Information Security

Lecture: 6-7

Dr. Tehsin Kanwal
Assistant Professor

What Are Common Types of Attacks?

Depending on the attacker's goal and objective, many different types of attacks can suit their needs and abilities. These attacks can be summarized in three categories:

- **Attacks on availability—**These attacks impact access or uptime to a critical system, application, or data.
- **Attacks on people—**These attacks involve using coercion or deception to get another human to divulge information or to perform an action (e.g., clicking on a suspicious URL link or opening an email attachment from an unknown email address).
- **Attacks on IT assets—**These attacks include penetration testing, unauthorized access, privileged escalation, stolen passwords, deletion of data, or performing a data breach

What Is Malicious Software?

- Some software infiltrates one or more target computers and follows an attacker's instructions.
- These instructions can include causing damage, escalating security privileges, divulging private data, or even modifying or deleting data.
- This type of software is malicious software, or malware for short.

Types of Malware

- **Infecting programs** actively attempt to copy themselves to other computers. Their main purpose is to carry out an attacker's instructions on new targets. Malware of this type includes the following:
  - Viruses
  - Worms
- **Hiding programs** hide in the computer, carrying out the attacker's instructions while avoiding detection. Malware that tends to hide includes the following:
  - Trojan horses
  - Rootkits
  - Spyware

Viruses

- A computer virus is a software program that attaches itself to or copies itself into another program on a computer.
- The purpose of the virus is to trick the computer into following instructions not intended by the original program developer.
- Users copy infected files from another computer on a network, from a flash drive, or from an online service.
- Alternatively, users can transport viruses from home and work on their portable computers, which have access to the Internet and other network services.

Worms

- A worm is a self-contained program that replicates and sends copies of itself to other computers, generally across a network, without any user input or action.
- The worm's purpose may be simply to reduce network availability by using up bandwidth, or it may take other nefarious actions.
- The main difference between a virus and a worm is that a worm does not need a host program to infect. The worm is a standalone program.

Virus	Worm
Virus infects a system by inserting itself into a file or executable program	Worm infects a system by exploiting a vulnerability in an OS or application by replicating itself
It might delete or alter content in files, or change the location of files in the system	Typically, a worm does not modify any stored programs. It only exploits the CPU and memory
It alters the way a computer system operates, without the knowledge or consent of a user	It consumes network bandwidth, system memory, etc., excessively overloading servers and computer systems
A virus cannot be spread to other computers unless an infected file is replicated and actually sent to the other computer	A worm, after being installed in a system, can replicate itself and spread by using IRC, Outlook, or other applicable mailing programs
A virus is spread at a uniform speed, as programmed	A worm spreads more rapidly than a virus.
Viruses are hard to remove from infected machines	As compared with a virus, a worm can be easily removed from a system

Trojan Horses

- A Trojan horse, is malware that masquerades as a useful program.
- Trojan horse programs look like it perform useful tasks, but actually, they hide malicious code. Once the program is running, the attack instructions execute with the user's permissions and authority.
- The first known computer Trojan was Animal, released in 1974. Animal disguised itself as a simple quiz game in which the user would think of an animal and the program would ask questions to attempt to guess the animal.
- In addition to asking questions, however, the program copied itself into every directory to which the user had write access.

Rootkits

- A rootkit modifies or replaces one or more existing programs to hide traces of attacks.
- Rootkits commonly modify parts of the operating system to conceal traces of their presence.

- Rootkits can exist at any level
  - Computer's boot instructions
  - the applications that run in the operating system

- Once installed, rootkits provide attackers with easy access to compromised computers to launch additional attacks.

TIP

Rootkits often work with other malware. For example, suppose a program, malware.exe, is running on a Windows system. A simple rootkit might replace the Windows Task Manager with a modified version that does not list any program named malware.exe. Administrators would not know the malware program is running.

Spyware

- Spyware is a type of malware that specifically threatens the **confidentiality** of information. It gathers information about a user through an Internet connection, without his or her knowledge.
  - Spyware can also spread via peer-to-peer file swapping.
  - Once installed, spyware monitors user activity on the Internet. Spyware can also gather information such as email addresses and even passwords and credit card numbers. The spyware can relay these data to the author of the spyware.
  - The author might use the data simply for advertising or marketing purposes but could employ it to facilitate identity theft.

Adware

- Adware is similar to spyware but does not transmit personally identifiable information (PII).
- PII is any information that can help identify a specific person. Examples of PII include driver's license numbers, Social Security numbers, credit card numbers, and so on. Instead, information collected by adware is meant to optimize marketing campaigns.
- For example, adware can help deliver popups tailored to purchasing habits or can be used for market research purposes. A popup is a type of window that appears on top of the browser window. Popups generally contain ads. Although popups are not strictly adware, many adware programs use them to interact with users. Some software products include an option for blocking popups.
- Spyware and adware have rapidly become increasingly common threats to computers, with some experts estimating that more than 90 percent of computers are already infected.
- Fortunately, a number of software suppliers make antispyware and anti-adware software. In fact, many antivirus and general anti-malware software programs also detect and remove spyware and adware. Sorting through these programs to find the right offering for your organization is a challenging task—but an important one

Social Engineering Attacks

- Social engineering is the art of one human attempting to deceive another human into doing something or divulging information.
- Criminals use social engineering tactics to get humans to divulge information about themselves or someone else.
- This is key in order to obtain private data to perfect identity theft.
- Hackers also attempt to social engineer targeted employees into divulging information about IT systems or applications so that the hackers can gain access.

Summary of social engineering attacks

- **Authority**—Using a position of authority to coerce or persuade an individual to divulge information.
- **Consensus/social proof**—Using a position that "everyone else has been doing it" as proof that it is okay or acceptable to do.
- **Dumpster diving**—Finding unshredded pieces of paper that may contain sensitive data or private data for identity theft.
- **Familiarity/liking**—Interacting with the victim in a frequent way that creates a comfort and familiarity and liking for an individual (e.g., a delivery person may become familiar to office workers over time) that might encourage the victim to want to help the familiar person.
- **Hoaxes**—Creating a con or a false perception in order to get an individual to do something or divulge information.
- **Impersonation**—Pretending to be someone else (e.g., an IT help desk support person, a delivery person, a bank representative).
- **Intimidation**—Using force to extort or pressure an individual into doing something or divulging information.
- **Scarcity**—Pressuring another individual into doing something or divulging information for fear of not having something or losing access to something.

Summary of social engineering attacks

- **Shoulder surfing**—Looking over the shoulder of a person typing into a computer screen.
- **Tailgating**—Following an individual closely enough to sneak past a secure door or access area.
- **Trust**—Building a human trust bond over time and then using that trust to get the individual to do something or divulge information.
- **Urgency**—Using urgency or an emergency stress situation to get someone to do something or divulge information (e.g., claiming that there's a fire in the hallway might get the front desk security guard to leave her desk).
- **Vishing**—Performing a phishing attack by telephone in order to elicit personal information; using verbal coercion and persuasion ("sweet talking") the individual under attack.
- **Whaling**—Targeting the executive user or most valuable employees, otherwise considered the "whale" or "big fish" (often called *spear phishing*).

Summary of social engineering attacks

- **Shoulder surfing**—Looking over the shoulder of a person typing into a computer screen.
- **Tailgating—**Following an individual closely enough to sneak past a secure door or access

area.

- **Trust—**Building a human trust bond over time and then using that trust to get the individual to do something or divulge information.
- **Urgency—**Using urgency or an emergency stress situation to get someone to do something or divulge information front desk security guard to leave her desk).
- **Vishing—**Performing a phishing attack by telephone in order to elicit personal information;
- **Whaling—**Targeting the executive user or most valuable employees (often called spear phishing

Wireless Network Attacks

- Wireless Network Attacks Wireless network attacks involve performing intrusive monitoring, packet capturing, and penetration tests on a wireless network.
- Given the rapid deployment of wireless network connectivity in both public and private places, the mobile user is under constant threat.
- Wireless networks may be compromised as a network access point into your IT infrastructure

Wireless Network Attacks

Bluejacking—Hacking and gaining control of the Bluetooth wireless communication link between a user's earphone and smartphone device.

Bluesnarfing—Packet sniffing communications traffic between Bluetooth devices.

Evil twin—Faking an open or public wireless network to use a packet sniffer on any user who connects to it.

IV attack—Modifying the initialization vector of an encrypted IP packet in transmission in hopes of decrypting a common encryption key over time.

Jamming/interference—Sending radio frequencies in the same frequency as wireless network access points to jam and interfere with wireless communications and disrupting availability for legitimate users.

Near field communication attack—Intercepting, at close range (a few inches), communications between two mobile operating system devices.

Packet sniffing—Capturing IP packets off a wireless network and analyzing the TCP/IP packet data using a tool such as Wireshark®.

Replay attacks—Replaying an IP packet stream to fool a server into thinking you are authenticating to it.

Rogue access points—Using an unauthorized network device to offer wireless availability to unsuspecting users.

War chalking—Creating a map of the physical or geographic location of any wireless access points and networks.

War driving—Physically driving around neighborhoods or business complexes looking for wireless access points and networks that broadcast an open or public network connection.

Web Application Attacks

- Web application attacks involve performing intrusive penetration tests on public-facing web servers, applications, and back-end databases.
- Given the rapid deployment of e-commerce and customer or member portals and websites, access to private data, sensitive data, intellectual property is abundant.
- Many different tactics are used by hackers and perpetrators when attempting to penetrate and attack web applications.

Web Application Attacks

- **Arbitrary/remote code execution**—Having gained privileged access or sys admin rights access, the attacker can run commands or execute a command at will on the remote system.
- **Buffer overflow**—Attempting to push more data than the buffer can handle, thus creating a condition where further compromise might be possible.
- **Client-side attack**—Using malware on a user's workstation or laptop, within an internal network, acting in tandem with a malicious server or application on the Internet (outside the protected network).
- **Cookies and attachments**—Using cookies or other attachments (or the information they contain) to compromise security.
- **Cross-site scripting (XSS)**—Injecting scripts into a web application server to redirect attacks back to the client. This is not an attack on the web application but rather on users of the server to launch attacks on other computers that access it.
- **Directory traversal/command injection**—Exploiting a web application server, gaining root file directory access from outside the protected network, and executing commands, including data dumps.
- **Header manipulation**—Stealing cookies and browser URL information and manipulating the header with invalid or false commands to create an insecure communication or action.
- **Integer overflow**—Creating a mathematical overflow which exceeds the maximum size allowed. This can cause a financial or mathematical application to freeze or create a vulnerability and opening.
- **Lightweight Directory Access Protocol (LDAP) injection**—Creating fake or bogus ID and authentication LDAP commands and packets to falsely ID and authenticate to a web application.

Web Application Attacks

- **Local shared objects (LSO)**—Using **Flash cookies** (named after the Adobe Flash player), which cannot be deleted through the browser's normal configuration settings. Flash cookies can also be used to reinstate regular cookies that a user has deleted or blocked.
- **Malicious add-ons**—Using software plug-ins or add-ons that run additional malicious software on legitimate programs or applications.
- **SQL injection**—Injecting Structured Query Language (SQL) commands to obtain information and data in the back-end SQL database.
- **Watering-hole attack**—Luring a targeted user to a commonly visited website on which has been planted the malicious code or malware, in hopes that the user will trigger the attack with a unknowing click.
- **XML injection**—Injecting XML tags and data into a database in an attempt to retrieve data.
- **Zero-day**—Exploiting a new vulnerability or software bug for which no specific defenses yet exist.

References

- David Kim, Michael G. Solomon Fundamentals of Information Systems Security, 4th Edition, Jones & Bartlett Learning, ISBN: 9781284116465 (https://books.google.com.pk/books?id=DiVGEAAAQBAJ&printsec=copyright&redir_esc=y#v=on epa ge&q&f=false)