International Journal of Mathematics and Computational Science
Vol. 1, No. 4, 2015, pp. 188-198
http://www.aiscience.org/journal/ijmcs

Social Engineering Attack Mitigation

Ahmad Uways Zulkurnain, Ahmad Kamal Bin Kamarun Hamidy, Affandi Bin Husain, Hassan Chizari*

Department of Computer Science, Faculty of Computing, Universiti Teknologi Malaysia, Skudai, Johor Bahru, Johor, Malaysia

Abstract

Protected from threats that can Information assets is the lifeblood for every organization and also for individual. These assets must be jeopardized the confidentiality, integrity and availability of the information. This is why the information security is important. Since the introduction of Internet and ICT, the information has been digitized for ease of information exchange which also increasing the risks to the information security. Nevertheless, the rapid growth in technology enables digital or technical based threats and attacks to be easily detected and prevented. This makes people with malicious intents turn their focus into another more sophisticated and hard-to-detect attacks, which is through social engineering. Social engineering preys on psychological and emotional aspects of human to gain access to restricted area or obtain sensitive information for various purposes. There are several human psychological traits that have been used by social engineers to manipulate human as human is the weakest link in information security. By using these traits, attacking strategy is laid out to accomplish the attacker's mission whether to gain access or to gather critical information. In this paper, few researches regarding mitigation of social engineering will be discussed. Social engineering mitigation method can be roughly divided into human based detection and technology based detection. Each of the mitigation methods proposed in the researches has its own strength and weaknesses. It has been found that using just one category of mitigation method is not enough to detect and prevent the social engineering attacks. The methods need to be used together to enhance and increase the accuracy of detection so that the social engineering attacks can be stop and prevented.

Keywords

Social Engineering, Attacks, Mitigations, Artificial Intelligence, Honeypot

Received: April 8, 2015 / Accepted: May 1, 2015 / Published online: June 3, 2015

1. Introduction

An asset in every organization consists of hardware, software, people, service and information. These assets are exposed to attacks or unauthorized access that can threaten the confidentiality, integrity and availability of the information. Manipulating compromised assets can bring further destruction towards the targeted organization, society or even human. There are a lot of threats and attacks that have been done in recent years that damaged organization's assets and reputation. This brings information security into the picture. The advancement of security technology enables most of the digital or technical based attacks and threats to be detected and prevented. However, attackers have searched for other more sophisticated ways of attacking the assets, which leads to social engineering attack. Social engineering became one of the most concerning problem faced by the organization and society. Social engineering is a method of attacks that related to psychological aspect of human where social engineering attacks the trust element of the human nature (Sandouka*et. al.*, 2009). Social engineering is the art of influencing or persuading people to deceive the targeted

* Corresponding author
E-mail address: chizari@fc.utm.my (H. Chizari)

personnel into revealing sensitive information of organization with or without the use of technology. In information world nowadays, software is not the weakest link in information security anymore. Human that operates information system is the main weakest link in the information security (Peltier, 2007). The main goal of social engineering is to gain access to certain information system, organization or other places that kept valuable assets without authorization by deceiving authorized personnel to give access to them. The next section will explain more about social engineering motives and their modus operandi.

1.1. Motivation of Social Engineering

There are several motives that drive social engineers to make such operation as being mentioned by Spinapolice (2011) and Oosterloo (2008), which are economic profit or financial gain, personal interest, personal grievance or revenge, external pressure and politics. Sensitive information obtained from social engineering attacks of personnel in an organization may become a source of financial and becomes an object of trading to the highest bidder among business competitors. Social engineers also may execute their attacks to gain information just out of curiosity towards the organization or certain information system without any malicious intent. Social engineers even do their operation as an intellectual challenge to satisfy their desire. Revenge or personal grievance is one of the motive that moves social engineers who are usually former staff, business competitors or someone who does not agreed to that organization's policies to damage the targeted organization's reputation or business to satisfy their grudge towards that organization. External pressures usually come from other peers within a group or subculture where they're challenging themselves to see who is the best among them. Social engineering may also operate based on political aspect where members from each political parties try to do social engineering attacks to gain critical information about their opposition or personal life information of their opposition's leader and used it to damage their reputation or to against them in political war.

1.2. Methods of Operation

To operate social engineering attacks, one must know the fundamental of human traits or psychological principles that can be used in exploiting their victims. Spinapolice (2011) quoted that there are six traits that social engineers will focus on to gain victim's trust in giving desired information which are reciprocation, commitment, social proof, friendliness, authority and scarcity. Reciprocation stated that people will automatically have the conscience to repay favors or information in return to the person they feel obligated (Workman, 2007). Reciprocation is the easiest to exploit and most commonly used by social engineers. People are easily indebt with the provider and even may introduced unequal exchanges of favors or information. Unequal exchange will make people who are indebt paying more than what have been originally given even if the original favor from the social engineers was not being asked for in return (Oosterloo, 2008). Commitment is where someone who has made his decision has the feeling of responsibility and will carry it out despite of inability to realize his decisions. This has been an advantage for the social engineer to pressure their target in disclosing sensitive information. When an attacker asked a series of question and the victim already answered those questions with unnecessary information, the attacker can further his or her question for disclosing sensitive information and the victim is pressured in providing the attacker with the answer that will disclose sensitive information. Social proof is used to intimidate someone within an organization to provide information by implanting the sense of conformity to that person into believing that other person have already done what the attacker is asking him or her to do. The victim is presented with proof of his or her colleagues' compliance and it makes the victim feels more secure and at ease in providing the attacker with desired information. Social proof is proven to be effective when the victim's colleagues are not around.

Friendliness exploits the sense of intimacy where people tend to be more open to the person whom they are friendly with. Social engineers use their high soft skills to befriend with the victim and try to make victim disclose sensitive information. The victim is willingly to give information to the person who has positive characteristics such as kind, social and courteous. People are also tending to be obedient to someone who has authority such as policeman, high-ranked government officer and so on. Social engineers use authoritative figures to make people follow their rules, requests or orders in hope of rewards or fear of punishments. Scarcity plays on the human psychology by suggesting that if certain action is not taken, they will be in tremendous loss or disadvantage situation. Business advertisement such as "Buy now, offer valid while stock last" or "Limited time offer, act now!" is one of the social engineering examples in terms of pursuing company profits instead of deception. In example of social engineering attacks, social engineer with malicious intent may set up a fake website look like legitimate retailer website selling products which are rare and hard to get items at affordable or low price, deceiving their victims into signing up forms that contains private information of the victims such as address, credit card information or online banking information. In the next section, this paper will discuss more on social engineering attack strategies, related works that have been done by researches in combating social engineering,

conceptual solution on mitigating social engineering attacks and finally conclusion of this paper.

1.3. Attacking Strategies

There is a common pattern that can be associated with social engineering attacks. According to Malcolm Allen (2006), this pattern can be referred to as 'the cycle' as shown in Figure 1.1. The cycle of social engineering consists of four phases, which are information gathering, relationship development, exploitation and execution. However, each individual social engineering attack is unique which may see use of repeating phases, multiple cycles, or incorporate other, more traditional attacks into the mix.

Information gathering or footprinting is the phase where attackers prepare their flow and identify target before launching an attack. The first phase, does not only includes gathering target related information; instead it is also gathers other (physical) attributes needed in the next phases of the attack, for example recreating letterheads of official documents or learning lingo or jargon that is related to the target. Various techniques can be used by an attacker to gather information about their target. Once gathered, this information can then be used to build a relationship with either the target or someone important that can help lead to a successful attack. The common mistakes made by personnel divulging the information is that they do not understand the value of the information to the social engineer, which led to information disclosure. These can include revealing information that is seemingly harmless from a security standpoint but can be useful for the attacker.

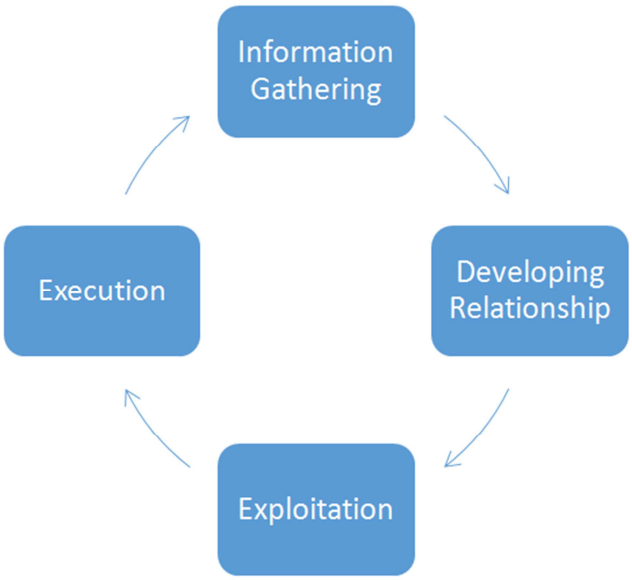

Figure 1.1. Social Engineering Attack Cycle.

In relationship development, an attacker exploits the natural willingness of a target to be trusting and develops rapport with them. While developing this relationship, the attacker will manoeuvre him into a position of trust which he can then exploit. Human has the nature to be trusting and caring for others. Social engineers often exploit these attributes to manipulate and influence targets to build authenticity and obtain trust. The act of manipulation can be done through interaction such as physical or virtual. Virtual interaction is an interaction through mediums such as phone, e-mail or even social media. There are basic psychological principles underlying manipulations such as overloading, reciprocation, and diffusion of responsibility, moral duty and authority. These principles will be discussed in the next section, social engineering attack tools and techniques. To summarize, trusts created by psychological principle creates a situation in which the social engineer's request in not questioned by the target, this situation thus create vulnerabilities in the security. During this stage, the social engineer can improve their success rates by using a less aggressive approach to avoid conflicts, such as appealing the targets by using senses like sound and sight to strengthen the trust relationships; but more important is that the social engineer needs to have relative amount of knowledge of the target and be willing to compromise. During this phase of relationship development, information gathering is not important as it is the stage where relationships are established to prepare the target for exploitation. Therefore, there is a strong link between relationship development and exploitation.

Exploitation is the act of the using the target to disclose information or perform actions that compromise the security of an information system by allowing unauthorized access, unauthorized use, or unauthorized disclosure. During this phase extended information or more specific information which was not available during the first phase can be obtained. By using the relationship and trust created with the target through the manipulation during the previous phase, social engineers now have the access to the target location or by applying other similar tactics. For instance, the target may be manipulated by the 'trusted' attacker to reveal passwords or perform actions like deleting a record that would not occur under normal operations. The attack could end at this point or continue to the next stage.

The execution phase is the phase where social engineer utilizing what has been achieved during the previous phase which means it is not specifically related to social engineering, nor the start of a new cycle. However, actions in this final phase could achieve the ultimate goal of the attack. To elaborate, actions made in this phase are more towards technical nature rather than psychological, for example during the execution phase actions taken are in the fields of hacking and cracking or plain theft rather than social engineering; though this phase attract special attention

because the success of this phase relies on the success of the social engineering act. For instance, in an attempt exploit a computer system that cannot be compromised from remote networks, gaining physical access to the system and uploading malware makes this objective achievable. The end goal of the attack could also be theft or destruction of a physical asset, which requires social engineering to obtain knowledge of its location and gain access to it. During this phase any information salvaged will depends on the attacker's goal though it might also be the whole information of the target's organization's infrastructure.

1.4. Social Engineering Tools and Techniques

This part of the paper is to elaborate different social engineering tactics used in an attack. The tactics are first deployed in the information-gathering phase. At this phase of social engineering cycle collecting information and attributes of the target does preparation for the next phase. Tactics used by social engineers for information gathering ranges from physical to virtual. One of the basic methods for gathering information is physical reconnaissance. Physical reconnaissance is an attack in which the social engineer will study about the organization through observation techniques such as shoulder surfing (spying during a situation e.g: ATM withdrawal) and eavesdropping (secretly listening to a conversation e.g: tapping phone lines) or even stalking (physically following a person). The intent of these activities is to gather useful information and pattern for the next step.

Another technique similar to physical reconnaissance is people spotting and dumpster diving. People spotting are the technique of loitering around a certain location a period of time to find targets related to the goal. Dumpster diving is a the technique which require the attacker to go through the discarded bin of the targeted organization searching for potentially information that should have been destroyed or artifacts such as official stationery which could be useful during other phases such as building relationship or exploitation. The plus point of dumpster diving is that it does not endanger social engineer in as it is not against the law in many countries. Forensic analysis is a social engineering technique similar to dumpster diving. Social engineer usually uses this technique on discarded artifact by an organization such as hard drives memory stick or a flash drive, which was not destroyed or erased properly as these artifacts might still have information written in it.

Aside from the previously mentioned tactics, which are largely passive and do not engage the targets directly, there are also more aggressive tactics used by social engineering attackers. As an example, phreaking breaks into a telephone system and manipulates the system, for example, the social engineers can change an exposed number by spoofing the caller's ID or by making the call reroutes to their own number. Phishing is a technique on electronic communication where social engineer baits for information and passwords by masquerading (appearing) as a trustworthy person or business. Previously, before it was popular on the Internet, phishing was performed by phone, which is why the technique it is spelt as phishing. The current method of phishing over the internet are in the form an e-mail or pop-up directing the target to a page similar to the page targets are familiar with, this page usually will demand user to log in their username and password. Mail-out is another phishing technique which social engineers use to gather information. An example of mail-out is a survey given to employees of an organization; in which offering prize as if it is a lucky draw contest. Mail-out is a technique that can also be used for malware spreading, usually attached within the files sent out to target. As Mail-out is a tool for social engineering, it can also be used to set up targets for reverse social engineering.

Social engineers can also gather needed knowledge and information through public sources such as web search and used to perform profiling of the target. Internet tools such as Search engines (e.g: Google, Yahoo, Bing), newsgroups (E.g: Yahoo), job sites (e.g: Jobstreet, LinkedIn) and corporate websites which most of them often revel too much information. Many organizations do not possess proper knowledge on information security, faithfully leaving the security to a third party, making the job easier for the social engineer to salvage desired information. With the increase of information sharing though social networks, valuable information may also be unintentionally leaked by employees through public discussions, status updates, and photos. Profiling is then done when information gathering is complete and will then be used for exploitation and execution. By profiling the lingo and routines of a chosen target, social engineers can now use what have been gathered to exploit the victim's information or impersonate the victim's for the social engineer's benefits. By using the victim's profile, weaknesses of the system will be revealed and information can be used to exploit and manipulate different targets, with these social engineers will be able to show authenticity by understanding the knowledge of an organization's business processes and internal language.

With the information-gathering phase complete, the attack tactics can now be employed by the social engineer. One of the primary tactics used by social engineers is impersonation. Social engineer will use the profiles of a targeted victim by following a scripted routine of an individual; this will be acoushion for the social engineer, as they would not be exposed in case the attack backfired because they are using a fake profile and identity is still unknown. Impersonation can

be performed virtually on the Internet for example by creating a fake profile and also physically in person by creating official organization items or stealing it. The most common roles, which are impersonated, include authority figures, colleagues, a new employee or intern in need of help, or someone offering help (Osterloo, 2008).

Once physical access can be gained through physical impersonation, the attacker can then employ additional tactics to further their access into the target premises. One of the easiest technique a social engineer could gain access to a restricted premise physically is by tailgating. Tailgating can be done by simply tailing an employee or delivery personnel whom are granted access to the targeted area without needing neither proper authorization nor verification. Social engineers will execute this action by waiting for the secure door to be unlocked by someone and get in before the door is closed discreetly to avoid suspicion. This way social engineer will not need to salvage information or create fake formal artifact to get access though it is risky and require a contingency plan in case the execution fails, usually the fallback plan retract to use impersonation. In larger organizations, most employees do not know every one of their coworkers will sometimes keep the door open, especially when a lady is passing by. Social engineer exploits the human nature of caring for others to enter the premise; though this plan will require social engineer to face a legitimate employee with a proper access, which means the social engineer will still need to impersonate as someone with legitimate access for example by wearing a corporate shirt of wearing a fake ID tag. Once inside the social engineer will be able to infiltrate the system and plan malwares, tapping bugs, packet sniffer, a tiny camera or may also be a helpdesk number for a reverse social engineering attack. A direct approach can also be used by the social engineer by asking directly from a chosen target for desired information or access; but the direct approach will be too risky as target is bound to get suspicious and chances of further manipulation is very low. Another technique that is used by social engineer to divert attention from being suspicious is to make different calls to different targets to get different kinds of desired information or access; this will create a situation where the target will answer to the request raising any questions toward as the social engineer will not pose a lengthy request

Most tactics are used in the information gathering stage where it is crucial to collect the right information about the target and to build an accurate profile of the one that will be impersonated. Once the actual attack is done, it is up to the social engineer to ensure flawless execution and do improvisation in unexpected situations. With the correct tactics employed and sufficient preparation by the social engineer, a social engineering attack can be successful using a number of different combinations of tactics and execution strategies.

2. Mitigation Method

In the earlier sections of this paper, there had been discussions on the social engineering terminology, how does social engineering operates which is by manipulating psychological principles or human traits to exploit their victims, the motivation of conducting social engineering attacks such as financial gain, politics, personal interest and revenge and also type of social engineering attacks including social engineering attack strategies. Social engineering attacks can be divided into two categories, which are human-based social engineering that includes real life direct physical interaction with its human victim through phone, by face-to-face communication or by using the surrounding environment and also technology-based social engineering such as online social networks impersonation, website phishing scams and email phishing (Peltier, 2007 and He *et. al.*, 2013). In the past few years, researchers had studied ways to detect and prevent social engineering attacks. The social engineering attack detection methods can be separated into two types of detection, human-based detection and technical-based detection. Figure 2.1 illustrates the taxonomy of social engineering detection method.

2.1. Human Based Mitigation

Human based mitigations a type of detection that involves human intervention in detecting and preventing social engineering. Human based mitigation is more towards judgment of humans to determine whether the activities that they encountered are related to social engineering attacks. There are two approaches that can be classified in human based mitigation which are policy and auditing approach and also education, training and awareness (ETA) approach. In these approaches, there are several works that have been studied to mitigate social engineering attacks using human decision-making.

2.1.1. Policy and Auditing

There are certain rules developed to help personnel in an organization in detecting and preventing social engineering attacks. The implementation of these rules are directed by policies that guides the personnel to decide whether the situation that they encountered is social engineering attack or a legitimate activity. Policy approach's applicability in human based social engineering detection has been studied by several researchers. The importance of having policies as a defense mechanism for social engineering attacks had been mentioned by Peltier (2007) in his work. Several policies such as clear desk policy to prevent password or sensitive

information being left lying about, the usage of paper shredder to avoid dumpster diving, implementation of caller ID technology for phone calls and service personnel identification checking policy had been mentioned to combat social engineering attacks. Twitchell (2006) had suggested common prevention method through policies such as rules of defining sensitive information in an organization, authorization and access control policy, data classification policy and security policies. Both of the studies focused on real world situation. A study conducted by Algarni *et. al.* (2013) also emphasized policy approach as common countermeasure in defending against social engineering attacks in cyber world. The authors stated that the policies similar to Twitchell (2006) were essential to provide some controls on their behavior in giving sensitive information or following the demands from the attacker.

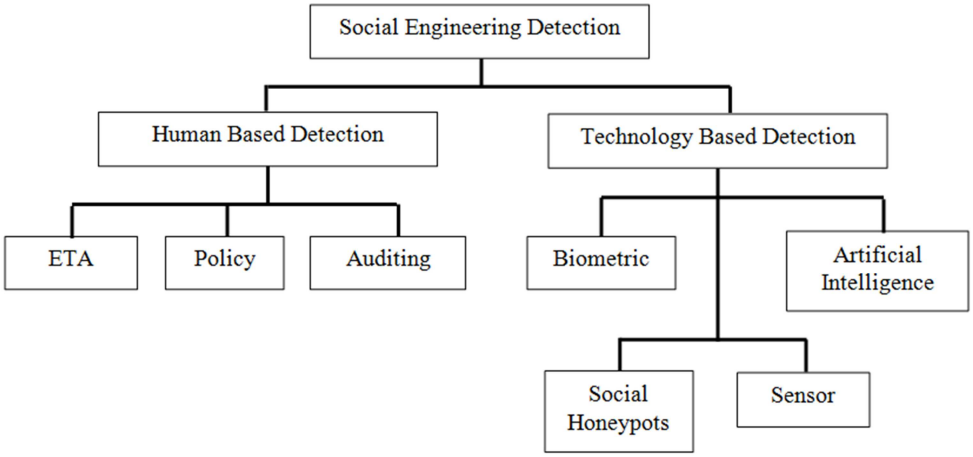

Figure 2.1. Taxonomy of Social Engineering Attacks Detection Method.

Auditing is a complimentary to policy based approach as mentioned in the previous work done by Twitchell (2006) and Algarni*et. al.* (2013). The objective of auditing is to test the level of awareness or exposure to social engineering attacks. This approach was also used to ensure the effectiveness of policies and ETA conducted in an organization against the attacks. Evaluations and experiments done by Gulenko (2013) and Smith *et. al.* (2013) can be considered as one of the auditing approach done in measuring the performance and effectiveness of the methods and approaches proposed in their studies.

2.1.2. Education, Training and Awareness

Education, training and awareness (ETA) approach in detecting social engineering is one of the approach in human based mitigation. Peltier (2007) emphasized that employee's education is important to ensure the policies, procedures and standards that have been developed in the organization able to be deployed effectively. ETA must be implemented especially for the newly employed staff in their orientation. The authors stated that another way to provide awareness to the employee in mitigating social engineering attacks is to deploy a dedicated, frequently updated web portal for security knowledge base. Twitchell (2006) and Algarni*et. al.* (2013) also mentioned the importance of ETA in enforcing developed policies in an organization to guide the personnel or individuals in recognizing the attacks and how to handle the attacks that they have encountered.

In technical-based attacks through social media network and online phishing, there were several studies focused into this area. Smith *et. al.* (2013) explained that most effective prevention method of social engineering attacks was through ETA although the attacks were getting more advance and hard to be recognized as the technology evolves. The authors suggested that common ETA were improved by developing interactive social engineering awareness website promoting awareness to the personnel which had been highly adapted by a lot of organizations nowadays. This interactive learning and education game-based system proved to be effective education tool in providing the users of this system with education experience on knowing social engineering and its attack patterns. Modular based design enabled the system to be updated with latest trends and additional techniques of social engineering attacks. Social engineering using phishing attacks using emails or websites in the cyber world had been studied by Khonji*et. al.* (2013). Several approaches in mitigation of phishing attacks had been discussed where one of the technique in detection approach was through user training. Most of the victims that fallen into phishing attacks due to lack of knowledge of the attack and ignorance towards passive warnings from security tools regarding phishing attacks. User training or education provided a solution in educating user to enhance their classification accuracy of phishing attacks and to take necessary action in preventing the attacks. Another study based on social engineering in Facebook was done by Gulenko (2013) where the author

developed a security awareness application in Facebook based on Theory of Planned Behavior (TPB) psychological model to predict user's behavior. This application helped user to ensure the security of their profile and to find out their friends' behavior and awareness towards security and privacy.

2.1.3. Issues with Human Based Mitigation

The approaches mentioned above are the most fundamental and common countermeasures in detecting and preventing social engineering attacks. Policy, auditing and ETA for users and employees in the organizations are a must as social engineering preys on psychological traits in exploiting their victims. Other technology based detection and countermeasures helps users and employees in recognizing the attacks, but in the end it depends on the decision-making and action taken by the individuals in classifying and avoiding social engineering. However, human judgment is somehow subjective and even with a good knowledge, awareness and policy against social engineering, the social engineers can find multiple ways to convince their victims and play on their emotion and psychology state to gain information or access to sensitive information or area. Therefore, there is a need of technology based mitigation methods as a complimentary to the human based mitigation to increase the detection and prevention accuracy.

The problem with security management standards is that they only determine if certain information security processes exist within an organization that adopts the standard. However, they do not usually outline the content of those processes in any sort of detail (Siponen, 2006). For example, a standard may state that an employee must "confirm the identity of a caller" before passing out information. However, most standards do not outline how exactly an identity in confirmed. It is completely up to the organization to decide how to implement this step, leading to varying degrees of quality between security in one organization and another which both adopt the exact same security standard. Standards are stating what activities should be done but not ensuring how these activities are done. They do not provide suggested guidelines when it comes to the specifics of implementing a security policy. In short, Siponen (2006) regards standards as too abstract and generalized, thus not being as useful as perceived by company management or provide the level of security that is expected, thus lulling an organization into a false sense of security.

Another problem is that the most popular targets of social engineering exploitation are new employees. This is because new employees and interns are one of the weakest links in an organization (Mitnick, 2003). New employees may not have completed security awareness training yet, they do not possess a protective loyalty or instinct towards company information and assets, and they are not familiar with all the staff within the organization or the proper business procedures. As such, they can be easily manipulated. Even with the best security education, awareness and training programs in place, new employees will always represent a threat. One method of limiting the damage that can be caused by a manipulated new employee is by severely limiting their access to sensitive organizational assets. However in doing so, it also impedes them from carrying out their duties as there is an obstacle to access the information and resources that they would need to be productive.

2.2. Technology Based Mitigation

Another method used for detecting and preventing social engineering attacks is through technology. Technology based mitigation method is another method that have been researched in detecting and preventing social engineering attacks. There are several categories that can represent this method. Next few sub sections will describe more on social engineering mitigation using sensors, biometrics artificial intelligence and also social honeypot.

2.2.1. Sensors

Physical tokens have been used as trusted identity verification methods in almost all areas of physical identification. For instance, a citizen's identity is usually determined using a national identity card of some sort. International travelers use passports to identify themselves. Authority figures use uniforms, badges, and identity cards to make their identities known. However, with the increasing complexity of social engineering attacks, a simple uniform may no longer be enough to verify the identity of an authority figure or employee of a company.

An example of the type of innovation that extends on the use of uniforms as an identity verification method and potentially increases the effectiveness of uniforms is the work proposed by Fujikawa and Nishigaki (2011). In their work, a uniform-wearing detection system using inter-body communication (IBC) technology was proposed. A prototype system was created which can notify the verifier (genuine officer/employee) whether the uniformed person in front of him/her is genuine officer/employee or not. The prototype system demonstrated high practicality, reliability, and safety through experimentation. The system works by genuine uniforms or door systems checking the signal transmitted by the target uniform. If the signal matches the genuine signal used by the genuine uniforms, they are verified as genuine police officer of employee. If the signal does not match, the verifier will be alerted that the target is not genuine uniform wearer. In addition, the signal generated is specific to the real owner of the uniform. Meaning, if the uniform were to be

stolen, the wearer would still be flagged as non-genuine as they are not the original owner of the uniform.

This system can be effective because it is easy to use by the uniform wearers and door operators. It creates a simple binary output of either genuine or non-genuine. Because the system is embedded into the uniform itself, the wearers also do not have to worry about carrying an additional device for verifying other uniform wearers. This type of system also does not rely on the personnel guarding access to a location to be able to identify fake uniforms or fake personnel wearing real uniforms. Instead, a database of genuine signals corresponding to different uniforms can be shared across all organizations and updated by the authorities as more uniforms are added to the system.

2.2.2. Biometrics

As stated in the section discussing social engineering tools and techniques, social engineers may attempt to impersonate a real employee by creating a profile of their character and mimicking their identity through appearance modifications, use of language and lingo, and knowledge of internal business processes. One method that can counteract physical impersonation is using biometrics. Biometrics does not rely on the perceived identity of a person, but rather distinguish someone using their unique biological traits such as fingerprints, voice signature and facial recognition. In fact, biometric systems have improved significantly in recent years. For instance, facial recognition systems have been designed to be robust against disguises (Pavlidis&Symosek, 2000; Yang *et. al.*, 2010; Li *et. al.*, 2013). Therefore, even physical disguise that may fool a human will not be successful when confronted with these biometric systems. However, biometrics do possess some weakness of their own that are still an issue. These issues will be discussed in a later section.

2.2.3. Artificial Intelligence

Using humans to detect social engineering is not a completely secure strategy because humans are flawed, will often make mistakes, and can be psychologically manipulated. Using technology based detections approaches adds a layer of security, but only provides that security within a narrow scope depending on what the system does. For example, biometrics can only work if the attacker is forced to be subjected to biometric tests. An attacker can bypass these systems using piggybacking, tailgating or other social engineering tactics. The attacker can also exploit the technological vulnerabilities of the security systems in place, thus avoiding detection. However, with the use of artificial intelligence systems, a detection system is no longer rigid and confined to specific detection parameters. Instead, it can learn and adapt according to the evolving tactics used by social engineers as time progresses.

One area where artificial intelligence is useful is detection of phishing attempts through mediums such as email. Multitier phishing detection and filtering approach would be ideal for an adaptive learning system to be implemented. For instance, Islam and Abawajy (2013) proposed using an innovative method for extracting the features of phishing email. The features are based on weighting of message content and message header. The features are selected according to the priority ranking. They also examined the impact of rescheduling the classifier algorithms in a multi-tier classification process to find out the optimum scheduling. The results of the experiments show that the proposed system reduced the false positive detections while having lower complexity compared to similar systems.

Baraclough (2013) did similar work by utilizing a Neuro-Fuzzy scheme to detect phishing sites with high accuracy in real time. Specifically, the author designed an intelligent phishing detection and protection scheme for online transactions. He does this by introducing new inputs including legitimate site rules, user-behavior profile, user-specific sites, and pop-ups from emails which were not considered previously in a single protection platform. In this study, a total of 288 features with 5 inputs were used, giving performance that surpasses all previously reported results in the field. An additional suggestion was to add a plug-in for real-time detection in future development.

Artificial intelligence systems rely on existing data for training, and will improve over time as more and more data comes in. While the intelligence level of systems that currently exist can be considered quite primitive, they can still be useful in doing some form of detection efforts that take some work off humans. An adaptive system will require less human intervention for improvement and can be useful even as time progresses as it continually evolves and improves itself.

2.2.4. Honeypot

Honeypot is a system that is created to imitate an existing working system to trap attackers and learning their behavior. A traditional honeypot may be a website, network or a computer (Wenda and Ning, 2012). Traditional type of honeypot usually focuses on attacks such as malware attacks, database attacks, email attacks and spam attacks on a system. New breed of honeypot includes social media honeypot and honeybot which tackles similar attacks but based on social media; other attacks that social media honeypot tackles are phishing and identity theft (Jin *et. al.*, 2011; Lee *et. al.*, 2010a; Lee *et. al.*, 2010b;Haddadi and Hui, 2010). Honeypot is similar to artificial intelligence system that learns based on patterns and data set that is fed for training. Based on these

information that the honeypot has been fed with it will auto harvest information based on user activities on the system, filter certain activities and develop statistics user model. The problem with honeypot is that in certain country it is against user privacy rights, which implementer of honeypot can be charged with breach of privacy (Jin *et. al.*, 2011;Haddadi and Hui, 2010; Walden and Flanagan, 2003). Another problem is honeypot is still new and not many accurate datasets are collected, so the ratio of false positive and false negative is still high, which results in inaccurate system execution. For social media honeypot, detection for spamming and phishing will need manual work with a personnel operating the honeypot profile as many spam works are in form of video, image, text and social network features being manipulated. For social media honeypot, Hadadhi and Hui (2010), Lee*et. al.* (2010a) and Jin *et. al.*(2011)had proposed that social media honeypot should be designed based on user feedback. These feedbacks do not only focus on interviews or surveys, instead by monitoring user on the social media itself by using a social media honeypot. This social media honeypot is still not fully automated, but is usable to collect information such as privacy setting, profiles, attraction, behavior patterns, connections & relations (Jin *et. al.*, 2011; Lee *et. al.*, 2010a; Lee *et. al.*, 2010b;Haddadi and Hui, 2010). Based on these collected information, statistics can be build to differentiate between real profile, fake profile, spam profile or bot profile. Jin *et. al.*(2011) proposed an automated active learning approach for the honeypot to detect spammers on social media network through data mining, listed below are the steps suggested:

1. Generate an initial set of instances for labeling and build initial classifier.
2. Prediction and ranking of remaining unlabeled instances (which is a huge number) using the existing classifier. Sort the test posts in decreasing order according to the ranking score and divide them into blocks.
3. Obtain an additional set of labeled posts. Such set is formed by examining the top blocks in both orders. Uncertain posts and a random set are also included.
4. Add the new labeled set to the training pool, and update the classification model.
5. Iterate steps 2 to 5 until satisfying stop criteria, such as the maximum number of iterations or the minimum number of additional spam detected.

Xie*et. al.* (2007) on the other hand proposed a honeypot for instant messaging where the honeypot acts as a decoy user to attract malware attacker. HoneyIM works by compromising a client, which will intentionally get attacked to receive the link or content; based on the content received, they HoneyIM will propagate the attack and based on the characteristic of the content any future attack on the traffic will be automatically blocked by the HoneyIM.

2.2.5. Issues with Technology Based Mitigation

With any use of technology comes the issue of added cost and complexity to the overall system composition within an organization. The systems that have been discussed would require significant monetary investment by an organization without a real measure of cost-benefit for any of these systems. Thus, spending large amounts of money on such systems can be quite a risk. The cost not only comes from the amount needed to purchase and install these systems, but also to manage and maintain them. Management and maintenance of added systems would require additional staff or add workloads to existing employees. The added complexity of the systems also means that there is potential for a business process to be interrupted when the systems malfunction. Using such complicated systems also increases the attack surface of the technological infrastructure and exposes the organization to added technological attacks. This may be in the form of software flaws found in the code running the security systems or design defects, which have yet to be fixed. The reliability of the systems can also be questioned in a lot of cases. There are issues with false positives and false negatives with all identity verification systems, and no system is perfect. Biometrics, while improved, is still vulnerable to attack. For example, Bustard *et. al.* (2013) showed that biometric systems are especially vulnerable to targeted impersonation attacks without manipulating the actual mechanisms of the device. This means that a social engineer who can also manipulate authentication devices can avoid detection.

As with the use of artificial intelligence systems, these systems usually require large datasets or long periods of training in order to be effective. The issue is that the datasets required are hard to come across unless there have been specific efforts to gather samples. The datasets themselves may also be of limited use as they become outdated as time progresses. This is because of the changing trends in behavior found in new data collections, making older datasets obsolete. The information gathering process itself may also be inaccurate and subject to high false positive rate, making the system an inconvenience rather that a useful detection tool.

3. Conclusion

Social engineering is a type of attack that takes advantage of the human psychological weaknesses. It can be formally

described as having four phases: information gathering, developing relationship, exploitation and execution. However, social engineering is not any specific type of attack limited to certain scenarios. Instead, it includes an array of tools, techniques, and approaches, which can be used to manipulate human beings to gain access to information or resources in an organization. Because the threat is so diverse, has no specific form and is continuously evolving to adopt new exploitation tactics, it is a serious threat to operational security.

Social engineering based attacks have been a threat to organizations for a very long time and although it has been a known threat with many cases of security incidents involving social engineering, there has still not been a clear answer on how to answer to this threat and thoroughly mitigate it. Traditionally, it has been proposed that social engineering be prevented though the use of security policies; education, training and awareness of employees; and establishing a security culture within the organization. However, it has been discussed that this is simply not enough as naïve adoption of security standards do not guarantee good security and new employees are preferred targets for social engineers, thus making education and awareness programs less effective as a mitigation strategy.

In this work, it has been shown that various technological measures exist to complement human based approaches to detection. These technological systems can lessen the impact of human weakness in detecting impersonators and help detect social engineering attempts as they occur. Among the measures presented were those that used sensors, biometrics and correlation for identity verification. In addition, honeypots and artificial intelligence systems can be used to progressively learn about and adapt to current social engineering tactics. With the use of social networks now being common, the social graph between individuals can also now be used to verify identities and monitor established relationships to further add another way to detect social engineering attempts. However, relying on technology also has its drawbacks in terms of cost and maintenance. It is also sometimes unknown whether a system robust enough to be relied upon to detect social engineering and opens up the organization to added attacks vectors via the additional software and hardware installed.

The threat of social engineering can never be totally eliminated as long as an organization includes the roles of human beings, as humans cannot be patched to make them more secure. All that can be done is efforts to educate and implement policies and regulations that minimize the potential for security breaches. Using technology can lessen the burden on humans in providing security, but a balance must be achieved where there is not total reliance on either humans or technology as both have their own issues and flaws. Going forward, the best thing that can be done to combat social engineering is to continue researching how organizations are being exploited leading to improvement of the security standards and technologies being developed for increasing security.

References

[1] Algarni, A. *et. al.* (2013). Social Engineering in Social Networking Sites : Affect-Based Model. The 8th International Conference for Internet Technology and Secured Transactions (ICITST). 9-12 December. London, United Kingdom : IEEE, 508-515.

[2] Barraclough, P.A. *et. al.* (2013). Intelligent Phishing Detection And Protection Scheme For Online Transactions. Journal of Expert Systems with Applications. Volume 40(11). 4697-4706.

[3] Bustard, J. D.*et. al.* (2013). Targeted Biometric Impersonation. International Workshop on Biometrics and Forensics (IWBF). 4-5 April. Lisbon, Portugal : IEEE, 1-4.

[4] Gulenko, I. (2013). Social Against Social Engineering: Concept And Development Of A Facebook Application To Raise Security And Risk Awareness. Journal of Information Management & Computer Security. Volume 21(2), 91-101. Emerald Group Publishing Limited.

[5] Haddadi, H. and P. Hui, P. (2010). To Add Or Not To Add: Privacy and Social Honeypots. IEEE International Conference on Communications Workshops (ICC). 23-27 May. Capetown, South Africa : IEEE, 1-5.

[6] He, B. *et. al.* (2013). A Defence Scheme Against Identity Theft Attack Based On Multiple Social Networks. Journal of Expert Systems With Application. Volume 41(5), 2345-2352.

[7] Islam, R. and Abawajy, J. (2013). A Multi-Tier Phishing Detection And Filtering Approach. Journal of Network and Computer Applications. Volume 36(1). 324-335.

[8] Jin, X. *et. al.* (2011). A Data Mining-Based Spam Detection System For Social Media Networks. International Conference on Very Large Data Bases (VLDB). 29 August - 3 September. Seattle, WA. 1458-1461.

[9] Khonji, M. *et. al.* (2013). Phishing Detection: A Literature Survey. IEEE Communications Surveys & Tutorials. Volume 15(4), 2091-2121. IEEE.

[10] Lee, K. *et. al.* (2010a). The Social Honeypot Project : Protecting Online Communities from Spammers. Proceedings of the 19th International Conference on World Wide Web. Raleigh, North Carolina, United States : ACM, 1139-1140.

[11] Lee, K. *et. al.* (2010b). Uncovering Social Spammers: Social Honeypots + Machine Learning. Proceedings of the 33rd International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR). Geneva, Switzerland : ACM, 435-442.

[12] Li, B. Y. L. *et. al.* (2013). Using Kinect For Face Recognition Under Varying Poses, Expressions, Illumination And Disguise. IEEE Workshop on Applications of Computer Vision (WACV). 15-17 January. Tampa, Florida : IEEE, 186-192.

[13] Mitnick, K. D. (2003). Are You The Weak Link. Harvard Business Review, 81(4), 18-20.

[14] Oosterloo, B. (2008). Managing Social Engineering Risk. Master, University of Twente, Netherlands.

[15] Pavlidis, I. and Symosek, P. (2000). The Imaging Issue In An Automatic Face/Disguise Detection System. Proceedings of the IEEE Workshop on Computer Vision Beyond the Visible Spectrum: Methods and Applications. 16 June. Hilton Head, SC : IEEE, 15-24.

[16] Peltier, T. R. (2007). Social Engineering: Concepts and Solutions. Information Systems Security. Volume 15(5), 13-21.

[17] Sandouka, H. *et. al.* (2009). Social Engineering Detection using Neural Networks. International Conference on CyberWorlds. 7-11 September. Bradford, United Kingdom: IEEE, 273-278.

[18] Siponen, M. (2006). Information Security Standards Focus On The Existence Of Process,Not Its Content. Communications of the ACM, 49(8), 97-100.

[19] Smith, A. *et. al.* (2013). Improving Awareness of Social Engineering Attacks. In Dodge Jr., R. C. and Futcher, L. (Eds.). Information Assurance and Security Education and Training (pp. 249-256). Berlin-Heidelberg : Springer.

[20] Spinapolice, M. (2011). Mitigating the Risk of Social Engineering Attacks. Master, Rochester Institute of Technology, New York, United States.

[21] Twitchell, D. P. (2006). Social Engineering In Information Assurance Curricula. Proceedings Of The 3rd Annual Conference On Information Security Curriculum Development (Info Sec CD). 22-23 September. Kennesaw, Georgia, United States : ACM, 191-193.

[22] Walden, I. and Flanagan, A. (2003). Honeypots: A Sticky Legal Landscape. Rutgers Computer and Technology Law Journal. Volume 29(2). 317-370.

[23] Wenda, D. and Ning, D. (2012). A Honeypot Detection Method Based on Characteristic Analysis and Environment Detection. In Chen, R. (Ed.). International Conference in Electrics, Communication and Automatic Control Proceedings (pp. 201-206). New York : Springer.

[24] Workman, M. (2007). Gaining Access with Social Engineering: An Empirical Study of the Threat. Volume 16(6). 315-331.

[25] Xie, M. *et. al.* (2007). HoneyIM: Fast Detection and Suppression of Instant Messaging Malware in Enterprise-like Networks. Twenty-Third Annual Computer Security Applications Conference (ACSAC). 10-14 December, Miami Beach, Florida : IEEE, 64-73.

[26] Yang, A. Y. *et. al.* (2010). Towards A Robust Face Recognition System Using Compressive Sensing. INTERSPEECH 2010 : 11th Annual Conference of the International Speech Communication Association (ISCA). 26-30 September. Makuhari, Chiba, Japan : ISCA, 2250-2253.