ATTACKS TO SOFTWARE SECURITY

M.S.I. Ricardo Reyes

Cybersecurity Threats, Vulnerabilities, and Attacks

Threats, vulnerabilities, and attacks are the central focus of cybersecurity professionals

- **A threat** is the possibility that a harmful event, such as an attack, will occur.
- **A vulnerability** is a weakness that makes a target susceptible to an attack.
- **An attack** is a deliberate exploitation of a discovered weakness in computer information systems, either as specific targets or merely as targets of opportunity.

Cyber criminals may have different motivations for selecting a target of an attack.

What is malware?

Malicious software, or malware, is a term used to describe software designed to disrupt computer operations, or gain access to computer systems, without the user's knowledge or permission. Malware has become an umbrella term used to describe all hostile or intrusive software.

The term malware includes computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs. Malware may be obvious and simple to identify or it can be very stealthy and almost impossible to detect.

Virus

A virus is malicious executable code attached to another executable file, such as a legitimate program. Most viruses require end-user initiation, and can activate at a specific time or date. Computer viruses usually spread in one of three ways: from removable media; from downloads off the Internet; and from email attachments.

Viruses can be harmless and simply display a picture or they can be destructive, such as those that modify or delete data. In order to avoid detection, a virus mutates.

Worms

Worms are malicious code that replicates by independently exploiting vulnerabilities in networks. Worms usually slow down networks. Whereas a virus requires a host program to run, worms can run by themselves. **Other than the initial infection, worms no longer require user participation**. After a worm affects a host, it is able to spread very quickly over the network.

Trojan Horses

A Trojan horse is malware that carries out malicious operations under the guise of a desired operation such as playing an online game. This malicious code exploits the privileges of the user that runs it. **A Trojan horse differs from a virus because the Trojan binds itself to non-executable files,** such as image files, audio files, or games.

Logic Bombs

A logic bomb is a malicious program that uses a trigger to awaken the malicious code. For example, triggers can be dates, times, other programs running, or the deletion of a user account. **The logic bomb remains inactive until that trigger event happens**. Once activated, a logic bomb implements a malicious code that causes harm to a computer.

A logic bomb can sabotage database records, erase files, and attack operating systems or applications.

Ransomware

Ransomware holds a computer system, or the data it contains, captive until the target makes a payment**. Ransomware usually works by encrypting data in the computer with a key unknown to the user**. The user must pay a ransom to the criminals to remove the restriction.

Payment through an untraceable payment system is always the criminal's goal.

Backdoors

A backdoor refers to the program or code introduced by a criminal who has compromised a system. **The backdoor bypasses the normal authentication** used to access a system.

The purpose of the backdoor is to grant the cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.

Rootkits

A rootkit modifies the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely. Most rootkits take advantage of software vulnerabilities to **perform privilege escalation** and modify system files.

How to defend against malware?

Antivirus Program - The majority of antivirus suites catch most widespread forms of malware.

Up-to-Date Software - Many forms of malware achieve their objectives through exploitation of vulnerabilities in software, both in the operating system and applications

Spam

Spam, also known as junk mail, is unsolicited email. In most cases, spam is a method of advertising. However, **spam can send harmful links, malware, or deceptive content**. Most spam comes from multiple computers on networks infected by a virus or worm. These compromised computers send out as much bulk email as possible.

Spyware

Spyware is software that **enables a criminal to obtain information about a user's computer activities**. Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings. Spyware often bundles itself with legitimate software or with Trojan horses. Many shareware websites are full of spyware.

Adware

Adware typically **displays annoying pop-ups to generate revenue for its authors**. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites. Some versions of software automatically install Adware.

Some adware only delivers advertisements, but it is also common for adware to come with spyware.

Scareware

Scareware **persuades the user to take a specific action based on fear**. Scareware forges pop-up windows that resemble operating system dialogue windows. These windows convey forged messages stating that the system is at risk or needs the execution of a specific program to return to normal operation.

In reality, no problems exist, and if the user agrees and allows the mentioned program to execute malware.

Phishing

Phishing is a form of fraud. Cyber criminals use email, instant messaging, or other social media to **try to gather information such as login credentials or account information** by masquerading as a reputable entity or person. Phishing occurs when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source.

Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing sends customized emails to a specific person. The criminal researches the target's interests before sending the email.

Vishing

Vishing is phishing using voice communication technology. Criminals can spoof calls from legitimate sources using voice over IP (VoIP) technology. Victims may also receive a recorded message that appears legitimate. Criminals want to obtain credit card numbers or other information to steal the victim's identity. Vishing takes advantage of the fact that people trust the telephone network.

Smishing

Smishing (Short Message Service phishing) is phishing using text messaging on mobile phones. Criminals impersonate a legitimate source in an attempt to gain the trust of the victim. For example, a smishing attack might send the victim a website link. When the victim visits the website, malware is installed on the mobile phone.

Pharming

Pharming is the **impersonation of a legitimate website** in an effort to deceive users into entering their credentials. Pharming misdirects users to a fake website that appears to be official. Victims then enter their personal information thinking that they connected to a legitimate site.

Whaling

Whaling is a **phishing attack that targets high profile targets** within an organization such as senior executives. Additional targets include politicians or celebrities.

Browser Plugins

Security breaches can affect web browsers by displaying pop-up advertising, collecting personally identifiable information, or installing adware, viruses, or spyware. A criminal can hack a browser's executable file, a browser's components, or its plugins.

Successful exploitation could cause a system crash or allow a criminal to take control of the affected system. Expect increased data losses to occur as criminals continue to investigate the more popular plugins and protocols for vulnerabilities

SEO Poisoning

Search engines such as Google work by ranking pages and presenting relevant results based on users' search queries. Depending on the relevancy of web site content, it may appear higher or lower in the search result list. While many legitimate companies specialize in optimizing websites to better position them, SEO poisoning **uses SEO to make a malicious website appear higher in search results.**

The most common goal of SEO poisoning is to increase traffic to malicious sites that may host malware or perform social engineering

How to defend against email and browser attacks?

- Email filtering
- Use of an antivirus
- User education and training
- Keep all software up to date

Social Engineering

Social engineering is a completely **non-technical** means for a criminal to gather information on a target. Social engineering is an attack that attempts to **manipulate individuals** into performing actions or divulging confidential information.

Social engineers often rely on people's willingness to be helpful but also prey on people's weaknesses.

Shoulder Surfing

A criminal observes, or shoulder surfs, to pick up PINs, access codes or credit card numbers. An attacker can be in close proximity to his victim or the attacker can use binoculars or closed circuit cameras to shoulder surf. That is one reason that a person can only read an ATM screen at certain angles.

Dumpster Diving

"One man's trash is another man's treasure". This phrase can be especially true in the world of dumpster diving which is the process of going through a target's trash to see what information an organization throws out. Consider securing the trash receptacle.

Any sensitive information should be properly disposed of through shredding or the use of burn bags, a container that holds classified or sensitive documents for later destruction by fire.

Piggybacking and Tailgating

Piggybacking or Tailgating occurs when a criminal tags along with an authorized person to gain entry into a secure location or a restricted area. Criminals use several methods to piggyback:

- They give the appearance of being escorted by the authorized individual
- They join a large crowd pretending to be a member
- They target a victim who is careless about the rules of the facility

How to defend against social engineering?

- Never provide confidential information or credentials via email, chat sessions, in-person, or on the phone to unknown parties.
- Resist the urge to click on enticing emails and website links.
- Keep an eye out for uninitiated or automatic downloads.
- Establish policies and educate employees about those policies.
- When it comes to security, give employees a sense of ownership.
- Do not fall to pressure from unknown individuals.

Denial of Service

Denial-of-Service (DoS) attacks are a type of network attack. A DoS attack results in some sort of interruption of network services to users, devices, or applications. There are two major types of DoS attacks:

- Overwhelming Quantity of Traffic
- Maliciously Formatted Packets

A Distributed DoS Attack (DDoS) is similar to a DoS attack, but it originates from multiple, coordinated sources.

Sniffing

Sniffing is similar to eavesdropping on someone. It occurs when **attackers examine all network traffic** as it passes through their NIC, independent of whether or not the traffic is addressed to them or not. Criminals accomplish network sniffing with a software application, hardware device, or a combination of the two.

Spoofing

Spoofing **is an impersonation attack, and it takes advantage of a trusted relationship between two systems**. If two systems accept the authentication accomplished by each other, an individual logged onto one system might not go through an authentication process again to access the other system. An attacker can take advantage of this arrangement by sending a packet to one system that appears to have come from a trusted system

There are multiple types of spoofing attacks such as : MAC address spoofing, IP spoofing, ARP spoofing, DNS spoofing.

Man-in-the-middle

A criminal performs a man-in-the-middle (MitM) attack by intercepting communications between computers to steal information crossing the network. The criminal can also choose to manipulate messages and relay false information between hosts since the hosts are unaware that a modification to the messages occurred. MitM allows the criminal to take control over a device without the user's knowledge.

Zero-day Attacks

A zero-day attack, sometimes referred to as a zero-day threat, is a computer attack that tries to exploit software vulnerabilities that **are unknown or undisclosed** by the software vendor. The term zero hour describes the moment when someone discovers the exploit. During the time it takes the software vendor to develop and release a patch, the network is vulnerable to these exploits.

Defending against these fast-moving attacks requires network security professionals to adopt a more sophisticated view of the network architecture.

Keyboard Logging

Keyboard logging is a software program that records or logs the keystrokes of the user of the system. Criminals can implement keystroke loggers through software installed on a computer system or through hardware physically attached to a computer. The criminal configures the key logger software to email the log file. The keystrokes captured in the log file can reveal usernames, passwords, websites visited, and other sensitive information.

How to defend against network attacks?

- Configure Firewalls IDS and IPS appliances to detect intrusions and block suspicious behaviors in the network
- Always use encrypted forms of communication
- Use strong methods of authentication

Grayware

Grayware is becoming a problem area in mobile security with the popularity of smartphones. Grayware includes applications that behave in an annoying or undesirable manner. Grayware may not have recognizable malware concealed within, but it still may pose a risk to the user.

Rogue Access Points

A rogue access point is a wireless access point installed on a secure network without explicit authorization.

A rogue access point can be set up in two ways. The first is when a well-intentioned employee is trying to be helpful by making it easier to connect mobile devices. The second way is when a criminal gains physical access to an organization by sneaking in and installs the rogue access point. Since both are unauthorized, both pose risks to the organization.

RF Jamming

Wireless signals are susceptible to electromagnetic interference (EMI), radio-frequency interference (RFI), and may even be susceptible to lightning strikes or noise from fluorescent lights. Wireless signals are also susceptible to deliberate jamming. Radio frequency (RF) jamming disrupts the transmission of a radio or satellite station so that the signal does not reach the receiving station.

The frequency, modulation, and power of the RF jammer needs to be equal to that of the device that the criminal wants to disrupt in order to successfully jam the wireless signal.

Bluejacking and Bluesnarfing

Bluejacking is the term used for sending unauthorized messages to another Bluetooth device. A variation of this is to send a shocking image to the other device.

Bluesnarfing occurs when the attacker copies the victim's information from his device. This information can include emails and contact lists.

Bluetooth vulnerabilities have surfaced, but due to the limited range of Bluetooth, the victim and the attacker need to be within range of each other.

WEP and WPA Attacks

WEP uses a key for encryption. There is no provision for key management with WEP, so the number of people sharing the key will continually grow. Since everyone is using the same key, the criminal has access to a large amount of traffic for analytic attacks.

WEP also has several problems with its initialization vector (IV) which is one of the components of the cryptographic system:

- It is a 24-bit field, which is too small.
- It is cleartext, which means it is readable.
- It is static so identical key streams will repeat on a busy network.

How to defend against mobile and wireless attacks?

- Change default configurations
- Continuously monitor for traffic and devices
- Develop a guest policy
- Restrict access to untrusted devices in the DMZ

Cross-Site Scripting

Cross-site scripting has three participants: the criminal, the victim, and the website. The cyber-criminal does not target a victim directly. The criminal exploits vulnerability within a website or web application.

Criminals inject client-side scripts into web pages viewed by users, the victims. The malicious script unknowingly passes to the user's browser. A malicious script of this type can access any cookies, session tokens, or other sensitive information. If criminals obtain the victim’s session cookie, they can impersonate that user.

Code Injection

One way to store data at a website is to use a database. There are several different types of databases such as a Structured Query Language (SQL) database or an Extensible Markup Language (XML) database. Both XML and SQL injection attacks exploit weaknesses in the program such as not validating database queries properly.

The problem occurs when the system does not properly scrutinize the input request provided by the user. Criminals can manipulate the query by programming it to suit their needs and can access the information on the database. All sensitive data stored in the database is accessible to the criminals and they can make any number of changes to the website.

Buffer Overflow

A buffer overflow occurs when data goes beyond the limits of a buffer. Buffers are memory areas allocated to an application. By changing data beyond the boundaries of a buffer, the application accesses memory allocated to other processes. This can lead to a system crash, data compromise, or provide escalation of privileges.

The CERT/CC at Carnegie Mellon University estimates that nearly half of all exploits of computer programs stem historically from some form of buffer overflow

Remote Code Executions

Vulnerabilities allow a cybercriminal to execute malicious code and take control of a system with the privileges of the user running the application. Remote code execution allows a criminal to execute any command on a target machine.

Java extensions

Java operates through an interpreter, the Java Virtual Machine (JVM). The JVM enables the Java program's functionality. The JVM sandboxes or isolates untrusted code from the rest of the operating system. There are vulnerabilities, which allow untrusted code to go around the restrictions imposed by the sandbox. There are also vulnerabilities in the Java class library, which an application uses for its security. J

Java is the second biggest number of security vulnerabilities next to Adobe's Flash plugin.

How to defend against application attacks?

The first line of defense against an application attack is to write solid code. Regardless of the language used, or the source of outside input, prudent programming practice is to treat all input from outside a function as hostile. Validate all inputs as if they were hostile.

Keep all software including operating systems and applications up to date, and do not ignore update prompts. Not all programs update automatically. At the very least, select the manual update option. Manual updates allow users to see exactly what updates take place.