THE 12 TYPES OF CYBER CRIME

There are literally a dozen ways in which a cybercrime can be perpetrated, and you need to know what they are

In order to protect yourself you need to know about the different ways in which your computer can be compromised and your privacy infringed. In this section, we discuss a few common tools and techniques employed by the cyber criminals. This isn't an exhaustive list by any means, but will give you a comprehensive idea of the loopholes in networks and security systems, which can be exploited by attackers, and also their possible motives for doing so.

1. Hacking

In simple words, hacking is an act committed by an intruder by accessing your computer system without your permission. Hackers (the people doing the 'hacking') are basically computer programmers, who have an advanced understanding of computers and commonly misuse this knowledge for devious reasons. They're usually technology buffs who have expert-level skills in one particular software program or language. As for motives, there could be several, but the most common are pretty simple and can be explained by a human tendency such as greed, fame, power, etc. Some people do it purely to show-off their expertise – ranging from relatively harmless activities such as modifying software (and even hardware) to carry out tasks that are outside the creator's intent, others just want to cause destruction.

Greed and sometimes voyeuristic tendencies may cause a hacker to break into systems to steal personal banking information, a corporation's financial data, etc. They also try and modify systems so hat they can execute tasks at their whims. Hackers displaying such destructive conduct are also called "Crackers" at times. they are also called "Black Hat" hackers On the other hand, there are those who develop an interest in computer hacking just out of intellectual curiosity. Some companies hire these computer enthusiasts to find flaws in their security systems and help fix them. Referred to as "White Hat" hackers, these guys are against the abuse of computer systems. They attempt to break into network systems purely to alert the owners of flaws. It's not always altruistic, though, because many do this for fame as well, in order to land jobs with top companies, or just to be termed as security experts. "Grey Hat" is another term used to refer to hacking activities that are a cross between black and white hacking.

Some of the most famous computer geniuses were once hackers who went on to use their skills for constructive technological development. Dennis Ritchie and Ken Thompson, the creators of the UNIX operating system (Linux's predecessor), were two of them. Shawn Fanning, the developer of Napster, Mark Zuckerberg of Facebook fame, and many more are also examples. The first step towards preventing hackers from gaining access to your systems is to learn how hacking is done. Of course it is beyond the scope of this Fast Track to go into great details, but we will cover the various techniques used by hackers to get to you via the internet.

a. SQL Injections: An SQL injection is a technique that allows hackers to play upon the security vulnerabilities of the software that runs a web site. It can be used to attack any type of unprotected or improperly protected SQL database. This process involves entering portions of SQL code into a web form entry field – most commonly usernames and passwords – to give the hacker further access to the site backend, or to a particular user's account. When you enter logon information into sign-in fields, this information is typically converted to an SQL command. This command checks the data you've entered against the relevant table in the database. If your input data matches the data in the table, you're granted access, if not, you get the kind of error you would have seen when you put in a wrong password. An SQL injection is usually an additional command that when inserted into the web form, tries to change the content of the database to reflect a successful login. It can also be used to retrieve information such as credit card numbers or passwords from unprotected sites.

b. Theft of FTP Passwords: This is another very common way to tamper with web sites. FTP password hacking takes advantage of the fact that many webmasters store their website login information on their poorly protected PCs. The thief searches the victim's system for FTP login details, and then relays them to his own remote computer. He then logs into the web site via the remote computer and modifies the web pages as he or she pleases.

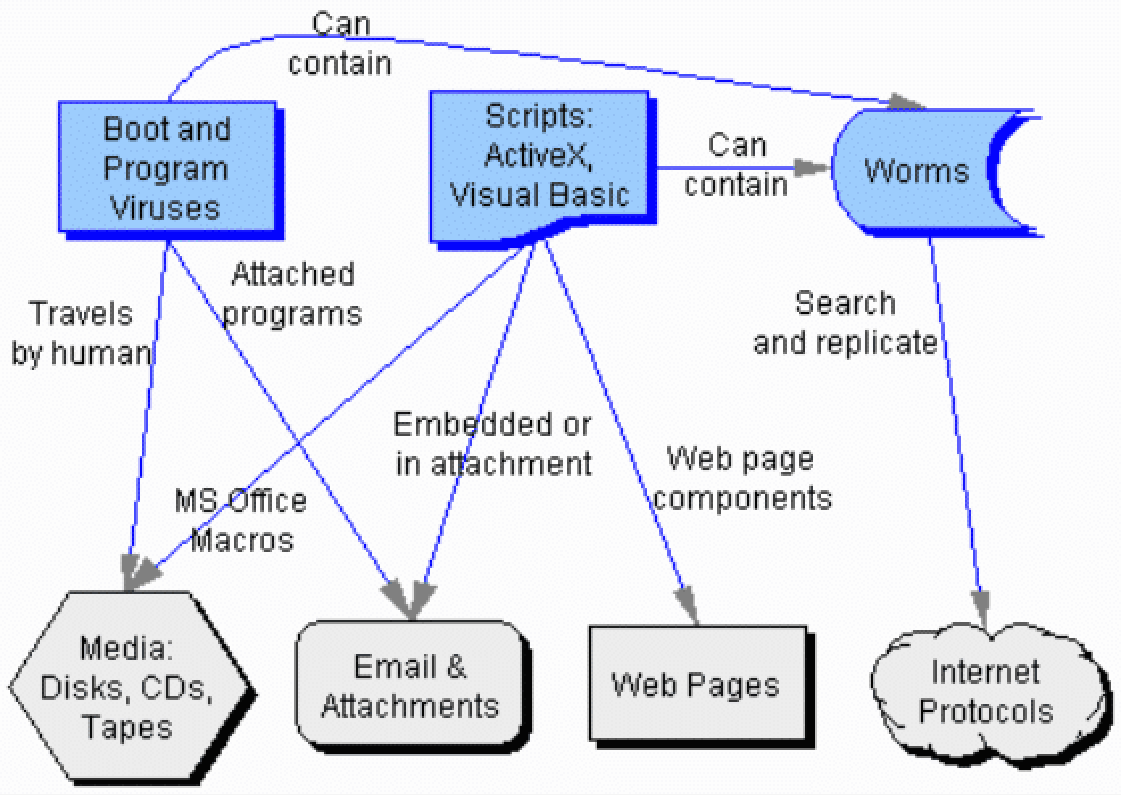
c. Cross-site scripting:

Also known as XSS (formerly CSS, but renamed due to confusion with cascading style sheets), is a very easy way of circumventing a security system. Cross-site scripting is a hard-to-find loophole in a web site, making it vulnerable to attack. In a typical XSS attack, the hacker infects a web page with a malicious client-side script or program. When you visit this web page, the script is automatically downloaded to your browser and executed. Typically, attackers inject HTML, JavaScript, VBScript, ActiveX or Flash into a vulnerable application to deceive you and gather confidential information. If you want to protect your PC from malicious hackers, investing in a good firewall should be first and foremost. Hacking is done through a network, so it's very important to stay safe while using the internet. You'll read more about safety tips in the last chapter of this book.

2. Virus dissemination

Viruses are computer programs that attach themselves to or infect a system or files, and have a tendency to circulate to other computers on a network. They disrupt the computer operation and affect the data stored – either by modifying it or by deleting it altogether. "Worms" unlike viruses don't need a host to cling on to. They merely replicate until they eat up all available memory in the system. The term "worm" is sometimes used to mean selfreplicating "malware" (MALicious softWARE). These terms are often used interchangeably in the context of the hybrid viruses/worms that dominatehe current virus scenario. "Trojan horses" are different from viruses in their manner of propagation.

They masquerade as a legitimate file, such as an email attachment from a supposed friend with a very believable name, and don't disseminate themselves. The user can also unknowingly install a Trojan-infected program via drive-by downloads when visiting a website, playing online games or using internet-driven applications. A Trojan horse can cause damage similar to other viruses, such as steal information or hamper/disrupt the functioning of computer systems.



A simple diagram to show how malware can propogate

How does this happen? Well, the malicious code or virus is inserted into the chain of command so that when the infected program is run, the viral code is also executed (or in some cases, runs instead of the legitimate program). Viruses are usually seen as extraneous code attached to a host program, but this isn't always the case. Sometimes, the environment is manipulated so that calling a legitimate uninfected program calls the viral program. The viral program may also be executed before any other program is run. This can virtually infect every executable file on the computer, even though none of those files' code was actually tampered with. Viruses that follow this modus operandi include “cluster” or “FAT” (File Allocation Table) viruses, which redirect system pointers to infected files, associate viruses and viruses that modify the Windows Registry directory entries so that their own code is executed before any other legitimate program.

Computer viruses usually spread via removable media or the internet. A flash disk, CD-ROM, magnetic tape or other storage device that has been in an infected computer infects all future computers in which it's used. Your computer can also contract viruses from sinister email attachments, rogue web sites or infected software. And these disseminate to every other computer on your network.

All computer viruses cause direct or indirect economic damages. Based on this, there are two categories of viruses:
1) Those that only disseminate and don't cause intentional damage
2) Those which are programmed to cause damage.

However, even by disseminating, they take up plenty of memory space, and time and resources that are spent on the clean-up job. Direct economic damages are caused when viruses alter the information during digital transmission. Considerable expenses are incurred by individuals, firms and authorities for developing and implementing the anti-virus tools to protect computer systems.

3. Logic bombs

A logic bomb, also known as “slag code”, is a malicious piece of code which is intentionally inserted into software to execute a malicious task when triggered by a specific event. It’s not a virus, although it usually behaves in a similar manner. It is stealthily inserted into the program where it lies dormant until specified conditions are met. Malicious software such as viruses and worms often contain logic bombs which are triggered at a specific payload or at a predefined time. The payload of a logic bomb is unknown to the user of the software, and the task that it executes unwanted. Program codes that are scheduled to execute at a particular time are known as “time-bombs”. For example, the infamous “Friday the 13th” virus which attacked the host systems only on specific dates; it “exploded” (duplicated itself) every Friday that happened to be the thirteenth of a month, thus causing system slowdowns.

Logic bombs are usually employed by disgruntled employees working in the IT sector. You may have heard of “disgruntled employee syndrome” wherein angry employees who’ve been fired use logic bombs to delete the databases of their employers, stultify the network for a while or even do insider trading. Triggers associated with the execution of logic bombs can be a specific date and time, a missing entry from a database or not putting in a command at the usual time, meaning the person doesn’t work there anymore. Most logic bombs stay only in the network they were employed in. So in most cases, they’re an insider job. This makes them easier to design and execute than a virus. It doesn’t need to replicate; which is a more complex job. To keep your network protected from the logic bombs, you need constant monitoring of the data and efficient anti-virus software on each of the computers in the network.

There’s another use for the type of action carried out in a logic bomb “explosion” – to make restricted software trials. The embedded piece of code destroys the software after a defined period of time or renders it unusable until the user pays for its further use. Although this piece of code uses the same technique as a logic bomb, it has a non-destructive, non-malicious and user-transparent use, and is not typically referred to as one.

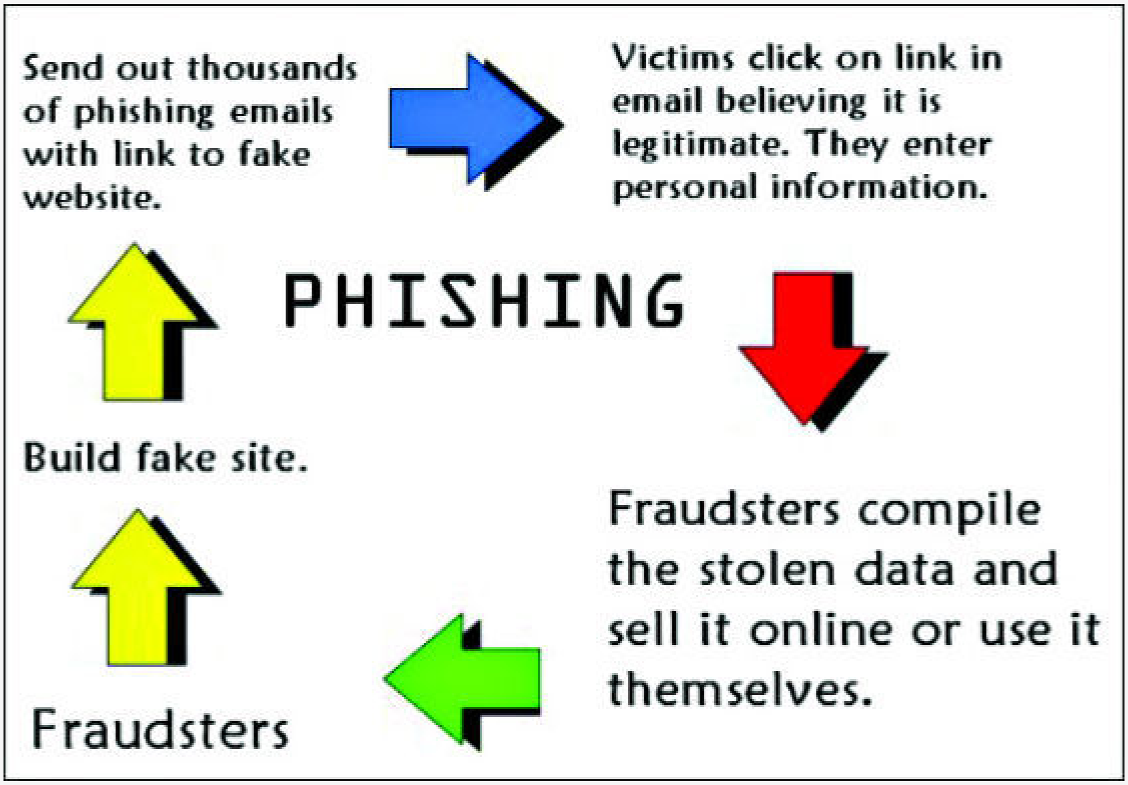
4. Denial-of-Service attack

A Denial-of-Service (DoS) attack is an explicit attempt by attackers to deny service to intended users of that service. It involves flooding a computer resource with more requests than it can handle consuming its available bandwidth which results in server overload. This causes the resource (e.g. a web server) to crash or slow down significantly so that no one can access it. Using this technique, the attacker can render a web site inoperable by sending massive amounts of traffic to the targeted site. A site may temporarily malfunction or crash completely, in any case resulting in inability of the system to communicate adequately. DoS attacks violate the acceptable use policies of virtually all internet service providers.

Another variation to a denial-of-service attack is known as a “Distributed Denial of Service” (DDoS) attack wherein a number of geographically widespread perpetrators flood the network traffic. Denial-of-Service attacks typically target high profile web site servers belonging to banks and credit card payment gateways. Websites of companies such as Amazon, CNN, Yahoo, Twitter and eBay! are not spared either.

5. Phishing

This a technique of extracting confidential information such as credit card numbers and username password combos by masquerading as a legitimate enterprise. Phishing is typically carried out by email spoofing. You’ve probably received email containing links to legitimate appearing websites. You probably found it suspicious and didn’t click the link. Smart move.


Send out thousands of phishing emails with link to fake website.
Victims click on link in email believing it is legitimate. They enter personal information.
PHISHING
Build fake site.
Fraudsters compile the stolen data and sell it online or use it themselves.
Fraudsters

How phishing can net some really interesting catches

The malware would have installed itself on your computer and stolen private information. Cyber-criminals use social engineering to trick you into downloading malware off the internet or make you fill in your personal information under false pretenses. A phishing scam in an email message can be evaded by keeping certain things in mind.

- Look for spelling mistakes in the text. Cyber-criminals are not known for their grammar and spelling.
- Hover your cursor over the hyperlinked URL but don’t click. Check if the address matches with the one written in the message.

- Watch out for fake threats. Did you receive a message saying “Your email account will be closed if you don’t reply to this email”? They might trick you by threatening that your security has been compromised.
- Attackers use the names and logos of well-known web sites to deceive you. The graphics and the web addresses used in the email are strikingly similar to the legitimate ones, but they lead you to phony sites.

Not all phishing is done via email or web sites. Vishing (voice phishing) involves calls to victims using fake identity fooling you into considering the call to be from a trusted organisation. They may claim to be from a bank asking you to dial a number (provided by VoIP service and owned by attacker) and enter your account details. Once you do that, your account security is compromised. Treat all unsolicited phone calls with skepticism and never provide any personal information. Many banks have issued preemptive warnings informing their users of phishing scams and the do’s and don’ts regarding your account information. Those of you reading Digit for long enough will remember that we successfully phished hundreds of our readers by reporting a way to hack other people’s gmail accounts by sending an email to a made up account with your own username and password… and we did that years ago in a story about , yes, you guessed it, phishing!

6. Email bombing and spamming

Email bombing is characterised by an abuser sending huge volumes of email to a target address resulting in victim’s email account or mail servers crashing. The message is meaningless and excessively long in order to consume network resources. If multiple accounts of a mail server are targeted, it may have a denial-of-service impact. Such mail arriving frequently in your inbox can be easily detected by spam filters. Email bombing is commonly carried out using botnets (private internet connected computers whose security has been compromised by malware and under the attacker’s control) as a DDoS attack.

This type of attack is more difficult to control due to multiple source addresses and the bots which are programmed to send different messages to defeat spam filters. “Spamming” is a variant of email bombing. Here unsolicited bulk messages are sent to a large number of users, indiscriminately. Opening links given in spam mails may lead you to phishing web sites hosting malware. Spam mail may also have infected files as attachments. Email spamming worsens when the recipient replies to the email causing all the original addressees to receive the reply. Spammers collect email addresses from customer lists, newsgroups, chat-rooms, web sites and viruses which harvest users’ address books, and sell them to other spammers as well. A large amount of spam is sent to invalid email addresses.

Email filters cleaning out spam mail

Sending spam violates the acceptable use policy (AUP) of almost all internet service providers. If your system suddenly becomes sluggish (email loads slowly or doesn’t appear to be sent or received), the reason may be that your mailer is processing a large number of messages. Unfortunately, at this time, there’s no way to completely prevent email bombing and spam mails as it’s impossible to predict the origin of the next attack. However, what you can do is identify the source of the spam mails and have your router configured to block any incoming packets from that address.

7. Web jacking

Web jacking derives its name from “hijacking”. Here, the hacker takes control of a web site fraudulently. He may change the content of the original site or even redirect the user to another fake similar looking page controlled by him. The owner of the web site has no more control and the attacker may use the web site for his own selfish interests. Cases have been reported where the attacker has asked for ransom, and even posted obscene material on the site.

The web jacking method attack may be used to create a clone of the web site, and present the victim with the new link saying that the site has moved. Unlike usual phishing methods, when you hover your cursor over the link provided, the URL presented will be the original one, and not the attacker’s site. But when you click on the new link, it opens and is quickly replaced with the malicious web server. The name on the address bar will be slightly different from the original website that can trick the user into thinking it’s a legitimate site. For example, “gmail” may direct you to “gmai1”. Notice the one in place of ‘L’. It can be easily overlooked.

Web jacking can also be done by sending a counterfeit message to the registrar controlling the domain name registration, under a false identity asking him to connect a domain name to the webjacker’s IP address, thus sending unsuspecting consumers who enter that particular domain name to a website controlled by the webjacker. The purpose of this attack is to try to harvest the credentials, usernames, passwords and account numbers of users by using a fake web page with a valid link which opens when the user is redirected to it after opening the legitimate site.

8. Cyber stalking

Cyber stalking is a new form of internet crime in our society when a person is pursued or followed online. A cyber stalker doesn’t physically follow his victim; he does it virtually by following his online activity to harvest information about the stalkee and harass him or her and make threats using verbal intimidation. It’s an invasion of one’s online privacy.

Cyber stalking uses the internet or any other electronic means and is different from offline stalking, but is usually accompanied by it. Most victims of this crime are women who are stalked by men and children who are stalked by adult predators and pedophiles. Cyber stalkers thrive on inexperienced web users who are not well aware of netiquette and the rules of internet safety. A cyber stalker may be a stranger, but could just as easily be someone you know.

Cyber stalkers harass their victims via email, chat rooms, web sites, discussion forums and open publishing web sites (e.g. blogs). The availability of free email / web site space and the anonymity provided by chat rooms and forums has contributed to the increase of cyber stalking incidents. Everyone has an online presence nowadays, and it’s really easy to do a Google search and get one’s name, alias, contact number and address, contributing to the menace that is cyber stalking. As the internet is increasingly becoming an integral part of our personal and professional lives, stalkers can take advantage of the ease of communications and the availability of personal information only a few mouse clicks away. In addition, the anonymous and non-confrontational nature of internet communications further tosses away any disincentives in the way of cyber stalking. Cyber stalking is done in two primary ways:

- **Internet Stalking:** Here the stalker harasses the victim via the internet. Unsolicited email is the most common way of threatening someone, and the stalker may even send obscene content and viruses by email. However, viruses and unsolicited telemarketing email alone do not constitute cyber stalking. But if email is sent repeatedly in an attempt to intimidate the recipient, they may be considered as stalking. Internet stalking is not limited to email; stalkers can more comprehensively use the internet to harass the victims. Any other cyber-crime that we’ve already read about, if done with an intention to threaten, harass, or slander the victim may amount to cyber stalking.

- **Computer Stalking:** The more technologically advanced stalkers apply their computer skills to assist them with the crime. They gain unauthorised control of the victim’s computer by exploiting the working of the internet and the Windows operating system. Though this is usually done by proficient and computer savvy stalkers, instructions on how to accomplish this are easily available on the internet.

Cyber stalking has now spread its wings to social networking. With the increased use of social media such as Facebook, Twitter, Flickr and YouTube, your profile, photos, and status updates are up for the world to see. Your online presence provides enough information for you to become a potential victim of stalking without even being aware of the risk. With the “check-ins”, the “life-events”, apps which access your personal information and the need to put up just about everything that you’re doing and where you’re doing it, one doesn’t really leave anything for the stalkers to figure out for themselves. Social networking technology provides a social and collaborative platform for internet users to interact, express their thoughts and share almost everything about their lives. Though it promotes socialisation amongst people, along the way it contributes to the rise of internet violations.

9. Data diddling

Data Diddling is unauthorised altering of data before or during entry into a computer system, and then changing it back after processing is done. Using this technique, the attacker may modify the expected output and is difficult to track. In other words, the original information to be entered is changed, either by a person typing in the data, a virus that’s programmed to change the data, the programmer of the database or application, or anyone else involved in the process of creating, recording, encoding, examining, checking, converting or transmitting data.

This is one of the simplest methods of committing a computer-related crime, because even a computer amateur can do it. Despite this being an effortless task, it can have detrimental effects. For example, a person responsible for accounting may change data about themselves or a friend or relative showing that they're paid in full. By altering or failing to enter the information, they're able to steal from the enterprise. Other examples include forging or counterfeiting documents and exchanging valid computer tapes or cards with prepared replacements. Electricity boards in India have been victims of data diddling by computer criminals when private parties were computerizing their systems.

10. Identity Theft and Credit Card Fraud

Identity theft occurs when someone steals your identity and pretends to be you to access resources such as credit cards, bank accounts and other benefits in your name. The imposter may also use your identity to commit other crimes. "Credit card fraud" is a wide ranging term for crimes involving identity theft where the criminal uses your credit card to fund his transactions. Credit card fraud is identity theft in its simplest form. The most common case of credit card fraud is your pre-approved card falling into someone else's hands.

Credit card fraud is the most common way for hackers to steal yoiur money

He can use it to buy anything until you report to the authorities and get your card blocked. The only security measure on credit card purchases is the signature on the receipt but that can very easily be forged. However, in some countries the merchant may even ask you for an ID or a PIN. Some credit card companies have software to estimate the probability of fraud. If an unusually large transaction is made, the issuer may even call you to verify.

Often people forget to collect their copy of the credit card receipt after eating at restaurants or elsewhere when they pay by credit card. These receipts have your credit card number and your signature for anyone to see and use. With only this information, someone can make purchases online or by phone. You won't notice it until you get your monthly statement, which is why you should carefully study your statements. Make sure the website is trustworthy and secure when shopping online. Some hackers may get a hold of your credit card number by employing phishing techniques. Sometimes a tiny padlock icon appears on the left screen corner of the address bar on your browser which provides a higher level of security for data transmission. If you click on it, it will also tell you the encryption software it uses.

A more serious concern is the use of your personal information with the help of stolen or fake documents to open accounts (or even worse, using your existing account) to take a loan in your name. These unscrupulous people can collect your personal details from your mailbox or trash can (remember to shred all sensitive documents). Think of all the important details printed on those receipts, pay stubs and other documents. You won't know a thing until the credit card people track you down and tail you until you clear all your dues. Then for months and months you'll be fighting to get your credit restored and your name cleared.

With rising cases of credit card fraud, many financial institutions have stepped in with software solutions to monitor your credit and guard your identity. ID theft insurance can be taken to recover lost wages and restore your credit. But before you spend a fortune on these services, apply the no-cost, common sense measures to avert such a crime.

11. Salami slicing attack

A "salami slicing attack" or "salami fraud" is a technique by which cyber-criminals steal money or resources a bit at a time so that there's no noticeable difference in overall size. The perpetrator gets away with these little pieces from a large number of resources and thus accumulates a considerable amount over a period of time. The essence of this method is the failure to detect the misappropriation. The most classic approach is "collect-the-roundoff" technique. Most calculations are carried out in a particular currency are rounded off up to the nearest number about half the time and down the rest of the time. If a programmer decides to collect these excess fractions of rupees to a separate account, no net loss to the system seems apparent. This is done by carefully transferring the funds into the perpetrator's account.

Attackers insert a program into the system to automatically carry out the task. Logic bombs may also be employed by unsatisfied greedy employees who exploit their know-how of the network and/or privileged access to the system. In this technique, the criminal programs the arithmetic calculators to automatically modify data, such as in interest calculations.

Stealing money electronically is the most common use of the salami slicing technique, but it's not restricted to money laundering. The salami technique can also be applied to gather little bits of information over a period of time to deduce an overall picture of an organisation. This act of distributed information gathering may be against an individual or an organisation. Data can be collected from web sites, advertisements, documents collected from trash cans, and the like, gradually building up a whole database of factual intelligence about the target.

Since the amount of misappropriation is just below the threshold of perception, we need to be more vigilant. Careful examination of our assets, transactions and every other dealing including sharing of confidential information with others might help reduce the chances of an attack by this method.

12. Software Piracy

Thanks to the internet and torrents, you can find almost any movie, software or song from any origin for free. Internet piracy is an integral part of our lives which knowingly or unknowingly we all contribute to. This way, the profits of the resource developers are being cut down. It's not just about using someone else's intellectual property illegally but also passing it on to your friends further reducing the revenue they deserve.

Piracy is rampant in India, but you knew that

Software piracy is the unauthorised use and distribution of computer software. Software developers work hard to develop these programs, and piracy curbs their ability to generate enoughrevenue to sustain application development. This affects the whole global economy as funds are relayed from other sectors which results in less investment in marketing and research.

The following constitute software piracy:

- Loading unlicensed software on your PC
- Using single-licensed software on multiple computers
- Using a key generator to circumvent copy protection
- Distributing a licensed or unlicensed ("cracked") version of software over the internet and offline

"Cloning" is another threat. It happens when someone copies the idea behind your software and writes his own code. Since ideas are not copy protected across borders all the time, this isn't strictly illegal. A software "crack" is an illegally obtained version of the software which works its way around the encoded copy prevention. Users of pirated software may use a key generator to generate a "serial" number which unlocks an evaluation version of the software, thus defeating the copy protection. Software cracking and using unauthorised keys are illegal acts of copyright infringement.

Using pirated material comes with its own risks. The pirated software may contain Trojans, viruses, worms and other malware, since pirates will often infect software with malicious code. Users of pirated software may be punished by the law for illegal use of copyrighted material. Plus you won't get the software support that is provided by the developers.

To protect your software from piracy if you're a developer, you should apply strong safeguards. Some websites sell software with a "digital fingerprint" that helps in tracing back the pirated copies to the source. Another common method is hardware locking. Using this, the software license is locked to a specific computer hardware, such that it runs only on that computer. Unfortunately, hackers continue to find their way around these measures.

13. Others

So far we've discussed the dedicated methods of committing cyber crimes. In a nutshell, any offence committed using electronic means such as net extortion, cyber bullying, child pornography and internet fraud is termed as cyber crime. The internet is a huge breeding ground for pornography, which has often been subject to censorship on grounds of obscenity. But what may be considered obscene in India, might not be considered so in other countries.

Since every country has a different legal stand on this subject matter, pornography is rampant online. However, according to the Indian Constitution, largely, pornography falls under the category of obscenity and is punishable by law. Child pornography is a serious offence, and can attract the harshest punishments provided for by law. Pedophiles lurk in chat rooms to lure children. The internet allows long-term victimisation of such children, because the pictures once put up, spread like wild-fire, and may never get taken down completely. Internet crimes against children are a matter of grave concern, and are being addressed by the authorities, but this problem has no easy solution.