Medicon Engineering Themes
Volume 2 Issue 4 April 2022
Research Article

Hacking Human: Hacking the Weakest link in the Security Chain

Eman Ali Metwally[1]* and Haytham Tarek Mohammed[2]

[1]*Faculty of Computers and Information Science, Mansoura University, Mansoura, Egypt*

[2]*Faculty of Computers and Information Science, Mansoura University, Mansoura, Egypt*

***Corresponding Author:** Eman Ali Metwally, Faculty of Computers and Information Science, Mansoura University, Mansoura, Egypt.

Received: March 15, 2022; **Published:** March 31, 2022

Abstract

"Social engineering (SE) is the art of operating people into performing actions or divulging confidential information". It is unique of the best creative and active means of achievement access to secure systems and gaining sensitive information up till now wants negligible technical knowledge. SE does not certainly need a big amount of official information in instruction to be successful. SE depends on person's psychology such as interest, courteousness, unwariness, greed, inattentiveness, wariness, and indifference. This paper shows the state of the art attacking methods especially SE and its countermeasures that will help the user be more secure and aware of these attacks.

Introduction

SE is aimed at persons who are looking for information. It manipulates human emotions in order to gain entry to restricted areas or obtain sensitive information for various purposes. The framework of SE attacks and many sorts of SE tactics are presented in this survey. Type, Operator, and Channel are the three different categories of SE attacks. SE attacks can take two forms: psychological and physical. In this attack, the attacker gathers sensitive information from a target and uses it for malicious purposes such as causing public embarrassment, financial loss, and service disruption. This survey presents mitigation methods and techniques for protecting sensitive information from SE attacks.

People, on the other hand, freely publish information through online communication and collaboration platforms like cloud services and social networks, with little regard for security or privacy [1]. A SE attack exploits this flaw by employing a variety of manipulative techniques to obtain sensitive information. In terms of formal definitions and attack frameworks, the topic of SE is still in its infancy [2].

A practical definition of Information Security

"Information Security" is an old term related to SE old school and here, it is important to know its meaning. The term of "information security" means protecting not only information but also information systems against an unauthorized usage, access, alternation, modification and or destruction to provide.

a) Integrity, which means saving and protecting against unauthorized data modification or destruction, as well as ensuring no repudiation and validity of data.
b) Confidentiality, which entails maintaining approved access and disclosure limits, as well as safeguards for personal privacy and proprietary data; and
c) Availability, which entails ensuring fast and reliable access to and use of data [3].

This definition is applied on the term of a user, firm or any connected business will suffer harm if there is a misbalance of confidentiality, integrity and or information availability. For that reason, Information security has a number of advantages as not to maximize the possibility of any harm occurrence.

Theoretic model of the SE threat

The information security definition proposed in the previously mentioned paragraph, means protecting assets that belongs to an electronic space As a result, there's a chance that all assets, electronic space, and terminals must be well protected.

As shown in Figure 1.1, any information space consists of an important part as humans and the technics. Both, from the information science point of view, store (i.e. knows) the assets that need to be protected (e.g., credentials).

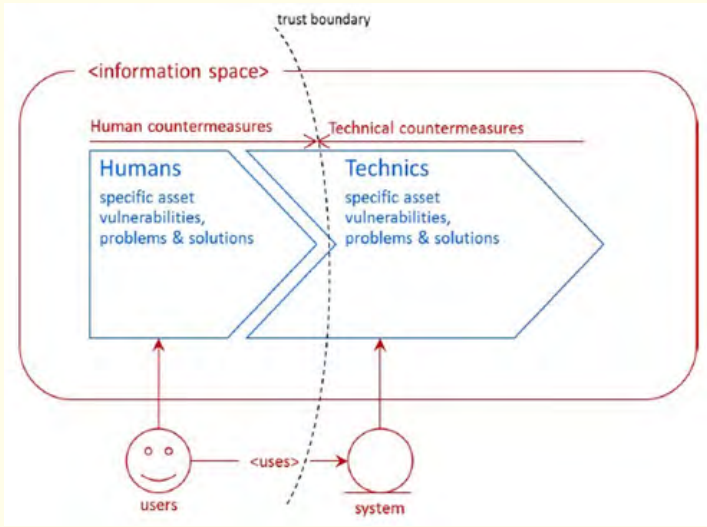

Figure 1.1: Model of information includes technology and the human data spaces.

A model level is presented in [4] based on triangle representation in which its three corners are Social (groups of people), Human (single human) and Technology. These angles form a space where the origin is and where all potential attacks occur, Figure 1.2 shows real representation of the concepts which is mapped over this theoretical model, although the Old School SE is stucked in the place in between human and social corners which is a little bit closer to human, and its "classic" classification keeps it outside the technology corner. Figure 1.3 describes how the modern strategies used and might fall into this triangle while the "classic" approach keeps it far from the technology corner. It describes how strategies used in modern attacks' could fall into this triangle [4].

Modern SE techniques are being widely used in addition to a complex mixture of different competencies (technological, cyber sociology, psychology, marketing, design, etc.) to create a full attack. In the other hand, the presence of the continuous development of the technological assets and cybercrime lessen the needed complexity level for launching the attack, threatens larger number of people to be victimized with SE [4].

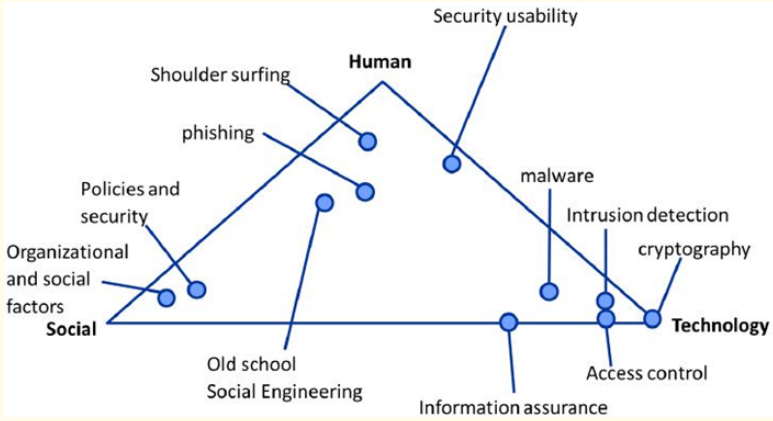

Figure 1.2: Security triangle in the old school of SE.

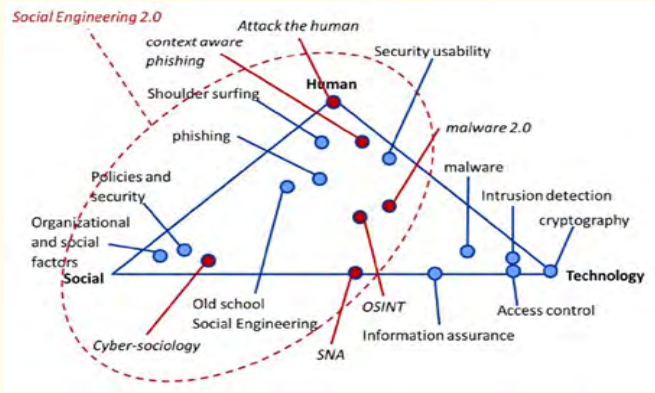

Figure 1.3: Security triangle of the modern school of SE.

Classifying SE Attacks

There are many researchers who have classified SE attacks with different classifications as:

Katharina Krombholz et al. have classified [5] SE attacks as follows in figure 1.4 as they defined SE attacks after forming three main categories: Based on Type, based on Operator, and a Channel based category.

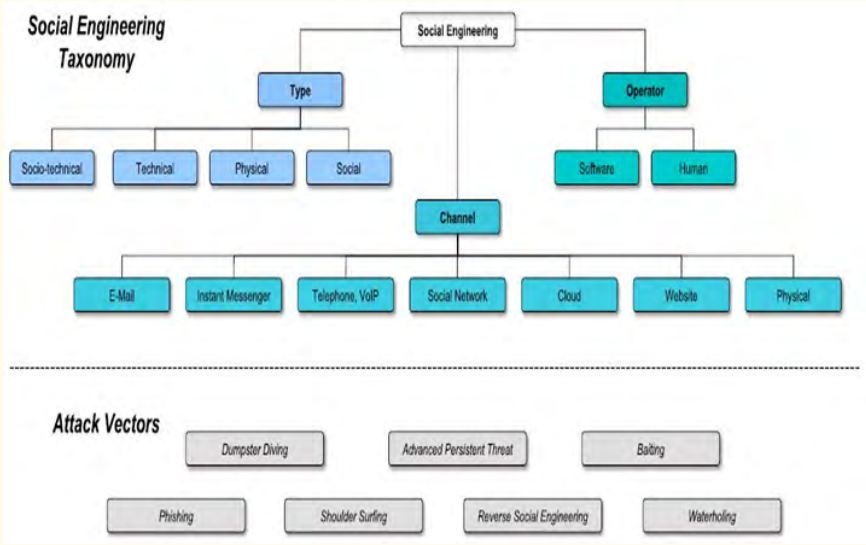

Figure 1.4: Attack Characteristics Classification and attack scenarios.

Classification of attack characteristics

There are three different main categories: Type, Operator, and Channel. In classifying the attack according to its operator. A SE attack can be carried out by:

- ***Humans*** If the attack is carried out directly by a human. In comparison to a software-based attack, the number of targets is limited due to capacity constraints. As noted by Boshmaf et al. in [6] and Huber et al. in [7], some sorts of SE attacks are simple to automate. The fundamental advantage of automated attacks is that they may hit a large number of targets in a short amount of time. The other Classification of the attack based on the channel over which an attack is launched can be as follows:
- ***E-Mail*** which is the most well-liked channel for implementing phishing attacks and the reversed SE attacks.
- ***Instant Messenger*** is famous between social engineers for conducting phishing and reversed SE. It is easily to be used for conducting the identity theft to exploit a trustworthy relationship.
- ***Telephone, Voice over IP*** They are common attack channels for social engineers to let a victim provide physically sensitive information.
- ***Social Networks*** It offers opportunities for social engineers to perform the expected attacks. Due to their ability to create fake identities and their complex model of sharing information, they make it simple for attackers to get into anonymize them and gather sensitive information.
- ***Cloud services*** are used for creating situational awareness within a collaboration scenario. Attackers might put a file or program in a shared ledger to get the victim to hand information to them.
- ***Websites*** They are most commonly used for water-holing attacks. Moreover, they can be used with emails to carry out a phishing attack as sending a banking email to a (potential) client of a bank that contains a link to a malicious website that looks exactly like the bank's website as the original site.
- ***Physical SE*** attacks are expensive, but they are extremely successful. This attack channel addresses the situation where the attacker is physically present while the attack is being carried out.

SE attack scenario

- ***Phishing*** Refers to the act of trying to get access to confidential information or get someone to act in the interest of the attacker

by posing as a reliable entity in an electronic means of communication. Phishing attacks can be executed on almost any channel, ranging from the physical presence of the attacker to websites, social networks, or even cloud services. Aside from the traditional phishing attacks, attacks that target specific individuals or companies are referred to as spear phishing. Spear phishing requires the attacker to gather information about the targeted victims, so the success rate is higher than not identifying a target group. If the phishing attack targets prominent enterprise targets, then the attack is referred to as whaling.

- ***Dumpster Diving*** It is the practice of sifting through physical waste or waste data of individuals or companies to find discarded items that contain sensitive information that can be used to settle a specific system or user account.
- ***Reverse SE*** Describes an attack that typically involves establishing trust between the attacker and the victim. The attackers create a situation where they must assist the target individual and then pretend to be some of the people whom the victim will recognize as individuals who can solve the victim's problem and obtain unique information. Of course, attackers try to choose someone they think has information to help them.
- ***Water holing*** is a type of targeted attack in which the attackers gain access to a website that is likely to be of interest to the intended victim. The hacked website has been left and the attackers are waiting on a "water pit" like a predator for their victim to visit. "water- hole" like a predator for their victim to visit.
- ***Advanced Persistent Attack*** It refers to long-range spying attacks that often take place on the Internet that are carried out by an attacker with the capabilities and intent to continuously configure a system.
- ***Baiting*** Indicates an attack in which malware-infected storage media is left in a location that future targeted victims will likely find.

Approaches to SE in Different Forms

Attacks under SE are complicated and have many aspects as the physical, the social, technical aspects or features that are being used in different platforms during the real scenario attack. As shown in Figure 1.5.

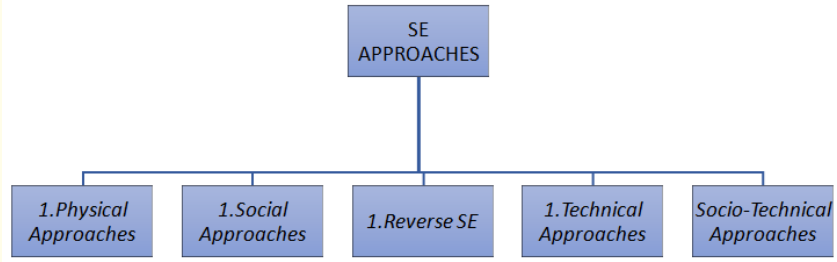

Figure 1.5: Representation of SE Approaches.

Physical Approaches

The intruder launches a form of physical actions for the reason of gaining information on a potential victim, these physical actions can vary from collecting personal information as date of birth, address, ID number to provide credentials for a computer system. Dumpster diving is another famous way for collecting information as it means digging at person and or an organization's trash [1, 8].

Social Methodologies

The most common type of social attack is happening over the phone. To increase the chances of these attacks, perpetrators try to develop a relationship with their future victims in advance [1].

Hereby attackers rely on socio-psychological techniques such as Cialdini's principles of persuasion [9] to manipulate their victims as persuasion with authority. Curiosity, which is employed in spear-phishing and luring attempts, is one common social vector that

Cialdini does not specifically address. According to [8], the most common type of social attack is one that is carried out over the phone.

Reverse SE

Rather than approaching the victim directly, attackers can try to persuade them to seek assistance from them. Reverse SE is a term for an indirect method like this. Then the attackers declare that they can solve the problem. Finally, when the victim requests the help of social engineers for solving the problem they previously created, and while doing so, ask the victims to comply with their requests [10] it is divided into three sections: sabotage, advertising, and aiding [11].

Technical Approaches

Often, users use the same credentials for more than one account. In addition to, most people are providing their personal information without no care of sequences, and that is so helpful for attackers. Therefore, the intruders use online search engines to gain personal information related to their potential victims. Noting that there are many available tools for collecting and aggregating information from different web resources [8].

Socio-Technical Approaches

Successful SE attacks often combine several or all the different techniques discussed above. However, social, and technical methods have created the social engineers' most powerful munitions. One example is a so-called phishing attack: Attackers accept malware-infected storage media in a location victim are likely to find in the future. In contrast, SE is classically directed at individuals or small groups of people. Fraudsters hope to fool enough people by sending messages to a large number of users to make the phishing attack profitable [12]. Hence, Spear phishing is being used against high-level targets, and is responsible for some recent, high-profile corporate data breaches [13, 5].

SE characteristics

The literature describes many of SE characteristics and types of exploits. To simplify this, Table 1.1 summarizes the main or salient characteristics of The SE. attacks, typical information sought, and possible outcomes or consequences of the attack. It is more likely to be the same steps and consequences used in cyber-attacks in general. Somehow the method of attack may differ especially regarding its main characteristics.

These characteristics describing SE incidents and identifying patterns of this attack.

Various techniques used for SE attack

The method in [14] Presented a classification of SE into two categories as shown in Figure 1.6 based on psychological attacks and physical attacks:

Salient characteristics	*Typical information requested*	*Potential consequences and outcome*
Appeal	• Account info • Username • Password and pin • Credit card number • Social security number • Bank account number • Bank routing number • Email address • Telephone number • Other personal information	• Financial loss • Identity theft • Stealing personal or confidential information • Intellectual property stolen • Implanting malware or virus • Destroying data, hardware asset and software • Denial of service
• Usually good or bad news • Sense of urgency • Sensitive or confidential matter • Impersonating known sender		
Desired Response		
• Provide specific information • Update personal account information • Clicking on link inside a message • Attachment opening		
Suspicious indicators		
• Poor grammar or spelling • Strange or unusual sender • Incorrect information • Illegitimate embedded URLs		

Table 1.1: SE incidents and identifying patterns.

Figure 1.6: Techniques used for SE.

Psychological Attacks

SE uses emotions like fear, curiosity, enthusiasm, empathy, and greed, as well as cognitive biases, to manipulate people.

Phishing

Phishing is defined as a technical method of collecting information through fraud, or usually, the act of sending an email to a target

that appears from a legitimate organization in an attempt to trick the victim into revealing private information, which could be used in identity theft. The email usually contains a link that directs the victim to a fake webpage where he is requested to update or change information about his account with a legitimate entity, such as a bank, but you must first log in. However, the website is designed to steal sensitive data such as passwords and credit card details. Phishing is a type of SE assault that takes the shape of an email or other online communication medium [15].

Spear Phishing

Any highly focused email or phone scam, commonly used in a commercial setting, is known as spear phishing. Spear phishing is a type of phishing that targets a specific set of people. So instead of spamming thousands of emails, phishing scammers target select groups of people who have something in common [8].

Watering Holes

This is a type of SE attack where cyber criminals identify important websites that individuals or groups would like to attack, such as mobile app developers. Then these targeted websites become infected with malware. An example of one such attack was the device for iOS mobile developers that hosted malware targeting Apple and Facebook [14].

Spoofing

"A spoofing attack occurs when a malicious actor impersonates a device or other network user in order to conduct attacks against network hosts, steal data, spread malware, or circumvent access controls".

Trojan Horse

Some social engineers exploit people's curiosity or greed to introduce "malware". The criminal sends an email with something free or urgent attached. The attachment can be called: the tracking number for the courier parcel or the winning prize. Opening the attachment downloads the Trojan horse to your computer. A Trojan horse can be designed to track keystrokes, download an address book, or search for financial software files for modification [14].

Physical Attacks

Dumpster Diving

The criminals take advantage of this law and try to deduce any secret information that could lead them to the victim's personal information. The attacker looks for the victim's phone number, credit card information, and other sensitive information.

In the case of an organization, however, the dumpster diver will look for the organization's phone books, policies, charts, and even meeting calendars [15].

Shoulder Surfing

When attackers try to monitor the shoulder of the victim for a password, PIN, or other sensitive information. In most crowded places, this type of attack works effectively while the attacker can sit behind the victim and observe the entry of his personal identification number into an ATM machine, enter the password to the system or even when he fills out forms that need sensitive information to present [15].

Road Apples

Refers to situations where the cybercriminal drops physical media such as CD or USB flash drives that have been rated to arouse curiosity ("Executive Salary Survey", "HR Reduction Scheme", "Secret Organizational Changes"). Once employees prefer media and slots in a computer to view, the AutoPlay feature will download a Trojan horse or virus to track keystrokes and harvest identifiers and passwords [14].

Staff Impersonation

The attacker convinces any employee of the IT department over the phone that he is an authorized person who has forgotten his password and needs the IT team's assistance in generating a new password. While most IT workers will ask the caller (who they believe is an authorized person) for basic information such as his complete name or date of birth, the attacker can readily respond, particularly if he has obtained all of the authorised person's information [15].

Countermeasures of SE

Anti-Phishing Tools

It is recommended to use anti-phishing tools that connect to a database of blacklisted phishing sites. Some examples include Web Sense, McAfee Anti-Phishing Filter, Net-craft Anti-Phishing System and Microsoft Phishing Filter. This cannot provide 100% security since phishing sites are cheap, easy to build, and have an average life of just a few days.

Increase of the Population of Cyber Security Professionals

There is a shortage of cyber security professionals due to the ever-changing threats and the need for monitoring and response; more professionals are required to be trained in this field.

Use of appropriate Internet Security Technologies

Companies with an online presence should make sure their Secure Sockets Layer (SSL) or a more robust version of the technology, Extended Validation (EV) SSL certificates are up to date and from reputable service providers; this is the only way to protect customers and businesses from phishing attacks. These are two crucial security features that might assist users in distinguishing between real and fraudulent websites.

Social Network Vulnerabilities

Individuals should not add strangers to their networks for their own safety, and they should use privacy settings on social networking sites that provide the most security and limit information shared with the social networking community.

Strong Passwords

Individuals should help themselves by having a strong password and changing it regularly. Organizations must ensure compliance with office networks. It is recommended that you do not use the same passwords for all accounts. Many people store vital information on phones, to avoid identity theft, these phones should have a password [14].

Education and Training

This includes developing security vigilance/ awareness programs and training to train employees in anti-SE techniques. It should also include regular rest on the necessity of security awareness.

Policy and Management

This includes creating simple rules that define sensitive information as well as defining clear and concise security policies that are routinely implemented throughout the company. This also requires applicant identity when requesting restricted procedures and develops data classification policy.

Auditing and Testing

This includes assessing employees' susceptibility to SE attacks. This countermeasure's purpose is to guarantee that staff are informed of the threat and that existing vulnerabilities are discovered [16].

Semantic Attacks

Semantic attacks is defined in [17] as "the manipulation of a user's interaction with the computer with the purpose of penetrating the security of computer system information by deceiving the user." The majority view of semantic attacks currently observed is presented in Table 1.2, which aggregates terms commonly used by information security practitioners to identify semantic attack exploits in related attack families. This consistent approach fails to capture common features of exploits clustered within different attack families. For example, a phishing URL on a webpage or email may share a similar obfuscation / phishing method with that used for a phishing video URL on a social networking site (SNS). Therefore, a defense mechanism that would defeat a particular method is likely to be beneficial for both types of semantic attacks [18].

Attack Families	***Exploits***
Phishing	Email, Website, URL, IM, Forums, SMS IRC
File Masquerading	Office Document File, Application File, System File
Application Masquerading	Scareware, Ransomware, Rogue ware
Web Pop-Up	Media Plugin, Error Message, Bogus Questionnaire
Malvertisement	Infected Ad, one click fraud, Download button
Social Networking	Friend injection, Fake Video Links, Game Requests
Removable media	USB, Flash, CD/DVD
Wireless	Rouge AP, Rouge RFID

Table 1.2: Semantic Attack Exploits.

The type of exploit does not typically constitute a single attack, but rather a step that occurs within a more complex sequence of actions that compose a larger fraud scheme as Single or multiple phase semantic attack as shown in Figure 1.7 in [19].

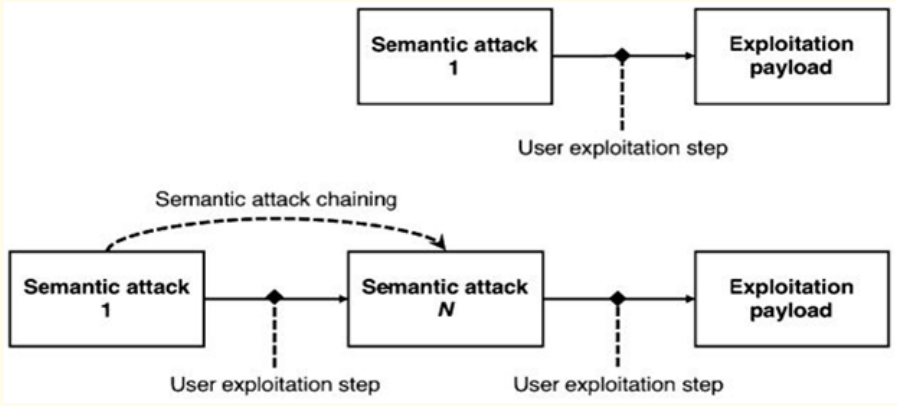

Figure 1.7: Attack model for a single phase and multi-phase semantic attack.

Types of Semantic Attacks in today's Information system

As mentioned in [18] and [19] by R. Heart field et.al, the different types of SSE (Semantic SE) attack are describes in Table 1.3, referring to a number of 35 different type. Because semantic attacks target the user interface and computer, it is very difficult for technical defenses to identify them. This is because the attacks primarily use cosmetic or behavioral phishing vectors that usually leave very few technical traces of a computer program to analyze a technical semantic attack.

Attack Pseudonym	*Description*
Spam	Inappropriate / spam messages sent over the Internet to a large number of users, often contain ad fraud.
Phishing	Attempting to gain access to sensitive information by masquerading as a trustworthy entity in electronic communication.
Spear phishing	Phishing attack designed to target a specific person and organization.
Pharming	Installing malicious code on a personal computer or server, and falsely directing users to fake websites without knowledge or consent.
Whaling	The type of phishing attack that targets prominent end users such as corporate executives, politicians, and celebrities.
QRishing	Phishing attack using Quick Response (QR) codes to distribute malicious files / links.
Blue snarfing	The phishing attack lures users to install malware that gives access to the target device via the Bluetooth protocol.
Drive by download	Implanting a malicious file through programmatic processing of texts on a vulnerable web platform.
Rogue AP	Wi-Fi access point installed on a network but is not authorized for operation on that network and appears to be legitimate
WIFI evil twin	A fraudulent WIFI access point that often spoofs other nearby access points that appears to be legitimate
Rogue ware	Standalone malware program pretending to be a well-known program or a non-malicious one in order to steal sensitive data
Scareware	Malicious program tricking a user into buying/downloading unnecessary often malicious software.
Visual SSL spoofing	Process of using fake SSL verification logos or browser GUI components to visually masquerade as a secure website.
SSL spoofing	MITM attack that intercepts HTTPS web requests, redirecting the users to malicious and fake HTTPS website
Adware	Software that automatically displays or downloads advertising material such as banners or pop-ups when a user is online
Waterhole	Targeted version of a Drive By download attack, typically targeting platforms a victim accesses.
File masquerading	Disguising a malicious file to appear as a legitimate file type
Multimedia masquerading	Disguising a malicious application appear as multimedia.
GUI confusion	A mobile application confusing user by impersonating as another app (e.g., banking app) to obtain sensitive information
Trojan horse	Type of malware that is often disguised as legitimate software, such as a game that is actually a key-logger
Self XSS	Operates by tricking users into copying and pasting malicious content into their browsers' web developer console
Typo squatting	Registering similar domain names which rely on typographical errors when inputting a website address into a browser

Share baiting	Enticing web content persuading users to share on their profile, often used to spread fake apps and phishing URLs
Browser extension malware	Malicious browser-add similar to Trojan app that steals personal information and/or add browser to attacker botnet
Mad ware	Aggressive advertising placement in mobile devices photo albums, calendar entries and notification bar
Fake plugin	Malicious media plugin typically spread by through a fake video post on social media posting
Fake App	Variation of trojan horse, rogue ware, scareware on mobile devices where a malicious app masquerade as a legitimate one.
Torrent poisoning	Intentionally sharing corrupt data and malware with misleading file names using
Cursor jacking	Variation of clickjacking where users are deceived by means of a custom cursor image and the pointer is displayed with an offset
Touch jacking	Variation of clickjacking which applies to mobile devices where users touch the interface instead of using a mouse.
DNS cache poisoning	Process by which DNS server records are illegitimately modified to replace a website address with a different address
Spamdexing	Manipulation of search engine indexes where a website repeats unrelated phrases to manipulate relevance.
Like jacking	Variation on clickjacking in which malicious coding is associated with a Facebook Like button
Click jacking	Concealing hyperlinks beneath legitimate click-able content, causing the user to perform actions of which they are unaware

Table 1.3: Different types of semantic attack observed in today's computer systems.

Defense lifecycle against semantic attacks

In Figure 1.8, as mentioned by G. Loukas et al. in [19]. The defence lifecycle against semantic threats is made up of three interconnected defence phases. Platform security, platform developer, and platform user.

Platform developer

Responsible for both user interface and internal functionality development for a secure but robust platform against technical threats or misuse of intended user space functionality that could lead to phishing vectors for semantic attacks.

Platform safety is important. The security job is in charge of both implementing preventative security measures (such as preventing vulnerabilities from being exploited or platform abuse) and supporting proactive defences.

Platform user

The sheer reliance on the platform's security, as well as the external technical defensive mechanisms offered by platform users, is frequently insufficient as a defence to identify a wide range of threats.

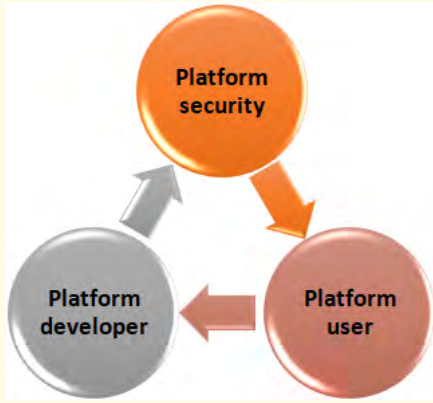

Figure 1.8: Defense lifecycle against semantic attacks.

Platform user

The sole reliance on the security of the platform along with the external technical defense mechanisms provided by the users of the platform is often insufficient as a defense to detect a wide range of semantic attacks, especially when the phishing vector uses legitimate user space functions.

Conclusion

The SE in information security systems is the art of availing the weakest point. It is a general term for a wide range of exploiting a computer that depends on a set of attack methods in order to deceive the user. This technique is used for bypassing the IDS (intrusion detection system), access control systems and firewalls. The main danger here is in its legitimate appearance; because the victim could not recognize that he is victimized and that leads to many security breaches [20, 21].

References

1. K Krombholz, H Hobel, M Huber and E Weippl. "SE attacks on the knowledge worker". SIN 2013 - Proc. 6th Int. Conf. Secur. Inf. Networks (2013): 28-35.
2. F Mouton, MM Malan, L Leenen, and HS Venter. "SE attack framework". 2014 Inf. Secur. South Africa - Proc. ISSA Conf (2014).
3. B Lundgren and N Möller. "Defining Information Security". Sci. Eng. Ethics 25.2 (2019): 419-441.
4. E Frumento., et al. "Advanced SE and Vulnerability Assessment Framework The role of SE in evolution of attacks". (2016): 147.
5. K Krombholz, H Hobel, M Huber and E Weippl. "Advanced SE attacks". J. Inf. Secur. Appl 22 (2015): 113-122.
6. Y Boshmaf, I Muslukhov, K Beznosov and M Ripeanu. "The Socialbot Network: When bots socialize for fame and money". ACM Int. Conf. Proceeding Ser (2011): 93-102.
7. E Weippl and S Roat. "Friend-in-the-middle Attacks Friend-in-the-middle Attacks". (2010).
8. S Granger. "SE Fundamentals, Part I: Hacker Tactics | Symantec Connect". Soc. Eng. Fundam 1527 (2001).
9. NJ Goldstein, ASU Cialdini and Robert B. "The Science and Pratice of Persuasion". Cornell Hotel Restaur. Adm. Q (2002): 40-50.
10. Kevin D Mitnick and WL Simon. "The art of deception: Controlling the human element of security". John Wiley Sons 70.3 (2001): 2001.
11. R Nelson. "Methods of Hacking: SE". Inst. Syst. Res (2001): 2-5.
12. TA Kher, SL Kariya and I Technology. "A Survey on SE : Techniques and Countermeasures". 4.7 (2016): 258-260.
13. J Hong. "The state of phishing attacks," Commun. ACM 55.1 (2012): 74-81.
14. EU Osuagwu, GA Chukwudebe, T Salihu, and VN Chukwudebe. "Mitigating SE for improved cybersecurity". CYBER-Abuja 2015 -

Int. Conf. Cybersp. Gov. Imp. Natl. Econ. Secur. - Proc (2015): 91-100.

15. AS Alazri. "The awareness of SE in information revolution: Techniques and challenges". 2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST (2016): 198-201.
16. A Algarni, Y Xu, and T Chan. "SE in social networking sites: The art of impersonation". Proc. - 2014 IEEE Int. Conf. Serv. Comput. SCC (2014): 797-804.
17. FL Greitzer., et al. "Analysis of unintentional insider threats deriving from SE exploits". Proc. - IEEE Symp. Secur. Priv (2014): 236-250.
18. R Heartfield and G Loukas. "A taxonomy of attacks and a survey of defence mechanisms for semantic SE attacks". ACM Comput. Surv 48.3 (2015): 1-38.
19. R Heartfield and G Loukas. Protection against Semantic SE Attacks.
20. JM Hatfield. "SE in cybersecurity : The evolution of a concept". Comput. Secur 73 (2018): 102-113.
21. M Jakobsson. Understanding SE Based Scams (2016).

Volume 2 Issue 4 April 2022