Chapter

Introductory Chapter: Computer Security Threats

Ciza Thomas

1. Introduction

Along with the tremendous progress in Internet technology in the last few decades, the sophistication of the exploits and thereby the threats to computer systems have also equally increased. The exploitation is done by malicious hackers who find vulnerabilities or weaknesses, which are the pre-existing errors in the security settings in the computer systems. The common types of vulnerabilities are errors in the design or configuration of network infrastructure, protocols, communication media, operating systems, web-based applications and services, databases, etc.

Threat is a potential risk that exploits a vulnerability to infringe security and cause probable damage/disruption to the information/service stored/offered in/by computer systems or through communication links. A threat to a computer systems occurs when the confidentiality (preventing exposure to unauthorized parties), integrity (not modified without authorization), and availability (readily available on demand by authorized parties) of information on systems are affected. Thus, a computer system threat in general can include anything deliberate, unintended, or caused by natural calamity that effects in data loss/manipulation or physical destruction of hardware. Accordingly, the threats on computer system are classified as physical threats and nonphysical threats. Physical threats cause impairment to hardware or theft to system or hard disk that holds critical data. Nonphysical threats target the data and the software on the computer systems by corrupting the data or by exploiting the errors in the software.

The exploits when successful result in security attacks on computer systems. Hence, threat is a possible danger caused by system vulnerability, while attack is the attempt of unauthorized action or a harmful action. The realization of a threat is usually detrimental and is termed an attack.

In this introductory chapter, the computer security threats are defined as probable attacks from hackers that let them to gain illicit entree to a computer. In this chapter, a detailed introduction is given on the common computer system threats. The logical threats are a main cause of security incidents on computer systems. Knowing these threats and their characteristics helps in identifying the threats and to proactively devise steps in protecting the systems. The organization of this chapter is as follows. Section 2 introduces the motivation and objective of the hackers. Section 3 is on the classification of threats, which also includes an exhaustive coverage of all the threats. The details of the top security menaces of 2020 and the expectation for the latter half of 2020 are introduced in Section 4. Section 5 concludes the chapter.

2. Motivation and objectives of hackers

The purpose of a hacker is to break the security of computers and networks affecting the confidentiality, integrity, and availability of information/service on systems. Such activities of hackers are considered illegal as they invest their time and know how, to make personal gains and breach the security across networks. Before looking at the taxonomy of computer threats, it is necessary to classify the different types of hackers. Each type of hacker is expected to have their own motivation for their activities. The most common of those are included here:

Fun: Fun is the only motivation for the script kiddies and lot of nonserious hackers. For them, the breaking into a secure system is a challenging and adventurous enjoyable game to test their wits and skills.

Vulnerability testing: Vulnerability testing is done by administrators to locate vulnerabilities and hence develop protections. The same is also done by hackers to identify vulnerabilities in target systems and to find the exploits for those vulnerabilities. This is almost a pre-phase of an attack.

Theft: Theft or stealing of data is when hackers infiltrate on a database of credentials of individuals or organizations.

Espionage: Espionage is another type of theft where the hacker tries to get protected information instead of the direct financial gain. The information stolen can be either sold in black market or used by adversaries to gain strategic advantages.

Spamming: Spamming is not just about unsolicited emails. This spam can be due to certain particular malware that invade the web browser and devastate with unwanted ads.

Control: The hacker uses a Trojan or other means to take remote control over another system. Then the hacker can turn that compromised system into a bot or a zombie computer that they use to power spam or to deploy distributed denial of service attacks.

Disruption: Disruption of services or access to information, by taking over websites or social media accounts, is usually an act of competition, protest, or rivalry. This effect will slow down or shut down of the target's Internet activity.

3. Classification of computer threats and attacks

Computer threats and attacks involve accessing information, obliterating or manipulating data, destabilizing the computer, or degrading its performance [1]. Computer attacks are mainly information gathering, privilege escalation, buffer overflow exploits, remote accessing by unauthorized users, and denial of service attacks [2]. Network attacks being a subset of computer attacks were mostly attacks on computer systems that form the basic infrastructure of a communication network. A network aids in sending an attack or it could be the means of attack.

There are various steps involved in the attacking scenario, and these steps are briefly listed here:

Step 1: spoofing

Before initiating any of the attacking steps, the hackers normally prefer to hide their identity and their activities. These are normally done by spoofing when the attacker hides his identity and pretends to be someone else. This can be done by MAC cloning, IP spoofing, or email spoofing.

Step 2: reconnaissance

It is always a good practice to plan well before undertaking any action, and this is applicable in the case of hacking too. The hackers first identifies a target to launch an attack, extract maximum information regarding this target, understand its vulnerabilities, and then only explore the best ways to exploit it.

Step 3: weaponization

The hacker with the information collected in the previous phase identifies/develops weapons in order to get into the computer or the network. During this phase, the hacker collects the tools that they plan to use once they gain access to the system for the successful exploitation of the vulnerabilities in the system.

Step 4: implementation

In the implementation phase, the attack starts working. It is when the phishing e-mails are sent or when the fake web pages are posted to the Internet and the attacker patiently waits for all the data they need to start rolling in.

Step 5: exploitation

This is a state when the sensitive and confidential data starts rolling in. It is the most exciting phase for the hackers, and they try out the usernames and passwords against web-based e-mail systems or secured connections to sensitive networks.

Step 6: installation

After a successful exploitation, the attacker will make sure to have continued access to the system. This is by installing a persistent backdoor or creating admin accounts on the system, disabling firewall rules, and perhaps even activating remote desktop access on computer systems on the network.

Step 7: control

Once the attacker gains access to the network or creates administrator accounts or installs all the necessary tools for backdoor entry any time to the system, the attacker is in control of the target.

Step 8: action on set goals

With total control on the target system, the attacker can set goals and achieve it with or without the knowledge of the genuine user.

The attacks are thus classified depending on the various steps taken by the hacker in the process of the attack, starting from hiding the identity to information collection, which is the pre-phase of an attack, to the actual attack.

4. Computer threats

4.1 Spoofing

Spoofing is when someone hides their identity to evade detection for their wrong acts and pretends to be someone else in an attempt to gain trust and get sensitive system information. The common spoofing done by changing the hardware or MAC address is called MAC cloning, changing the IP address or the unique identity on the network is called IP spoofing, and impersonating as someone else in their digital communication is called email spoofing.

4.2 Information-gathering attacks

Information gathering is the practice of attacker gaining priceless details about probable targets. This is not an attack but only a pre-phase of an attack and is totally passive as there is no explicit attack. Systems including computers, servers, and network infrastructure, including communication links and inter networking devices, are sniffed, scanned, and probed for information like whether the target system is up and running, what all ports are open, details regarding the operating system and its version, etc. Some of the information-gathering attacks are sniffing, mapping, vulnerability scanning, phishing, etc.

4.3 Password attacks

The simplest way to achieve control of a system, or any user account, is through a password attack. If the personal and behavioral details of the victim are known, the attacker starts with guessing password. Frequently, the attacker uses some form of social engineering to trace and find the password. Dictionary attack is the next step in password attacks and is automated.

4.4 Malware

After gaining access to a system, the attacker takes the support of malware or malicious software that clandestinely acts against the interests of the computer user.

4.5 Virus

Computer viruses are the most communal threat to the computer users. Computer viruses are malicious software designed to blow out from one computer to another through file transfer, piggybacks on genuine programs and OS, or e-mails. The email attachments or downloads from particular websites contaminate the computer and also other computers on its list of contacts by using the communication network. Viruses influence the system security by changing the settings, accessing confidential data, displaying unwanted advertisements, sending spam to contacts, and taking control of the web browser [2]. The viruses are identified as executable viruses, boot sector viruses, or e-mail viruses.

4.6 Worms

Computer worms are fragments of malicious software that reproduce swiftly and blow out from one computer to another through its contacts, again spreading to the contacts of these other computers and so on and reaching out to a large number of systems in no time. Captivatingly, worms are prepared for spreading by exploiting software vulnerabilities. Worms display unwanted advertisements. It uses up tremendous CPU time and network bandwidth in this process thereby denying access to the systems or network of the victim, creating chaos and trust issues on a communication network.

4.7 Trojans

Trojans are programs that appear as perfectly genuine but, in reality, have a malicious part embedded in it. Trojans are spread usually through email attachment from the trustworthy contacts and also on clicking on fake advertisements. The payload of Trojans is an executable file that will install a server program on the victim's system by opening a port and always listening to that port whereas the server is run on the attacker's system. Hence, whenever the attacker wants to login to the victim machine, they can do so by means of the backdoor entry making it hidden from the user.

4.8 Spyware and adware

Spyware and adware are software with a common property of collecting personal information of users without their knowledge. Adware is intended to track data of the user's surfing behaviors, and, based on that, pop-ups and advertisements are displayed. The adware clause in the agreement during the installation process is often skipped with least seriousness. Spyware on the other hand gets installed on a computer and gathers information about the user's online activities without their knowledge. Spyware contains keyloggers that record everything typed on the keyboard, making it unsafe due to the high threat of identity mugging.

4.9 Scareware

Scareware is yet another malware that tricks victims by displaying fake alerts and forcing the victim to buy protective software that is fraudulent. The alerts or the pop-up messages sound like warning messages along with proper protective measures, which if followed creates security issues.

4.10 Rootkit

Rootkit is a pool of software tools that gets mounted in stealth along with some genuine software. Rootkit allows remote access and administrative control on a system. With these privileges, the rootkit performs malicious activities like disabling of antivirus, password sniffing, keylogging, etc.

4.11 Keylogger

Keylogger software has the ability to record keystrokes and also capture screenshots and save it to a log file in encrypted form. Keylogger software can record all the information that is typed on the keyboard including passwords, e-mail, and instant messages. The log file created by the keylogger is saved and mailed to the attacker on a remote machine with the motive to extract password and banking details for financial fraud.

4.12 Ransomware

Ransomware is a malicious software that hampers admission to computer or files on the computer. The computers may be locked or files encrypted. Accordingly, the two common types of ransomware are lock screen ransomware and encryption ransomware. The victim will be demanded ransom for the restriction to be removed, and this gets displayed on victim's system. There can also be notification stating that establishments have detected illicit activity on this computer and demands ransom as fine to avoid prosecution.

4.13 Rogue security software

Rogue security software is another malicious program that deceives users to believe that there is malware installed on their system or the security measures are outdated and hence of concern. They offer installing or updating users' security settings. Then it is an actual malware that gets installed on the computer.

4.14 Botnets

A collection of compromised systems or bots acts as a team of infected computers under the control of a bot master to remotely control and send synchronized attacks on a victim host. This army of bots, agents, and bot master constitute a botnet. Botnets are used for sending spams and also for distributed denial of service attacks.

4.15 Denial-of-service attacks

Denial-of-service (DoS) attacks as the name suggests deny users from accessing or using the service or system. This is mainly done by overwhelming the bandwidth, CPU, or memory wherein the access to the network of the victim machine or server offering the service gets denied. DoS attacks thus interrupt the service of a computer or network systems, making it inaccessible or too inferior in performance.

4.16 Distributed DoS

In distributed DoS (DDoS) attacks, the victim is targeted from a large number of individual compromised systems simultaneously. The DDoS attacks are normally done with the help of botnets. The botmaster is the attacker who indirectly attacks the victim machine using the army of bots or zombies. The DDoS attacks occur when a large number of compromised systems act synchronously and are being coordinated under the control of an attacker in order to totally exhaust its resources and force it to deny service to its genuine users. It is the upsurge in the traffic volume that loads the website or server causing it to appear sluggish [2].

4.17 IoT-based attacks

The last decade has seen exponential increase in the use of Internet of Things (IoT) that are smart devices used at home, organizations, and businesses. The issue with these IoT is its weak security as these devices are often overlooked when it comes to applying security patches that create lead-ins for attackers to seize these devices to infiltrate the networks. An IoT-based attack is any cyberattack that leverages a victim's use of IoT to sneak malware onto a network.

4.18 Session hijacking

In session hijacking, the hacker takes control of a session going on between two hosts. Session hijacking usually takes place in applications that use TCP with a sequence number prediction. With that sequence number, the attacker sends a TCP packet.

4.19 Blended attacks

A blended attack is a software exploit that encompasses a mixture of exploit techniques to attack and propagate threats, for example, viruses, worms, and Trojan horses.

4.20 Website attacks

Website attacks are targeting browser components that are at risk of being unpatched even when the browser is patched. SQL injection attacks are intended to target any website or web application that uses an SQL database such as MySQL, Oracle, etc. by taking advantage of the security flaws in the application's software. This attack is used to obtain and corrupt user's sensitive data.

4.21 Mobile phone and VOIP threats

Malware target mobile phones, VoIP systems, and the IP PBXs as these devices have plentiful published vulnerabilities. There are attack tools freely available on the Internet, and misusing these vulnerabilities makes these attacks too common and simple even for a script kiddie.

4.22 Wi-Fi eavesdropping

Wi-Fi eavesdropping is an attack used by network attackers to grab sensitive information of a target system. It is the act of silently listening on an unencrypted Wi-Fi network.

4.23 WPA2 handshake vulnerabilities

The key reinstallation attack (KRACK) lets an attacker to decipher the network traffic on Wi-Fi routers. Every device connected to Wi-Fi, such as computers, smartphones, smart devices, and wearables, can be identified by the hacker.

4.24 Insider attacks

One of the prevalent all-time computer security threats faced by any organization is from its own employees. Insider attacks are initiated by disgruntled employees of an organization. Insider usually has certain privileges to the data as well as rights on the systems and networks that they attack, giving them an advantage over external attackers. These attacks can be hard to prevent with firewalls, which are the first level of defense.

4.25 Supply chain attacks

A supply chain attack seeks to cause harm by targeting the least secured elements in the supply network.

4.26 Buffer overflows

Buffer overflows are used to exploit programming glitches that do not take care of the buffer size. If a buffer is jam-packed beyond its size, the data overflows into the contiguous memory. This flaw gets smartly used by hackers to change the execution of the program.

4.27 User to root attack

User to root attack is a case of privilege escalation where a user gains a higher privilege than that authorized. This is not a class of attack as such, and it is the process of any attack. Every attack will do activities the attacker is not privileged to do.

4.28 Man-in-the-middle attacks

Man-in-the-middle attacks allow the hacker to snoop on the communication between two systems, affecting the privacy. A common method of doing this is to place the attacker at a point and redirect all the communication through the route that includes that hacker so that eavesdropping is possible by the hacker.

4.29 Pharming

Pharming is a widespread online fraud that will automatically point to a nasty and illicit website by relaying the authentic URL. Even when the URL is correctly entered, the redirection happens to some forged website looking similar to the actual one. This fake site prompts one to enter personal information that gets to someone with a wicked intent.

4.30 Spam

Spams are unsolicited bulk e-mail messages that annoy the user with unwanted and junk mails. It gives burden for communications service providers, organizations and individuals alike. These emails can be commercial ones like an advertisement or noncommercial one like chain letters or anecdotes. Spam is considered an active vehicle for virus propagation, scams, fraud and is a threat to computer privacy. Spam also phishes for interesting information with offers and promotions that trick victims into following links or entering details.

5. Present-day computer security threats and trends

Predicting the computer security threats and trends is usually done to lend a hand to the security experts who take proactive measures to protect security. Normally the predictions for any year depends on how it went in the previous years, and the changes expected are mainly in terms of the tactics and scale of the biggest and significant threats that were successful in implementation and also in evading detection. The investment on security is justified in many organizations only after analyzing these predictions.

Phishing and other social engineering tactics are likely to continue in the coming years too with increased complexity and sophistication. They will appear to be more and more convincing to trick people into clicking on a link or opening attachments. Even with strong defenses to protect against ransomware, hackers are expected to all the time target more victims with large digital assets. The rise of cryptocurrency like bitcoin will also trigger more ransomware attacks by letting demands for payment made incognito. Cryptojacking can also be seen as a common trend of future as it involves hackers hijacking with a purpose of mining for cryptocurrency.

As the Internet of Things is becoming widely popular and more ubiquitous, the IoT attacks will be on the upsurge. IoT includes laptops, tablets, smart wearable devices, webcams, household appliances, Wi-Fi-enabled speakers, appliances, alarm clocks, medical devices, manufacturing equipment, automobiles and networking devices like routers, gateways, switches, NAS servers, and even home security systems. Security is rarely the first concern in the competition to bring new products and technologies. Thus the more IoT devices, the greater the risk, making IoT attacks to be on the rise in coming years.

Data breaches will continue in the coming years as data remains a valuable black market attraction.

Totally new approaches for data and infrastructure protection are essential as more and more data is moved to the cloud. Also, in the coming years, there will be more attacks targeting electrical grids, automated transportation systems, computerized water treatment facilities, etc.

State-sponsored attacks are when states or nations are using their cyber skills to infiltrate other governments and execute attacks on severe infrastructure. As political strains grow, state-sponsored attacks steal political and industrial secrets, spread misinformation, perform DDoS attacks, execute prominent data breaches, etc.

Another target of attacker is the all-time sensitive medical record of patients. As the healthcare industry gets used to the digital age, concerns around privacy, safety, and computer security threats are also seen to rise. There are worries about a hacker taking over and changing dosages of medicines, disabling vital sign monitoring, etc., as these are life-threatening to the patients.

Now, with the self-driving cars, semiautonomous vehicles, and the connected cars, the risk of cyber security is stringent and serious. With high-tech automobiles, the future will likely see an increase in not only the number of connected cars but in the number and severity of system vulnerabilities detected. For hackers, this means yet another opportunity to exploit vulnerabilities and cause threat to life.

Endpoint security will be a major concern for organizations as malware infections of employee-owned devices are going to be a major security issue in 2020 when employees start "working from home" in the wake of COVID 19 pandemic. When organizations permit employees not to risk their health and safety and allow them to use their own devices, attackers will target those devices to bypass the multilayered defenses of the organization. The advantage to hackers is that the users' personal devices are less protected compared to corporate devices as users rarely apply added measures to protect their smart devices from impending threats.

Artificial intelligence also gets applied on both sides of the barricade for protecting and attacking the computers. Artificial intelligence is being used for person identification, threat detection, etc. to aid security; however it is also being weaponized by hackers to develop increasingly complex malware and attack methods.

6. Conclusion

A lot of computer threats have been included in this chapter with many terms tending not to be mutually exclusive. Again, an attack may get classified into different classes since attackers use multiple techniques or strategies. The irony is that even with lot of advanced defensive mechanism put in place by security experts, the hackers may still use the same attacking techniques and will take advantage of the same vulnerabilities they have used in the past. It is important to defend the attacks by paying attention to the internal systems, deploying multiple defenses for enhanced security, and avoiding irreparable damage. This requires the implementation of security policy as an ongoing process with tight access control mechanism and deployment of advanced multiple layer security devices.

Author details

Ciza Thomas
Directorate of Technical Education, Government of Kerala, India

*Address all correspondence to: cizathomas@gmail.com

References

[1] Thomas C, Balakrishnan N. Improvement in intrusion detection with advances in sensor fusion. IEEE Transactions on Information Forensics and Security. 2009;**4**(3):542-551

[2] Thomas C. Performance enhancement of intrusion detection systems using advances in sensor fusion [Ph. D dissertation report]; 2009