Computer Security

Rajesh Palit, Ph.D.

Electrical & Computer Engineering

North South University

NIST Definition of Computer Security

- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Threats/Consequences

- Loss of Confidential Data
- Loss in Productivity
- Identity Theft
- Compromised Data Integrity
- Unavailability of Access to Data or Computer Network
- Lawsuits & Judicial Actions
- Termination of Employment

Security Attack Types

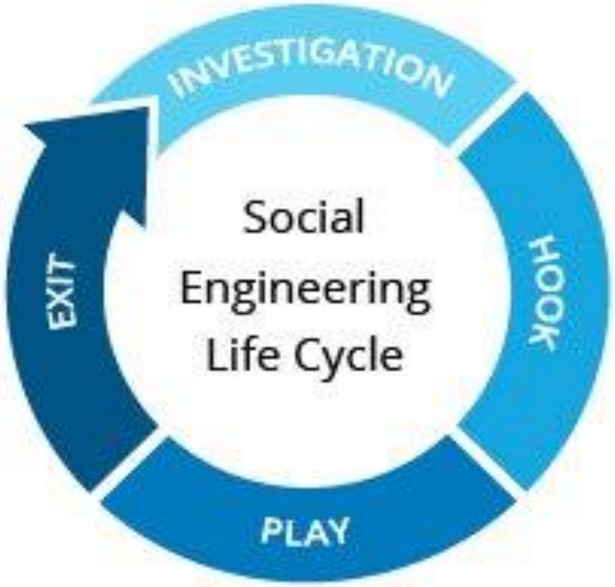
1. Social Engineering – Baiting, Scareware, Phishing, Pretexting
2. Reverse Social Engineering
3. Malicious Software
   a. Virus
   b. Worm
   c. Trojan Horse
   d. Spyware
   e. Ransomware
   f. adware
   g. Rouge Antivirus
   h. Rootkit
   i. Cookies
   j. Autorun worm
4. Keylogger
5. DDOS

Social Engineering

- This term used for a broad range of malicious activities accomplished through human interactions.
- It uses psychological manipulation to trick users into making security mistakes or giving away sensitive information.
- A perpetrator first investigates the intended victim to gather necessary background information, such as potential points of entry and weak security protocols, needed to proceed with the attack.
- The attacker moves to gain the victim’s trust and provide stimuli for subsequent actions that break security practices, such as revealing sensitive information or granting access to critical resources.

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).



Closing the interaction,
ideally without arousing suspicion:

- Bringing the charade to a natural end.
- Removing all traces of malware.
- Covering tracks.

Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Social Engineering Attack – Baiting

- Baiting attacks use a false promise to pique a victim’s greed or curiosity
- They lure users into a trap that steals their personal information or inflicts their systems with malware.
- The most reviled form of baiting uses physical media to disperse malware. For example, attackers leave the bait—typically malware-infected flash drives—in conspicuous areas where potential victims are certain to see them (e.g., bathrooms, elevators, the parking lot of a targeted company)
- The bait has an authentic look to it, such as a label presenting it as the company’s payroll list.
- Baiting scams don’t necessarily have to be carried out in the physical world. Online forms of baiting consist of enticing ads that lead to malicious sites or that encourage users to download a malware-infected application.

Social Engineering Attack – Scareware

- Scareware involves victims being bombarded with false alarms and fictitious threats.
- Users are deceived to think their system is infected with malware, prompting them to install software that has no real benefit (other than for the perpetrator) or is malware itself.
- Scareware is also referred to as deception software, rogue scanner software and fraudware.
- A common scareware example is the legitimate-looking popup banners appearing in your browser while surfing the web, displaying such text such as, “Your computer may be infected with harmful spyware programs.” It either offers to install the tool (often malware-infected) for you, or will direct you to a malicious site where your computer becomes infected.
- Scareware is also distributed via spam email that doles out bogus warnings, or makes offers for users to buy worthless/harmful services.

Social Engineering Attack – Pretexting

- Here an attacker obtains information through a series of cleverly crafted lies. The scam is often initiated by a perpetrator pretending to need sensitive information from a victim so as to perform a critical task.
- The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. The pretexter asks questions that are ostensibly required to confirm the victim's identity, through which they gather important personal data.
- All sorts of pertinent information and records is gathered using this scam, such as social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Social Engineering Attack – Phishing

- As one of the most popular social engineering attack types, phishing scams are email and text message campaigns aimed at creating a sense of urgency, curiosity or fear in victims. It then prods them into revealing sensitive information, clicking on links to malicious websites, or opening attachments that contain malware.
- An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action on their part, such as a required password change. It includes a link to an illegitimate website—nearly identical in appearance to its legitimate version—prompting the unsuspecting user to enter their current credentials and new password. Upon form submittal the information is sent to the attacker.
- Given that identical, or near-identical, messages are sent to all users in phishing campaigns, detecting and blocking them are much easier for mail servers having access to threat sharing platforms.

Social Engineering Attack – Spear Phishing

- This is a more targeted version of the phishing scam whereby an attacker chooses specific individuals or enterprises. They then tailor their messages based on characteristics, job positions, and contacts belonging to their victims to make their attack less conspicuous. Spear phishing requires much more effort on behalf of the perpetrator and may take weeks and months to pull off. They're much harder to detect and have better success rates if done skillfully.
- A spear phishing scenario might involve an attacker who, in impersonating an organization's IT consultant, sends an email to one or more employees. It's worded and signed exactly as the consultant normally does, thereby deceiving recipients into thinking it's an authentic message. The message prompts recipients to change their password and provides them with a link that redirects them to a malicious page where the attacker now captures their credentials.

Reverse Social Engineering Attack

- Reverse social engineering is a very unique form of social engineering. In most social engineering attacks, the attacker goes to the victim to obtain information. In reverse social engineering, however, the victim unwittingly goes to the attacker
- Reverse social engineering is performed through the following steps:
  - An attacker first damages the target's equipment.
  - He next advertises himself as a person of authority, ably skilled in solving that problem.
  - In this step, he gains the trust of the target and obtains access to sensitive information.
- If this reverse social engineering is performed well enough to convince the target, he often calls the attacker and asks for help.

Social Engineering Prevention

- Social engineers manipulate human feelings, such as curiosity or fear, to carry out schemes and draw victims into their traps. Therefore, be wary whenever you feel alarmed by an email, attracted to an offer displayed on a website, or when you come across stray digital media lying about.
- Being alert can help you protect yourself against most social engineering attacks taking place in the digital realm. Moreover, the following tips can help improve your vigilance in relation to social engineering hacks.
- **Don't open emails and attachments from suspicious sources** – If you don't know the sender in question, you don't need to answer an email. Even if you do know them and are suspicious about their message, cross-check and confirm the news from other sources, such as via telephone or directly from a service provider's site. Remember that email addresses are spoofed all of the time; even an email purportedly coming from a trusted source may have actually been initiated by an attacker.
- **Use multifactor authentication** – One of the most valuable pieces of information attackers seek are user credentials. Using multifactor authentication helps ensure your account's protection in the event of system compromise. Imperva Incapsula Login Protect is an easy-to-deploy 2FA solution that can increase account security for your applications.
- **Be wary of tempting offers** – If an offer sounds too enticing, think twice before accepting it as fact. Googling the topic can help you quickly determine whether you're dealing with a legitimate offer or a trap.
- **Keep your antivirus/antimalware software updated** – Make sure automatic updates are engaged, or make it a habit to download the latest signatures first thing each day. Periodically check to make sure that the updates have been applied, and scan your system for possible infections

Computer Virus (Vital Information Resource Under Siege)

- Perhaps the most well known computer security threat, a computer virus is a program written to alter the way a computer operates, without the permission or knowledge of the user.
- A virus replicates and executes itself, usually doing damage to your computer in the process.
- The term 'computer virus' was first formally defined by Fred Cohen in 1983. Computer viruses never occur naturally. They are always induced by people.
- Once created and released, however, their diffusion is not directly under human control. After entering a computer, a virus attaches itself to another program in such a way that execution of the host program triggers the action of the virus simultaneously.
- It can self-replicate, inserting itself onto other programs or files, infecting them in the process. Not all computer viruses are destructive though.

Computer Worm

- A worm is a standalone program that doesn’t require user intervention to spread. Worms don’t infect existing files – they spread copies of themselves instead.
- It fits the description of a computer virus in many ways. For example, it can also self-replicate itself and spread across networks. That is why worms are often referred to as viruses also.
- But computer worms are different from computer viruses in certain aspects. First, unlike viruses which need to cling on to files (host files) before they can diffuse themselves inside a computer, worms exist as separate entities or standalone software.
- They do not need host files or programs. Secondly, unlike viruses, worms do not alter files but reside in active memory and duplicate themselves.

Trojan Horse Malware

- A Trojan horse program presents itself as a useful computer program, while it actually causes havoc and damage to your computer.
- Increasingly, Trojans are the first stage of an attack and their primary purpose is to stay hidden while downloading and installing a stronger threat such as a bot.
- Unlike viruses and worms, Trojan horses cannot spread by themselves.
- They are often delivered to a victim through an email message where it masquerades as an image or joke,
- or by a malicious website, which installs the Trojan horse on a computer through vulnerabilities in web browser software such as Microsoft Internet Explorer.
- After it is installed, the Trojan horse lurks silently on the infected machine, invisibly carrying out its misdeeds, such as downloading spyware, while the victim continues on with their normal activities.

Computer Spyware

- Spyware is a general term used for programs that covertly monitor your activity on your computer, gathering personal information, such as usernames, passwords, account numbers, files, and even driver’s license or social security numbers.
- Some spyware focuses on monitoring a person’s Internet behavior; this type of spyware often tracks the places you visit and things you do on the web, the emails you write and receive, as well as your Instant Messaging (IM) conversations.
- After gathering this information, the spyware then transmits that information to another computer, usually for advertising purposes.
- Spyware is similar to a Trojan horse in that users unknowingly install the product when they install something else. However, while this software is almost always unwelcome, it can be used in some instances for monitoring in conjunction with an investigation and in accordance with organizational policy.
- Most often spyware is installed unknowingly with some other software that you intentionally install. For example, if you install a "free" music or file sharing service or download a screensaver, it may also install spyware. Some Web pages will attempt to install spyware when you visit their page.

Ransomware

- Ransomware is a malicious program that performs the following malicious activities after infecting a computer.
  - Makes the system non-functional unless the victim agrees to pay a ransom.
  - Encrypts the computer’s data and demands a ransom to release it to the victim.
- this malware variety hijacks files (and sometimes an entire hard drive), encrypts them, and demands money from its victim in exchange for a decryption key (which may or may not work, but it probably won’t).
- The ransomware business model has a number of benefits over banking trojans and other forms of malware:
  - First, it’s easier to launder cryptocurrencies than it is to launder traditional money. Additionally, if the funds aren’t withdrawn right away, the fluctuation of Bitcoin could make the ransom even more valuable.
  - Second, since fewer people are involved in the operation, the Controlling Coders keep most of the stolen currency.

Financially-Motivated Ransomware

- 1. Locky first appeared in February 2016 and is now one of the most distributed forms of ransomware. In late 2016 it became so proliferate that it was named one of the three most common forms of malware. There are distribution campaigns of Locky via email almost every day.
- 2. Troldesh is mostly distributed in Russia and European countries. It is not prevalent in the U.S.
- 3-5. GlobeImposter, Philadelphia, and Cerber are all ransomware threats using the “Ransomware as a Service” (RaaS) model. While some cyber criminals make and distribute their own ransomware, some have begun to provide a software package—complete with ransom note customization—to other cyber criminals for a fee.

Disruption-Motivated Ransomware

Interestingly, some of the biggest ransomware names of 2017 are believed to be motivated by operational disruption or systemic harm, *not* financial gain. Two recent attacks used a single Bitcoin wallet to collect ransom, placing greater emphasis on the disruption itself rather than payment collection; this tactic also makes it impossible for the distributor to know which victims actually paid the ransom requested.

- 6. **WannaCry** is a wormable ransomware that spreads like a virus. Interestingly, it only collected a bit over $100,000 dollars total, quite a small sum considering its global spread. To that point, between May 12 and May 15, 2016, WannaCry was observed on over 160,000 unique IP addresses.
- 7. **NotPetya** used a compromised accounting software provider as its initial point of distribution, and impacted many Ukrainian companies. But NotPetya didn’t stop in Ukraine. Multinational companies with arms in Ukraine were compromised as well. While NotPetya was also not believed to be financially motivated, it did impact the bottom line of some large companies. According to this Insurance Journal article, “Package delivery company FedEx Corp. said on Tuesday a June [NotPetya] attack on its Dutch unit slashed $300 million from its quarterly profit, and the company lowered its full-year earnings forecast. The company said the cyber attack slashed 79 cents per share from its profit.”
- 8. **Bad Rabbit** is a variant of NotPetya that was also primarily distributed in Ukraine and Russia to a number of major corporations. NotPetya and Bad Rabbit share the same code, indicating that the same group is responsible for both ransomware examples. But unlike NotPetya, Bad Rabbit uses unique Bitcoin wallets for every victim. For this reason, the motivation behind these attacks is unclear.

Adware

- this exceedingly irritating kind of malware floods victims with unwanted ads, and opens up vulnerable security spots for other malware to wiggle its way in.

Rogue Antivirus

- A rogue antivirus, also known as scareware, is a fake program that disguises itself as a genuine software but performs malicious activities in user’s machine.
- Not so safe: security software can put computers at risk
- Antivirus software is 'increasingly useless' and may make your computer less safe
- http://www.cbc.ca/news/technology/antivirus-software-1.3668746

Rootkit

- A rootkit is a program (or a collection of programs) that in itself is not harmful, but helps viruses and malware
- Rootkits are a particularly insidious form of malware because they load before an operating system boots and can hide from ordinary antimalware scans and protection. Their ability to elude detection also makes them extraordinarily difficult to remove and clean up after.re hide from antivirus software.

Rootkit symptoms

- A typical symptom of rootkit infection is that antimalware protection stops working. You will get alerts about various causes that prevent antimalware from protecting your PC. If an antimalware application simply refuses to run, you have reason for concern, because this is often an unequivocal indicator that a rootkit infection is active.
- Another clear symptom is when Windows settings change independently, without any user interaction. If you notice unexpected behavior, such as pinned items changing on the Taskbar or background images changing or disappearing (such as on the lock screen or in the screen saver), that might also indicate a rootkit infection.
- Frozen input devices can also signal infection. If you suddenly get no response from your mouse or keyboard, lasting from a few seconds to few minutes, check to see if USB devices and other I/O devices keep disconnecting and reconnecting. If such behavior occurs in tandem with inoperative antimalware programs and/or mysterious changes to Windows settings, rootkit infection becomes a distinct possibility.
- Finally, monitor your network usage. When a system is idle, there should be only minimal network traffic. If, however, your machine sends and receives a lot of data when apparently idle, this might indicate an infection. Use Resource Monitor to check which processes or services are involved with the traffic. Do not trust the process or service names shown. Instead, you must try to determine whether those processes or services have valid, understandable reasons to access the network. If not, such behavior may signal a rootkit masking itself as a normal Windows process (or processes).

Cookies

- Cookies are files on your computer that enable websites to remember your details. When you visit a website, it can place a file called a cookie on your computer. This enables the website to remember your details and track your visits. Cookies can be a threat to confidentiality, but not to your data.

Autorun Worms

- Autorun worms are malicious programs that take advantage of the Windows AutoRun feature.
- They execute automatically when the device on which they are stored is plugged into a computer.

Keyloggers

- A keylogger builds a log of everything typed into a keyboard to be reviewed by a third party.
- Keyloggers can be used for legitimate purposes to troubleshoot networks, analyze employee productivity, or to assist law enforcement, for example; or they can be used for illegitimate purposes to surreptitiously spy on people for personal gain.
- A keylogger can be a hardware device or a software program.
- Keyloggers are indeed a real threat to your Internet security and privacy. Some keylogging programs can even take snapshots of the users Desktop, record both side of instant messenger chat conversations(AOL, Windows Messenger, ICQ, etc.), and record every website the unsuspecting computer user makes.

DDOS (Denial-of-service attack)

- A denial-of-service (DoS) attack prevents users from accessing a computer or website. In a DoS attack, a hacker attempts to overload or shut down a computer, so that legitimate users can no longer access it.
- Typical DoS attacks target web servers and aim to make websites unavailable. No data is stolen or compromised, but the interruption to the service can be costly for a company.

Recommendations

- Mannan, Haynes and Sjouwerman all have similar recommendations:
  - **Back up everything regularly.** You can back up photos and non-sensitive files to the cloud. But you should also keep a backup on an external hard drive that is not physically connected to your computer (otherwise it can be compromised in a ransomware attack). That way, if you get attacked by ransomware or another threat, you can roll back to the previous version of your computer.
  - **Keep your operating system and software such as browsers up to date and patched. Turn on automatic updates if they're available.**
  - **Think before you click on links or attachments.** If you're not sure about them, get in touch with the person who sent them to double-check.