PSYCHOLOGY OF CRIME – II

Unit V

CYBER-CRIME

Subject Name	Subject Code	Prepared by
Psychology of Crime	18BPS63C	Dr. B. Selvaraj, M.A, M.Phil, Ph.D Dept. of Psychology Mob- 9442766594

CYBER-CRIME:

Cybercrime is criminal activity that either targets or uses a computer, a computer network or a networked device. Most, but not all, cybercrime is committed by cybercriminals or hackers who want to make money. Cybercrime is carried out by individuals or organizations.

There are literally a dozen ways in which a cybercrime can be perpetrated, and 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.

Types of cybercrime:

- ✓ Email and internet fraud.
- ✓ Identity fraud (where personal information is stolen and used).
- ✓ Theft of financial or card payment data.
- ✓ Theft and sale of corporate data.
- ✓ Cyberextortion (demanding money to prevent a threatened attack).
- ✓ Ransomware attacks (a type of cyberextortion).
- ✓ Cryptojacking (where hackers mine cryptocurrency using resources they do not own).
- ✓ Cyberespionage (where hackers access government or company data).

Most cybercrime falls under two main categories:

- Criminal activity that uses computers to commit other crimes.

- Cybercrime that targets computers often involves viruses and other types of malware.

CYBER ATTACKS:

A cyber attack is any type of offensive action that targets computer information systems, infrastructures, computer networks or personal computer devices, using various methods to steal, alter or destroy data or information systems.

1. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks

A denial-of-service attack overwhelms a system's resources so that it cannot respond to service requests. A DDoS attack is also an attack on system's resources, but it is launched from a large number of other host machines that are infected by malicious software controlled by the attacker.

Unlike attacks that are designed to enable the attacker to gain or increase access, denial-of-service doesn't provide direct benefits for attackers. For some of them, it's enough to have the satisfaction of service denial. However, if the attacked resource belongs to a business competitor, then the benefit to the attacker may be real enough. Another purpose of a DoS attack can be to take a system offline so that a different kind of attack can be launched. One common example is session hijacking, which I'll describe later.

There are different types of DoS and DDoS attacks; the most common are TCP SYN flood attack, teardrop attack, smurf attack, ping-of-death attack and botnets.

TCP SYN flood attack

In this attack, an attacker exploits the use of the buffer space during a Transmission Control Protocol (TCP) session initialization handshake. The attacker's device floods the target system's small in-process queue with connection requests, but it does not respond when the target system replies to those requests. This causes the target system to time out while waiting for the response from the attacker's device, which makes the system crash or become unusable when the connection queue fills up.

There are a few countermeasures to a TCP SYN flood attack:

- Place servers behind a firewall configured to stop inbound SYN packets.
- Increase the size of the connection queue and decrease the timeout on open connections.

Teardrop attack

This attack causes the length and fragmentation offset fields in sequential Internet Protocol (IP) packets to overlap one another on the attacked host; the attacked system attempts to reconstruct packets during the process but fails. The target system then becomes confused and crashes.

If users don't have patches to protect against this DoS attack, disable SMBv2 and block ports 139 and 445.

Smurf attack

This attack involves using IP spoofing and the ICMP to saturate a target network with traffic. This attack method uses ICMP echo requests targeted at broadcast IP addresses. These ICMP requests originate from a spoofed "victim" address. For instance, if the intended victim address is 10.0.0.10, the attacker would spoof an ICMP echo request from 10.0.0.10 to the broadcast address 10.255.255.255. This request would go to all IPs in the range, with all the responses going back to 10.0.0.10, overwhelming the network. This process is repeatable, and can be automated to generate huge amounts of network congestion.

To protect your devices from this attack, you need to disable IP-directed broadcasts at the routers. This will prevent the ICMP echo broadcast request at the network devices. Another option would be to configure the end systems to keep them from responding to ICMP packets from broadcast addresses.

Ping of death attack

This type of attack uses IP packets to 'ping a target system with an IP size over the maximum of 65,535 bytes. IP packets of this size are not allowed, so attacker fragments the IP packet. Once the target system reassembles the packet, it can experience buffer overflows and other crashes.

Ping of death attacks can be blocked by using a firewall that will check fragmented IP packets for maximum size.

Botnets

Botnets are the millions of systems infected with malware under hacker control in order to carry out DDoS attacks. These bots or zombie systems are used to carry out attacks against the target systems, often overwhelming the target system's bandwidth and processing capabilities. These DDoS attacks are difficult to trace because botnets are located in differing geographic locations.

2. Man-in-the-middle (MitM) attack

A MitM attack occurs when a hacker inserts itself between the communications of a client and a server. Here are some common types of man-in-the-middle attacks:

Session hijacking

In this type of MitM attack, an attacker hijacks a session between a trusted client and network server. The attacking computer substitutes its IP address for the trusted client while the server continues the session, believing it is communicating with the client. For instance, the attack might unfold like this:

1. A client connects to a server.
2. The attacker's computer gains control of the client.
3. The attacker's computer disconnects the client from the server.
4. The attacker's computer replaces the client's IP address with its own IP address and spoofs the client's sequence numbers.
5. The attacker's computer continues dialog with the server and the server believes it is still communicating with the client.

Replay

A replay attack occurs when an attacker intercepts and saves old messages and then tries to send them later, impersonating one of the participants. This type can be easily countered with session timestamps or nonce (a random number or a string that changes with time).

Currently, there is no single technology or configuration to prevent all MitM attacks. Generally, encryption and digital certificates provide an effective safeguard against MitM attacks, assuring both the confidentiality and integrity of communications. But a man-in-the-middle attack can be injected into the middle of communications in such a way that encryption will not help — for example, attacker "A" intercepts public key of person "P" and substitute it with his own public key. Then, anyone wanting to send an encrypted message to P using P's public key is unknowingly using A's public key. Therefore, A can read the message intended for P and then send the message to P, encrypted in P's real public key, and P will never notice that the message was compromised. In addition, A could also modify the message before resending it to P. As you can see, P is using encryption and thinks that his information is protected but it is not, because of the MitM attack.

3. Phishing and spear phishing attacks

Phishing attack is the practice of sending emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something. It combines social engineering and technical trickery. It could involve an attachment to an email that loads malware onto your computer. It could also be a link to an illegitimate website that can trick you into downloading malware or handing over your personal information.

Spear phishing is a very targeted type of phishing activity. Attackers take the time to conduct research into targets and create messages that are personal and relevant. Because of this, spear phishing can be very hard to identify and even harder to defend against. One of the simplest

ways that a hacker can conduct a spear phishing attack is email spoofing, which is when the information in the “From” section of the email is falsified, making it appear as if it is coming from someone you know, such as your management or your partner company. Another technique that scammers use to add credibility to their story is website cloning — they copy legitimate websites to fool you into entering personally identifiable information (PII) or login credentials.

To reduce the risk of being phished, you can use these techniques:

- **Critical thinking** — Do not accept that an email is the real deal just because you’re busy or stressed or you have 150 other unread messages in your inbox. Stop for a minute and analyze the email.
- **Hovering over the links** — Move your mouse over the link, but **do not click it**! Just let your mouse cursor h over over the link and see where would actually take you. Apply critical thinking to decipher the URL.
- **Analyzing email headers** — Email headers define how an email got to your address. The “Reply-to” and “Return-Path” parameters should lead to the same domain as is stated in the email.
- **Sandboxing** — You can test email content in a sandbox environment, logging activity from opening the attachment or clicking the links inside the email.

4. Drive-by attack

Drive-by download attacks are a common method of spreading malware. Hackers look for insecure websites and plant a malicious script into HTTP or PHP code on one of the pages. This script might install malware directly onto the computer of someone who visits the site, or it might re-direct the victim to a site controlled by the hackers. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window. Unlike many other types of cyber security attacks, a drive-by doesn’t rely on a user to do anything to actively enable the attack — you don’t have to click a download button or open a malicious email attachment to become infected. A drive-by download can take advantage of an app, operating system or web browser that contains security flaws due to unsuccessful updates or lack of updates.

To protect yourself from drive-by attacks, you need to keep your browsers and operating systems up to date and avoid websites that might contain malicious code. Stick to the sites you normally use — although keep in mind that even these sites can be hacked. Don’t keep too many unnecessary programs and apps on your device. The more plug-ins you have, the more vulnerabilities there are that can be exploited by drive-by attacks.

5. Password attack

Because passwords are the most commonly used mechanism to authenticate users to an information system, obtaining passwords is a common and effective attack approach. Access to a person's password can be obtained by looking around the person's desk, ''sniffing'' the connection to the network to acquire unencrypted passwords, using social engineering, gaining access to a password database or outright guessing. The last approach can be done in either a random or systematic manner:

- **Brute-force** password guessing means using a random approach by trying different passwords and hoping that one work Some logic can be applied by trying passwords related to the person's name, job title, hobbies or similar items.
- In a **dictionary attack,** a dictionary of common passwords is used to attempt to gain access to a user's computer and network. One approach is to copy an encrypted file that contains the passwords, apply the same encryption to a dictionary of commonly used passwords, and compare the results.

In order to protect yourself from dictionary or brute-force attacks, you need to implement an account lockout policy that will lock the account after a few invalid password attempts. You can follow these in order to set it up correctly.

6. SQL injection attack

SQL injection has become a common issue with database-driven websites. It occurs when a malefactor executes a SQL query to the database via the input data from the client to server. SQL commands are inserted into data-plane input (for example, instead of the login or password) in order to run predefined SQL commands. A successful SQL injection exploit can read sensitive data from the database, modify (insert, update or delete) database data, execute administration operations (such as shutdown) on the database, recover the content of a given file, and, in some cases, issue commands to the operating system.

7. Cross-site scripting (XSS) attack

XSS attacks use third-party web resources to run scripts in the victim's web browser or scriptable application. Specifically, the attacker injects a payload with malicious JavaScript into a website's database. When the victim requests a page from the website, the website transmits the page, with the attacker's payload as part of the HTML body, to the victim's browser, which executes the malicious script. For example, it might send the victim's cookie to the attacker's server, and the attacker can extract it and use it for session hijacking. The most dangerous consequences occur when XSS is used to exploit additional vulnerabilities. These vulnerabilities

can enable an attacker to not only steal cookies, but also log key strokes, capture screenshots, discover and collect network information, and remotely access and control the victim's machine.

8. Eavesdropping attack

Eavesdropping attacks occur through the interception of network traffic. By eavesdropping, an attacker can obtain passwords, credit card numbers and other confidential information that a user might be sending over the network. Eavesdropping can be passive or active:

- **Passive eavesdropping** — A hacker detects the information by listening to the message transmission in the network.
- **Active eavesdropping** — A hacker actively grabs the information by disguising himself as friendly unit and by sending queries to transmitters. This is called probing, scanning or tampering.

Detecting passive eavesdropping attacks is often more important than spotting active ones, since active attacks requires the attacker to gain knowledge of the friendly units by conducting passive eavesdropping before.

9. Birthday attack

Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature. A message processed by a hash function produces a message digest (MD) of fixed length, independent of the length of the input message; this MD uniquely characterizes the message. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. If an attacker calculates same MD for his message as the user has, he can safely replace the user's message with his, and the receiver will not be able to detect the replacement even if he compares MDs.

10. Malware attack

Malicious software can be described as unwanted software that is installed in your system without your consent. It can attach itself to legitimate code and propagate; it can lurk in useful applications or replicate itself across the Internet. Here are some of the most common types of malware:

- **Macro viruses** — These viruses infect applications such as Microsoft Word or Excel. Macro viruses attach to an application's initialization sequence. When the application is opened, the virus executes instructions before transferring control to the application. The virus replicates itself and attaches to other code in the computer system.

- **File infectors** — File infector viruses usually attach themselves to executable code, such as .exe files. The virus is installed when the code is loaded. Another version of a file infector associates itself with a file by creating a virus file with the same name, but an .exe extension. Therefore, when the file is opened, the virus code will execute.

- **System or boot-record infectors** — A boot-record virus attaches to the master boot record on hard disks. When the system is started, it will look at the boot sector and load the virus into memory, where it can propagate to other disks and computers.

- **Polymorphic viruses** — These viruses conceal themselves through varying cycles of encryption and decryption. The encrypted virus and an associated mutation engine are initially decrypted by a decryption program. The virus proceeds to infect an area of code. The mutation engine then develops a new decryption routine and the virus encrypts the mutation engine and a copy of the virus with an algorithm corresponding to the new decryption routine. The encrypted package of mutation engine and virus is attached to new code, and the process repeats. Such viruses are difficult to detect but have a high level of entropy because of the many modifications of their source code. Anti-virus software or free tools like Process Hacker can use this feature to detect them.

- **Stealth viruses** — Stealth viruses take over system functions to conceal themselves. They do this by compromising malware detection software so that the software will report an infected area as being uninfected. These viruses conceal any increase in the size of an infected file or changes to the file's date and time of last modification.

- **Trojans** — A Trojan or a Trojan horse is a program that hides in a useful program and usually has a malicious function. A major difference between viruses and Trojans is that Trojans do not self-replicate. In addition to launching attacks on a system, a Trojan can establish a back door that can be exploited by attackers. For example, a Trojan can be programmed to open a high-numbered port so the hacker can use it to listen and then perform an attack.

- **Logic bombs** — A logic bomb is a type of malicious software that is appended to an application and is triggered by a specific occurrence, such as a logical condition or a specific date and time.

- **Worms** — Worms differ from viruses in that they do not attach to a host file, but are self-contained programs that propagate across networks and computers. Worms are commonly spread through email attachments; opening the attachment activates the worm program. A typical worm exploit involves the worm sending a copy of itself to every contact in an infected computer's email address In addition to conducting malicious activities, a worm spreading across the internet and overloading email servers can result in denial-of-service attacks against nodes on the network.

- **Droppers** — A dropper is a program used to install viruses on computers. In many instances, the dropper is not infected with malicious code and, therefore might not be detected by virus-scanning software. A dropper can also connect to the internet and download updates to virus software that is resident on a compromised system.

- **Ransomware** — Ransomware is a type of malware that blocks access to the victim's data and threatens to publish or delete it unless a ransom is paid. While some simple computer ransomware can lock the system in a way that is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, which encrypts the victim's files in a way that makes them nearly impossible to recover without the decryption key.

- Adware — Adware is a software application used by companies for marketing purposes; advertising banners are displayed while any program is running. Adware can be automatically downloaded to your system while browsing any website and can be viewed through pop-up windows or through a bar that appears on the computer screen automatically.

- Spyware — Spyware is a type of program that is installed to collect information about users, their computers or their browsing habits. It tracks everything you do without your knowledge and sends the data to a remote user. It also can download and install other malicious programs from the internet. Spyware works like adware but is usually a separate program that is installed unknowingly when you install another freeware application.

ARGOT OF COMPUTER CRIME

Hackers are those who break into someone else's computer system,

There are three main types:-

- ✓ ***Black-hat hackers***
  Black Hat hackers are criminals who break into computer networks with malicious intent. They may also release malware that destroys files, holds computers hostage, or steals passwords, credit card numbers, and other personal information.

- ✓ ***White-hat hackers***
  A **white hat** hacker evaluates the security posture of an organization by identifying potential vulnerabilities. These professionals fortify a firm's security before a hacker can exploit the existing flaws. **White hat hackers** are also known as ethical **hackers**

- ✓ ***Gray-hat hackers***

A **grey hat** (greyhat or **gray hat**) is a computer hacker or computer security expert who may sometimes violate laws or typical ethical standards, but does not have the malicious intent typical of a black **hat** hacker

Providing parents an understanding of predator's methods helps parents protect their children. A predator's goal is to lure and manipulate a child into believing they care for your child more than his or her parents or family. An Internet predator creates a fictitious online personality that emotionally replaces the trusted parent or guardian in a child's mind. The tragedy of Internet victims is that they are not only physically and emotionally harmed, but they also harbor feelings of guilt and shame because in many instances they have willfully met their "fictitious friend".

METHODS OF ONLINE PREDATORS:

Grooming

Predators view the process of finding and tracking down a child as a hunt and a game. They spend a lot of time, over many months, breaking down barriers to get the child to feel comfortable enough to divulge personal information. We refer to this process as "grooming."

Grooming includes fishing, mirroring, luring, and any other means by which a predator prepares a child to become a victim. Predators develop relationships by offering whatever a child seems to need, emotionally or literally luring them with gifts. Some children who are sad, bored, or lonely will turn to the Internet to have an emotional need met. These children are particularly vulnerable to "grooming" and need to internalize the importance of protecting their personal information.

Fishing

Personal information is much more than just a name, address, or phone number—it includes anything that lets a predator know something specific about the child: the name of their school, soccer team, favorite professional sports team, or specialized hobbies. An online predator will "fish" for information by asking basic questions, followed by more specific questions.

A combination of unrelated bits of information can direct a predator to a very narrow area. For example:

With these two pieces of information, a predator can check specific weather maps and narrow down the child's possible location to a very small area. The predator will then search for details

about the area in an attempt to draw more out of the child. When the predator's area is small enough, a simple detail such as, "My teacher won't let me climb the big willow tree," can be enough for the predator to find the child.

Parks and schools and their surrounding areas are favorite places for predators to make contact with children; if possible, predators avoid a child's home and street—where they are more easily identified as out of place. In some tragic cases, children were victimized during recess and returned to the playground before anyone knew the child was missing.

Mirroring

Online predators are skilled in playing back emotionally what they see in the child. This "mirroring" creates an illusion of camaraderie designed to break down the barriers of "stranger danger." For example, if a child is lonely, the predator mirrors that emotion and tries to fill the void by telling the child that he understands how it feels to be lonely and that he would like to be his/her friend. Predators mimic the child's emotional language and play back the emotions they see in an attempt to diminish his or her inhibitions.

PREDICTIVE OF CRIME:

Predictive policing involves using algorithms to analyze massive amounts of information in order to **predict** and help prevent potential future **crimes**. Place-based **predictive** policing, the most widely practiced method, typically uses preexisting **crime** data to identify places and times that have a high risk of **crime**

Eight future cyber crimes that could affect you in the not-so-distant future:

Cyber-Jacking. Why bother physically hijacking a plane, when you can simply cyber-jack it? The mysterious disappearance of Malaysian Air flight 370 had some speculating that it might have been hacked, and while that's unrealistic in this case, future attacks probably will leverage some type of cyber attack to pull it off.

This could range from exploiting the plane's flight management system (as demonstrated by researcher Hugo Teso last year), to attacking ground-based systems that the plane relies on, spoofing or interfering with air traffic control transmissions or infecting the air traffic control system with fake "ghost" planes and making real planes disappear (as discovered by researcher Brad 'Renderman' Haines in 2012).

Human Malware - There's a good chance that at some point in the near future, humans will be infected with malware. How could this happen? If you rely on a WiFi-enabled medical implant (e.g., pacemaker, cardioverter-defibrillator, insulin pump, etc.), your body could be physically harmed by a cyber attack on that device. Researchers have already demonstrated that it's possible for a determined hacker to break into your implant and hurt or kill you. But down the road, this threat could become even easier to distribute. New research released earlier this year by the University of Liverpool found that it's possible to spread computer viruses via WiFi routers. Infected WiFi routers could pose a serious long-term risk - particularly with implant patients. In the future, a compromised WiFi network (at a hospital or the Starbucks across the street) could be used to spread medical viruses to patients.

Cyber Assault - As networked appliances, home automation systems and wearables become more widespread, hackers will have another way to invade your life - and physically harm you. Because all of these rely on basic operating systems or firmware to work properly and are connected to the Internet, they can be remotely controlled by hackers - as has been demonstrated already by numerous researchers, including a home appliance 'botnet' recently discovered by one security firm. These attacks could include things like raising or lowering the thermostat, shutting off or malfunctioning appliances (like turning off the refrigerator or bypassing the temperature restriction on the water heater), causing wearables to overheat or making augmented reality glasses flicker bright blinding lights in your eyes. In most cases, these wouldn't put a person's life at risk, but they could cause physical harm, not to mention make you feel unsafe in your own home. Consider this cyber-stalking taken to the next level.

Cyber Extortion. With so much of our personal lives, work and finances tied up in online accounts, anyone who's able to take over those accounts is in a great position to demand a ransom payment.

"Ransomware" attacks are already taking place throughout Europe and, more recently, in the U.S. with the so-called 'CryptoLocker' virus. These attacks are not very common today, but expect them to become as widespread as email spam in the next five to 10 years. However, in the future, these attacks could become considerably more dangerous, potentially including home, car and smart grid meter jacking attacks followed by payment demands to make them stop.

Car Sploiting. Viruses are likely to become a more serious problem for our cars in the near future. As cars become more computerized, their systems (which also include Windows, Android, iOS and BlackBerry operating systems) are more vulnerable to attacks, and automotive viruses and malware are likely to spread.

Earlier this year, a Formula One racing team had to cut its preseason test short after the vehicle became infected with malware. Ford (NYSE:F) is taking the threat so seriously that it's already begun testing its car systems against possible hacks. In fact, automotive malware actually goes all the way back to 2007 when TomTom first discovered its navigation devices had been

infected. In the not so distant future, car viruses could become a real nuisance for drivers - and car anti-virus is likely to be a regular feature in most car models.

Brick Attacks. When it comes to bank fraud, account takeovers and stolen credit card numbers aren't the only thing you'll have to worry about. What if your account was completely erased from the bank's records?

In the "brick attack," hackers don't just try to steal money or information--they just destroys it. They do so by infecting the computers and servers that store this data with malware that renders them completely useless, unable to be turned on again (i.e., 'bricks').

Saudi Aramco, the world's largest oil company, was already hit with a brick attack in 2012, which destroyed 30,000 computers. And in December 2013, the National Security Agency claimed it had foiled a plot by foreign adversaries to "brick" computers all across the U.S. Now imagine attackers hitting a major retail bank and targeting customer account information. It could happen in the not so distant future.

Identity Theft Squared. You think it's bad now with identity theft? Well, just wait. Right now, biometric security (e.g., fingerprint scanners, retina scans, voice prints, etc.) is limited to a few consumer devices, but once it becomes a key way to authenticate your online accounts, biometric data will become an important commodity to the criminal underground. Genetic data theft is also an increasing risk as more consumers sign up for genetic testing and their data is stored on vulnerable networks.

Mini-Power Outages. As more homes transition to 'smart meters,' they could also become vulnerable to new types of criminal tampering. Two key features of today's smart meters that could be taken advantage of by hackers are their ability to wirelessly update the firmware and remotely disconnect users. This could allow attackers to corrupt the smart meters of individual homes, running up bogus charges or causing the electrical system to malfunction, shut down or surge (frying all of your outlets and anything connected to them). They could also allow attackers to disconnect homes at will.