Social Engineering Attack Framework

Francois Mouton*, Mercia M. Malan†, Louise Leenen* and H.S. Venter‡
*Defence Peace Safety & Security, Council for Industrial and Scientific Research
Pretoria, South Africa
E-mail: moutonf@gmail.com, lleenen@csir.co.za
†University of Pretoria, Information and Computer Security Architecture
Pretoria, South Africa
E-mail: malan747@gmail.com
‡University of Pretoria, Department of Computer Science
Pretoria, South Africa
E-mail: hventer@cs.up.ac.za

***Abstract*—The field of information security is a fast growing discipline. Even though the effectiveness of security measures to protect sensitive information is increasing, people remain susceptible to manipulation and the human element is thus a weak link. A social engineering attack targets this weakness by using various manipulation techniques in order to elicit sensitive information. The field of social engineering is still in its infancy stages with regards to formal definitions and attack frameworks.**

This paper proposes a social engineering attack framework based on Kevin Mitnick's social engineering attack cycle. The attack framework addresses shortcomings of Mitnick's social engineering attack cycle and focuses on every step of the social engineering attack from determining the goal of an attack up to the successful conclusion of the attack. The authors use a previously proposed social engineering attack ontological model which provides a formal definition for a social engineering attack. The ontological model contains all the components of a social engineering attack and the social engineering attack framework presented in this paper is able to represent temporal data such as flow and time. Furthermore, this paper demonstrates how historical social engineering attacks can be mapped to the social engineering attack framework. By combining the ontological model and the attack framework, one is able to generate social engineering attack scenarios and to map historical social engineering attacks to a standardised format. Scenario generation and analysis of previous attacks are useful for the development of awareness, training purposes and the development of countermeasures against social engineering attacks.

***Index Terms*—Bidirectional Communication, Indirect Communication, Mitnick's Attack Cycle, Ontological Model, Social Engineering, Social Engineering Attack, Social Engineering Attack Framework, Unidirectional Communication.**

I. Introduction

The field of information security is a fast growing discipline. The protection of information is of vital importance to organisations and governments, and the development of countermeasures against illegal access to information is an area that receives increasing attention. Organisations and governments have a vested interest in securing sensitive information and thus securing the trust of clients and citizens. Technology on its own is not a sufficient safeguard against information theft; staff is often the weak link in an information security system. Staff members can be influenced to divulge sensitive information which subsequently allow unauthorised individuals to access protected systems.

The 'art' of influencing people to divulge sensitive information is known as social engineering and the process of doing so is known as a social engineering attack. There are various definitions of social engineering and a number of different models of a social engineering attack [1]. The authors considered a number of definitions of social engineering and social engineering attack taxonomies in a previous paper, *Towards an Ontological Model Defining the Social Engineering Domain* [1], and formulated a standardised, detailed definition. They also proposed an ontological model for a social engineering attack. The authors define social engineering as "the science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity" [1].

The previously proposed ontological model includes components of a social engineering attack and divides the attack into different classes and subclasses. The two classes of a social engineering attack are: Direct communication and indirect communication. The direct communication class is further divided into two subclasses: Bidirectional communication and unidirectional communication. A social engineering attack is then further explained to contain the following components: one Social Engineer; one Target; one or more Compliance Principles; one or more Techniques; one Medium; and one Goal [1].

Although the ontological model contains all the components of a social engineering attack, an ontological model struggles to depict temporal data, such as flow and time [2]. One of the main features of an ontology is that it separates the domain knowledge from the operational knowledge [2]. Due to this shortcoming, the ontological model is not sufficient to depict the process and the steps involved in executing a social engineering attack. The purpose of this paper is to present a social engineering attack framework which, in conjunction with the ontological model, investigate the attack process in detail. The framework refers to the components in the ontological model, but focuses on the process flow

978-1-4799-3383-9/14/$31.00 ©2014 IEEE

starting at the point at which an attacker initially thinks about gaining sensitive information from some target up to the point of succeeding in the goal of gaining this information.

The ontological model provides the basic structure of a social engineering attack whereas the social engineering attack framework adds both time and flow components. The combination of the ontological model and the attack framework can be used to generate social engineering attack scenarios and to map historical social engineering attacks to a standardised format. These scenarios are useful to educate individuals about social engineering and to gauge their awareness of social engineering. Scenario generation is also useful in the development of countermeasures against attacks. Having a standardised formulation of a social engineering attack as well as the flow and time events, allow researchers to compare different social engineering attacks.

Section II provides a background on social engineering attacks and further discusses the authors' previous work. Section III discusses the proposed social engineering attack framework and section IV provides some applications of the social engineering attack framework. Section V concludes the paper.

II. Defining Social Engineering Attacks

There are many models and taxonomies concerning social engineering attacks which are explored and analysed in the author's previous paper [1] such as [3], [4], [5], [6], [7]. The most commonly known model is Kevin Mitnick's social engineering attack cycle as described in his book, *The art of deception: controlling the human element of security*, [8]. Mitnick's attack model has four phases: research, developing rapport and trust, exploiting trust and utilising information. These four phases are not explained in great detail in Mitnick's book.

The picture below is a representation of Mitnick's attack cycle created by the authors. Figure 1 depicts the four phases and the flow between each of the phases. Each of these phases are briefly discussed below as explained in Mitnick's book.

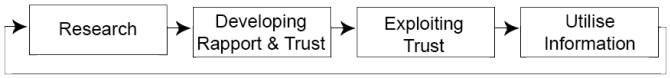

Fig. 1. Kevin Mitnick's Social Engineering Attack Cycle

Research is an information gathering process where information about the target is retrieved. The attacker should know as much as possible about the target before starting the attack.

The next phase is the **Development of the rapport and trust** with the target. A target is more likely to divulge requested information to an attacker if he trusts the attacker. According to Mitnick [8], rapport and trust development can be done by using insider information, misrepresenting an identity, citing those known to the victim, showing a need for assistance, or occupying an authoritative role.

When a target appears to trust an attacker, the attacker **Exploits the trust** to elicit information from the target: this can either take the form of a request for information, a request for a specified action from the victim or, alternatively, to manipulate the victim into asking the attacker for help [8]. This phase is where the previously established relationship is abused to get the initially desired information or action.

Finally, the outcome of the previous phase is **Utilised** to reach the goal of the attack or to move on to further steps which may be required to reach the goal.

A trivial example is when an attacker supposedly needs to connect to an organisation's network. As a result of his research the attacker finds out that a help-desk staff member knows the password to the organisation's wireless network. In addition, the attacker found personal information regarding the staff member who has been identified as the target. The attacker initiates a conversation with the target, using the acquired information to establish trust; in this case the attacker misrepresents himself as an old school acquaintance of the target. The attacker subsequently exploits the established trust by asking permission to use the company's wireless network facility to send an e-mail. The help-desk attendant is willing to supply the required password to the attacker due to the misrepresentation, and is able to gain access to the organisation's network and achieve his objective.

The authors' ontological model defines that a social engineering attack "employs either direct communication or indirect communication, and has a social engineer, a target, a medium, a goal, one or more compliance principles and one or more techniques" [1]. The attack can be split into more than one attack phase, each phase handled as a new attack according to the model. The model is depicted in figure 2.

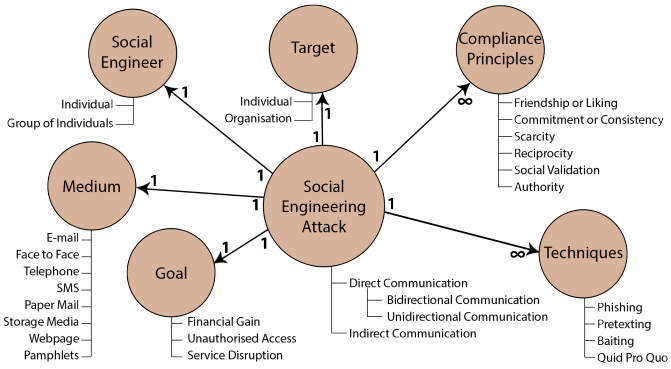

Fig. 2. An Ontological Model of a Social Engineering attack

Direct communication, where two or more people communicating directly with each other, is sub-divided into "Bidirectional communication" and "Unidirectional communication". Bidirectional communication occurs when both parties participate in the conversation. For example, an e-mail is sent from the attacker to the target and the target replies to the attacker.

Unidirectional communication occurs when the conversation is one-way only: from the attacker to the target. For example, if the attacker sends a message through paper mail without a return address, the target cannot reply to the message. Phishing attacks are also a popular type of attack in this category.

Indirect communication is when there is no actual interaction between the target and the attacker; communication occurs through some third party medium. An example of this type of communication is when the attacker infects a flash drive and leaves it somewhere to be found by some target. The target is curious to find out what is on the flash drive for personal gain or, motivated by ethical consideration, to attempt to find the owner of the flash drive. The target inserts the flash drive into their computer, and the infection on the flash drive is activated.

The ontological model further contains several components as mentioned in the introduction. The goal can be financial gain, unauthorised access or service disruption. The medium is a way of communication such as e-mail, face to face, telephone etc. The social engineer can be either an individual or a group of individuals. The target can either be an individual or an organisation.

Compliance principles refer to the reasons why a target complies with the attacker's request, and techniques include those used to perform social engineering attacks. Examples of techniques include phishing, pretexting, baiting and quid pro quo [1]. Examples of compliance principles include:

- *Friendship or liking*: People are more willing to comply with requests from friends or people they like.
- *Commitment or consistency*: Once committed to something, people are more willing to comply with requests consistent with this position.
- *Scarcity*: People are more willing to comply to requests that are scarce or decreasing in availability.
- *Reciprocity*: People are more willing to comply with a request if the requester has treated them favourably in the past.
- *Social Validation*: People are more willing to comply to a request if it is seen as the socially correct thing to do.
- *Authority*: People comply easily to requests given by people with more authority than they have.

Once the compliance principles, techniques and medium have been selected, the attack vector can be set-up and the social engineer can continue to the actual attacking phase.

The next section introduces the proposed social engineering attack framework.

III. Social Engineering Attack Framework

In this section the authors propose an extension of Kevin Mitnick's original social engineering attack cycle [8]. Mitnick's attack cycle is explained very briefly in his book and does not contain a lot of detail. Mitnick's attack cycle is very broad and is open to interpretation in some aspects. Figure 3 depicts the new proposed social engineering attack framework. This framework clarifies Mitnick's phases and is more detailed.

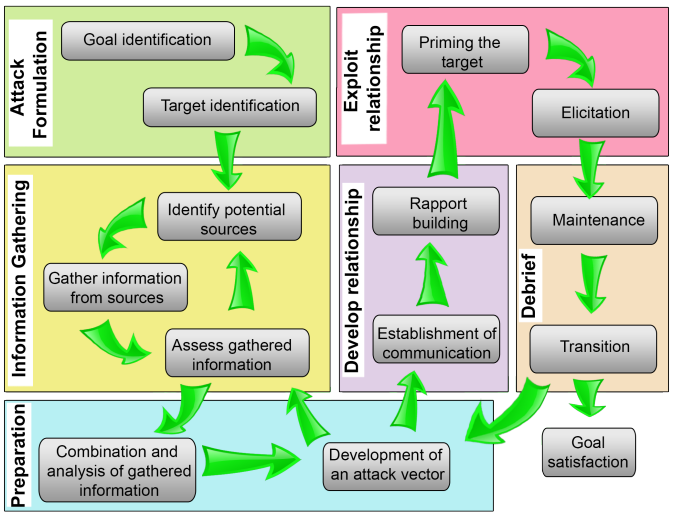

Fig. 3. Social Engineering Attack Framework

In Mitnick's first phase, the research phase, he states that when executing a social engineering attack one needs to get the most possible information about the target. Even though this is true, this is a very broad statement and it also assumes that the target is already known and that the goal is already set. The authors propose an additional step before gathering the information which is meant for determining what the goal of the attack is and the best possible target to assist with reaching the goal. Once the goal and target is known, the actual information gathering can start. This process is also described in more detail than Mitnick's model as one needs to identify sources of information before anything can be gathered and it is beneficial to assess the gathered information to ensure that there is sufficient information to execute the attack. Mitnick's attack cycle does not contain a preparation phase which is also needed during the social engineering attack. The authors propose a preparation phase which is used to prepare the gathered information and to develop the attack vector that will be used during the social engineering attack.

Mitnick's next phase, development of rapport and trust, is very similar in the proposed framework but the starting point is modelled as a separate step. Establishment of communication is a requirement for any relationship to be built with the target. The gathered information is used to assist in establishing communication. Once the attacker and the target are communicating, the rapport and trust building can commence.

The third phase, according to Mitnick, is the exploitation phase. This phase also requires more detail than that given in Mitnick's attack cycle. Exploiting a relationship is done with different manipulation techniques and in order for these techniques to work the target has to be in an emotional state where the exploitation is possible. This differs between all human beings and it is thus necessary to first determine what that emotional state is of the target and then get the target into the desired emotional state. Once the target is in the right emotional state, the information can be elicited. The other

important step not mentioned in Mitnick's attack cycle is the debriefing step. The target has to be brought back to a normal emotional state to avoid further consequences. The idea is to have the target feel good about giving out unauthorised information instead of feeling guilty about it.

Finally Mitnick has a fourth phase, utilising the information, which the authors argue to be not part of the actual social engineering attack. The social engineering attack focuses on attacking the human aspect with the intention to achieve a specified goal, in this case to gain privileged information. This information can be used to perform a different action, but this is no longer part of the social engineering attack. For instance if the information is a password to the system, gaining the password from a person is a social engineering attack whereas using the password to break into the system has no human element to it and is thus not a social engineering attack.

The framework is completed by having a transition phase after debriefing to either go back and gather more information if it is found that more information is needed to be able to complete the attack, or go to the goal satisfaction. Mitnick also states that previous steps can be repeated if the goal is not satisfied, though this is not described in much detail. The proposed framework provides a more precise transition phase specifying the exact phase to return to and repeat if necessary.

The following subsections describe each of these phases in more detail.

A. Attack Formulation

The first step of a social engineering attack is to address the question "What does the social engineer want?". This goal of the social engineer is the purpose of the entire attack and should be very clear. Once the goal is identified, the target should be selected, as depicted by Figure 4. The target can be an individual or a group of individuals.

The target may belong to an organisation that is under attack as part of the goal. For example, the goal may be to infiltrate an organisation and the target is a security guard who possesses information required to accomplish the goal. Both the organisation and the selected target are important in the information gathering phase.

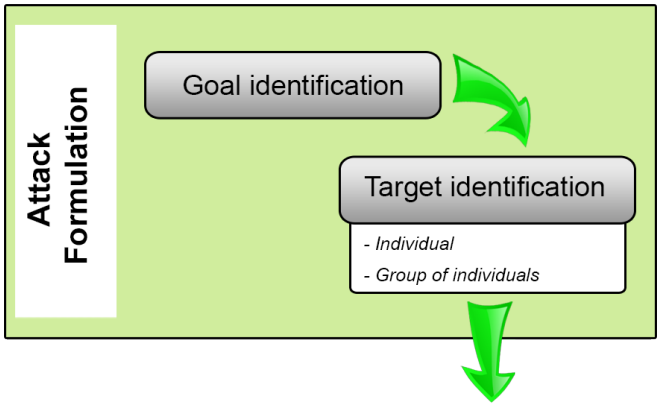

Fig. 4. Social Engineering Attack : Attack Formulation

B. Information Gathering

Information gathering is a very important part of the social engineering attack because the probability of developing a trusting relationship with a target is increased by the quality of the information regarding the target. A target is more likely to share information with the attacker if a relationship exists between the two.

Information is gathered about the target and everything related to the attack. As depicted in Figure 5, the first step of gathering information is to 'identify the possible sources' from which information can be obtained. The sources can be anything or anyone with access to the information required for the attack. These sources can be any publicly available sources such as company websites, social networking sites or personal blogs and forums, or private information that is not publicly available. Techniques such as dumpster diving can be used where discarded items are scanned for private information, such as an address on a bank statement. Dumpster diving is the technique of sifting through trash such as medical records or bank statements to find anything that can be useful to the dumpster diver [9].

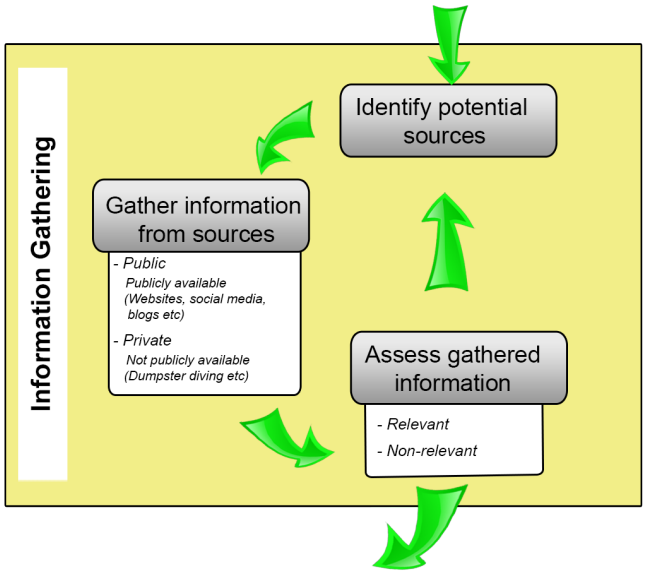

Fig. 5. Social Engineering Attack : Information Gathering

After gathering information, the information is assessed to be relevant or not. If the social engineer still does not have enough information, he can go back to identifying more sources and restart the information process.

The 'information gathering' phase is repeated until the social engineer is satisfied that sufficient information has been obtained, such that he can start his preparation for the attack.

C. Preparation

During preparation the social engineer ensures that everything is ready before starting the actual attack. As depicted by Figure 6, the first step of this phase is to combine

all information gathered to form a bigger picture about the planned attack.

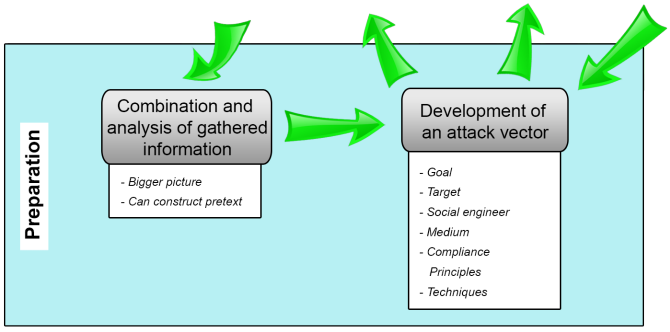

Fig. 6. Social Engineering Attack : Preparation

This combined view of the scenario can be used for pre-texting where a scenario is devised to lure the target into a required action. An effective pretext should be believable and withstand scrutiny from the target. It often relies on the quality of the information gathered on the target's personality. An attack vector is now developed; it should contain all the elements of a social engineering attack [1]. The attack vector is the attack plan which leads to the satisfaction of the goal. It has a goal, a target and a social engineer. In addition, the plan must identify a medium, compliance principles and techniques.

D. Develop a Relationship

As mentioned previously, developing a good relationship with the target is an essential part of the social engineering attack. If trust cannot be established, the required information is unlikely to be elicited from the target. Figure 7 depicts the first step involved in building a relationship with the target, namely the 'establishment of communication' step. This step is executed by using the medium identified during the preparation phase. If a pretext has been included in the plan, it is used along with the initial communication.

The next step in developing a relationship is the 'rapport building'. This entails the actual building of the relationship and establishment of trust using the devised plan. Various techniques can be employed to establish trust. This step is not trivial and can be time consuming. A good pretext simplifies this step. Once the social engineer has built a good relationship with the target, the relationship can be exploited to obtain the information the social engineer requires from the target.

E. Exploit the Relationship

As depicted in Figure 8, exploiting the relationship consists of two parts: 'priming the target' and 'elicitation'. The first part is for the attacker to use manipulation tactics and his preparation to get the target in a desired emotional state suited to the plan, such as feeling sad or happy. For example, relating to a sad story can evoke the target into remembering a sad incident, and subsequently to feel sad.

Once the target is in the desired emotional state, the elicitation process can start. At the conclusion of the elicitation

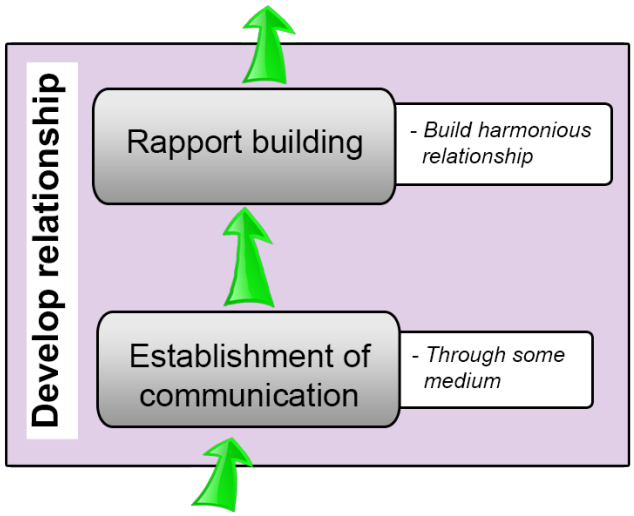

Fig. 7. Social Engineering Attack : Develop Relationship

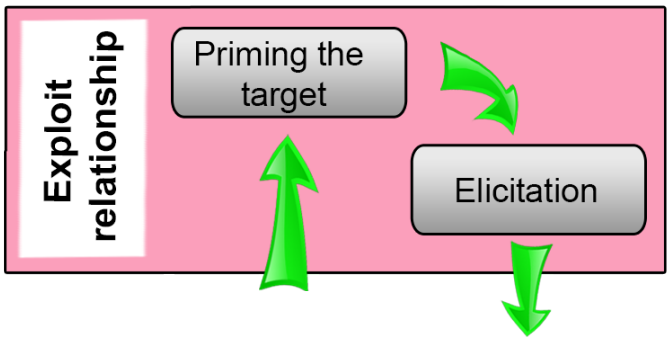

Fig. 8. Social Engineering Attack : Exploit Relationship

phase the social engineer should have obtained the required information from the target. This may be a password which is needed for the eventual satisfaction of the goal of the social engineering attack. After the exploitation phase, it is important to debrief the target.

F. Debrief

Debriefing the target involves returning the target to a desired emotional state of mind, as shown in the 'maintenance' step in figure 9. It is important for the target not to feel that he was under attack; if he is in a normal state of mind, he will probably not reflect too much on the activities that occurred. For example, if the target had been manipulated into a sad emotional state and the attacker then elicited a password from him, the target may feel inadequate because he has released sensitive information. This feeling of inadequacy may consequently lead to emotional states such as depression. It may even lead to suicide by the target as evidenced in an incident in 2012 involving the solicitation of private information concerning the British Royal family [10], [11]. During the confinement of Princess Catherine, an Australian radio talk show host socially engineered a staff member of the

maternity ward where the princess was a patient, to release information regarding the Princess' condition.

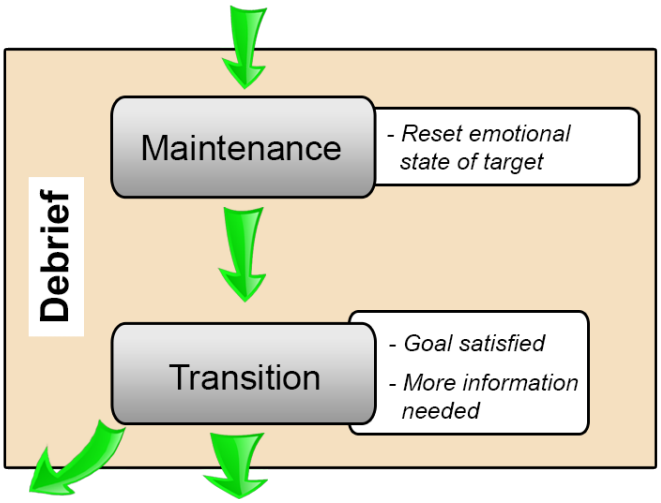

Fig. 9. Social Engineering Attack : Debrief

Figure 9 depicts the next step in the debriefing phase, namely 'transition'. This is where the social engineer either decides that the goal has been satisfied or that more information is needed and the engineer returns to the information gathering phase.

The next section discusses the applications of the framework on two examples.

IV. Framework Application

This section discusses two examples of well-known social engineering attacks which have also been documented in news articles. Each of the examples are individually mapped to the proposed Social Engineering Attack Framework. This exercise shows that the Social Engineering Attack Framework can be utilised to convert historical social engineering attacks to a standardised format. Having historical social engineering attacks in a standardised format allows one to perform comparisons between two different social engineering attacks. These standardised social engineering attack scenarios can also be used for social engineering training and awareness testing.

The next subsections analyse each of the examples according to the attack framework. Important features of each social engineering attack are mapped to the components in the definition of a social engineering attack. The different components of a social engineering attack are: the type of communication, the social engineer, the target, a medium, a goal, one or more compliance principles and one or more techniques.

A. Example 1 Analysis

The first example happened in 2013 and is described in the following excerpt [12]:

> "In April 2013, the administrative assistant to a vice-president at a French-based multinational company received an e-mail referencing an invoice hosted on a popular file sharing service. A few minutes later, the same administrative assistant received a phone call from another vice president within the company, instructing her to examine and process the invoice. The vice president spoke with authority and used perfect French. However, the invoice was a fake and the vice president who called her was an attacker.
>
> The supposed invoice was actually a remote access Trojan (RAT) that was configured to contact a command and control (CC) server located in Ukraine. Using the RAT, the attacker immediately took control of the administrative assistant's infected computer. They logged keystrokes, viewed the desktop, and browsed and ex-filtrated files.
>
> These tactics, using an e-mail followed up by a phone call using perfect French, are highly unusual and are a sign of aggressive social engineering. In May 2013, Symantec Security Response published details on the first attacks of this type targeting organisations in Europe. Further investigations have revealed additional details of the attack strategy, attacks that are financially motivated and continue to this day."

This example is now mapped to the Social Engineering Attack Framework. It consists of two different phases and also demonstrates how the Social Engineering Attack Framework can handle two different Social Engineering Attacks.

1) First Attack Phase:

The important features of the social engineering attack are specified below:

Communication — The Social Engineering Attack is using direct communication with the subclass of unidirectional communication.
Social Engineer — The Social Engineer is an individual.
Target — The Target is an individual. In this instance the target is an administrative assistant to the vice-president at a French-based multinational company.
Medium — The medium is e-mail.
Goal — The goal of the attack is to gain unauthorised access to the organisation.
Compliance Principles — The compliance principles that are used are consistency and authority.
Technique — The technique that is used is phishing.

The next part steps through this example by means of the attack framework.

Step 1: Attack Formulation

Goal identification: The goal of the attack is to gain unauthorised access to the organisation's systems and thus to the organisation's information.
Target identification: The target of the attack is the administrative assistant to the vice-president at a French-based multinational company.

Step 2: Information Gathering

Identify potential sources: Public records of the company and e-mail communication samples from the organisation.

Gather information from sources: Collect and find the public records of the company and collect samples of e-mail communication.

Assess gathered information: Determine the organisational hierarchy and assess the e-mail format of internal organisational e-mail communication.

Step 3: Preparation

Combination and analysis of gathered information: Identify where the target fits into the organisational hierarchy and identify the superiors of the target. Identify the e-mail structure of internal e-mails sent in the organisation and the type of information that should be sent to the target.

Development of an attack vector: Write an e-mail which is similar to other e-mails exchanged within the organisation but also contains the malicious Remote Access Trojan (RAT). More specifically, the e-mail's format should be similar to the format used in typical e-mail invoices the administrative assistant receives.

Step 4: Develop Relationship

Establishment of communication: The physical action of sending the e-mail that was developed during the 'development of an attack vector' step is the initial establishment of communication.

Rapport building: The e-mail contents should be similar to a typical e-mail the administrative assistant can expect.

Step 5: Exploit Relationship

Priming the target: The e-mail should be of such a nature that the administrative assistant would not immediately delete or discard the e-mail.

Elicitation: In the 'priming the target' step, the goal is for the target to not delete the e-mail immediately. The elicitation will be deemed successful if the target does not delete the e-mail.

Step 6: Debrief

Maintenance: The e-mail should be worded in such a manner that the target is not perturbed by the e-mail.

Transition: The e-mail should note that there will be some follow-up communication. The target is then prepared for follow-up communication and thus a transition is made to the 'development of an attack vector' step and not to the 'goal satisfaction' step.

2) Second Attack Phase:

The important features of the social engineering attack are specified below:

Communication — The Social Engineering Attack is using direct communication with the subclass of bidirectional communication.

Social Engineer — The Social Engineer is an individual.

Target — The Target is an individual. In this instance he is an administrative assistant to the vice-president at a French-based multinational company.

Medium — The medium is the telephone.

Goal — The goal of the attack is to gain unauthorised access to the organisation.

Compliance Principles — The compliance principles that are used are consistency and authority.

Technique — The technique that is used is phishing.

The next part steps through this example by means of the attack framework.

Step 1: Attack Formulation

Nothing here as it is a transition to the 'development of an attack vector' step.

Step 2: Information Gathering

Nothing here as it is a transition to the 'development of an attack vector' step.

Step 3: Preparation

Combination and analysis of gathered information: Nothing here as it is a transition to the 'development of an attack vector' step.

Development of an attack vector: The target already has an e-mail in his inbox containing a malicious invoice, and during phase 1 this e-mail was not deleted. This attack vector is aimed at getting the target to open the malicious invoice so that the social engineer can gain unauthorised access. In this phase one is required to develop a transcript to be followed which will use both authority and consistency principles to get the target to comply with the request to open the malicious invoice.

Step 4: Develop Relationship

Establishment of communication: The physical action of making the phone call of which the transcript has been developed during the 'development of an attack vector' step is the initial establishment of communication.

Rapport building: The telephonic conversation should start off by the attacker introducing himself as the second vice-president of the organisation (This information was gathered from the organisational hierarchy).

Step 5: Exploit Relationship

Priming the target: The target should be aware that the caller requesting him to process the invoice is a person in an authoritative position. It must also be consistent with requests that the target would normally be required to process as well as consistent with the e-mail containing the invoice.

Elicitation: Since the target has been primed to comply with the requests by means of authority and consistency, the social engineer can now request the target to process the malicious invoice.

Step 6: Debrief

Maintenance: The malicious invoice should be similar to one that the target would normally receive. The target should be unaware that he has provided the

social engineer with unauthorised access by opening the malicious invoice. Whilst on the phone, the social engineer should be friendly and reassuring towards the target. The target must always feel good about helping the social engineer in order to avoid suspicion.

Transition: The Social Engineer has now obtained his unauthorised access and can proceed to the goal satisfaction state.

Goal Satisfaction: The Social Engineer has obtained his initial goal of obtaining unauthorised access.

B. Example 2 Analysis

The second example happened in 2009 when fliers appearing to be traffic violations were placed on cars in a parking lot. On these supposed parking violations a website link was included where one could view pictures associated with the so-called violation. The website extracted a Dynamic Link Library (DLL) into the system32 directory on the computer used to access the website. The DLL installs as an internet explorer browser helper object once the system is rebooted. Next a pop-up would appear, informing the user that his computer contains signs of viruses and Antivirus 360 needs to perform a scan. If the user agrees to let the anti-virus application install itself, (it was later found that the anti-virus application was a virus dropper) it in turn installed a virus. The attacker did not continue with the attack, however if he had continued he could have taken full control of the computer since it was already infected with his software [13].

An excerpt of this article reads as follows [13]:

> "I had the opportunity to examine malware whose initial infection vector was a car windshield flier with a website address. The malicious programs were run-of-the-mill; however, the use of fliers was an innovative way of social engineering potential victims into visiting a malicious website.
>
> Several days ago, yellow fliers were placed on the cards in Grand Forks, ND. They stated:
>
> *PARKING VIOLATION This vehicle is in violation of standard parking regulations. To view pictures with information about your parking preferences, go to website-redacted.*
>
> The website showed several photos of cars on parking lots in that specific town. EXIF data in the JPG files show that they were edited using Paint Shop Pro Photo 12 to remove license plate details of the cars and that the photos were taken using a Sony DSC-P32 camera. Installing PictureSearch-Toolbar.exe led to DNS queries for childhe.com, a domain with a bad reputation according to Symantec, McAfee, etc. Even without the Internet connection, the program installed (extracted) a DLL into C:/WINDOWS/system32."

This example is now demonstrated through the use of the Social Engineering Attack Framework.

1) The Attack Phase:

The important features of the social engineering attack are specified below:

Communication — The Social Engineering Attack is using indirect communication through third party mediums.

Social Engineer — The Social Engineer is an individual.

Target — The Target is an individual. In this instance, it is any owner of a car parked in the parking lot.

Medium — The medium is fliers.

Goal — The goal of the attack is to gain unauthorised access to an individuals computer.

Compliance Principles — The compliance principles that are used are social compliance and authority.

Technique — The technique that is used is phishing.

The next part steps through this example by means of the attack framework.

Step 1: Attack Formulation

Goal identification: The goal of the attack is to gain unauthorised access to an unspecified individuals' computer.

Target identification: The target of the attack is any person who owns a car and is parked in the parking lot at the time of spreading the fliers.

Step 2: Information Gathering

Identify potential sources: Public websites with the ability to view parking violations and any institute with authority to reach out a parking violation.

Gather information from sources: Collect sample parking violations which are placed on windshields of cars and sample websites where one can view parking violations.

Assess gathered information: Determine which parking violations are relevant to the specific parking lot, perhaps on location, region etc. The violation, in this case, should specifically conform to the standard parking violations reached out in Grand Forks, ND. Also filter out the website that is consistent with the parking violation.

Step 3: Preparation

Combination and analysis of gathered information: Choose one final parking violation / website pair and finalise the structure of the parking violation, the style and working of the website.

Development of an attack vector: Develop a parking violation consistent to the finalised structure as well as a phishing website which looks similar to the one chosen in the previous step. On the parking violation, ensure that there is a section stating that pictures with information about the parking violation are on a certain website, with a link to the phishing website.

Step 4: Develop Relationship

Establishment of communication: The physical action of putting the created fliers on the cars in the parking

lot.

Rapport building: The parking violation placed on the windshield of the cars should be consistent with parking violations handed out in that parking lot under standard conditions. The owner of the car receiving the violation should not doubt whether it is official; it should look legitimate. When the target visits the website, the website should also look legitimate, not raising doubt with the user.

Step 5: Exploit Relationship

Priming the target: The flier should be realistic so that the owner of the car would take it seriously and not just throw it away. While driving home the target should ideally think about the violation and prepare himself to go to the website to view the parking violation, feeling pressured due to social compliance to do the right thing and pay the fine.

Elicitation: Provide a link on the flier which links to the phishing website. Upon clicking on the link, a backdoor is installed on the person's computer, giving the social engineer the opportunity to gain unauthorised access to the computer.

Step 6: Debrief

Maintenance: The flier and website should be created in such a way that the target does not feel threatened. The website should be similar to the real violations website so that the victim is confident that he should take the steps required to pay the violation.

Transition: The social engineer can use the backdoor to gain unauthorised access to the computer and can thus proceed to the 'goal satisfaction' step.

Goal Satisfaction: The Social Engineer has obtained his initial goal of unauthorised access.

V. Conclusion

The protection of information is extremely important in a modern society and even though the security around information is continuously improving, the one weak point is still the human being who is susceptible to manipulation techniques. This paper explored social engineering as a domain and social engineering attacks as a process inside this domain. A previous paper by the authors, *Towards an Ontological Model Defining the Social Engineering Domain* [1], is revisited and the ontological model proposed in the paper is explored in order to further define the social engineering domain.

Kevin Mitnick's social engineering attack cycle [8] is analysed and discussed in detail. The authors propose a social engineering attack framework based on Mitnick's attack cycle. The shortcomings in Mitnick's attack cycle are explored and improvements of these short-comings are reflected in the proposed attack framework. Each phase in the proposed social engineering attack framework is discussed in detail and two life scenarios are explored as an application of the combination of the attack framework and the previously proposed ontological model.

The authors found that Mitnick's attack cycle is a good base for social engineering attacks, but lacks significant detail. It is a very broad explanation of an attack and assumes that certain components of the attack are already known, such as the goal of the attack and the target. The attack framework provides specific steps to identify these component and detailed steps for all other aspects of an attack.

This paper provides an in depth social engineering attack framework as an extension to the previously proposed ontological model. The framework adds temporal data such as flow and time whereas the ontological model contains all the components of a social engineering attack. The framework and the ontological model can be used to generate social engineering attack scenarios as well as to map historical social engineering attacks to a standardised format. This is important as these scenarios can be used for education and awareness purposes and enables anyone to analyse and compare different social engineering attacks. Future work includes the actual creation of such scenarios.

References

[1] F. Mouton, L. Leenen, M. M. Malan, and H. S. Venter, "Towards an ontological model defining the social engineering domain," in *11th Human Choice and Computers International Conference*, Turku, Finland, July 2014, pp. 266–279.

[2] N. F. Noy and D. L. McGuinness, "Ontology development 101: A guide to creating your first ontology," Stanford Knowledge Systems Laboratory, Technical Report KSL-01-05, March 2001.

[3] D. Harley, "Re-floating the titanic: Dealing with social engineering attacks," in *European Institute for Computer Antivirus Research*, 1998.

[4] L. Laribee, "Development of methodical social engineering taxonomy project," MSc, Naval Postgraduate School, Monterey, California, June 2006.

[5] K. Ivaturi and L. Janczewski, "A taxonomy for social engineering attacks," in *International Conference on Information Resources Management*, G. Grant, Ed. Centre for Information Technology, Organizations, and People, June 2011.

[6] F. Mohd Foozy, R. Ahmad, M. Abdollah, R. Yusof, and M. Mas'ud, "Generic taxonomy of social engineering attack," in *Malaysian Technical Universities International Conference on Engineering & Technology*, Batu Pahat, Johor, November 2011.

[7] P. Tetri and J. Vuorinen, "Dissecting social engineering," *Behaviour & Information Technology*, vol. 32, no. 10, pp. 1014–1023, 2013.

[8] K. D. Mitnick and W. L. Simon, *The art of deception: controlling the human element of security*, W. Publishing., Ed. Indianapolis: Wiley Publishing, 2002.

[9] J. Long, *No tech hacking: A guide to social engineering, dumpster diving, and shoulder surfing*, S. Pinzon, Ed. Syngress, 2011.

[10] F. Mouton, M. M. Malan, and H. S. Venter, "Social engineering from a normative ethics perspective," in *Information Security for South Africa*, Johannesburg, South Africa, August 2013, pp. 1–8.

[11] Social-Engineer.org. (2012, December) One royal pwning. Social-Engineer.org. [Online]. Available: http://www.social-engineer.org/social-engineering/one-royal-pwning/

[12] Symantec Security Response. (2014, January) Francophoned a sophisticated social engineering attack. Symantec. [Online]. Available: http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack

[13] L. Zeltser. (2009, February) Malware infection that began with windshield fliers. Internet Storm Center. [Online]. Available: https://isc.sans.edu/diary/5797