Cybersecurity Threats, Vulnerabilities, and Attacks

16 January 2024 20:02

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. Cyber criminals succeed by continuously searching for and identifying systems with clear vulnerabilities. Common victims include unpatched systems or systems missing virus and spam detection.

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.

Viruses, Worms, and Trojan Horses

Viruses
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. The simple act of opening a file can trigger a virus. A boot sector, or file system virus, infects USB flash drives and can spread to the system's hard disk. Executing a specific program can activate a program virus. Once the program virus is active, it will usually infect other programs on the computer or other computers on the network. The Melissa Virus was an example of a virus spread via email. Melissa affected tens of thousands of users and caused an estimated $1.2 billion in damage. Click here to read more about viruses.

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. Worms share similar patterns. They all have an enabling vulnerability, a way to propagate themselves, and they all contain a payload.
Worms are responsible for some of the most devastating attacks on the Internet. For example, in 2001, the Code Red worm infected 658 servers. Within 19 hours, the worm infected over 300,000 servers.

Trojan horse
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. Cybersecurity specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, CPU, memory, hard drives and power supplies. The logic bomb overdrives these devices until they overheat or fail.

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.
Some other versions of ransomware can take advantage of specific system vulnerabilities to lock down the

system. Ransomware propagates as a Trojan horse and is the result of a downloaded file or some software weakness.
Payment through an untraceable payment system is always the criminal's goal. Once the victim pays, the criminal supplies a program that decrypts the files or sends an unlock code. Click here to read more about ransomware.

Backdoors and Rootkits

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. A few common backdoor programs are Netbus and Back Orifice, which both allow remote access to unauthorized system users. 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. Usually, criminals have authorized users unknowingly run a Trojan horse program on their machine to install the backdoor.
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. Privilege escalation takes advantage of programming errors or design flaws to grant the criminal elevated access to network resources and data. It is also common for rootkits to modify system forensics and monitoring tools, making them very hard to detect. Often, a user must wipe and reinstall the operating system of a computer infected by a rootkit.

Defending Against Malware

A few simple steps can help defend against all forms of malware:

- **Antivirus Program -** The majority of antivirus suites catch most widespread forms of malware. However, cyber criminals develop and deploy new threats on a daily basis. Therefore, the key to an effective antivirus solution is to keep the signatures updated. A signature is like a fingerprint. It identifies the characteristics of a piece of malicious code.
- **Up-to-Date Software -** Many forms of malware achieve their objectives through exploitation of vulnerabilities in software, both in the operating system and applications. Although operating system vulnerabilities were the main source of problems, today's application-level vulnerabilities pose the greatest risk. Unfortunately, while operating system vendors are becoming more and more responsive to patching, most application vendors are not.

Spam

Email is a universal service used by billions worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations. 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. The end goal is to obtain sensitive information such as a social security number or bank account information. 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.
Even with these security features implemented, some spam might still get through. Watch for some of the more common indicators of spam:

- An email has no subject line.
- An email is requesting an update to an account.
- The email text has misspelled words or strange punctuation.
- Links within the email are long and/or cryptic.
- An email looks like correspondence from a legitimate business.
- The email requests that the user open an attachment.

Spyware, Adware, and Scareware

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 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 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 infects his or her system.

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. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information. An example of phishing is an email forged to look like it came from a retail store asking the user to click a link to claim a prize. The link may go to a fake site asking for personal information, or it may install a virus.
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. For example, a criminal learns that the target is interested in cars and has been looking to buy a specific model of car. The criminal joins the same car discussion forum where the target is a member, forges a car sale offering, and sends an email to the target. The email contains a link for pictures of the car. When the target clicks on the link, he or she unknowingly installs malware on the computer. Click here to learn more about email frauds.

Vishing, Smishing, Pharming, and Whaling

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

Browser Plugins and Browser Poisoning

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.

Plugins

The Flash and Shockwave plugins from Adobe enable the development of interesting graphic and cartoon animations that greatly enhance the look and feel of a web page. Plugins display the content developed using the appropriate software.
Until recently, plugins had a remarkable safety record. As Flash-based content grew and became more popular, criminals examined the Flash plugins and software, determined vulnerabilities, and exploited Flash Player. 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. SEO, short for Search Engine Optimization, is a set of techniques used to improve a website's ranking by a search engine. 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. To force a malicious site to rank higher in search results, attackers take advantage of popular search terms.

Browser Hijacker

A browser hijacker is malware that alters a computer's browser settings to redirect the user to websites paid for by the cyber criminals' customers. Browser hijackers usually install without the user's permission and are usually part of a drive-by download. A drive-by download is a program that automatically downloads to the computer when a user visits a web site or views an HTML email message. Always read user agreements carefully when downloading programs to avoid this type of malware.

Defending Against Email and Browser Attacks

Methods for dealing with spam include filtering email, educating the user about being cautious towards unknown email(s), and using host/server filters.
It is difficult to stop spam, but there are ways to diminish its effects. For example, most ISPs filter spam before it reaches the user's inbox. Many antivirus and email software programs automatically perform email filtering. This means that they detect and remove spam from an email inbox.
Organizations must also make employees aware of the dangers of opening email attachments that may contain a virus or a worm. Do not assume that email attachments are safe, even when they come from a trusted contact. A virus may be trying to spread by using the sender's computer. Always scan email attachments before opening them.
The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from phishing and email spoofing.
Keeping all software updated ensures that the system has all of the latest security patches applied to take away known vulnerabilities. Click here to learn more about avoiding browser attacks

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. For example, an attacker could call an authorized employee with an urgent problem that requires immediate network access. The attacker could appeal to the employee's vanity, invoke authority using name-dropping techniques, or appeal to the employee's greed.
These are some types of social engineering attacks:
Pretexting - This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. An example involves an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.
Something for Something (Quid pro quo) - This is when an attacker requests personal information from a party in exchange for something, like a gift.

Social Engineering Tactics

Social engineers rely on several tactics. Social engineering tactics include:

- **Authority** – people are more likely to comply when instructed by "an authority"
- **Intimidation** – criminals bully a victim into taking action
- **Consensus/Social Proof** – people will take action if they think that other people like it too
- **Scarcity** – people will take action when they think there is a limited quantity
- **Urgency** – people will take action when they think there is a limited time
- **Familiarity/Liking** – Criminals build a rapport with the victim to establish a relationship
- **Trust** – Criminals build a trusting relationship with a victim which may require more time to establish

Shoulder Surfing and Dumpster Diving

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. These types of safeguards make shoulder surfing much more difficult.
"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

mpersonation and Hoaxes

Impersonation is the action of pretending to be someone else. For example, a recent phone scam targeted taxpayers. A criminal, posing as an IRS employee, told the victims that they owed money to the IRS. The victims must pay immediately through a wire transfer. The impersonator threatened that failure to pay will result in an arrest. Criminals also use impersonation to attack others. They can undermine the credibility of individuals by using website or social media postings.
A hoax is an act intended to deceive or trick. A cyber hoax can cause just as much disruption as an actual breach would cause. A hoax elicits a user reaction. The reaction can create unnecessary fear and irrational behavior. Users pass hoaxes through email and social media.

Piggybacking and Tailgating

Piggybacking 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

Tailgating is another term that describes the same practice.
A mantrap prevents piggybacking by using two sets of doors. After individuals enter an outer door, that door must close before entering the inner door.

Defending Against Deception

Organizations need to promote awareness of social engineering tactics and properly educate employees on prevention measures, such as the following:

- 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** – The attacker sends an enormous quantity of data at a rate that the network, host, or application cannot handle. This causes a slowdown in transmission or response, or a crash of a device or service.
- **Maliciously Formatted Packets** – The attacker sends a maliciously formatted packet to a host or application and the receiver is unable to handle it. For example, an application cannot identify packets containing errors or improperly formatted packets forwarded by the attacker. This causes the receiving device to run very slowly or crash.

DoS attacks are a major risk because they can easily interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled attacker.
The goal of a denial-of-service attack is to deny access to authorized users making the network unavailable (remember the three underlying security principles: confidentiality, integrity, and availability). Click Play in Figure 1 to view the animation of a DoS attack.
A Distributed DoS Attack (DDoS) is similar to a DoS attack, but it originates from multiple, coordinated sources. As an example, a DDoS attack could proceed as follows:
An attacker builds a network of infected hosts, called a botnet, comprised of zombies. Zombies are the infected hosts. The attacker uses handler systems to control the zombies. The zombie computers constantly scan and infect more hosts, creating more zombies. When ready, the hacker instructs the handler systems to make the botnet of zombies carry out a DDoS attack.

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. As shown in the figure, sniffing views all network traffic or it can target a specific protocol, service, or even string of characters such as a login or password. Some network sniffers observe all traffic and modify some or all of the traffic as well.
Sniffing also has its benefits. Network administrators may also use sniffers to analyze network traffic, identify bandwidth issues, and troubleshoot other network issues.
Physical security is important in preventing the introduction of sniffers on the internal network.

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. Since the trusted relationship is in place, the targeted system may perform the requested task without authentication.
There are multiple types of spoofing attacks.

- MAC address spoofing occurs when one computer accepts data packets based on the MAC address of another computer.
- IP spoofing sends IP packets from a spoofed source address to disguise itself.
- Address Resolution Protocol (ARP) is a protocol that resolves IP addresses to MAC addresses for

transmitting data. ARP spoofing sends spoofed ARP messages across a LAN to link the criminal's MAC address with the IP address of an authorized member of the network.

- The Domain Name System (DNS) associates domain names with IP addresses. DNS server spoofing modifies the DNS server to reroute a specific domain name to a different IP address controlled by the criminal

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.
Click the steps in the figure to learn the basics of a MitM attack.
Man-In-The-Mobile (MitMo) is a variation of man-in-middle. MitMo takes control over a mobile device. The infected mobile device sends user-sensitive information to the attackers. ZeuS, an example of an exploit with MitMo capabilities, allows attackers quietly to capture 2-step verification SMS messages sent to users. For example, when a user sets up an Apple ID, he or she must provide an SMS-capable phone number to receive a temporary verification code via text message to prove the user's identity. Malware spies on this type of communication and relays the information back to the criminals.
A replay attack occurs when an attacker captures a portion of a communication between two hosts and then retransmits the captured message later. Replay attacks circumvent authentication mechanisms.

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, as shown in the figure. Defending against these fast-moving attacks requires network security professionals to adopt a more sophisticated view of the network architecture. It is no longer possible to contain intrusions at a few points in the network.

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.
Keyboard loggers can be legitimate, commercial software. Parents often purchase key logger software to track the websites and behavior of children using the Internet. Many anti-spyware applications are able to detect and remove unauthorized key loggers. Although keylogging software is legal, criminals use the software for illegal purposes.

Defending Against Attacks

An organization can take a number of steps to defend against various attacks. Configure firewalls to discard any packets from outside of the network that have addresses indicating that they originated from inside the network. This situation does not normally occur, and it indicates that a cybercriminal attempted a spoofing attack.
To prevent DoS and DDoS attacks, ensure patches and upgrades are current, distribute the workload across server systems, and block external Internet Control Message Protocol (ICMP) packets at the border. Network devices use ICMP packets to send error messages. For example, the ping command uses ICMP packets to verify that a device can communicate with another on the network.
Systems can prevent falling victim to a replay attack by encrypting traffic, providing cryptographic authentication, and including a time stamp with each portion of the message. Click here to learn more about ways to prevent cyber attacks.

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. For example, Grayware can track the user's location. The authors of grayware usually maintain legitimacy by including an application's capabilities in the small print of the software license agreement. Users install many mobile apps without really considering their capabilities.

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.
A rogue access point can also refer to a criminal's access point. In this instance, the criminal sets up the access point as a MitM device to capture login information from users.
An Evil Twin attack uses the criminal's access point improved with higher power and higher gain antennas to look like a better connection option for users. After users connect to the evil access point, the criminals can analyze traffic and execute MitM attacks.

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

Bluetooth is a short-range, low-power protocol. Bluetooth transmits data in a personal area network, or PAN, and can include devices such as mobile phones, laptops, and printers. Bluetooth has gone through several version releases. Easy configuration is a characteristic of Bluetooth, so there is no need for network addresses.
Bluetooth uses pairing to establish the relationship between devices. When establishing the pairing, both devices use the same passkey.
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.

- 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.

WEP and WPA Attacks

Wired Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network (WLAN) with the same level of security as a wired LAN. Since physical security measures help to protect a wired LAN, WEP seeks to provide similar protection for data transmitted over the WLAN with encryption.
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.

Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by observing traffic. WPA2 is susceptible to attack because cyber criminals can analyze the packets going between the access point and a legitimate user. Cyber criminals use a packet sniffer and then run attacks offline on the passphrase.

Defending Against Wireless and Mobile Device Attacks

There are several steps to take to defend against wireless and mobile device attacks. Most WLAN products use default settings. Take advantage of the basic wireless security features such as authentication and encryption by changing the default configuration settings.
Restrict access point placement with the network by placing these devices outside the firewall or within a demilitarized zone (DMZ) which contains other untrusted devices such as email and web servers.
WLAN tools such as NetStumbler may discover rogue access points or unauthorized workstations. Develop a guest policy to address the need when legitimate guests need to connect to the Internet while visiting. For authorized employees, utilize a remote access virtual private network (VPN) for WLAN acces

Cross-Site Scripting

Cross-site scripting (XSS) is a vulnerability found in web applications. XSS allows criminals to inject scripts into the web pages viewed by users. This script can contain malicious code.
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.

XML Injection

When using an XML database, an XML injection is an attack that can corrupt the data. After the user provides input, the system accesses the required data via a query. 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. An XML injection attack threatens the security of the website.

SQL Injection

The cybercriminal exploits a vulnerability by inserting a malicious SQL statement in an entry field. Again, the system does not filter the user input correctly for characters in an SQL statement. Criminals use SQL injection on websites or any SQL database.

Criminals can spoof an identity, modify existing data, destroy data, or become administrators of the database server.

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. The generic classification of buffer overflows includes many variants, such as static buffer overruns, indexing errors, format string bugs, Unicode and ANSI buffer size mismatches, and heap overruns.

ActiveX Controls and Java

When browsing the web, some pages may not work properly unless the user installs an ActiveX control. ActiveX controls provide the capability of a plugin to Internet Explorer. ActiveX controls are pieces of software installed by users to provide extended capabilities. Third parties write some ActiveX controls and they may be malicious. They can monitor browsing habits, install malware, or log keystrokes. ActiveX controls also work in other Microsoft applications.

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. Java is the second biggest security vulnerability next to Adobe's Flash plugin.

Defending 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.