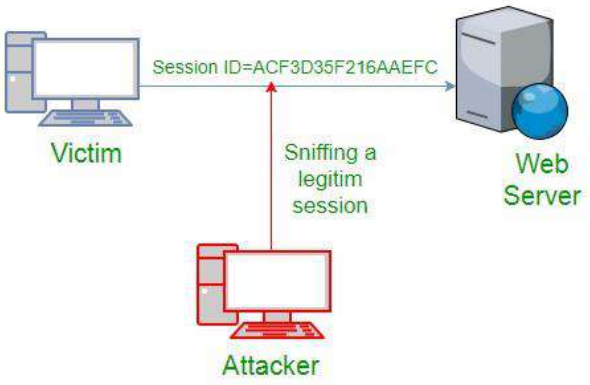

Figure 2.2: Session Hijacking

A session token is normally composed of a string of variable width and it could be used in different ways, likein 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.

Get real-time updates from RGPV

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in

RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Cyber Security**

Subject Code: **CS-503**

Semester: **5th**

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in

Downloaded from www.rgpvnotes.in

Topics to be covered

UNIT 3

Cyber Crime and Criminal justice: Concept of Cyber Crime and the IT Act, 2000, Hacking, Teenage Web Vandals, Cyber Fraud and Cheating, Defamation, Harassment and E-mail Abuse, Other IT Act Offences, Monetary Penalties, jurisdiction and Cyber Crimes, Nature of Criminality, Strategies to tackle Cyber Crime and Trends.

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. Cybercrime is a Offences that are committed against individuals or groups of i 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 limit end 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, a n d child grooming. There arealso 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. Cybercrimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of I.T. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cybercrimes. The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

Cybercrimes under the IT Act

- Tampering with Computer source documents - Sec.65
- Hacking with Computer systems, Data alteration - Sec.66
- Publishing obscene information - Sec.67
- Un-authorized access to protected system Sec.70 Breach of Confidentiality and Privacy - Sec.72
- Publishing false digital signature certificates - Sec.73

Cyber Crimes under IPC and Special Laws

- Sending threatening messages by email - Sec 503 IPC
- Sending defamatory messages by email - Sec 499 IPC
- Forgery of electronic records - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC
- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

Cyber Crimes under the Special Acts

- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

- Online sale of Arms Act

The newly amendment Act came with following highlights;

- It focuses on privacy issues.
- It focuses on Information Security.
- It came with surveillance on Cyber Cases.
- The Concept of Digital Signature was elaborated.
- It clarified reasonable security practices for corporate.
- Role of Intermediaries were focuses.
- It came with the Indian Computer Emergency Response Team.
- New faces of Cyber Crime were added.
- Powers were given to Inspector to investigate cyber-crimes as against only to DSP.
- Severe Punishments and fine were added.

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.
Hackers are classified according to the intent of their actions. The following list classifies hackers according to their intent.

Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the identified weaknesses. They may also perform penetration testing and vulnerability assessments.
Ethical hackers must abide by the following rules.

- Get **written permission** from the owner of the computer system and/or computer network before hacking.
- **Protect the privacy of the organization** been hacked.
- **Transparently report** all the identified weaknesses in the computer system to the organization.
- **Inform** hardware and software vendors of the **identified weaknesses**.

Cracker (Black hat): A hacker who gains unauthorized access to computer systems for personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer funds from bank accounts etc.

Grey hat: A hacker who is in between ethical and black hat hackers. He/shebreaks into computer systems without authority with a view to identify weaknesses and reveal them to the system owner.

Script kiddies: A non-skilled person who gains access to computer systems using already made tools.

Hacktivist: A hacker who use hacking to send social, religious, and political, etc. messages. This is usually done byhijacking websites and leaving the message on the hijacked website.

Phreaker: A hacker who identifies and exploits weaknesses in telephones instead of computers.
Ethical Hacking is identifying weakness in computer systems and/or computer networks and coming withcountermeasures that protect the weaknesses.

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.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

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. Any derogatory statement, which is designed to injure aperson's business or reputation, constitutes cyber defamation. Defamation can be accomplished as libel or slander. Cyber defamation occurs when defamation takes place with the help of computers and / or the Internet. E.g. Someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends.

Harassment -Harassment is a form of discrimination. It involves any unwanted physical or verbal behaveor 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:

- Tampering with the computer source documents.
- Hacking with computer system.
- Publishing of information which is obscene in electronic form.
- Power of Controller to give directions
- Directions of Controller to a subscriber to extend facilities to decrypt information
- Protected system
- Penalty for misrepresentation
- Penalty for breach of confidentiality and privacy
- Penalty for publishing Digital Signature Certificate false in certain particulars
- Publication for fraudulent purpose
- Act to apply for offence or contravention committed outside India
- Confiscation
- Penalties or confiscation not to interfere with other punishments.
- 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 s 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.

Electronic Governance- In this era of computer where every word is getting prefixed by word 'E', Government of India is also not lacking behind and to provide its services to the citizens at their fingertips the Government is also turning in E- Governance. E-Governance is nothing but providing Government Services cheaper, faster and efficiently to thecitizens through internet and computer. The Information Technology Act, 2000 gives recognition to the Electronic Governance. Chapter III, Section 4 to Section 10-A, of the Act provides for the provisions regarding Electronic Governance. Section 4 and 5

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

gives Legal Recognition to electronic records and electronic signatures. Section 6 of the Act authenticates use of electronic record and electronic signatures in Government and its agencies. The aim electronic government is to ensure transparency in Government. It also makes the Government accessible to the citizen residing in the most remote village of the country.

Jurisdiction and Cyber Crimes:

Jurisdiction over Internet-The whole trouble with internet jurisdictionis 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: -

- The Place where the defendant reside.
- 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 forconduct 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:

- The laws of the state/nation in which the user resides,
- The laws of the state/nation that apply where the server hosting the transaction is located.
- The laws of the state/nation which apply to the person or business with whom the transaction takes place.

Nature of Criminality- 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.

Compounding of Offences

As per Section 77-A of the I. T. Act, any Court of competent jurisdiction may compound offences, other than offences for which the punishment for life or imprisonment for a term exceeding three years has been provided under the Act.

No offence shall be compounded if;

- The accused is, by reason of his previous conviction, is liable to either enhanced punishment or to the punishment of different kind; OR
- Offence affects the socio economic conditions of the country; OR
- Offence has been committed against a child below the age of 18 years; OR
- Offence has been committed against a woman.

The person accused of an offence under this Act may file an application for compounding in the Court in which offence is pending for trial and the provisions of Sections 265-B and 265-C of Cr. P. C. Shall apply.

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

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

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 theindividual.

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 is 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:

- **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.
- **Focus on Effects-** I t'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.
- **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.
- Prevention is always better than cure. It is always better to take certain precautions while working on the net. One should make them a part of his cyber life. Sailesh KumarZarkar, technical advisor and network security consultant to the Mumbai Police Cybercrime Cell, advocates the 5P mantra for online security: Precaution, Prevention, Protection, Preservation and Perseverance.
- Identification of exposures through education will assist responsible companies and firms to meet these challenges.
- One should avoid disclosing any personal information to strangers, the person whom they don t know, via e-mail or while chatting or any social networking site.
- One must avoid sending any photograph to strangers by online as misusing or modification of photograph incidents increasing day by day.
- An update Anti-virus software to guard against virus attacks should be used by all the netizens and should also keep back up volumes so that one may not suffer data loss in case of virus contamination.
- A person should never send his credit card number or debit card number to any site that is not secured, to guard against frauds.
- It is always the parents who have to keep a watch on the sites that their children are accessing, to prevent any kind of harassment or depravation in children.

Get real-time updates from RGPV

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in

RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Cyber Security**

Subject Code: **CS-503**

Semester: **5th**

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

Unit -4

Topics to be covered

UNIT 4

The Indian Evidence Act of 1872 v. Information Technology Act, 2000: Status of Electronic Records as Evidence, Proof and Management of Electronic Records; Relevancy, Admissibility and Probative Value of E-Evidence, Proving Digital Signatures, Proof of Electronic Agreements, Proving Electronic Messages.

The Indian EvidenceAct of 1872 v. Information Technology Act, 2000- Conventional Crime is a social and economic phenomenon and is as old as the human society. Crime is a legal concept and has the sanction of the law. Crime or an offence is a legal wrong that can be followed by criminal proceedings which may result into punishment.' The hallmark of criminality is that, it is breach of the criminal law. Per Lord the criminal quality of an act cannot be discovered by reference to any standard but one: is the act prohibited with penal consequences'. A crime may be said to be any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by penal consequences.

There is apparently no distinction between cyber and conventional crime. However on a deep introspection we may say that there exist a fine line of demarcation between the conventional and cybercrime, which is appreciable. The demarcation lies in the involvement of the medium in cases of cybercrime. The sine qua non for cybercrime is that there should be an involvement, at any stage, of the virtual cyber medium.

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.

Reasons for Cyber-crime:

Hart in his work The Concept of Law' has said —human beings are vulnerable so rule of law is required toprotect them . Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cybercrime. The reasons for the vulnerability of computers may be said to be:

- Capacity to store data in comparatively small space:The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much easier.
- Easy to access :The problem encountered in guarding a computer system from unauthorized access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. That can fool biometric systems and bypass firewalls can be utilized to get past many a security system.
- Complex: The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.
- Negligence: Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cybercriminal to gain access and control over the computer system.
- Loss of evidence : Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyzes this system of crime investigation.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

The Information Technology Act was originally passed on 17th October 2000 withone ofthe 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 –

- Defining Electronic Record.
- Scope of definition of evidence expanded to include electronic records.
- Admissibility of electronic records.
- Presumption as to electronic messages

Digital evidence- Digital data are all around us and should be collected routinely in any investigation.Even if digital data do not provide a link between a crime and its victim or a crime and its perpetrator, they can be useful in an investigation. Digital evidence can reveal howa crime was committed, provide investigative leads, disprove or support witness statements, and identify likely suspects.
Digital evidence is defined as any data stored or transmitted using a computer that support or refute (counter)a theory of how an offense occurred or that address critical elements of the offense such as intent or alibi(excuse).Data - a combination of numbers that represent information of various kinds, including text, images, audio, and video.
Types of digital data that exist and how they might be useful in an investigation?
Computers are ubiquitous and digital data are being transmitted through the air around us and through wires in the ground beneath our feet. When considering the many sources of digital evidence, it is useful to Categorize computer systems into three groups:
Open Computer System Communication System Embedded Computer System

I. Digital Evidence – Communication System

- Traditional telephone systems, wireless telecommunication systems, the Internet, and networks ingeneral can be a source of digital evidence.
- For instance, telecommunication systems transfer SMS/MMS messages, and the Internet carries e- mail messages around the world.
- The time a message was sent, who likely sent it, or what the message contained can all be important in an investigation.
- To verify when a message was sent, it may be necessary to examine log files from intermediate servers and routers that handled a given message.
- Some communication systems can be configured to capture the full contents of traffic, giving digital investigators access to all communications (e.g., message text and attachments, and telephone conversations.

II. Digital Evidence –Embedded Computer System

- Mobile devices, smart cards, and many other systems with embedded computers may contain digital evidence. Mobile devices can contain communications, digital photographs and videos, and other personal data. Navigation systems can be used to determine where a vehicle has been.
- Sensing and Diagnostic Modules in many vehicles hold data that can be useful for understanding accidents, including the vehicle speed, brake status, and throttle position during the last 5s before impact.
- Microwave ovens are now available with embedded computers that can download information from the Internetand some home appliances allow users to program them remotely via a wireless network or the Internet.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

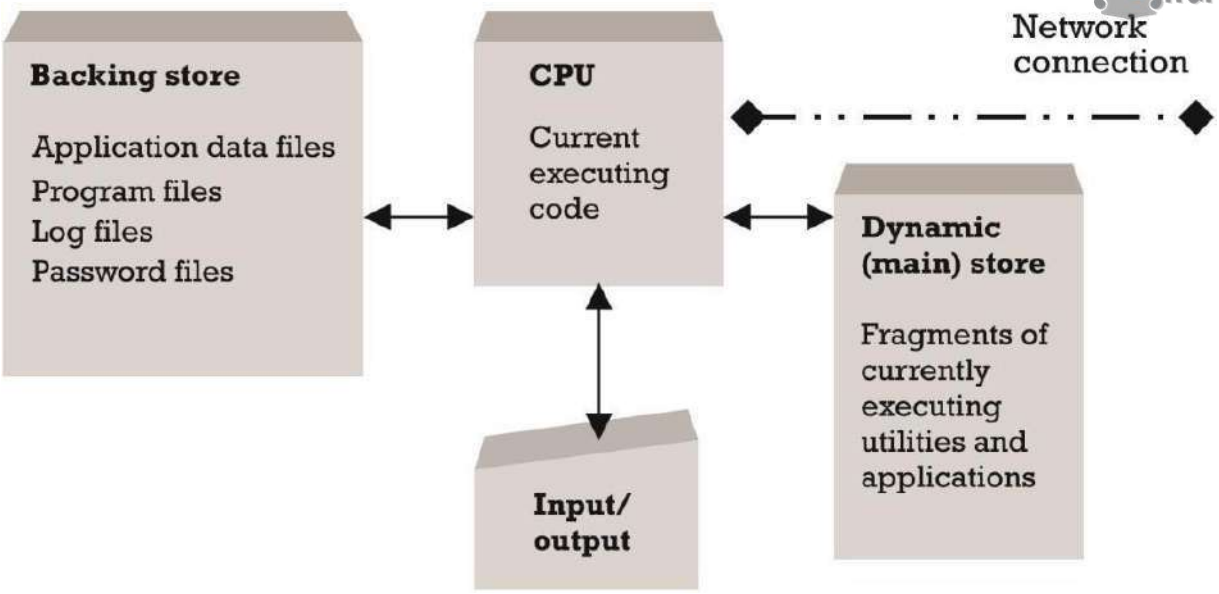

Figure 4.1: Embedded Computer System

Status of Electronic Records as Evidence

- 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 i s 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.

Proof and Management of Electronic Records

- 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.
- 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 transaction.

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.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

Admissibility and Probative Value of E-Evidence

Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a partyto a court casemay 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.

The use of digital evidence has increased inthe past few decades ascourts 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.

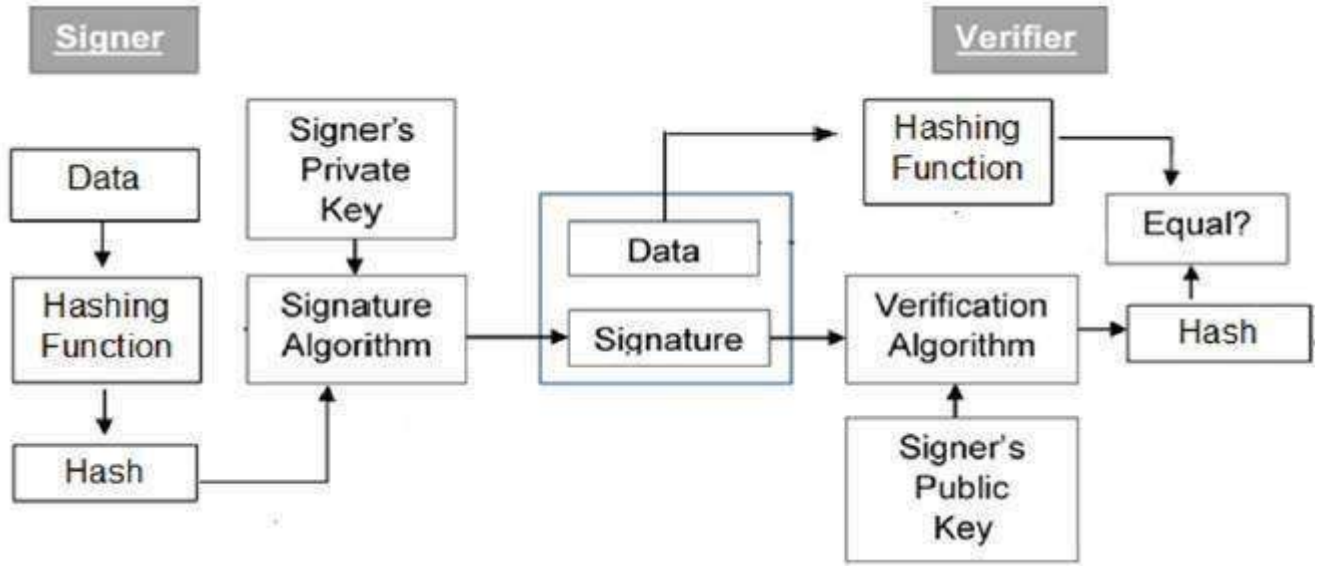

Figure 4.2: Proving Digital Signature

Proof of Electronic Agreements

- 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.
- 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 tobe 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.

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.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

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.

RGPVNOTES.IN

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

Unit-5

Topics to be covered

UNIT 5

Tools and Methods in Cybercrime: Proxy Servers and Anonymizers, Password Cracking, Key loggers and Spyware, virus and worms, Trojan Horses, Backdoors, DoS and DDoS Attacks , Buffer and Overflow, Attack on Wireless Networks, Phishing : Method of Phishing, Phishing Techniques.

Proxy Servers

A proxy server is a server (a computer system or an application) that acts as an intermediary for requestsfrom 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.

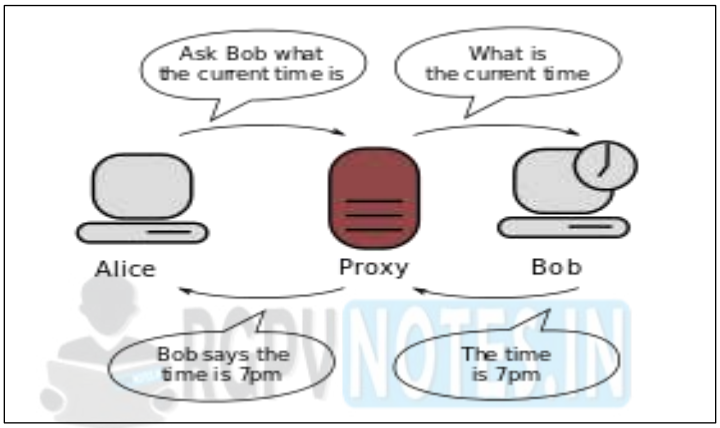

Figure5.1: Communication between two computers connected through a third computer acting as a proxy. Bob does not know to whom the information is going, which is why proxies can be used to protect privacy.

Anonymizers- An Anonymizers 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 Anonymizers. Anonymizers 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. Anonymizers can help in allowing freeaccess to all of the internet content, but cannot help against persecution for accessing the Anonymizers website itself. **Password Cracking**

Password cracking is the process of recovering passwords from data that have been stored in ortransmitted 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 usuallyaccomplished by recovering passwords from data stored in, or transported from, a computer

 Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

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.

Key loggers-A Key loggers 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.

Key loggers 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 Key loggers are perfect for corporate espionage.

Key loggers 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 andsearch history. But when a spyware is used maliciously, it is hidden in the system files of thecomputer and difficult to differentiate.

One of the simplest and most popular, yet dangerous is Key loggers. It is used to record the keystrokes which could be fatal as it can record passwords, credit card information etc. In someshared 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 right s, 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 itselfto another program, computerboot 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 caninfect 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

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

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 programsor 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

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

infected system so that when the system is booted next, the virus willbe 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 ifonly 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, frombanks to news websites, and present a major challenge to making sure people can publish and access important information.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

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 rouge 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 accesspoints. With this, one's evil twin will tend to have a stronger network signal and therefore people will

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

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.
- **Blue Jacking**-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. Blue jacking is possible where a Bluetooth network is present and it is limit end 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. Blue jacking 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 Blue jacking.
- **Bluesnarfing-**Bluesnarfing is far much more malicious than Blue jacking 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.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

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 aswell as amessage 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 bysigning 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 sendmessages 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 legitimatesocial networkwebsite pass through the phisher who can inspect the messages and acquire valuable information.

Get real-time updates from RGPV

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in

RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Cyber Security**

Subject Code: **CS-503**

Semester: **5th**

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

Unit-5

Topics to be covered

UNIT 5

Tools and Methods in Cybercrime: Proxy Servers and Anonymizers, Password Cracking, Key loggers and Spyware, virus and worms, Trojan Horses, Backdoors, DoS and DDoS Attacks , Buffer and Overflow, Attack on Wireless Networks, Phishing : Method of Phishing, Phishing Techniques.

Proxy Servers

A proxy server is a server (a computer system or an application) that acts as an intermediary for requestsfrom 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.

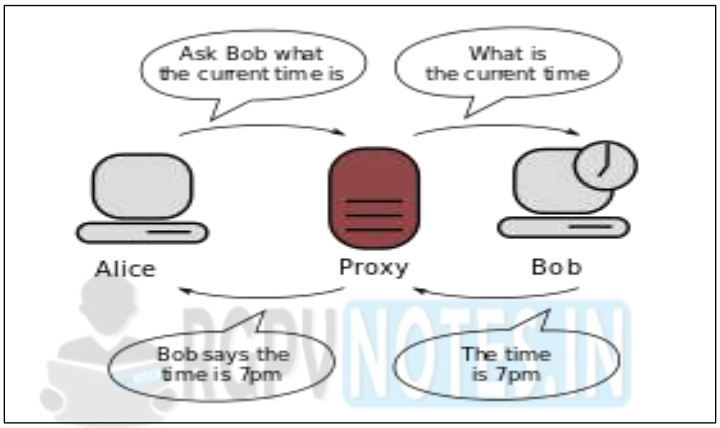

Figure5.1: Communication between two computers connected through a third computer acting as a proxy. Bob does not know to whom the information is going, which is why proxies can be used to protect privacy.

Anonymizers- An Anonymizers 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 Anonymizers. Anonymizers 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. Anonymizers can help in allowing freeaccess to all of the internet content, but cannot help against persecution for accessing the Anonymizers website itself. **Password Cracking**

Password cracking is the process of recovering passwords from data that have been stored in ortransmitted 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 usuallyaccomplished by recovering passwords from data stored in, or transported from, a computer

 Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

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.

Key loggers-A Key loggers 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.

Key loggers 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 Key loggers are perfect for corporate espionage.

Key loggers 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 andsearch history. But when a spyware is used maliciously, it is hidden in the system files of thecomputer and difficult to differentiate.

One of the simplest and most popular, yet dangerous is Key loggers. It is used to record the keystrokes which could be fatal as it can record passwords, credit card information etc. In someshared 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 right s, 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 itselfto another program, computerboot 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 caninfect 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

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

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 programsor 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

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

infected system so that when the system is booted next, the virus willbe 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 ifonly 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, frombanks to news websites, and present a major challenge to making sure people can publish and access important information.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

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 rouge 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 accesspoints. With this, one's evil twin will tend to have a stronger network signal and therefore people will

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

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.
- **Blue Jacking**-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. Blue jacking is possible where a Bluetooth network is present and it is limit end 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. Blue jacking 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 Blue jacking.
- **Bluesnarfing-**Bluesnarfing is far much more malicious than Blue jacking 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.

Get real-time updates from RGPV

Downloaded from www.rgpvnotes.in

RGPVNOTES.IN

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 aswell as amessage 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 bysigning 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 sendmessages 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 legitimatesocial networkwebsite pass through the phisher who can inspect the messages and acquire valuable information.

Get real-time updates from RGPV

RGPVNOTES.IN

We hope you find these notes useful.

You can get previous year question papers at https://qp.rgpvnotes.in .

If you have any queries or you want to submit your study notes please write us at rgpvnotes.in@gmail.com

LIKE & FOLLOW US ON FACEBOOK
facebook.com/rgpvnotes.in