Social Engineering Framework: Understanding the Deception Approach to Human Element of Security

Richardus Eko Indrajit
Faculty of Information Technology, ABFI Institute Perbanas
Jakarta 12720, Indonesia

Abstract

Social engineering has become serious phenomenon in the history of information security worldwide. Although this approach is widely used by criminals to exploit the human aspect as the security weakest link, there is not many studies focusing on such issue. Fail to understand the nature of social engineering will increase the security risk posture of the organisation. Inspite of the fact that most of social engineering attacks are seemed to be unstructure and diverse in nature, this research result shows that there exists common patterns that can be mapped and organised in a logical and structured way. This study is aimed to develop and to propose a framework to help security practitioners in having better and wholistic understanding on the nature and characteristics of such humen-based attack. By understanding the detail characteristics of social engineering, an effective countermeasure effort can be designed and developed. This concept shall be used by the management of organisation or institution in developing its security mitigation strategy.

Keywords: *Social Engineering, Security, Deception, Attack, Human Element.*

1. Introduction

Information security has become a very serious issue faced by today's organisation and enterprise. While information technology creates a spectrum of benefits to the stakeholders, at the same time a portfolio of risks occurred within the context. As stated by a good number of researchers and practitioners, in any internetworking system, the level of security strength highly depends on the weakest link or/and node. Among all information system components, human has been considered as the most vulnerable entity due to its nature that can be easily exploited by criminals to conduct their unlawful activities. The most common attack performed by black hackers or other lawbreakers to make use of these human vulnerabilities is called social engineering. This notorious technique of deception has been largely adopted by many wrongdoers in order for them to achieve their criminal objectives. Global statistics have shown that most of the attacks nowadays involves social engineering activities. It grows significantly and exponentially from time to time. In developing country such as Indonesia, this type of attack has become very popular among criminals due to its simple yet cost effective nature of deployment. Regardless its existence, there is only a few study which analyse this social engineering phenomenon in a holistic and a systemic way. Most of discourses in social engineering are focusing on or based upon instances or case studies – not perceiving it from the totality of a dynamic system. This creates the difficulty for enterprise management to come up with mitigation strategy that can be effectively protect their human capitals from being exploited by social engineers. For the purposes of developing an effective mitigation approach, a full and a thorough understanding about social engineering phenomenon should be well conducted. By comprehending social engineering occurrence in a holistic and a systemic manners, a set of effective mitigation strategy can be analysed, selected, developed, and implemented within the enterprise or other organisation/institution setting.

2. Research Methodology

This study investigates a good number of social engineering cases ever happened within the history of computer security. The first domain consists of classic and famous cases occurred in different countries. The following table lists 25 (twenty five) cases of previous social engineering attempts that are involved in the study.

Table 1: World Wide Social Engineering Cases

No	Case	Method	Remark
1	The 419 Nigerian Scam	Offering percentage of huge amount of money that should be cashed out from the foreign bank	Average loss of $10,000–$50,000 USD
2	Dalai Lama Server	Offering help for Tibetian movement through uploading malware	Network owned by Dalai Lama was compromised
3	Dark Market and Market Splyter	Stealing credit card numbers and information	Most victims were eBay customers
4	Mati Bite	Asking for exchanging collection of stamps through clicking malicious link	Trojan malware was deployed upon the clicking
5	Alcohol Impact	Buying drinks to make people get drunk and disclosing confidential information	Effective to be used to victimise close related friends

			or colleagues
6	IT Division Support	Asking personal information for the purpose of upgrading the system	Quite effective for manipulating common or regular users
7	Stanley Mark Rifkin	Using legitimate id to enter bank and get bank's security code to rob the bank	About $10.2 million was gone
8	Overconfident CEO	Using personal details found in social media to get close to executive for information leak	Executives are considered to have most vulnerabilities
9	Theme-Park Scandal	Bringing family to compromise entrance ticketing system	Children are used as a decoy figure
10	Hack the Hackers	Pretending as newbie to get close to experience hackers	Vanity is a common vulnerability
11	AOL Tech Support	Offering to buy car at a great price through clicking a car-picture malware	200 accounts were compromised
12	Surveillance Camera Peeking	Positioning surveillance camera on the back of users allowing people to zoom at keyboard striking	Normally it is a part of personal safety, but vulnerable for security
13	Fake Fire Alarms	Offering help during a fake emergency situation to save somebody's information assets by asking their passwords remotely	Using panic mode to exploit people
14	Computer Teacher	Assisting student who is using new software while at the same time peeking at the finger while typing password in keyboard	Look natural but danger
15	Lost in Space	Pretending has just lost access card or other ID so that the person can enter the perimeter	Anybody can do it
16	ISP Services	Calling customers about the incoming connection problems for the reason of asking their passwords	Hard to avoid and to acknowledge
17	Consultancy Services	Offering services in the website that require personal information for further communication	It is quite difficult to differentiate the formal services and the fake ones
18	Parking Ticket	Acting as if an official police that gives ticket to the drivers that need to access website	Using fake authority to manipulate users
19	Transfer Notification	Telling the users that something have wrong with their past payment transaction	Frequent Paypal customers are the easy target for this
20	Profile Update Confirmation	Confirming whether there is a change or not in user's profile by asking to click yes/no button	Social media users are the main target
21	Push Mail or Advertisement	Sending compelling professional ads that require some actions of the receivers	Can be performed by legal or official site
22	Breaking News	Soliciting special coverage of the hot breaking news of the day	Exclusive information is hard to get
23	Alumnie Gathering	Greeting from the old campus that call for participation in many events	Using emotional factors of human to deceive
24	Warning System	Sending machine look-alike message from the system that require attention from the users	Like an error message, it seems very normal to have one
25	Sampling Product	Sending special package randomly as a trial product	Part of marketing gimmick

As stated earlier, there are also a few famous social engineering cases ever happening in Indonesia previously. This study also investigates several cases occurred in Indonesia in the last 10 (ten) years.

Table 2: Social Engineering Cases in Indonesia

	Case	Method	Remark
1	ATM Support	Offering help to banking customers in using ATM functions by asking their passwords	Exploit the less educate people (non technology literate person)
2	Goodbye Culture	Overhearing people conversation while they are talking during special cases	Nobody pays attention to stranger(s) who can hear his/her conversation.
3	TV Show Passwords	Asking passwords to individual like what a TV show does for marketing purposes	Use the confusion of people on passwords terminology
4	Old CC Machine	Using old manual machine to gather critical information from credit card	Still being used in remote areas
5	Emergency Surgery	Telling the family that a critical condition relative needs an emergency treatment that requires money to be transferred	Most panic intelligent persons were victimised by this attack
6	Prize Winning	Informing individual who wins the big prize that will be delivered after the prizing tax has been transferred	Over excited people are easy to get manipulated
7	Forget-Password Remembering	Browsing somebody's profile in the social media network to guess password after getting forgetting-password keywords	Common feature for forgetting password by public email and cloud services
8	Maintenance Call	Asking personal information and passwords for system maintaining reasons	Targeting the customers of ISP or other technology providers
9	Cross Password Referral	Gaining a person's password to get other ones	Commonly, veteran generations choose similar passwords for all accounts
10	Phony Email	Communicating with phony email using legitimate profile as address id	Easy to conduct due to many public email services
11	Former Executive Pass	Using friendships (formal and informal) as key to get permission to enter perimeters	Perception is a reality (assumption)
12	Wall Mart Logistic Contract	Pretending as government officer who offer a potential contract to get detail information on IT assets	Blind by fake business opportunities
13	Y2K Probono Consultant	Offering help to fix Y2K bug while at the same time analyse the vulnerabilities and/or plant a malware	Embedded risk of a project

14	Virus Cleaning	Reporting for viruses and offering free cleansing by using malware/trojan program	Massively broadcasted too email address lists
15	Secretary Privilege	Helping boss in opening his/her email while at the same time using the authority to conduct other activities	Most of executives are non IT-savvy people who seldom outsource their work to secretary
16	Flash Disk Copying	Helping files transfer while at the same time moving unnecessary ones	Sharing file(s) is a common activity
17	Software Installation	Offering help to conduct complicated installation that require legitimate user's passwords	Effective to be exploited to a low literate community
18	Fake Website	Opening up welcoming page that is familiar to the real one for the purpose of fooling people	Old time phishing type
19	Credit Card Call Center	Giving false information that somebody's credit card is being used to get privacy information	Difficult to differentiate the real and the fake one
20	Used-Papers for Sale	Buying official documents (used papers) to be used for other good purposes	Sometimes used documents contain confidential information
21	Device Installation Services	Installing extra applications for hardware's customers	Embedded in legal/formal transaction
22	After Sales Services	Serving people's branded devices for free (maintenance and troubleshooting)	Usually taking form as small kiosk
23	Hot Spot Request	Asking personal email address and password to join free internet connection	Low literate users are the easy target of the attack
24	Post It on the Table	Using someone's else office table that full of personal property	Common practices among good friends or colleagues
25	Active Login Decoy	Calling somebody who is actively working in PC as a decoy while other friends exploit an attack	Many users only do login and logout one time a day

Based on these 20 (twenty) cases, a qualitative research is conducted to investigate following aspects of social engineering: (i) Scope and Definition; (ii) Reasons for the Effort; (iii) Nature of Attacks; (iv) Psychological Aspects of Deception; (v) Objectives and Motivation; (vi) Types and Category; (vii) Stages and Life-Cycle; (viii) Tools and Techniques; and (ix) Tendency of Patterns.

3. Data Gathering and Analysis

3.1 Scope and Definition

Cyber crime and the threat of computer-related attacks are increasing significantly, and the need for security professionals and practitioners who understand how attackers compromise ineternet or network perimeter is growing right along with the thread (Simpson et.al., 2013). The use of social engineering is a common occurenece in society, and moreover is being recognised as one of the most effective mode of attack in the field. As a matter of fact, using relationships between people to obtain a goal is an every day occurrence and does not have to be nefarious in purpose (Hoescele, 2006). In principle, social engineering is the exploitation of basic behavioral and cultural constructs to achieve an objective (Watanabe, 2008). Within security world, a social engineering is a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures or perimeters. There are several theories, concepts, and school of thoughts related in defining and characterising this type of attack, such as:

- Social engineering refers to various techniques that are utilized to obtain information in order to bypass security systems, through the exploitation of human vulnerability (Bezuidenhout et.al., 2010).
- Social Engineering is the term for using human deception as means for information theft (Hermansson et.al., 2005).
- Social Engineering is the art of exploiting the weakest link of information security systems: the people who are using them (Huber, 2009).
- Social Engineering is the malicious intent of cyber attackers attempting to ilegally compromise an organisation's assets by using relationships with people (Dolan, 2004).
- Social engineering does not rely on a faulty piece of high-tech equipment to mount the attack; rather, it uses a skilled attack on the psyche of the opponent (Long, 2008).
- Social engineering attacks have the goal of collecting a certain amount of data to be used later in a technical attack (Evans, 2009).
- Social engineering purpose of attacks is to get direct access by using physical or digital access to an organisation's information or information system (Foozy, 2011).
- Social Engineering is a description of techniques using persuasion and / or deception to gain access to information systems (McClure, 2005).

Based on the study of these phenomena, there are commmon principles as the ground rules of social engineering:

1. All of the attacts are launched to exploit human vulnerabilities;
2. The attempt is considered as the step stone of conducting the real attacks;
3. Most of the missions are aimed to gather confidential information;
4. There are many means and variants of performing the practices; and

5. It has a nature of arts and sciences at the same time.

3.2 Reasons for the Effort

Social engineering itself can be considered as either pre-attack attempt or real attack endevour. It is recognised as a pre-attack if the objective is to acquire what so called as confidential data or information. These data – such as password, credit card number, personal information, identification profile, etc. – will later be used as tool for conducting real attacks, such as: password cracking, phishing, spoofing, and hundreds type of other offensive activities. In the other domain, social engineering can be considered as an attack if such practice has victimised one or a group of people in terms of economic loss, destroyed image, political disadvantage, and other types of disbenefits. Whether it is a pre-attact or an attack, there are some background reasons why most of criminals have chosen this technique. The first reason is because it is easy to deploy by anybody without having to spend so much time in developing necessary competencies, skills, and/or capabilities. The second reason is due to the fact that this type of attack is relatively cost efficient because most of the cases do not require many resources. The third reason is because there is statistics showing that the success rate of such type of attack is comparatively high. The fourth reason is driven by the fact that the risk of getting caught by authority is relatively low because "the control" is in victim's hand – not within the social engineer posession. And the fifth reason is because the variants of social engineering type is unlimited, where everybody can use their creativity and innovation to come out with the new effective scenario. In conclusion, many observers argue that the human factor is truly security's weakest link – so focusing an attack to this component will guarantee a success (Grossklags et.al., 2009).

3.3 Nature of Attacks

People, who are all fallible, are usually recognized as one of the weakest links in securing information. The problem is that no matter how much work and effort is placed in the protection of data or information, it only takes one misguided soul to completely defeat all endeavors (Mattord, 2006). The natural human willingness to accept and to trust someone at his or her word leaves many of us vulnerable to attack. Many experienced security experts emphasize this fact (Granger, 2001). By social engineering, social engineers exploit the natural tendency of a person to trust rather than exploiting technical computer security holes. Although social engineering can be complex and clever, it's usually simple and shortlived in nature. There will be extenuating circumstances where people will not have much time to think, and the emotional pressure—typically anger, camaraderie, or desperation—will escalate quickly (Tomhave, 2007). Social engineeris use tactis to leverage trust, helpfulness, easily attainable information, knowledge of internal processes, authority, technology and any combination there of (Hoeschele, 2006). In other words, Social engineering relies fundamentally on the victim's willingness to trust or help other people. Social engineers get personal information or access to computing systems by exploiting people's natural tendency to want to trust and be helpful, and by taking advantage of the tendency to act quickly when faced with a crisis. Common human behaviors that are oftenly exploited by social engineers are: appeal to ego, appeal to authority, desire to be helpful, low perceived cost of information, fear of losing, lazyness or ignorance, attitude to trust, and enthusiasm to get free rewards (Thapar, 2007). Through three simple principles – compliance, trust, and benefits – a social engineering attempt can be exploited successfully (Murray, 2011). Other study has showed that deception has been used since the dawn of time to gain advantage (Warren et.al., 2006). Social Engineering attacks involve the use of deceptive or manipulative tactics on an individual to gain a result – orten to gain unauthorised access to information assets (Lineberry, 2007). Examples of deception are: masking, repackaging, dazzling, mimicking, inventing, and decoying. Most social engineers are good in utilising these deception techniques in influencing people so that they behave as targeted.

3.4 Psychological Aspects

As stated earlier, basically social engineers are using psychological approaches to deceive people. There is a good number of techniques commonly used by criminals in trying to get what they want such as:

- Elicitation means to bring or draw out, or to arrive at a conclusion (truth, for instance) by logic. Elicitation works so well for several reasons (Hadnagy, 2011): (i) most people have the desire to be polite, especially to strangers; (ii) professionals want to appear well informed and intelligent; (iii) if people are praised, they will often talk more and divulge more; (iv) most people would not lie for the sake of lying; and (v) most people respond kindly to people who appear concerned about them.
- Preloading means planting specific ideas or thoughts to individual(s) in a way that is not obvious or overbearing. Once the ideas are accepted, it can be used later by social engineers to start initiating an attack (for instance through building rapport during

the conversation, or by aggreeing upon some planted principles).

- Pretexting means telling the background story, dress, grooming, personality, and attitude that make up the character the social engineers will be for the social engineering audit (Hadnegy, 2011). Because the pretexteing is defined as the act of creating an invented scenario to persuade a targeted victim to release information or perform some action, a good social engineer has to really play its role seriously – as if he/she is the real one. Convincing people is the name of the game in pretexting to gain their trust.
- Building Rapport for Mind Tricks means using friendly and empaty approach to gain trust from other people. Body gestures, voices, and senses are playing important roles within this context. Microexpressions such as happiness, sadness, fear, hesitation, madness, surprise, disgust, contempt, or anger are often utilised by social engineers to set up the circumstances. These means are used to gain control over the victims before conducting social engineering attacks.
- Influencing means acting to get someone else to want to do, react, think, or believe in the way you want them to. As an art of persuasion, building rapport is the key for this act. Trying to be empathy with other's condition is one of an effective way to get someone's trust and confidence. Marketing people and sales persons are very good in using this method of persuasion.

Other techniques that are oftenly used by influencer are: framing, concession, conditioning, manipulation, intimidation, authority, etc. (Hadnagy, 2011).

3.5 Objectives and Motivation

The purpose of social engineering approach is to persuade the victim to be helpful (Pfleeger, 2003). There are different type of social engineers who are classified based on their activities and objectives of conducting various type of pre-attacks. Some of them that are highly recognised are (Hadnagy, 2012):

- Hackers/Crackers: individuals who have self motivation or professionals who are hired by person(s) or organisation to compromise computer system for the purpose of gaining economic benefits, ruinning people/company image, altering political agenda, or other outlaw scenarios.
- Penetration Testers: highly competent people who utilise their capabilities to examine and to identify the level of security within a perimeter for the purpose of finding vulnerabilities to exploit.
- Spies: people who have been assigned by official organisation to gather special information or knowledge about specific parties as a part of intelligent activities;
- Identity Thieves: persons who steal somebody's identity to act as if they are authorised personels.
- Disgruntled Employees: staffs of the organisation who have bad experience in the past that make them willing to take revenge against the institution.
- Scam Artists: masters on influencing and tricking people so that they will do whatever is being told for the purpose of gaining personal benefits.

3.6 Types and Category

Social Engineering is mainly divided in two different categories, namely technical or computer based deception, and human interaction based deception (Hermansson et. al., 2005). In the technical or computer based approach of deception the Social Engineer, as the name implies, relies on the technology to deceive the victim of the attack to supply the information needed to fulfill the purpose. While the other approach of Social Engineering is based simply on deception through human interaction. But some practitioners and researchers often classify the types based on its modes or techniques of attack, such as:

- Technical attack, ego attack, sympathy attack, and intimidation attack (Turner, 2005).
- Impersonation, trust, diffusion, overloading, moral duty, reciprocation, urgency, and direct approach (Redmon, 2006).
- Non Technical, which are hoaxing, pretexting, dumpster diving, spying, authoritative voice, support staff, and technical expert; and Technical which are phishing, vishing, popup window, interesting software, and spam malls (Thapar, 2007).
- Pretexting, phishing, vishing (phone phishing), trojan horse, baiting, quid pro quo, and hybrid attack (Prince, 2009).
- Vishing, dumpster diving, online social engineering, persuasion, and reverse social engineering (Granger, 2001).
- Impersonating, third-party authorisation, in person, dumpster diving, shoulder surving, pop- up windows, email attachements, and web sites (Foozy et.al., 2011).

3.7 Stages and Lifecycle

Even though social engineering can be performed in many various ways, a common pattern has emerged according to Gartner. Those stages consists of the following steps, which are: information gathering, developing relationship, exploitation of relationship, and execution to achieve objective (Gartner, 2001). Another study uses the terminology in cyber cycle of social engineering which consists of several steps, such as: reconnaissance, collect information, build up information, and using the information (Warren et.al., 2006). The Social-Engineering Trust and Attack Model shows the four stages of deploying an attack, which are: situation researched, target researched, trust obtained, and attack launched. In ethical hackers perspective, there are also four phases existed in the process of undergoing social engineering attack, which are: reconniassance, scanning, exploitation, and maintaining access (Engebretson, 2013). Another sequential steps is also introduced as research, hook, play, and exit (Singh, 2013).

3.8 Tools and Techniques

Like other attacking methods, there are some tools highly used by social engineers to help them managing the attacks. Some of the famous ones are as follows (Hadnagy, 2011):

- Back Track – a Linux distribution software that assists in collecting and then using this data for penetration tests and social engineering audits.
- BasKet – functionally like a notepad, to gather and to organise huge data collected for social engineering needs.
- Dradis - a selfcontained web application that provides a centralized repository of information gathered.
- Google Advanced Search - a search engine with numerous features for finding information with specific characteristics.
- Social Media (Facebook, Twitter, Linkedln, MySpace, etc.) – a social media network that consits of huge data from all members registered to the service.
- Common User Passwords Profiler and Who's Your Daddy – a special tool designed to help people on guessing the most likely passwords used by somebody.
- Maltego – an application that allows a social engineer to perform many web-based and passive information gathering searches without having to use any utilities.
- SET (Social Engineering Tool) – a Python-driven suite of custom tools featuring a menu- driven attack system that mainly concentrates on attacking the human element of security.

Basically there are hundreds even thousands of ready to use (and free) software that can be used by social engineers to assist their effort. Of course to determine which tools are the most effective one(s) is highly depending upon the typa and scenario of attack a social engineers is trying to deploy. Note that there are also many websites that offer help for social engineers in conducting their activities.

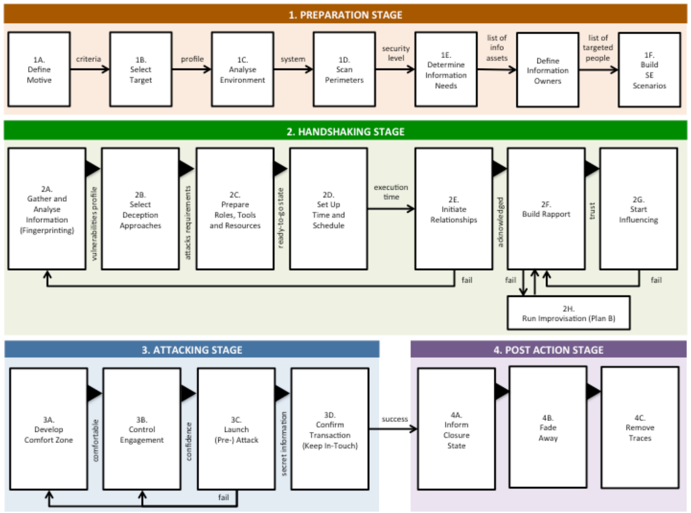
3.9 Tendency and Pattern

According to Gartner, even though social engineering can be performed in many various ways, a common pattern has emerged. Those stages consists of the following steps, which are: information gathering, developing relationship, exploitation of relationship, and execution to achieve objective (Gartner, 2001). Another study uses the terminology cyber cycle of social engineering which consists of several steps, such as: reconnaissance, collect information, build up information, and using the information (Warren et.al., 2006). The Social-Engineering Trust and Attack Model shows the four stages of deploying an attack, which are: situation researched, target researched, trust obtained, and attack launched. In ethical hackers perspective, there are also four phases existed in the process of undergoing social engineering attack, which are: reconniassance, scanning, exploitation, and maintaining access (Engebretson, 2013). Another sequential steps is also introduced as research, hook, play, and exit (Singh, 2013).

4. Results and Discussion

4.1 The Framework

Based on the study, the proposed social engineering framework is divided into 4 (four) stages, namely: Preparation Stage, Handshaking Stage, Attacking Stage, and Post-Action Stage.



Picture: Social Engineering Framework

https://doi.org/10.20943/01201702.816

4.2 Preparation Stage

Before the attack takes place, a social engineer usually has to undergo a series of activities. There are commonly seven activities that are conducted as follows:

1. Motive of Attacks - Based on the observation of cases and the analysis of survey, there are at least 7 (seven) type of common motives of launching social engineering attacks, namely: Economic Benefits, Political Gain, Social Disorder, Image Spoiling, Cultural Disruption, Ideology/Value Challenge, War and Terror Creation.
2. Target Selection - In every attack, there will be an individual or a group of victims that are targeted by the social engineer. Based on the type and characteristics of the victims, a simple classification can be made as follows: Individual, Group, Organisation, Community, Public, Hybrid, and Random.
3. Environment Analysis - The target lives in an closed environment that has its security perimeter intact. Special observation and analysis should be conducted to study the attribute and all elements characteristics within the following perimeter: Internal and External.
4. Perimeter Scanning - As a digital/electronics-based system, information system and technology are constructed through the development of tangible and intangible assets. It means that a special scanning activity should be conducted in both substances, which are: Physical and Logical.
5. Information Requirements Analysis - Based on the environmental analysis and perimeter scanning results, a list of requirement regarding what type of information assets need to make the effort succeed is defined. These information should be gathered by social engineers as the main target of an attack. In order to do that, a set of resources should be prepared which are: Technical Requirements and Non-Technical Requirements.
6. Asset Owners Determination - Every information has owner, an individual who has formal possession to its existence. According to their level of literacy with related to information and technology, this targeted victim can be divided into: Literate People and Non/Low-Literate People.
7. Scenario Development - In this last phase of the first stage, after defining the target and the victim of the attack, social engineers state their final definition of scope, objectives, cost, and time of the exploitation plan. They have to ensure that all things required have been acquired and possessed. The process can be divided into three domain, which are: Pre-Attack Preparation, Attack Deployment, and Post-Attack Action.

4.3 Handshaking Stage

This is the process where the first contact is established between social engineer and his/her targeted victim(s). There are at least 8 (eight) phases occurred within the stage described in the following elaboration:

1. Fingerprinting - It is the process of collecting or gathering details information of the target(s). This phase requires special effort of researching. Core data that need to be acquired are: Profiling, Value and Behavioural Analysis, Relationships Awareness System, Social and Authority Status, Potential Vulnerabilities Posture.
2. Deception Model - There are many techniques to deceive people so that they will do what social engineers are expecting, which are: Phishing, Pretexting, Baiting, Impersonating, Quid Pro Quo, Malware Planting, Physical Observation, Hoaxing, Elicitation, Reverse Social Engineering, and Hybrid (Combination).
3. Resource Preparation - Every attempt of attack requires resources. Those resources can be classified into 3 (three) types, which are: People, Process, and Technology.
4. Time and Schedule - Having preparing all resources required to run the scenario, the next thing that should be done is planning the time of attack. There are three time horisons that are important to be planned, which are: Prior to the D-Day, Deployment Time and Post Attack Period.
5. Relationship Initiation - In order not to create suspicious, an initiation of the first contact should be as if it is a normal condition. It means that a logical relationship between social engineers and targeted victims should be well developed. There are a good number of ways to do such effort, as follows: Official Structure, Friends-and-Family, Supplier-Customer, Personal Needs, Technical Requirements - providing suggestions as solution, and Passive Roles - waiting to be contacted (e.g. reverse social engineering).
6. Rapport Building - Rapport is a close and harmonious relationship in which the people or groups concerned understand each other's feelings or ideas and communicate well. Developing this relationship can only be done if the social engineers have special ability to do that. There are several approaches that can be used to build rapport such as: Empathy, Compliance, Solution, Protection, Scarcity, Comfort, and Assistance.
7. Influencing (Trust Building) - After the victims feel comfortable with attacker the next step a social engineer has to be accomplished is trying to influence them. The approach that can be used are: Moral Duty, Help Desire, Suggesstion, Order, Persuasion, etc.

8. Improvisation Model - As shown in the scheme, not all efforts of building building rapport and influencing people are smooth. Sometimes a social engineer find a difficulty to talk with the victims due to many circumstances. An improvisation should be done should this situation occurs. Before going back to either building rapport or influencing phase, a social engineer has to conduct the following activities: Approach Alternate and Key Message Conveying.

4.4 Attacking Stage

This is the main stage where an attack is deployed by social engineers. It consists of 4 (four) phases that are elaborated in the following sections:

1. Comfort Zone Establishment - The first thing to be done after a social engineer feels that they are succeed on building victim's trust is to put his/her in comfort zone. The most important acts that need to be established are: Listening Well, Consistent Conversation, and Value Driven Topics.
2. Engagement Control - While the comfort zone established, ensure that the social engineer has taken a control over the victim(s) through performing some duties that should be followed, based on: Command-Base Interaction and Encouragement – praising the victim(s) of what they have done to bring spirit of complying the orders.
3. (Pre) Attacking Mode - This phase is where the targeted information is being released or disclosed by the victim(s). There are two models of releasing the information made by the victim(s), which are: Direct/Explicit (Asset Disclosure) and Indirect/Implicit (Leading Information) – implicitly telling how to acquire such confidential data or information.
4. Confirmation of Accomplishment - Simultaneously, after the required data/information is being acquired, the social engineer should verify the validity of it. The things that should be done are: Final Verification and Fake Governance.

4.5 Post Action Stage

After an attack has been executed, it is a time to withdraw from the relationship connection. A smooth techniques should be performed to protect social engineers from any risk possible during the post attack. Three phases occurred during this final stage:

1. Closures - This is a "good bye" message from social engineer to the victim(s). There are two things that usually performed, which are: Sympathy Message and Assistance Offering.
2. Fading Away - In this phase, all link or direct information regarding the social engineer's perimeter is slowly removing from the system. Two consecutive processes should be done during this phase. Those are: Standby and Disappearance.
3. Traces Removal - Finally, as normally conducted by any attacker, it is a must to have process to remove all traces that can possibly link the victim(s) to the attacker (social engineer) through: Zero Path and Quick Audit/Assurance.

5. Conclusion and Further Study

As technology and society emerge, the studies of social engineering has extended to different angles. For example a discourse that suggests that law ought to be an instrument of social engineering (Omote, 2008). Other scholar focuses on the deontological theory of social engineering, one that accepts the inviolability of the person while still pursuing ambitious long-term teleological strategies through state action (Duff, 2005). There is also a depth study upon social engineering that is based on the doctrine for cyber security (Mulligan et.al., 2011). The social engineering attack has been also recognised and "re-branded" as "cognitive hacking" (Thompson, 2003) – under the "security informatics" field of study.

References

Allen, Malcol. (2005). "The use of "Social Engineering". Taken from the website http://www.sans.org/rr/paper.php?id=529.

Bezuidenhout, Monique, Francois Mouton, and HS Venter. (2010). "Social Engineering Attack Detection Model: SEADM". Information Security for South Africa (ISSA), IEEE Publication Inc.

Dolan, A. (2004). "Social Engineering". Retrieved October 10, 2004, from http://www.sans.org/rr/catindex.php?cat_id=51.

Duff, Alistair S. (2005). "Social Engineering in the Information Age". The Information Society, 21: 67–71. Taylor and Francis Group.

EC-Council. (2005). "Chapter 11: Social Engineering". Certified Ethical Hacker Training Materials. EC-Council: United States.

Engebretson, Patrick. (2013). "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy". Elsevier: Massachusetts, United States.

Evans, Nathaniel Joseph. (2009). "Information technology social engineering: an academic definition and study of social engineering - analyzing the human firewall". A dissertation submitted to the graduate faculty in partial fulfillment of the requirements for the degree of Doctor of Philosphy in Computer Engineering, Iowa State University.

Foozy, Cik Feresa Mohd, Rabiah Ahmad, Mohd Faizal Abdollah, Robiah Yusof, and Mohd Zaki Mas'ud. (2011). "Generic Taxonomy of Social Engineering Attack". Malaysian Technical Universities International Conference on Engineering & Technology (MUiCET 2011).

Gartner. (2001). “Gartner’s Information Security Strategies Research Note TU-14-5662”.

Granger, Sarah. (2001). “Social Engineering Fundamentals, Part I: Hacker Tactics”.

Grossklags, Jens, and Benjamin Johnson. (2009). “Uncertainty in the Weakest-Link Security Game”. School of Information, University of California Berkeley, United States.

Hadnagy, Christopher. (2011). “Social Engineering: the Art of Human Hacking”. Wiley Publishing Inc. Indianapolis, Indiana, United States.

Hermansson, Mikael, and Robert Ravne. (2005). “Fighting Social Engineering: Increasing information security in organizations by combining scenario based learning and psychological factors of persuasion”.

Hoescele, Michael. (2006). “Detecting Social Engineering”. Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette.

Huber, Markus, Stewark Kowalski, Marcus Nohlberg, and Simon Tjoa. (2009). “Towards Automating Social Engineering Using Social Networking Sites”. Proceeding CSE '09 Proceedings of the 2009 International Conference on Computational Science and Engineering - Volume 03, IEEE Computer Society.

Lineberry, Stephen. (2007). “The Human Element: The Weakest Link in Information Security”.

Long, Johnny. (2008). “No Tech Hacking: A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing”. Elsevier, Inc. Journal of Accountancy, American Institute of Certified Public Accountants, November Edition.

Mattord, Herbert J. (2006). “Social Engineering: the Non-Technical Threat to Information Security”. Center for Information Security Education and Awareness, Kennesaw State University.

McClure, Stuart, Joel Scambray and George Kurtz. (2005). Hacking Exposed Fifth Edition. New York: McGraw-Hill.

Morgan, Russel. (2006). “Social Engineering Defense for Small Business”. East Carolina University.

Mulligan, Deirdre K. and Fred B. Schneider. (2011). “Doctrine for Cyber Security”. Dædalus, the Journal of the American Academy of Arts & Sciences 140 (4) Fall Edition. UC Berkeley School of Information, California, United States.

Murray, Campbell. (2011). “Social Engineering: Strategies and Defence – a White Paper by Encription Limited. Foley Drive, Kidderminster.

Omote, Robert. (2008). “Law Ought to be an Instrument of Social Engineering”.

Pfleeger, Charles. (2003). “Security in Computing”. New York: Pearson Education.

Prince, Kevin. (2009). The ABC’s of Social Engineering and Five Ways to Protect Your Organisation. Perimeter eSecurity.

Redmon, Kevin C. (2006). “Mitigation of Social Engineering Attacks in Corporate America”. East Carolina University.

Simpson, M. T., et al. (2013). Hands-on ethical hacking and network defense. Boston, MA, Course Technology.

Singh, Rahul. (2013). “Kali Linux Social Engineering”. Packt Publishing: Birmingham, United Kingdom.

Speed, T. J. (2012). Asset protection through security awareness. Boca Raton, FL, CRC Press.

Thompson, Paul. (2003). “Cognitive Hacking and Intelligence and Security Informatics”. Thayer School of Engineering and Department of Computer Science, Darmouth College, New Hampshire, United States.

Tomhave, Ben. (2007). “How to Thwart a Social Engineering Exploit: Manipulation Tactics Three Apporaches”. T2P Reality-Based Guide.

Thapar, Ashish. (2007). “Social Engineering: An Attact Vector Most Inticrate to Tackle!”. White Paper on Social Engineering.

Turner, Terry. (2005). “Social Engineering – Can Organizations Win the Battle?”. East Carolina University.

Warren, Matthew J, and Shona Leitch. (2006). “Social Engineering and Its Impact via the Internet”. School of Information Systems, Faculty of Business and Law, Deakin University, Victoria, Australia.

Watanabe, Tohru. (2008). “Decomposing the Social Engineering Threat: A Behavioral Science Perspective”. The Global Voice of Information Security, ISSA Journal, December Edition.

Weingarten, F.W. (1989). “Federal Information Policy Development: The Congressional Perspective”. In C. McClure, P. Hernon and H. Relyea (eds), United States Government Information Policies: views and Perspectives - Ablex, Norwood, NJ.

Richardus Eko Indrajit is a profesor of information system from ABFI Instiute Perbanas, Indonesia. Graduated as Bachelor fo Engineering from Sepuluh Nopember Institute of Technology, Surabaya, Indonesia. Holding a Master of Computer Science Degree from Harvard University, USA and Doctor of Business Administration from Pamantasan ng Lungsod ng Maynila, the Philippines. Presently, chairing the Association of Global IT Architect (IASA) – Indonesian Chapter, and acting as Strategic Advisor of Cyber Operation Center, Ministry of Defense, Republic of Indonesia.