RGPVNOTES.IN

Program : **B.Tech**

Subject Name: **Cyber Security**

Subject Code: **CS-503**

Semester: **5th**

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.

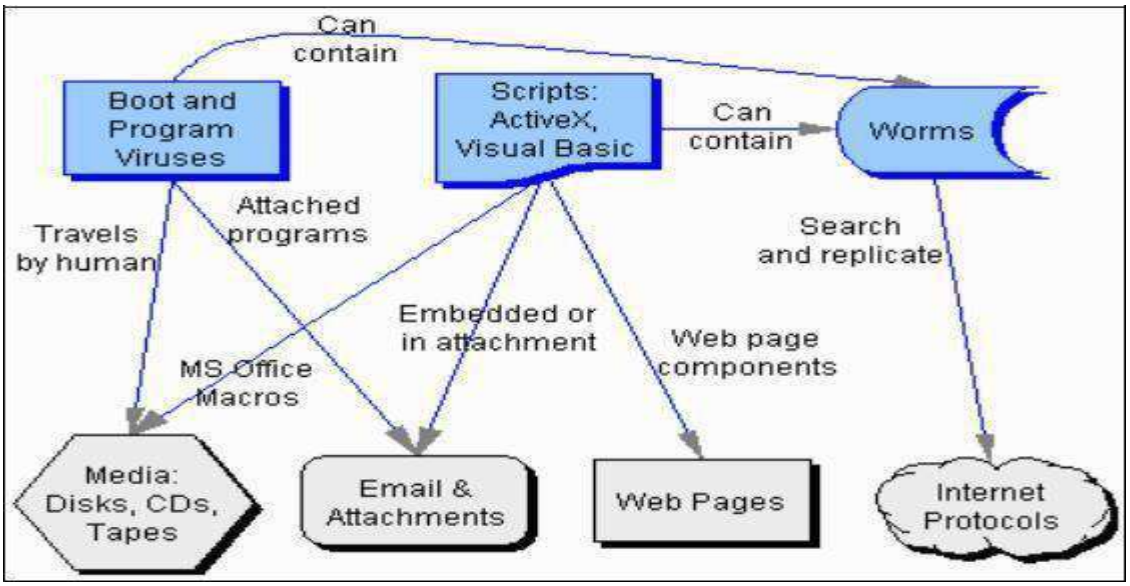

Figure 1.1: Web attacks

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

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.

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.

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

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.

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