COMPUTERS & SECURITY 59 (2016) 186–209

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Social engineering attack examples, templates and scenarios

Francois Mouton [a,b,*], *Louise Leenen* [a], *H.S. Venter* [b]

[a] *Command, Control and Information Warfare, Defence, Peace, Safety and Security, Council for Scientific and Industrial Research, Pretoria, South Africa*

[b] *Department of Computer Science, University of Pretoria, Pretoria, South Africa*

ARTICLE INFO

Article history:
Received 24 December 2015
Received in revised form 13 March 2016
Accepted 15 March 2016
Available online 21 March 2016

Keywords:
Bidirectional communication
Indirect communication
Mitnick's attack cycle
Social engineering
Social engineering attack detection model
Social engineering attack examples
Social engineering attack framework
Social engineering attack scenario
Social engineering attack templates
Unidirectional communication

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 thus the human element remains a weak link. A social engineering attack targets this weakness by using various manipulation techniques to elicit sensitive information. The field of social engineering is still in its early stages with regard to formal definitions, attack frameworks and templates of attacks. This paper proposes detailed social engineering attack templates that are derived from real-world social engineering examples. Current documented examples of social engineering attacks do not include all the attack steps and phases. The proposed social engineering attack templates attempt to alleviate the problem of limited documented literature on social engineering attacks by mapping the real-world examples to the social engineering attack framework. Mapping several similar real-world examples to the social engineering attack framework allows one to establish a detailed flow of the attack whilst abstracting subjects and objects. This mapping is then utilised to propose the generalised social engineering attack templates that are representative of real-world examples, whilst still being general enough to encompass several different real-world examples. The proposed social engineering attack templates cover all three types of communication, namely bidirectional communication, unidirectional communication and indirect communication. In order to perform comparative studies of different social engineering models, processes and frameworks, it is necessary to have a formalised set of social engineering attack scenarios that are fully detailed in every phase and step of the process. The social engineering attack templates are converted to social engineering attack scenarios by populating the template with both subjects and objects from real-world examples whilst still maintaining the detailed flow of the attack as provided in the template. Furthermore, this paper illustrates how the social engineering attack scenarios are applied to verify a social engineering attack detection model. These templates and scenarios can be used by other researchers to either expand on, use for comparative measures, create additional examples or evaluate models for completeness. Additionally, the proposed social engineering attack templates can also be used to develop social engineering awareness material.

* *Corresponding author.*
E-mail address: moutonf@gmail.com (F. Mouton).

http://dx.doi.org/10.1016/j.cose.2016.03.004
0167-4048/

1. Introduction

Information security is a fast-growing discipline. The protection of information is of vital importance to organisations and governments, and the development of measures to counter illegal access to information is an area that receives increasing attention. Organisations and governments have a vested interest in securing sensitive information and hence in securing the trust of clients and citizens. Technology on its own is not a sufficient safeguard against information theft; staff members are often the weak link in an information security system. Staff members can be influenced to divulge sensitive information, which subsequently allows unauthorised individuals access to 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 also a number of different models of social engineering attack (Åhlfeldt et al., 2005; Culpepper, 2004; Hadnagy, 2010; Hamill et al., 2005; Kingsley Ezechi, 2011; Lenkart, 2011; Mitnick and Simon, 2002; Mouton et al., 2012, 2014; Nohlberg, 2008; Thornburgh, 2004). 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* (Mouton et al., 2014), and formulated a definition for both social engineering and social engineering attack. In addition, the authors proposed an ontological model for a social engineering attack. They defined 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" (Mouton et al., 2014).

Although the ontological model contains all the components of a social engineering attack, it fails to depict temporal data such as flow and time (Noy and McGuinness, 2001). Due to this shortcoming, the authors developed a social engineering attack framework that expands on Kevin Mitnick's social engineering attack cycle (Mitnick and Simon, 2002; Mouton et al., 2014). The social engineering attack framework depicts the logical flow of a social engineering attack (Mouton et al., 2014). This framework refers to the components in the ontological model but focuses on the process flow – 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 (Mouton et al., 2014).

Each step within the social engineering attack framework has been verified using real-life social engineering examples (Mouton et al., 2014). The researchers found that there are limited practical examples of social engineering in literature. Current literature on social engineering attacks does not depict the full process flow of a social engineering attack and when researchers use these examples, several steps and phases of the attack have to be inferred (Mouton et al., 2014; Symantec Security Response, 2014; Zeltser, 2009).

The researchers has also found that social engineering attacks that are similar, in terms of the type of communication, medium, goal, compliance principles and techniques, share a similar set of steps and phases throughout the social engineering attack. Social engineering attack examples that share a similar set of steps and phases can be grouped together to form social engineering attack templates that encapsulate the detailed flow of the attack whilst abstracting the subjects and objects from the attack. The benefit of grouping similar social engineering attack examples into social engineering attack templates is that a single social engineering attack template can be used to depict several social engineering attack scenarios.

In order to compare and verify different models, processes and frameworks within social engineering, it is required to have a set of fully detailed social engineering attack scenarios. Having a set of social engineering attack templates will allow researchers to test their models, processes and frameworks and compare their performances against other models, processes and frameworks. This paper proposes social engineering attack templates that encapsulate several similar social engineering attack examples into templates, which provide details on each step and phase of the attack. These generic templates provide a description of the attack, detailing each step and phase of the attack, as well as a list of real-world social engineering attack examples that can be depicted within the social engineering attack template. Each of the social engineering attack templates is explained by mapping each step and phase of the template to the social engineering attack framework. This paper also delves into how these social engineering attack templates are used to verify models within the field of social engineering. This is illustrated by combining the social engineering attack templates with real-world examples to develop social engineering attack scenarios that are mapped to a social engineering attack detection model.

Section 2 provides some background on social engineering and on social engineering attacks, and discusses the authors' previous work. Section 3 proposes the social engineering attack templates and maps each template to both the social engineering ontological model and the social engineering attack framework. Section 4 illustrates the need for the social engineering attack templates by using the templates to verify a social engineering attack detection model. Section 5 concludes the paper.

2. Defining social engineering attacks

A trivial example of a social engineering attack is when an attacker wishes 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 gained 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 the attacker is able to gain access to the organisation's network and achieve his objective.

There are many models and taxonomies for social engineering attacks (Harley, 1998; Ivaturi and Janczewski, 2011; Laribee, 2006; Mohd Foozy et al., 2011; Mouton et al., 2014; Tetri and Vuorinen, 2013). 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* (Mitnick and Simon, 2002). 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. In previous research the authors developed the social engineering attack framework that fully expands on each phase (Mouton et al., 2014).

According to the authors' ontological model, 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" (Mouton et al., 2014). The attack can be split into more than one attack phase, and each phase is handled as a new attack according to the model. The model is depicted in Fig. 1.

Direct communication, where two or more people are 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 via 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 random target. The target is curious to exploit the contents of the flash drive for personal gain or, motivated by ethical considerations, to attempt to find the owner of the flash drive. The target inserts the flash drive into his/her computer, and the infection on the flash drive is activated.

The ontological model also contains components such as a goal, a medium, a social engineer, a target, compliance principles and techniques. The goal of an attack can be financial gain, unauthorised access or service disruption. The medium is a way of communication such as e-mail, face-to-face contact, a telephone call, 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 (Mouton et al., 2014). Examples of compliance principles include the following:

- *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 with 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 with a request if it is seen as the socially correct thing to do.
- *Authority*: People easily comply with requests received from 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 with the actual attacking phase.

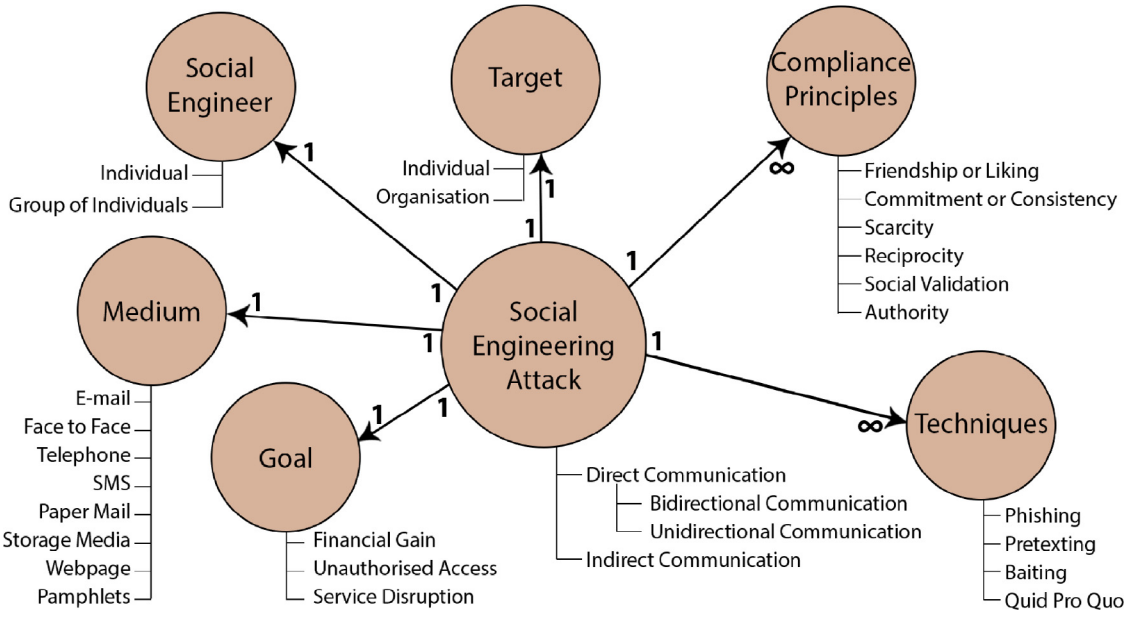

Fig. 1 – An ontological model of a social engineering attack.

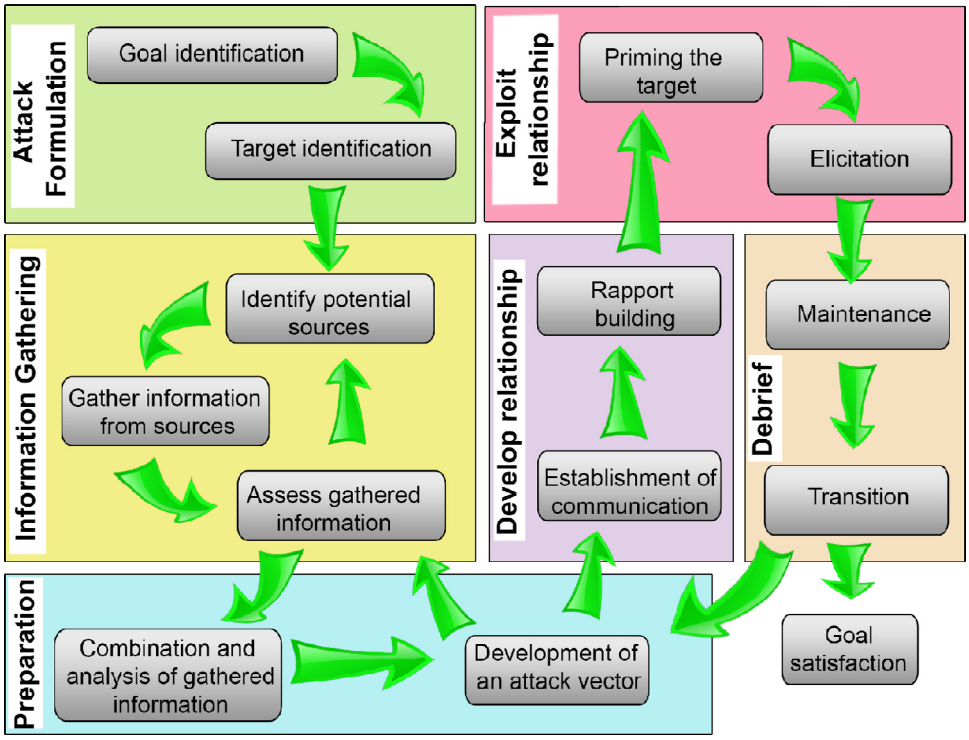

Fig. 2 – Social engineering attack framework.

The social engineering attack framework can be used to depict the planning and flow of the full attack. Fig. 2 depicts the social engineering attack framework.

The social engineering attack framework has six core phases, namely attack formulation, information gathering, preparation, develop relationship, exploit relationship and debrief.

The "attack formulation" phase is used to identify both the goal and the target of the specific attack. The "information gathering" phase is used to identify all sources of information on both the goal and the target, as well as to gather information from the identified sources. In the "preparation" phase, all the gathered information is combined and the social engineering attack vector is developed. It is during the "preparation" phase that all the elements in the social engineering ontological model can be identified. The "develop relationship" phase is where the attacker establishes communication with the target and attempts to build a trust relationship with the target. The "exploit relationship" phase is used to prime the target and to elicit the target to perform the request or action. The final phase is the "debrief" phase, in which the target is brought out of a primed state during the "maintenance" step, and the "transition" step tests whether the goal has been satisfied.

The next section describes why a set of detailed social engineering attack templates are required and presents the set of templates.

3. Templates for social engineering attacks

The authors previously proved the usefulness of the social engineering attack framework by mapping well-known social engineering attacks (which have been widely documented in news articles) to the social engineering attack framework. During this research it was found that several pieces of information about the social engineering attack were not included in the documentation and that several steps of the social engineering attack had to be inferred.

The "goal identification" and "target identification" steps are usually not documented. News articles report on an attack after it has occurred and typically focuses on how the attack affected the specific target. There is also very little information on what steps were followed during the "information gathering" phase. The reader of the news article is to assume that the social engineer performed extensive information gathering on both the goal and the target, which in turn led to a successful social engineering attack. Depending on the type of attack, the "preparation" phase and the "develop relationship" phase normally have information that can be used directly in the social engineering attack framework. The "exploit relationship" phase is not always documented as the specific priming and elicitation techniques are not mentioned specifically. It is normally only mentioned whether the attack was successful or not. The "debrief" phase is usually also not covered in a report or news article as the "maintenance" step is a step the social engineer follows to reassure the victim that he/she is not the prey of a social engineering attack. The "transition" step is something only the social engineer has knowledge of, as the report or news article only reports on the final successful social engineering attack.

The proposed templates attempt to address the problem described above by detailing every phase and associated steps of the social engineering attack framework in such a way that each template will provide repeatable results. The templates

are also kept as simple as possible so that they can be expanded upon to create more elaborate scenarios with exactly the same principal structures. The templates were developed in such a way that other researchers can use them to perform repeatable experiments of social engineering attacks, with repeatable results, without having to physically perform the attack and potentially cause harm to innocent targets (Mouton et al., 2013, 2015).

The templates are fairly diverse in order to show and test different social engineering attack scenarios. They are grouped according to the communication type, namely bidirectional communication, unidirectional communication or indirect communication. The classification structure is based on the fact that each template has a specific communication method and that there is almost no overlap of attacks that use the same communication method.

All of the templates are derived from real-world social engineering attacks that have been documented in either news articles, technical reports, research reports, films or blogs. The news articles, technical reports, research reports or blogs do not always contain all of the information regarding the social engineering attack. This lack of information is addressed by discussing the template as a more generalised form of the social engineering attacks provided in the literature. The proposed template combines elements from all of the provided real-world examples into a single social engineering attack template. The templates are derived in this manner to ensure that each template contains all the elements of a social engineering attack whilst still being representative of a real-world scenario.

In the discussion of each template, the real-world social engineering attacks are first provided. Each real-world example is briefly explained in terms of what actions the social engineer (SE) takes in order to get the target to comply to the specified request, after which, the citation of where the attack can be found. Using the the aforementioned examples as a guideline, the reader is provided with a short description of a generalised template that contains elements from the real-world social engineering attacks. This generalised template is then mapped to the social engineering attack framework that provides more detailed information about every phase and step of the social engineering attack.

The rest of this section proposes four bidirectional communication templates, three unidirectional communication templates and three indirect communication templates.

3.1. *Bidirectional communication – template 1*

The detailed template of this attack is developed by using elements from the following examples in literature:

- The SE pretends to be someone who works on the management floor and convinces a cleaner of his supposed role. The cleaner grants the social engineer access to the building. This allows the SE to gain physical access to the computerised terminals on the management floor (Dimkov et al., 2010; Janczewski and Fu, 2010).
- The SE pretends to be part of the organisation, dresses in the appropriate attire, and then tailgates into the building behind other employees (Granger, 2001; Long, 2011). This is one of the more difficult attacks to prevent, because people generally feel compelled to hold open the door for other individuals (Brainard et al., 2006; Brody et al., 2012).
- The SE can use fake credentials or even just a good story to gain access to an organisation. This can be done by simply printing fake business cards, dressing the part or just carrying the correct security badge (Major, 2009).

This template illustrates a social engineering attack (SEA) where the attacker attempts to gain physical access to a computerised terminal at the premises of an organisation. The assumption is that when the attacker has once gained access to the computerised terminal, he/she is deemed to have been successful. The attacker is now able to install a backdoor onto the computerised terminal for future and further access from the outside.

The important features of the SEA are specified below:

Communication – The SEA is using bidirectional communication.
Social Engineer – The Social Engineer (SE) is an individual.
Target – The target is an organisation.
Medium – The communication medium is face-to-face.
Goal – The goal of the attack is to gain unauthorised access to a computerised terminal within the organisation.
Compliance Principles – The compliance principles that are used are authority, commitment and consistency.
Techniques – The technique that is used is pretexting.

The following text dissects and maps the template to the Social Engineering Attack Framework (SEAF).

3.1.1. *Step 1: attack formulation*

3.1.1.1. Goal identification. The goal of the attack is to gain unauthorised access to any computerised terminal within the organisation.

3.1.1.2. Target identification. The target of the attack is the organisation as a whole. This allows the attacker to target any individual within the organisation who has the capability of allowing the attacker access to the computerised terminal.

3.1.2. *Step 2: information gathering*

3.1.2.1. Identify potential sources. The information sources include the company website, any individuals who deal directly with the technical support organisation contracted by the target organisation, and information from the technical support organisation gained directly.

3.1.2.2. Gather information from sources. Gather information from all above mentioned sources that relate directly to how and when technical support is requested and performed.

3.1.2.3. Assess gathered information. Determine which technical support company used by the target organisation is most likely to have the authority to gain physical access to the computerised terminal. In addition, determine what time slots can be used to gain physical access to the computerised terminal and whether additional information is required, such as

whether the technical support organisation staff must wear corporate uniforms.

3.1.3. *Step 3: preparation*

3.1.3.1. Combination and analysis of gathered information. Determine the best single time slots in which the attacker can attempt to gain physical access to the computerised terminal. This decision will be based on likely time slots during which technical support may be required. The attacker must also ensure that he is aware of whether corporate uniform is used by the technical support organisation.

3.1.3.2. Development of an attack vector. Develop an attack plan that contains the exact time the attacker will visit the premises, the precise individual at the premises whom the attacker will ask to gain access to the computerised terminal, and conversation guidelines that should be followed during the attack. The attacker also has the option to perform another SEA in which he can make an appointment for the time slot during which he will attempt to gain unauthorised access to the computerised terminal.

3.1.4. *Step 4: develop relationship*

3.1.4.1. Establishment of communication. The physical action of engaging the individual within the organisation who can potentially provide the attacker unauthorised access to the computerised terminal.

3.1.4.2. Rapport building. The attacker is required to develop a friendly relationship with the targeted individual in order for that individual to gain trust in the attacker.

3.1.5. *Step 5: exploit relationship*

3.1.5.1. Priming the target. The attacker is required to discuss some concerns that he has with the targeted computerised terminal and to prime the targeted individual so that the latter is fully capable and willing to assist with resolving this concern.

3.1.5.2. Elicitation. The attacker offers to assist in addressing or resolving the concern that the targeted individual experienced with the computerised terminal.

3.1.6. *Step 6: debrief*

3.1.6.1. Maintenance. After the attacker has performed all tasks required on the computerised terminal, he approaches the targeted individual again and assures the latter that all concerns with regard to the computerised terminal have been addressed.

3.1.6.2. Transition. The attacker was able to successfully gain unauthorised access to the computerised terminal and can thus proceed to the "goal satisfaction" step.

3.1.6.3. Goal satisfaction. The SE has attained his initial goal of gaining unauthorised access.

3.2. *Bidirectional communication – template 2*

The detailed template of this attack is developed by using elements from the following examples in literature:

- The theory of group conformity is well entrenched in social psychology. The SE uses this theory to his/her advantage by starting a conversation in the group and providing false sensitive information to the group. If most of the other participants in the group are trained by the SE, they also start providing false sensitive information. This will cause any other individual who is part of the conversation to also feel the need to share sensitive information, as he/she will have the ultimate need to belong to the group (Dittes and Kelley, 1956; Gerard et al., 1968; Hill, 1971; Insko et al., 1985; Jetten et al., 2006; Lott and Lott, 1961; Simon, 1957).
- The SE abuses the fact that people feel the need to conform to the group. The SE attempts to convince the target that everyone else has been giving the SE the same information that is now requested from the target (Granger, 2001).

This template illustrates an SEA where the attacker attempts to obtain access to an individual's personal log-on credentials for a specific log-on location. In this case, an attempt is made to gain access to the individual's workstation. The attack will be performed by abusing the psychological principle that an individual has the desire to feel part of a group. Due to commitment and consistency, that individual will feel compelled to conform to what the rest of the group does. In this case, the group of individuals will all reveal their log-on credentials and because the target is the last person in the group to be approached, he/she will feel obliged to also reveal his/her own log-on credentials. The assumption is made that after the attacker has gained the log-on credentials, the SEA is deemed to be successful because these credentials can be used to access the individual's workstation.

The important features of the SEA are specified below:

Communication – The SEA is using bidirectional communication.
Social Engineer – The SE is a group of individuals.
Target – The target is an individual.
Medium – The communication medium is face-to-face.
Goal – The goal of the attack is unauthorised information disclosure from the target to the attacker.
Compliance Principles – The compliance principles that are used are commitment and consistency.
Techniques – The technique that is used is quid pro quo.

The following text dissects and maps the template to the SEAF.

3.2.1. *Step 1: attack formulation*

3.2.1.1. Goal identification. The goal of the attack is to get the target to disclose information, which the attacker is not authorised to have.

3.2.1.2. Target identification. The target of the attack is an individual whose workstation the SE needs to access.

3.2.2. *Step 2: information gathering*

3.2.2.1. *Identify potential sources*. The information sources include the places the target visits, any social gatherings the target attends and any interests that the target might have.

3.2.2.2. *Gather information from sources*. Gather information from all the above-mentioned sources that relate directly to the specific events the target attends, during which time intervals these events occur and what interests the target has.

3.2.2.3. *Assess gathered information*. Determine which of the events the SE is able attend and the length of interaction the SE can have with the target at each of these events. Also, determine how likely individuals will be to interact socially at each of these events and whether the SE will be able to have a conversation with the target at these events.

3.2.3. *Step 3: preparation*

3.2.3.1. *Combination and analysis of gathered information*. Determine which social events are most likely to present the attacker the possibility to perform an SEA. The events with the highest probability of social interaction and the longest duration with the target should be selected.

3.2.3.2. *Development of an attack vector*. Develop an attack plan that contains the chosen event the SE will attend and that states the time interval when the SE will interact with the target. In addition, develop conversational guidelines that will be used during the SEA.

3.2.4. *Step 4: develop relationship*

3.2.4.1. *Establishment of communication*. Take the physical action of engaging in conversation with the individual at the chosen event.

3.2.4.2. *Rapport building*. The SE, in this case a group of individuals, is required to engage in friendly conversation with the target and make him/her feel part of the group. The SE attempts to build a trust relationship with the targeted individual.

3.2.5. *Step 5: exploit relationship*

3.2.5.1. *Priming the target*. After the trust of the target has been gained, the group of individuals is required to steer the conversation onto the topic of password security and how people rarely use complex passwords.

3.2.5.2. *Elicitation*. One of the individuals in the group close to the target is required to start off by asking another individual in the group what their log-on credentials are to illustrate that most users use insecure passwords. After the individual has provided his log-on credentials, each of the other individuals should comply with the request and provide their log-on credentials as well. When all the other individuals in the group have provided their log-on credentials, the target must be requested to provide his log-on credentials. Because of his desire to be part of the group, the target is likely to feel obliged to supply his log-on credentials.

3.2.6. *Step 6: debrief*

3.2.6.1. *Maintenance*. After the target has provided his log-on credentials, the group should continue with friendly conversation and steer the topic onto some other topic that is of interest to the target. This will have a calming effect on the target and will put him at ease over the fact that he has just released information to which the SE should not have access.

3.2.6.2. *Transition*. The attacker was able to successfully persuade the target to disclose unauthorised information and thus the SE can proceed to the "goal satisfaction" step.

3.2.6.3. *Goal satisfaction*. The SE has attained his initial goal of unauthorised information disclosure.

3.3. *Bidirectional communication – template 3*

The detailed template of this attack is developed by using elements from the following examples in literature:

- The SE pretends to be a network administrator and requests the organisation to provide or reset a user's password on the organisation's system (Granger, 2001).
- The SE gathers information from a third party organisation that can then be used against another organisation (Bader et al., 2010; Tam et al., 2010).
- The SE pretends to be an authoritative figure who is requesting the target to perform a task. Since the target is reluctant to deny requests from such an authoritative figure, the target may feel compelled to comply with the request (Peltier, 2006).
- The SE pretends to be the organisation's bank, requesting information to address security concerns. The SE requests that the target navigates to a web address and enter confidential information (CERT Insider Threat Team, 2014; Greitzer et al., 2014).
- The SE convinces a domain registrar to change the default e-mail account associated with a financial institution. The SE also convinced the registrar to reset the default password (CERT Insider Threat Team, 2014).

This template illustrates an SEA where the attacker attempts to gain the password of a specific individual's e-mail account where the e-mail account is managed by an organisation. This attack is aimed at the organisation who is in control of the individual's e-mail account and not directly at the individual. Due to this, the individual is considered to be the primary target while the organisation that is targeted is considered a secondary target. The assumption is made that after the attacker has been able to successfully request a password reset for the individual's e-mail account from the organisation, the attacker will be able to gain access to the e-mail account. This is then deemed to be a successful SEA.

The important features of the SEA are specified below:

Communication – The SEA is using bidirectional communication.
Social Engineer – The SE is an individual.
Target – The primary target is an individual. This individual has an e-mail account at a specified organisation, and the latter is considered to be a secondary target.
Medium – The communication medium is a telephone.
Goal – The goal of the attack is to gain unauthorised access to the individual's e-mail account.
Compliance Principles – The compliance principles that are used are authority and scarcity.
Techniques – The technique that is used is pretexting.

The following text dissects and maps the template to the SEAF.

3.3.1. Step 1: attack formulation

3.3.1.1. Goal identification. The goal of the attack is to gain unauthorised access to the primary target's e-mail account by requesting a secondary target to have the password for the e-mail account reset.

3.3.1.2. Target identification. The primary target of the attack is an individual with an e-mail account at the specified organisation. The specified organisation has control over the target's e-mail account and thus an individual at the organisation (which is considered the secondary target) will be persuaded by social engineering to provide access to the primary target's e-mail account. This allows the attacker to target any individual within the organisation who has the capability of allowing the attacker to reset the password of the target's e-mail account.

3.3.2. Step 2: information gathering

3.3.2.1. Identify potential sources. The information sources include the organisation's website, organisational policies and any source that can provide personal information of the primary target.

3.3.2.2. Gather information from sources. Gather information from all the above-mentioned sources that relate directly to how and when password resets can be requested and what information is required to be provided during the password reset request. This is an example of where the "information gathering" phase as a whole will be cyclic, because the SE will analyse the information that is required to perform the password reset request and then during the "assess gathered information" step, it is required to move back to the "identify potential sources" step to determine from where the additional personal information can be gathered. To keep the attacks as generic and simplistic as possible, this cyclic process is omitted during the description that follows.

3.3.2.3. Assess gathered information. Determine what process is followed during the password reset request, what information is requested from the individual requesting a password reset, and assess the validity of all gathered personal information of the primary target.

3.3.3. Step 3: preparation

3.3.3.1. Combination and analysis of gathered information. Using all the assessed information, determine the best time slots during which a specific staff member of the organisation who has control over the password request process (the secondary target) can be contacted. In addition, it is required to develop a full profile of the primary target's personal information. This profile is used to ensure that the attacker will be able to answer any questions that the secondary target may direct at the attacker during the password reset request.

3.3.3.2. Development of an attack vector. Develop an attack plan that contains the exact time that the organisation will be phoned, a full script of the planned telephonic conversation and an organised list of the personal information of the primary target.

3.3.4. Step 4: develop relationship

3.3.4.1. Establishment of communication. The physical action of making the phone call to the organisation, up to the point where the secondary target can assist the attacker with the password reset request.

3.3.4.2. Rapport building. The attacker is required to develop a friendly relationship with the individual (secondary target) who can assist with the password reset request. The attacker's intention is to get the targeted individual to trust the attacker.

3.3.5. Step 5: exploit relationship

3.3.5.1. Priming the target. The attacker who is impersonating the primary target will explain to the individual (secondary target) that he/she (the attacker) urgently requires to regain access to "his/her" e-mail account. One example of a way in which a sense of urgency is created is telling the individual how important it is for the attacker to retrieve a specific document from the primary target's e-mail account and that this document is required immediately for some emergency.

3.3.5.2. Elicitation. The attacker (who is still impersonating the primary target) will request a password reset for the primary target's e-mail account and put forward as the reason for this request that the attacker is using an alternate workstation to access the e-mail account, therefore it does not have the logon credentials stored.

3.3.6. Step 6: debrief

3.3.6.1. Maintenance. After the attacker has successfully requested the password reset, the attacker will profusely thank the individual for the assistance and congratulate him/her on a job well done.

3.3.6.2. Transition. Since the attacker was able to successfully request a password reset for the primary target's e-mail account, he/she can thus proceed to the "goal satisfaction" step.

3.3.6.3. *Goal satisfaction*. The SE has attained his initial goal of gaining unauthorised access.

3.4. *Bidirectional communication – template 4*

The detailed template of this attack is developed by using elements from the following examples in literature:

- The SE pretends to be a customer who has in-depth knowledge of the services that an organisation offers. The SE is able to obtain sensitive information from the help-desk staff by bypassing any checks that require authorisation to be granted (Janczewski and Fu, 2010).
- The SE uses the corporate language of the organisation to gain the trust of the other employees (Thornburgh, 2004).
- The SE pretends to be a new employee and requests information from reception (Thornburgh, 2004).
- The SE pretends to be in distress, in a difficult situation or in a life-threatening emergency. The SE calls the targeted department in an organisation and convinces the target that in order to overcome the distress or emergency, his/her request needs to be fulfilled (Rao and Nayak, 2014).

This template illustrates an SEA where the attacker attempts to obtain sensitive information of an organisation to which only the employees of the organisation have access. The information is not available to members of the public. Once the attacker has been provided with the sensitive information, the SEA is deemed to have been successful.

The important features of the SEA are specified below:

Communication – The SEA is using bidirectional communication.
Social Engineer – The SE is an individual.
Target – The target is an organisation.
Medium – The communication medium is e-mail.
Goal – The goal of the attack is unauthorised information disclosure from the target to the attacker.
Compliance Principles – The compliance principles that are used are friendship and liking.
Techniques – The technique that is used is pretexting.

The following text dissects and maps the template to the SEAF.

3.4.1. *Step 1: attack formulation*

3.4.1.1. *Goal identification*. The goal of the attack is to get an employee of the organisation to disclose to the attacker information that the attacker is not authorised to have.

3.4.1.2. *Target identification*. The target of the attack is the organisation as a whole. This allows the attacker to target any individual within the organisation who has the sought-after capability of providing the attacker with the sensitive information.

3.4.2. *Step 2: information gathering*

3.4.2.1. *Identify potential sources*. The information sources include the organisation's website, any individuals in the organisation who have access to the information, and any organisational policies and procedures.

3.4.2.2. *Gather information from sources*. Gather information from all above-mentioned sources that relate directly to the access level of each employee and his/her status in the organisation.

3.4.2.3. *Assess gathered information*. Determine which of the employees have access to the sensitive information that the attacker is trying to obtain. Also, assess all the gathered information about each employee and perform information gathering on each of the employees individually. This cyclic process is excluded from the template and it is assumed that for the next phase all personal information about each employee has been gathered and assessed.

3.4.3. *Step 3: preparation*

3.4.3.1. *Combination and analysis of gathered information*. Determine the level of susceptibility of each employee, how much access to information each employee has and what type of personal information the attacker was able to gather and assess about him/her. Also, develop an information profile on each employee to determine which employee would be the best target from whom to request the sensitive information.

3.4.3.2. *Development of an attack vector*. Develop an attack vector that contains the chosen employee whom the attacker will be targeting, the full personal profile of this employee and what level of access this employee has. In addition, develop the planned e-mail communication with the employee to fit the specific personal profile of the employee.

3.4.4. *Step 4: develop relationship*

3.4.4.1. *Establishment of communication*. The very first e-mail communication that the attacker has with the targeted employee of the organisation. This e-mail establishes the basis for all future communication between the attacker and employee.

3.4.4.2. *Rapport building*. This step will be a continuous process of back and forth e-mail communication between the attacker and the employee. Several e-mails will be transferred in a bidirectional manner between the attacker and the employee in order to gain the trust of the employee. An example of trust building is where the attacker appears to be interested in the hobbies and interests of the targeted employee. The similarity between the attacker and the targeted employee's preferences is used to build trust.

3.4.5. *Step 5: exploit relationship*

3.4.5.1. *Priming the target*. The exploitation of the relationship will occur within a single e-mail communication to the targeted employee. In the priming and elicitation e-mail, the attacker will inform the employee of a scenario in which the attacker requires access to the sensitive information. An example of this could be that the attacker is requesting

sensitive information about the company policies because the attacker, as part of the pretext, will be attending an interview at the targeted employee's organisation.

3.4.5.2. *Elicitation*. The attacker will request the assistance of the targeted employee to retrieve the sensitive information and due to the friendship and liking and the trust relationship that have been established, the targeted employee will feel obliged to comply with the request.

3.4.6. *Step 6: debrief*

3.4.6.1. *Maintenance*. It is important that the attacker does not abruptly end the communication between himself and the targeted employee as this may cause suspicion and the organisation may be alerted to a breach of information. The attacker is required to continue the e-mail communication until such time as the request that was made is likely to have been forgotten by the targeted employee and the topic of communication has moved on away from the information request. The e-mail communication should thus continue until the sensitive information has been utilised by the attacker and is no longer of use.

3.4.6.2. *Transition*. The attacker was able to successfully gain unauthorised information disclosure from the targeted employee and can thus proceed to the "goal satisfaction" step.

3.4.6.3. *Goal satisfaction*. The SE has attained his initial goal of unauthorised information disclosure.

3.5. *Unidirectional communication – template 1*

The detailed template of this attack is developed by using elements from the following examples in literature:

- The SE deploys a fake website that sells tickets for a sporting event. The SE also sends out phishing e-mails to inform people that they can buy discounted tickets (Janczewski and Fu, 2010).
- The SE sends out phishing e-mails that falsely originate from the e-mail addresses of known contacts. Due to the targeted nature of the phishing attempts, the success ratio increases significantly (Jagatic et al., 2007).
- The SE sends out an e-mail that directs the target to navigate to a fraudulent website, which in turn collects credentials such as identity document numbers and bank account numbers from the target (Abraham and Chengalur-Smith, 2010).
- The SE sends out an e-mail about financial benefits that exploited a zero-day vulnerability, upon clicking a link, and downloaded malicious code. The malware masked itself on systems and was designed to erase itself if it tried to compromise a system and was unsuccessful (CERT Insider Threat Team, 2014; Greitzer et al., 2014).

This template illustrates an SEA where the attacker attempts to obtain financial gain by sending out e-mails that request a group of individuals to make a small deposit into a bank account owned by the attacker. The "419 scams", which are very popular social engineering attacks, are examples of this type of attack. Once the attacker has received the small deposit from the targeted individual, the SEA is deemed to have been successful.

The important features of the SEA are specified below:

Communication – The SEA is using unidirectional communication.
Social Engineer – The SE is an individual.
Target – The target is a group of individuals.
Medium – The communication medium is e-mail.
Goal – The goal of the attack is financial gain, as the targets are requested to make a deposit into a bank account owned by the attacker.
Compliance Principles – The compliance principle that is used is scarcity.
Techniques – The technique that is used is phishing.

The following text dissects and maps the template to the SEAF.

3.5.1. *Step 1: attack formulation*

3.5.1.1. *Goal identification*. The goal of the attack is to get an individual to deposit money into a bank account owned by the attacker and thus to provide financial gain to the attacker.

3.5.1.2. *Target identification*. The target of the attack is any individual of which the attacker has an e-mail address.

3.5.2. *Step 2: information gathering*

3.5.2.1. *Identify potential sources*. The information sources include any publicly available e-mail lists, websites selling e-mail lists and any other locations that are used to store e-mail addresses.

3.5.2.2. *Gather information from sources*. Gather from all the above-mentioned sources information that relates directly to the individuals' personal information and e-mail addresses.

3.5.2.3. *Assess gathered information*. Determine whether each e-mail list that has been gathered contains all information about each individual and whether each individual has an associated e-mail address.

3.5.3. *Step 3: preparation*

3.5.3.1. *Combination and analysis of gathered information*. Combine all the lists obtained into a single list that contains the personal details of each individual and his/her associated e-mail address. After the lists have been combined, prune all duplicates from the list to create a single list with only unique e-mail addresses.

3.5.3.2. *Development of an attack vector*. Develop an attack plan that details all the information that should be contained in each e-mail, what personal information to use in each e-mail and exactly how each section of the e-mail should be worded. It is also important to determine the duration of the attack,

because the attacker will have to close the bank account after a specified amount of time to ensure that individuals are not able to reverse any funds transferred.

3.5.4. *Step 4: develop relationship*

3.5.4.1. *Establishment of communication*. This involves the physical action of sending out an e-mail to each of the e-mail addresses on the list.

3.5.4.2. *Rapport building*. Rapport building in an e-mail usually occurs in the subject line and in the first few paragraphs of the e-mail. The reason behind this is that individuals scan only the subject line and the first few paragraphs of an e-mail, and trust should be built so that the target is enticed to read the entire e-mail.

3.5.5. *Step 5: exploit relationship*

3.5.5.1. *Priming the target*. In this attack, priming is done by using the scarcity principle. Priming usually occurs in the paragraphs following the "rapport building" step. In these paragraphs, the target is informed that he/she is a specially selected individual and that there is only a limited time frame within which to claim the reward offered to him/her in this e-mail.

3.5.5.2. *Elicitation*. In the next paragraph, the attacker requests the individual to make a smaller deposit than the reward offered, in order to be eligible to claim the full reward.

3.5.6. *Step 6: debrief*

3.5.6.1. *Maintenance*. The e-mail is ended off by thanking the target so as to make him/her feel at ease about making the payment and being selected for the specific reward.

3.5.6.2. *Transition*. If the attacker is successful in his/her request that the target makes a payment into the attacker's bank account, the attacker can proceed to the "goal satisfaction" step.

3.5.6.3. *Goal satisfaction*. The SE has attained his initial goal of financial gain.

3.6. *Unidirectional communication – template 2*

The detailed template of this attack is developed by using elements from the following examples in literature:

- The SE utilises a pop-up-window attack that is deployed on the user's workstation. When the user logs on to the specific service for which the SE requires the user's log-on credentials, a pop-up window can appear that requires the user to repeat his/her log-on credentials (Jahankhani, 2012).
- The SE also uses a pop-up-window attack while the user is logged into a system. The SE lets the workstation show a pop-up window that informs the user that the specific application has had a problem and that the user is required to re-authenticate. This re-authentication dialogue box then captures the user's log-on credentials and provides them to the SE (Laribee, 2006).
- The SE sends the target a message by using a mobile device. The message indicates that the user has to update the application that is used to access the system or the product to which the user has access. This can convince the user to visit the link and during the update process, the user is asked to provide his/her log-on credentials (Salem et al., 2010).
- The SE sent an innocent-looking e-mail to news service staffers urging them to click on a link to an important article on another news organisation's blog that, unknown to the victims, would infect their computers with malware. The malware allowed the SE to capture passwords to the news service's Twitter account (CERT Insider Threat Team, 2014).

This template illustrates an SEA where the attacker attempts to obtain log-on credentials from a group of individuals who are all using a certain system or product provided by an organisation. It is assumed that individuals are required to log-on to this system or product using log-on credentials unique to each individual. Individuals who are using the system are not allowed to share their log-on credentials and thus the goal of this attack is unauthorised information disclosure. The SE can have a further goal to obtain unauthorised access to the system or product, but that is seen as a separate goal. Once the attacker has obtained the log-on credentials from the individual, the SEA is deemed to be successful.

The important features of the SEA are specified below:

Communication – The SEA is using unidirectional communication.
Social Engineer – The SE is an individual.
Target – The target is a group of individuals.
Medium – The communication medium is a Short Message Service (SMS).
Goal – The goal of the attack is unauthorised information disclosure from the target to the attacker.
Compliance Principles – The compliance principles that are used are scarcity, commitment and consistency.
Techniques – The technique that is used is phishing.

The following text dissects and maps the template to the SEAF.

3.6.1. *Step 1: attack formulation*

3.6.1.1. *Goal identification*. The goal of the attack is to get an individual to provide to the attacker information that the attacker is not authorised to have.

3.6.1.2. *Target identification*. The target of the attack is all individuals in the group who are using the system provided by an organisation.

3.6.2. *Step 2: information gathering*

3.6.2.1. *Identify potential sources*. The information sources include any information about the system, the organisation's website and any lists that contain details of the users of the system.

3.6.2.2. Gather information from sources. Gather from all the above-mentioned sources information that relates directly to the individuals' personal information, cellphone numbers and any information regarding the product and the appearance of the log-on screen for the product.

3.6.2.3. Assess gathered information. Determine whether each identified user has an associated cellphone number and that the cellphone number is valid. Also, assess if enough information has been gathered to correctly duplicate the log-on screen for the specific system.

3.6.3. Step 3: preparation

3.6.3.1. Combination and analysis of gathered information. Develop a single list that contains the names of all users of the system and their associated cellphone numbers. In addition, develop a mock-up of how the log-on screen should look, so that this can be replicated to ensure that the screen is familiar to the targets during the attack.

3.6.3.2. Development of an attack vector. Develop an attack plan that details all the information that should be contained in each SMS, what personal information to use in each SMS and exactly how each section of the SMS should be worded. For this template, the attackers are required to develop a log-on screen that looks similar to the original screen and that is able to capture the log-on credentials when individuals attempt to log-on.

3.6.4. Step 4: develop relationship

3.6.4.1. Establishment of communication. This is done by the physical action of sending out all the SMSs to each of the cellphone numbers on the list.

3.6.4.2. Rapport building. Rapport building in an SMS usually occurs in the very first sentence of the SMS. The reasoning behind this is that SMSs are limited to 160 characters and thus you are required to keep the content brief. The first sentence of the SMS should build trust in the individual and entice him/her to read the rest of the SMS. In this template, the SMS would mention that it is an automated SMS from the organisation providing the system.

3.6.5. Step 5: exploit relationship

3.6.5.1. Priming the target. The second sentence of the SMS is used both to prime the target and to elicit action. The attacker will prime the target by using the scarcity principle, and by saying that a free update for the system will be available for a limited period only.

3.6.5.2. Elicitation. The sentence continues by providing a shortened hyperlink in the SMS on which the individual will be requested to click to obtain the free update to the system. The first screen that the individual would see after clicking on the link would be a log-on screen similar to what he/she is used to. Using the commitment and consistency principles, the user will trust the familiar-looking site and enter his/her log-on credentials.

3.6.6. Step 6: debrief

3.6.6.1. Maintenance. In this template, maintaining rapport is actually performed on the log-on screen and not in the SMS itself. After the user has logged on to the fraudulent system, a message appears thanking the individual for updating to the latest version and the individual is then redirected to the original system.

3.6.6.2. Transition. The attacker was able to successfully gain unauthorised information from the target and can thus proceed to the "goal satisfaction" step.

3.6.6.3. Goal satisfaction. The SE has attained his initial goal of unauthorised information disclosure.

3.7. Unidirectional communication – template 3

The detailed template of this attack is developed by using elements from the following examples in literature:

- The SE performs a pretext using postal letters. The SE pretends to be various officials, internal employees, employees of trading partners, customers, utility companies or financial institutions and the SE solicits confidential information by using a wide range of persuasive techniques (Workman, 2008).
- The SE has the capability of spoofing the sender ID on popular mobile messaging applications (Schrittwieser et al., 2012). This capability can further be used to perform an SEA and to send messages to other users whilst impersonating friends of these users (Krombholz et al., 2013).
- Typical SE attacks, specifically phishing, used to occur via postal mail. The term "419 scams" refers to section 419 of the Nigerian Criminal Code, which outlaws this type of scam. During the 1970s, postal mail was mostly used in these scams and during the 1980s, the medium of communication changed to faxes. Both are examples of forms used by the SE to initiate unidirectional communication (Dang, 2008).

This template illustrates an SEA in which the attacker attempts to obtain financial gain by sending out paper mail. This letter requests a group of individuals to make a small deposit into a bank account owned by the attacker. In this template, the attacker develops a phishing letter that masks the attacker as a charity organisation requesting donations. Once the attacker has received the small deposit from the targeted individual, the SEA is deemed to be successful.

The important features of the SEA are specified below:

Communication – The SEA is using unidirectional communication.
Social Engineer – The SE is an individual.
Target – The target is a group of individuals.
Medium – The communication medium is paper mail.
Goal – The goal of the attack is financial gain because the targets are requested to make a deposit into a bank account owned by the attacker.
Compliance Principles – The compliance principle that is used is scarcity.

Techniques – The technique that is used is phishing.

The following text dissects and maps the template to the SEAF.

3.7.1. *Step 1: attack formulation*

3.7.1.1. *Goal identification*. The goal of the attack is to get an individual to make a deposit into a bank account owned by the attacker and thus allowing the attacker to achieve financial gain.

3.7.1.2. *Target identification*. The target of the attack is any individual for whom the attacker has a postal address.

3.7.2. *Step 2: information gathering*

3.7.2.1. *Identify potential sources*. The information sources include any publicly available telephone records and address lists.

3.7.2.2. *Gather information from sources*. Gather from all the above-mentioned sources information that relates directly to the individuals' personal information and postal address.

3.7.2.3. *Assess gathered information*. Determine whether each address list that has been obtained contains all information about each individual and whether each individual has an associated postal address.

3.7.3. *Step 3: preparation*

3.7.3.1. *Combination and analysis of gathered information*. Combine all the lists obtained into a single list that contains the personal details of each individual and his/her associated postal address. After the lists have been combined, prune all duplicates from the list to create a single list with only unique postal addresses.

3.7.3.2. *Development of an attack vector*. Develop an attack plan that details all the information that should be contained in each letter, what personal information to use in each letter and exactly how each section of the letter should be worded. It is also important to determine the duration of the attack, as the attacker will have to close the bank account after a specified amount of time to ensure that individuals are not able to reverse any funds transferred.

3.7.4. *Step 4: develop relationship*

3.7.4.1. *Establishment of communication*. This is done by the physical action of sending out letters to each of the postal addresses on the list.

3.7.4.2. *Rapport building*. Building rapport in postal mail is very similar to building rapport in an e-mail and it should occur in the first few paragraphs of the letter. In this template, the first few paragraphs should introduce the charity requesting the donation and what the charity has done so far with previous donations received. This information is used to build trust in the individual and to ensure that the individual will support the charity and want to read the rest of the letter.

3.7.5. *Step 5: exploit relationship*

3.7.5.1. *Priming the target*. The individual is primed by providing him/her with a list of the current donations that have been received by the charity, what the charity needs to purchase and specifically why these donations are needed. The received donations section will assure the individual that there are other people donating and that it is socially acceptable to donate to the charity. The additional work the charity can perform and why the donations are requested are included to provoke an emotional response from the individual so that he/she can relate to the charity.

3.7.5.2. *Elicitation*. Using an empathetic tone of writing, the attacker requests the individual to make a small donation to the specified charity. It is very important to provide several options on how the individual can donate to the charity and the procedure to perform the donation should be as simple as possible.

3.7.6. *Step 6: debrief*

3.7.6.1. *Maintenance*. The letter is finalised by thanking the individual for his potential generosity and to assure the individual that any donation that is made will be spent wisely.

3.7.6.2. *Transition*. If the attacker succeeds in persuading the target to make a payment into the attacker's bank account, the attacker can proceed to the "goal satisfaction" step.

3.7.6.3. *Goal satisfaction*. The SE is satisfied as he/she attained the initial goal of financial gain.

3.8. *Indirect communication – template 1*

The detailed template of this attack is developed by using elements from the following examples in literature:

- The SE scatters USB drives in the parking lot, smoking areas and other areas that employees frequent. The employees plug in the USB drives the minute they get to their workstations (Stasiukonis, 2006).
- The SE attempts to gain unauthorised access to a workstation in an organisation by using a storage medium device (Esmail, 2015; Jodeit and Johns, 2010). This attack is also depicted in a popular television series about penetration testing, Mr. Robot (Esmail, 2015).
- Spreading malware through means of storage media or storage devices is nothing new; this practice can be traced back to the use of floppy drives (Abraham and Chengalur-Smith, 2010).

This template illustrates an SEA in which the attacker attempts to gain unauthorised access to a workstation within an organisation by using a storage device. Once the target has plugged the storage device (in this case a USB flash drive) into the targeted workstation, the SEA is deemed to be successful.

This is because the attacker is now able to install a backdoor onto the workstation via the storage device. The SE can then proceed to use this workstation as a pivot point for any further attacks on the organisation. This type of an attack is viable due to an unintentional insider threat (CERT Insider Threat Team, 2013; Greitzer et al., 2014).

The important features of the SEA are specified below:

Communication – The SEA is using indirect communication.
Social Engineer – The SE is an individual.
Target – The target is an organisation.
Medium – The communication medium is a storage device. In this case, the storage device to be used is a USB flash drive.
Goal – The goal of the attack is to gain unauthorised access to a workstation within the organisation.
Compliance Principles – The compliance principle that is used is social validation.
Techniques – The technique that is used is baiting.

The following text dissects and maps the template to the SEAF.

3.8.1. *Step 1: attack formulation*

3.8.1.1. Goal identification. The goal of the attack is to gain unauthorised access to any workstation within the organisation.

3.8.1.2. Target identification. The target of the attack is the organisation as a whole. This allows the attacker to target any individual within the organisation who has a workstation or who has access to a workstation.

3.8.2. *Step 2: information gathering*

3.8.2.1. Identify potential sources. The information sources include physical scouting of the premises, monitoring of the movement of employees, and any schedules or appointments posted on the organisation's website.

3.8.2.2. Gather information from sources. Gather from all the above-mentioned sources information that relates directly to how and when employees are entering and leaving the office building and specifically which entrances are being used.

3.8.2.3. Assess gathered information. Determine which of the entrances are the most viable target, based on the time intervals when individuals enter and exit the organisation at these entrances. Also, determine the possible ways the attacker can approach these entrances without looking suspicious or showing suspicious behaviour.

3.8.3. *Step 3: preparation*

3.8.3.1. Combination and analysis of gathered information. Determine the best time slots during which the attacker can attempt to deploy the storage medium at the entrance without having to perform any suspicious behaviour. It is important to choose a time slot when most individuals are entering the building, because it is always possible that an individual exiting the building may also pick up the storage medium.

3.8.3.2. Development of an attack vector. Develop an attack plan that contains the exact time that the attacker will visit the premises, which entrance the storage medium will be deployed at, how the storage medium will be marked to prompt the individual to return it to its owner and what data will be deployed onto the storage medium. The storage medium should contain a Trojan (malware) that will attempt to connect to the attacker's network infrastructure.

3.8.4. *Step 4: develop relationship*

3.8.4.1. Establishment of communication. Communication is established via the physical action of deploying the storage medium at an entrance and it lasts up to the time when an individual picks up the storage medium.

3.8.4.2. Rapport building. In this case, rapport is developed by ensuring that the storage medium looks similar to those that are typically used by the organisation and that are branded with the organisation's logo.

3.8.5. *Step 5: exploit relationship*

3.8.5.1. Priming the target. Attach a label to the storage medium that states that the information on the storage medium is very valuable and that, if lost, it should be returned to the owner. The label or sticker to convey this message is normally only a sticker saying "Important" or "Confidential". The target is required to plug the storage medium into a workstation in order to determine the owner.

3.8.5.2. Elicitation. The "elicitation" step is almost implicit in this template. Most people will attempt to return lost valuables or they could just be curious to find out what information is stored on the storage medium. Both of these situations will lead to a successful "elicitation" step.

3.8.6. *Step 6: debrief*

3.8.6.1. Maintenance. Once the storage medium has been connected to a workstation, the Trojan will automatically execute in a hidden fashion. In order to avoid suspicion, it is good practice by the attacker to include either contact details to return the storage medium or an encrypted document to indicate the importance of the information.

3.8.6.2. Transition. Once the attacker was able to successfully gain unauthorised access to the workstation of the individual, he/she can proceed to the "goal satisfaction" step.

3.8.6.3. Goal satisfaction. The SE has attained his/her initial goal of gaining unauthorised access.

3.9. *Indirect communication – template 2*

The detailed template of this attack is developed by using elements from the following examples in literature:

- The SE studies the available attributes on public profiles within specific social networks and determines how they

may be exploited. Context-aware e-mail spam is then generated and sent to users of the network (Brown et al., 2008). This same attack can be repeated by posting the context-aware spam within the social networks of the users.
- Users of social networking websites exhibit a high degree of trust in both friend requests and messages from other users. This research also covers reverse social engineering attacks where the victim initiates the conversation with the attacker (Irani et al., 2011).
- The SE creates a fake profile that propagates click-bait posts that all use shortened forms of the Uniform Resource Locator (URL). This lets unsuspecting victims click on the links, which can lead them to websites containing malware (Ivaturi and Janczewski, 2011).
- The SE crafted malware that was placed on a popular website for software developers. The malware was advertised as a Java plug-in that could be installed on desktops (CERT Insider Threat Team, 2014).

This template illustrates an SEA where the attacker attempts to obtain log-on credentials from a group of individuals who are all using a certain social media website. It is assumed that individuals are required to log-on to this website using log-on credentials unique to each individual. Individuals who use the particular social media website are not allowed to share their log-on credentials and thus the goal of this attack is unauthorised information disclosure. The SE may have a further goal, namely to obtain unauthorised access to the individual's social media account, but that is seen as a separate goal. Once the attacker has obtained the log-on credentials from the individual, the SEA is deemed to be successful.

The important features of the SEA are specified below:

Communication – The SEA is using indirect communication.
Social Engineer – The SE is an individual.
Target – The target is a group of individuals.
Medium – The communication medium is via a website. In this specific case, it is a social media website.
Goal – The goal of the attack is unauthorised information disclosure from the target to the attacker.
Compliance Principles – The compliance principles that are used are social validation and friendship and liking.
Techniques – The technique that is used is baiting.

The following text dissects and maps the template to the SEAF.

3.9.1. *Step 1: attack formulation*

3.9.1.1. Goal identification. The goal of the attack is to get an individual to provide to the attacker information that the attacker is not authorised to have.

3.9.1.2. Target identification. The target of the attack is all individuals in the group who are using the specific social media website.

3.9.2. *Step 2: information gathering*

3.9.2.1. Identify potential sources. The information sources include any information about the social media website, the users of the social media website and the policies of the social media website.

3.9.2.2. Gather information from sources. Gather from all the above-mentioned sources information that relates directly to the individuals' personal information and any information regarding the log-on page of the social media website.

3.9.2.3. Assess gathered information. Determine whether all the required information to determine the likes and dislikes of each individual have been gathered. Also, assess if enough information has been gathered to correctly duplicate the log-on screen for the social media website.

3.9.3. *Step 3: preparation*

3.9.3.1. Combination and analysis of gathered information. Develop a combined personality profile based on all the information gathered from the individuals and determine what type of social media posts will be of interest to these individuals. Also, develop a mock-up of how the log-on screen should look, so that the replicated log-on screen looks familiar to the individuals when they are required to enter their log-on credentials during the attack.

3.9.3.2. Development of an attack vector. Develop an attack plan that details the formulation of a post on which most of the individuals will click, based on their personality profile. In this template, the attacker is also required to develop a log-on screen that is similar to the original, and that is able to capture the log-on credentials when individuals attempt to log-on. Once an individual has fallen prey to the attack, each target that has been compromised by the malicious post will be forced – unbeknown to the target – to automatically replicate the attacker's social media post to that of the target's friends.

3.9.4. *Step 4: develop relationship*

3.9.4.1. Establishment of communication. This involves the physical action of posting the first social media post on the social media website.

3.9.4.2. Rapport building. Posts on social media websites are usually very short and often consist of one or two sentences only. The "rapport building" step is mostly performed as a continuous process because individuals trust people with whom they have been friends on social media for a long period. In this template, the first post by the attacker should be enticing enough for any of the targets to click on it without having gained a lot of trust in the attacker. Once a single individual has fallen prey to the attack, he/she will automatically, due to the malicious post, propagate the post to his/her social media friends, seeing that a trust relationship already exists between friends.

3.9.5. *Step 5: exploit relationship*

3.9.5.1. Priming the target. On social media websites, the target is almost already primed to be reading and clicking on posts. Individuals usually tend to read social media to find interesting

activities that their friends are participating in or have posted. In the post that the attacker provides, the image that accompanies the post and the short content description represent both the "priming the target" and the "elicitation" steps.

3.9.5.2. Elicitation. The post that is made available by the attacker contains both an image and a short description based on the personality profile of the group of individuals who are being targeted. These individuals should be interested in the subject matter that is posted and thus they would hardly hesitate to click on the post and read more about it. Once the individual has clicked on the post to read it, it will ask the individual for his/her log-on credentials for the particular social media website as if he/she has been logged out. The individual is then prompted to log back in to the social media website, after which the post is propagated to all of the target's social media friends.

3.9.6. Step 6: debrief

3.9.6.1. Maintenance. In this template, the maintenance of rapport actually occurs on the log-on screen and not in the post made on social media. After the targeted individual has logged on to the fraudulent log-on screen, the information that was discussed in the fraudulent post should be provided, after which the individual is navigated back to the real social media website. This allows the targeted individual to think that he/she gained access to the post that he/she wanted to read and the target remains unaware that all his/her social media friends have also been posted the fraudulent post.

3.9.6.2. Transition. The attacker was able to successfully gain unauthorised information from the target and can thus proceed to the "goal satisfaction" step.

3.9.6.3. Goal satisfaction. The SE has attained his/her initial goal of unauthorised information disclosure.

3.10. *Indirect communication – template 3*

The detailed template of this attack is developed by using elements from the following examples in literature:

- The SE creates fake traffic violation notices and places them onto cars at a parking lot. The owner of the car returns to his/her car, finds the notice and later navigates to the URL provided on the traffic violation notice. In this way the owner of the car is tricked to visit a malicious website. This template is directly derived from the example quoted by Zeltser (2009).
- The SE prints posters that contain a QR code. The poster is then placed close to a popular restaurant and mentions that scanning this QR code with your phone provides you access to a voucher for the restaurant. Upon scanning the code, the QR code directs the target to a malicious website or requests a signup to harvest usernames and passwords (Kieseberg et al., 2010).
- The SE creates a URL that points to malicious malware on a cloud-based system (Gruschka and Jensen, 2010). This URL is printed on a pamphlet and provided to job seekers who seek employment. The pamphlet advertises a job opportunity and provides a URL to a website where additional information can be found, or where the job seeker must apply.

This template illustrates an SEA in which the attacker attempts to gain unauthorised access to any individual's computer. In the current template, fliers appearing to be fines for traffic violations are placed on different individuals' cars in a parking lot. On these notices of supposed parking violations a website URL is provided where one could view pictures associated with the so-called violation. When the individual visits the website, a backdoor Trojan is installed onto the individual's workstation. Once the individual has accessed the malicious website, the attacker successfully installs the backdoor Trojan and that SEA is deemed to be successful.

This template is now demonstrated through the use of the SEAF.

The important features of the SEA are specified below:

Communication – The SEA is using indirect communication through third-party media.
Social Engineer – The SE 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 communication medium is a flier.
Goal – The goal of the attack is to gain unauthorised access to an individual's computer.
Compliance Principles – The compliance principles that are used are social compliance and authority.
Techniques – The technique that is used is phishing.

The following text dissects and maps the template to the SEAF.

3.10.1. Step 1: attack formulation

3.10.1.1. Goal identification. The goal of the attack is to gain unauthorised access to an unspecified individual's computer.

3.10.1.2. Target identification. The target of the attack is any person who owns a car and is parked in the parking lot at the time when the fliers are spread.

3.10.2. Step 2: information gathering

3.10.2.1. Identify potential sources. Public websites that provide the feature to view parking violation details and any institute with the authority to issue a parking violation.

3.10.2.2. Gather information from sources. Collect sample parking violation notices that are placed on windshields of cars and on sample websites where one can view parking violation information.

3.10.2.3. Assess gathered information. Determine which parking violations are relevant to the specific parking lot, perhaps on location, region, etc. In this case, the violation should specifically conform to the standard parking violations that occur in the target region. Also filter out the website that is consistent with the parking violation.

3.10.3. *Step 3: preparation*

3.10.3.1. *Combination and analysis of gathered information*. Choose one parking violation and website pair and finalise the structure of the parking violation notice, the style and working of the website.

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

3.10.4. *Step 4: develop relationship*

3.10.4.1. *Establishment of communication*. This is done via the physical action of placing the created fliers on the cars in the parking lot.

3.10.4.2. *Rapport building*. The parking violation notices placed on the windshields of the cars should be consistent with parking violation notices handed out in that parking lot under standard conditions. The owner of the car receiving the violation notice should not doubt whether it is official; it should look legitimate. When the target visits the website, the website should also appear to be legitimate and may not raise doubt with the user.

3.10.5. *Step 5: exploit relationship*

3.10.5.1. *Priming the target*. The flier should be realistic so that the owner of the car will take it seriously and not simply 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 resolve the violation.

3.10.5.2. *Elicitation*. The attacker provides a URL on the flier of the phishing website to allow the target to take action. Upon typing in the URL, a backdoor is installed on the target's computer, giving the SE the opportunity to gain unauthorised access to his/her computer.

3.10.6. *Step 6: debrief*

3.10.6.1. *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/she is performing the correct procedure to resolve the violation.

3.10.6.2. *Transition*. The SE can use the backdoor to gain unauthorised access to the computer and can thus proceed to the "goal satisfaction" step.

3.10.6.3. *Goal satisfaction*. The SE has attained his initial goal of gaining unauthorised access.

The next section briefly discusses the need for these social engineering attack templates, after which, the usability of the templates are shown by using them to verify a social engineering attack detection model.

4. Application of the social engineering attack templates

The social engineering attack templates have been proposed with the goal in mind to provide researchers with a set of social engineering attack templates that can be used to verify or compare other models, processes and frameworks within social engineering. Each template contained the full description of every phase and associated steps of the social engineering attack framework in such a way that each template will provide repeatable results when used to verify or compare other models, processes and frameworks. The templates are also kept as simple as possible so that they can be expanded upon to create more elaborate scenarios with exactly the same principal structures. The templates can also be used to verify or compare other models, processes and frameworks without having to physically perform the attack and potentially cause harm to innocent targets (Mouton et al., 2015).

In previous research, the authors proposed a social engineering attack detection model (SEADM), which was designed to allow users of the model to be more vigilant against social engineering attacks (Mouton et al., 2015). The model is depicted in Fig. 3. This model makes use of a decision tree and breaks down the process into more manageable components to aid decision making. The model is discussed in more detail in an article entitled "Social Engineering Attack Detection Model: SEADMv2" and only a brief summary is provided here to assist the reader with how the social engineering attack templates are mapped to the social engineering attack detection model.

The model depicts the flow of action and how any type of request should be handled by a "receiver". Throughout this discussion this term is understood as the person dealing with the request, while the term "requester" is defined as the person or object who requests the specific action or information from the receiver. The model should be used as a guideline to aid in decision making and it is an improvement on the initial SEADM due to its ability to cater for both typical requests and inherent requests. This generalisation allows the revised SEADM to cater for the both the unidirectional communication and indirect communication categories of social engineering.

An example of a typical request is where the requester, in this case a person, requests the receiver to perform a task/favour for him/her. This request can range from the requester requesting information about an organisation to the requester requesting that the receiver performs a password reset for an individual's Internet banking logon.

An example of an inherent request is where the receiver receives a request, in this case an object that contains either a request or a process that needs to be completed by the receiver. This type of request can range from a parking ticket detailing how to pay the ticket on the pamphlet to a receiver finding a storage medium device and wanting to return the device to its rightful owner. In the case of the parking ticket, the receiver is inherently requested to pay the ticket using the

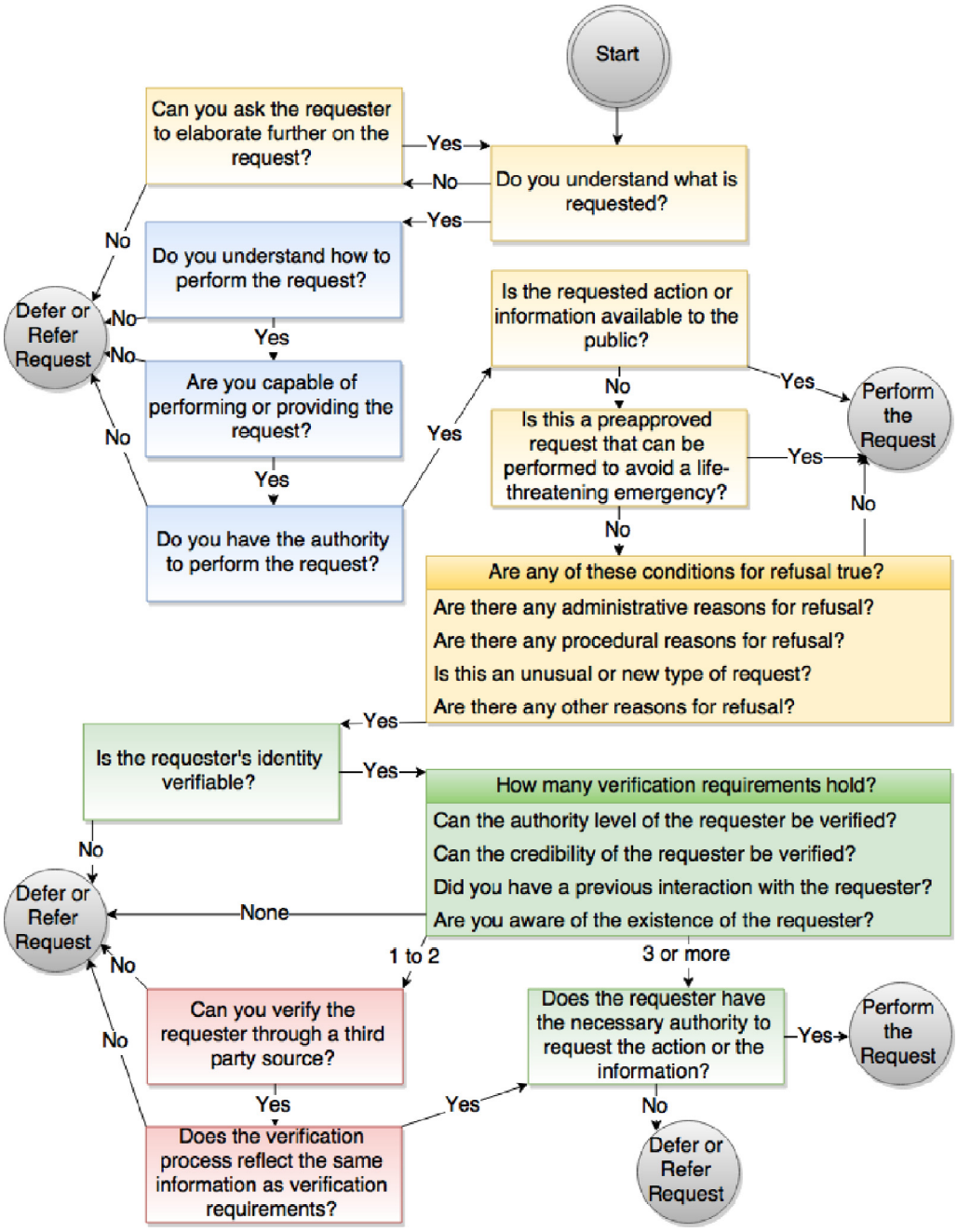

Fig. 3 – Social engineering attack detection model (Mouton et al., 2015).

information on the pamphlet. In the case of the storage device the situation is a little bit more complicated. The receiver, upon finding the device, is inherently requested to return it to its rightful owner.

The model provides for four different types of states – the request, receiver, requester and third party – that provide a brief idea of what can be expected to be performed in each state. The request states, indicated in yellow, directly deals with information about the request itself. The receiver states, indicated in blue, directly deals with the person handling the request and whether this person (the receiver) understands and is allowed to perform the request. The requester states, indicated in green, directly deals with the requester and whether any information about the requester can be verified. The third party states, indicated in red, directly depict the involvement of a third party in the model and whether the information about the requester can be externally verified.

The social engineering attack templates, as proposed in this paper, are used to verify this model and to show the need for these proposed social engineering attack templates. Social engineering is divided into three distinct categories based on the type of communication utilised (see Section 2). The three categories are respectively bidirectional communication, unidirectional communication and indirect communication. A template from each of these categories is used to verify that the model can be used to detect social engineering attacks.

In the first scenario, from the bidirectional communication templates (template in Section 3.1), the social engineer pretends to be someone who works on the management floor and has to convince a cleaner that he is indeed an employee. He requests the cleaner to give him access to the management floor. In the second scenario, from the unidirectional communication templates (template in Section 3.7), the social engineer attempts to obtain financial gain by sending out paper mail in which the letter requests a group of individuals to make a small deposit into a bank account owned by the attacker. In the third scenario, from the indirect communication templates (template in Section 3.8), the social engineer attempts to gain unauthorised access to a workstation in an organisation by using a storage medium device.

In each scenario the reader is provided with a generic description of the attack as taken from social engineering attack templates. This generic description is then populated with elements, both subjects and objects, from real-world examples of social engineering attacks, as provided in the discussion of the specific social engineering attack template. Using the generic description, the elements from the real-world examples and the fully detailed flow of the attack as provided in each phase and step of the social engineering attack framework, one is able to devise a social engineering attack scenario. This scenario is then reflective of a real-world example of which every phase and step is fully documented as per the social engineering attack framework. Using the proposed social engineering attack templates, one is able to formulate a social engineering attack scenario that always follows the same process, with regards to phases and steps, whilst the social engineering attack is still representative of a real-world scenario.

The remainder of this section is dedicated to mapping the social engineering attack templates to the social engineering attack detection model and verifying whether the social engineering attack detection model can assist in detecting social engineering attacks.

4.1. *Bidirectional communication scenario*

The generic description for this scenario (template in Section 3.1) reads as follows: "This template illustrates a SEA where the attacker attempts to gain physical access to a computerised terminal at the premises of an organisation. The assumption is that when the attacker has once gained access to the computerised terminal, he/she is deemed to have been successful. The attacker is now able to install a backdoor onto the computerised terminal for future and further access from the outside." This scenario is populated with elements from the real-world example where the social engineer pretends to be someone who works on the management floor and convinces a cleaner of his supposed role. The cleaner grants the social engineer access to the building. This allows the social engineer to gain physical access to the computerised terminals on the management floor (Dimkov et al., 2010; Janczewski and Fu, 2010).

In this scenario a social engineer has to convince the cleaner, the receiver, to believe that he is indeed a staff member. In this scenario, the cleaners have full access to the building, yet, their security awareness is very low. They are not trained to respond to unusual requests such as giving other employees access to the management floor. If the request is successful, access has been gained to the management floor, and a key logger is deployed onto a workstation. This attack is performed using bidirectional communication because the social engineer communicates with the cleaner and convinces him that the social engineer is allowed to have access to the management floor and the workstations.

4.1.1. *Do you understand what is requested?*

The request from the social engineer should clearly state that access needs to be gained to the management floor. The social engineer can also justify to the receiver why access is required to further allow the receiver to understand the request. When the receiver understands the request, the "yes" option is selected.

4.1.2. *Do you understand how to perform the request?*

The social engineer would have made certain that the targeted employee fully understands the request, is capable of performing the request and has the authority to perform the request. This will allow the current step, and the following two steps to take the "yes" option.

4.1.3. *Are you capable of performing or providing the request?*

As indicated earlier, the "yes" option is chosen.

4.1.4. *Do you have the authority to perform the request?*

In this scenario, the receiver does not specifically have the authority to grant access to the management floor; however, the receiver has the authority to deny access. Typically, at this question the "no" option should be followed; however, in the scenario it is mentioned that the receiver was not trained to be able to handle unusual requests so the receiver assumes that he or she has access to grant the request. Due to the assumption, the "yes" option is taken.

4.1.5. *Is the requested action or information available to the public?*

In the scenario only management and cleaners should have access to the management floor and thus the "no" option is chosen.

4.1.6. *Is this a preapproved request that can be performed to avoid a life-threatening emergency?*

This is not a life-threatening request and thus the "no" option is selected.

4.1.7. *Are any of these conditions for refusal true?*

Seeing that the requested access is an unusual request, as discussed in the description, the "yes" option is selected.

4.1.8. *Is the requester's identity verifiable?*

In this case, bidirectional communication is utilised; thus it allows for the receiver to communicate back via face to face communication and ask more questions to verify the requester. Hence the "yes" option is taken.

4.1.9. *How many verification requirements hold?*
In this case, the authority principle is utilised and the social engineer mimics an authoritative figure whom should have access to the management floor. The pretext utilised during this attack is that the social engineer is part of management and that he or she should have access to the management floor. The receiver is only able to verify the authority level, even if it is false information, from the social engineer in this scenario. Since only a single verification requirement is met, the "one to two" option is selected.

4.1.10. *Can you verify the requester through a third party source?*
The receiver will now have the ability to verify the information from another employee on the management floor. In the case that there are no other employees on the management floor, the "no" option will be taken and the social engineering attack will be thwarted. It is assumed that there are other people on the management floor who can be contacted to verify the information and thus the "yes" option is taken.

4.1.11. *Does the verification process reflect the same information as the verification requirements?*
It is at this step that the receiver will be able to ask the other employee whether the authority level of the social engineer is indeed true. The other employee will deny this and thus the verification process will show that the information provided is not the same as the verification requirements. Consequently, the "no" option will be taken and the social engineering attack will be thwarted.

4.2. *Unidirectional communication scenario*

The generic description for this scenario (template in Section 3.7) reads as follows: "This template illustrates an SEA in which the attacker attempts to obtain financial gain by sending out paper mail. This letter requests a group of individuals to make a small deposit into a bank account owned by the attacker. In this template, the attacker develops a phishing letter that masks the attacker as a charity organisation requesting donations. Once the attacker has received the small deposit from the targeted individual, the SEA is deemed to be successful." This scenario is populated with elements from the real-world example where the social engineer performs a pretext using postal letters. The social engineer pretends to be various officials, internal employees, employees of trading partners, customers, utility companies or financial institutions and the social engineer solicits confidential information by using a wide range of persuasive techniques (Workman, 2008).

In this scenario, a social engineer attempts to obtain financial gain by sending out paper mail. In the letter, a group of individuals are requested to make a small deposit into a bank account owned by the attacker. In this scenario, the attacker will develop a phishing letter that masks the attacker as a charity organisation requesting donations. The phishing letter contains the contact details, the logo and the purpose of the charity to improve the authenticity of the letter. This attack uses unidirectional communication and thus the receiver is not able to communicate with the attacker. The rest of this section maps the scenario to the model.

4.2.1. *Do you understand what is requested?*
The letter from the social engineer should clearly state that a receiver is requested to make a donation to the specific charity. The letter will include all the required details because this receiver cannot communicate with the social engineer. The "yes" option is taken.

4.2.2. *Do you understand how to perform the request?*
The social engineer would have ensured that the targeted individual fully understands the request, is capable of performing the request and has the authority to perform the request. This will cause the receiver to select the "yes" option in this step, as well as in the following two steps.

4.2.3. *Are you capable of performing or providing the request?*
As indicated before, the "yes" option is taken.

4.2.4. *Do you have the authority to perform the request?*
As was the case earlier, the "yes" option is chosen.

4.2.5. *Is the requested action or information available to the public?*
The requested action is to make a deposit into the bank account of the requester. This request is directed at the receiver and not at the public. The action of the specific receiver making a deposit is only available to the specific receiver, thus the "no" option is taken.

4.2.6. *Is this a preapproved request that can be performed to avoid a life-threatening emergency?*
This is not a life-threatening request and thus the "no" option is selected.

4.2.7. *Are any of these conditions for refusal true?*
This request can be seen as either unusual or new as the requester would not usually receive this specific type of letter from the charity. It can also be the case that the requester feels uneasy about the request and his or her uneasiness about the request can be seen as a reason to refuse at this point. The "yes" option is selected because there is sufficient reason to refuse the request without even verifying the identity of the requester.

4.2.8. *Is the requester's identity verifiable?*
Since unidirectional communication is utilised in this case, the receiver can only verify the identity using the information as provided in the letter. At this point one can defer or refer the request if it does not contain additional information such as the requester's contact details. In the current scenario, the letter actually contains the contact details of the charity organisation and thus the "yes" option is chosen.

4.2.9. *How many verification requirements hold?*
The requirement that the receiver should be aware of the existence of the requester will definitely hold, because the social engineer would have chosen a well-known charity. One can also argue that receiver may have had a previous interaction with the charity; however, from the letter alone, the authority and

credibility of the requester cannot be verified. In this case the "one to two" option is selected.

4.2.10. *Can you verify the requester through a third party source?*
The receiver will now have the ability to verify the information in the letter directly from the charity organisation. The receiver will make a phone call to the charity to verify the information. It is assumed that the charity organisation can be reached to verify the information and thus the "yes" option is taken.

4.2.11. *Does the verification process reflect the same information as the verification requirements?*
It is at this step that the receiver will be able to ask the organisation whether such a letter has in fact been sent out. The charity organisation will deny this and thus the verification process will show that the information provided is not the same as the verification requirements. Consequently, the "no" option will be taken and the social engineering attack will be thwarted.

4.3. *Indirect communication scenario*

The generic description for this scenario (template in Section 3.8) reads as follows: "This template illustrates an SEA in which the attacker attempts to gain unauthorised access to a workstation within an organisation by using a storage device. Once the target has plugged the storage device (in this case a USB flash drive) into the targeted workstation, the SEA is deemed to be successful. This is because the attacker is now able to install a backdoor onto the workstation via the storage device. The SE can then proceed to use this workstation as a pivot point for any further attacks on the organisation." This scenario is populated with elements from the real-world example where the social engineer attempts to gain unauthorised access to a workstation in an organisation by using a storage medium device (Esmail, 2015; Jodeit and Johns, 2010). This attack is also depicted in a popular television series about penetration testing, Mr. Robot (Esmail, 2015).

In this scenario the social engineer attempts to gain unauthorised access to a workstation in an organisation by using a storage medium device. The organisation does not have a company policy in place that disallows employees plugging storage devices into their workstations. The social engineer will leave the device outside the organisation's building to be found by an employee. The device will be infected with a trojan so that when it is plugged into the workstation, it opens a backdoor for the social engineer to connect to the system remotely. As the storage device is left unattended, this attack utilises indirect communication. The rest of this section maps this scenario to the model.

4.3.1. *Do you understand what is requested?*
The storage medium device planted by the social engineer should be marked clearly to indicate that it contains important and confidential information. Thus, the receiver who finds this device will want to return it to its rightful owner. As it is an inherent request that the receiver should return the device, the request is easily understandable and the "yes" option is selected.

4.3.2. *Do you understand how to perform the request?*
The social engineer would have made certain that the storage medium device is deployed at such a location that only individuals who have access to a workstation and who understand how such devices work should find the device. This will cause the receiver to take the "yes" option in this step as well as in the following step.

4.3.3. *Are you capable of performing or providing the request?*
As was the case previously, the "yes" option is selected.

4.3.4. *Do you have the authority to perform the request?*
In this step, the receiver should ask him- or herself whether he or she has the authority to plug the storage device into a workstation at the organisation. If there is a company policy that disallows or forbids this, then the "no" option will be selected and the attack be thwarted. However, for the present scenario there are no company policies in place and thus the receiver has the necessary authority. Consequently, the "yes" option is taken.

4.3.5. *Is the requested action or information available to the public?*
The inherent requested action is to return the storage device to its rightful owner. This request is directed at the receiver who found the device. Because only the receiver can perform this action, the "no" option is taken.

4.3.6. *Is this a preapproved request that can be performed to avoid a life-threatening emergency?*
The scenario does not involve a life-threatening request and thus the "no" option is chosen.

4.3.7. *Are any of these conditions for refusal true?*
In this scenario, the storage device has been marked as confidential and important. Hence, the receiver will not be allowed to plug the device into a workstation. This will be considered as a reason for refusal and cause the "yes" option to be taken. Administrative and procedural reasons are ruled out for this scenario because there are no company policies that govern storage devices.

4.3.8. *Is the requester's identity verifiable?*
Since indirect communication is utilised in this case, the only piece of information the receiver has is the physical storage medium device. Due to the confidentiality of the device, the receiver is unable to verify the requester's identity, therefore the request is deferred or referred and the attack is thwarted. In the present scenario, the request will most likely be referred to another individual in the organisation who is allowed to safely, and on a secure workstation, verify the contents of the storage device and potentially contact the rightful owner.

5. Conclusion

The protection of information is extremely important in a modern society and even though the level of security around

information is continuously improved, the one weak point remains the human being who is susceptible to manipulation techniques. The current paper explored social engineering as a domain and social engineering attacks as a process inside this domain. Two previous papers by the authors, *Towards an Ontological Model Defining the Social Engineering Domain* (Mouton et al., 2014) and *Social Engineering Attack Framework* (Mouton et al., 2014), are revisited. Both the ontological model and the social engineering attack framework are explored in order to further expand the social engineering domain.

The authors found that reports and news articles on social engineering do not provide all the information on social engineering attacks. There is usually no information available on either the "attack formulation" phase or the "information gathering" phase. There is also very little information on the "exploit relationship" phase, because reports or news articles tend to mention only the technique that was used and that it was successful. In order to do comparative studies of social engineering models, processes and frameworks, it is essential to have a set of fully detailed social engineering attack templates.

This paper proposed ten templates that provide fully detailed steps and phases throughout a social engineering attack. These templates were designed to be diverse and unique so that there is little overlap between each of them. The templates were also categorised based on the type of communication that was utilised. The authors proposed four templates in which bidirectional communication was used, three for unidirectional communication and three for indirect communication.

This paper also demonstrated the need for the social engineering attack templates and how they can be used to verify or compare other models, processes and frameworks within social engineering. The social engineering attack templates were used to create social engineering attack scenarios that were used to verify the social engineering attack detection model. Having the social engineering attack templates, the researchers were able to verify whether the social engineering attack detection model was able to assist users of the model to be more vigilant against social engineering attacks.

The proposed social engineering attack templates can now be used as a resource by researchers to expand on, use for comparative measures, create additional template or evaluate models for completeness. Having the social engineering attack templates, researchers are able to verify their models, processes and frameworks and compare their performances against other models, processes and frameworks. The templates provide a repeatable instance of a social engineering attack that can be stepped through a model, process or framework without the need to perform the attack and potentially harming individuals.

Additionally, the proposed social engineering attack templates can also be used to develop social engineering awareness material. The templates can be used to develop social engineering attack scenarios that are populated with subjects and objects of an organisation in order to demonstrate scenarios that are applicable to a specific environment. These scenarios can then be discussed with the individuals from the organisation in a way that enhances the individual's security awareness to be more vigilant against such a type of an attack.

In future work, the social engineering attack templates can be utilised as social engineering awareness material. A controlled experiment can be performed comparing the performance of individuals who had access to the awareness material versus individuals who did not have access. Also, the authors will use these templates to expand on existing research on social engineering attack detection models and to propose specific attack detection models for each type of communication.

REFERENCES

Abraham S, Chengalur-Smith I. An overview of social engineering malware: trends, tactics, and implications. Technol Soc 2010;32(3):183–96. <http://dx.doi.org/10.1016/j.techsoc.2010.07.001>, <http://www.sciencedirect.com/science/article/pii/S0160791X10000497>.

Åhlfeldt R-M, Backlund P, Wangler B, Söderström E. Security issues in health care process integration? A research-in-progress report, in: EMOI-INTEROP, 2005, pp. 1–4.

Bader G, Anjomshoaa A, Tjoa A. Privacy aspects of mashup architecture, in: Social Computing (SocialCom), 2010 IEEE Second International Conference on, 2010, pp. 1141–6. doi:10.1109/SocialCom.2010.169.

Brainard J, Juels A, Rivest RL, Szydlo M, Yung M. Fourth-factor authentication: somebody you know, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, CCS '06, ACM, New York, NY, USA, 2006, pp. 168–78. doi:10.1145/1180405.1180427. http://doi.acm.org/10.1145/1180405.1180427.

Brody RG, Brizzee WB, Cano L. Flying under the radar: social engineering. Int J Account Inf Manage 2012;20(4):335–47. doi:10.1108/18347641211272731.

Brown G, Howe T, Ihbe M, Prakash A, Borders K. Social networks and context-aware spam, in: Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work, CSCW '08, ACM, New York, NY, USA, 2008, pp. 403–12. doi:10.1145/1460563.1460628. http://doi.acm.org/10.1145/1460563.1460628.

CERT Insider Threat Team, Unintentional insider threats: a foundational study, Tech. Rep. CMU/SEI-2013-TN-022, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA; 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=58744.

CERT Insider Threat Team, Unintentional insider threats: social engineering, Tech. Rep. CMU/SEI-2013-TN-024, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA; 2014. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=77455.

Culpepper AM. Effectiveness of using red teams to identify maritime security vulnerabilities to terrorist attack [Master's thesis]. Naval Postgraduate School, Monterey, California; 2004.

Dang H. The origins of social engineering. McAfee Secur J 2008;1(1):4–9.

Dimkov T, van Cleeff A, Pieters W, Hartel P. Two methodologies for physical penetration testing using social engineering, in: Proceedings of the 26th Annual Computer Security Applications Conference, ACSAC '10, ACM, New York, NY, USA, 2010, pp. 399–408. doi:10.1145/1920261.1920319. http://doi.acm.org/10.1145/1920261.1920319.

Dittes JE, Kelley HH. Effects of different conditions of acceptance upon conformity to group norms. J Abnorm Soc Psychol 1956;53(1):100–7. doi:10.1037/h0047855.

Esmail S. eps1.5_br4ve-trave1er.asf , mr. Robot: Season 1. Episode 2015;6:URL: <http://www.usanetwork.com/mrrobot/episode-guide/season-1-episode-6-eps15br4ve-trave1erasf>; [cited 2015.08.19].

Gerard HB, Wilhelmy RA, Conolley ES. Conformity and group size. J Pers Soc Psychol 1968;8(1p1):79–82. doi:10.1037/h0025325.
Granger S. Social engineering fundamentals, part i: Hacker tactics (December 2001) URL: <http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics>; [cited 2013.11.11].
Greitzer FL, Strozer JR, Cohen S, Moore AP, Mundie D, Cowley J. Analysis of unintentional insider threats deriving from social engineering exploits, in: IEEE Security and Privacy Workshops (SPW 2014), San Jose, California, USA, 2014, pp. 236–50. doi:10.1109/SPW.2014.39.
Greitzer FL, Strozer J, Cohen S, Bergey J, Cowley J, Moore A, et al., Unintentional insider threat: contributing factors, observables, and mitigation strategies, in: 47th Hawaii International Conference on Systems Sciences (HICSS-47), Big Island, Hawaii, 2014, pp. 2025–34. doi:10.1109/HICSS.2014.256.
Gruschka N, Jensen M. Attack surfaces: a taxonomy for attacks on cloud services, in: Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, IEEE Computer Society, Los Alamitos, CA, USA, 2010, pp. 276–9. http://doi.ieeecomputersociety.org/10.1109/CLOUD.2010.23.
Hadnagy C. Social engineering: the art of human hacking. Wiley Publishing, Inc.; 2010.
Hamill JT, Deckro RF, Kloeber JM Jr. Evaluating information assurance strategies. Decis Support Syst 2005;39(3):463–84. <http://dx.doi.org/10.1016/j.dss.2003.11.004>, <http://www.sciencedirect.com/science/article/pii/S0167923604000284>.
Harley D. Re-floating the titanic: dealing with social engineering attacks, in: European Institute for Computer Antivirus Research, 1998, pp. 4–29.
Hill D. Peer group conformity in adolescent smoking and its relationship to affiliation and autonomy needs. Aust J Psychol 1971;23(2):189–99. doi:10.1080/00049537108254613. <http://www.tandfonline.com/doi/pdf/10.1080/00049537108254613>, <http://www.tandfonline.com/doi/abs/10.1080/00049537108254613>.
Insko CA, Smith RH, Alicke MD, Wade J, Taylor S. Conformity and group size the concern with being right and the concern with being liked. Pers Soc Psychol Bull 1985;11(1):41–50. doi:10.1177/0146167285111004.
Irani D, Balduzzi M, Balzarotti D, Kirda E, Pu C. Reverse social engineering attacks in online social networks. In: Holz T, Bos H, editors. Detection of intrusions and malware, and vulnerability assessment, vol. 6739 of lecture notes in computer science. Springer Berlin Heidelberg; 2011. p. 55–74.
Ivaturi K, Janczewski L. A taxonomy for social engineering attacks, in: G. Grant (Ed.), International Conference on Information Resources Management, Centre for Information Technology, Organizations, and People, 2011, pp. 1–12.
Jagatic TN, Johnson NA, Jakobsson M, Menczer F. Social phishing. Commun ACM 2007;50(10):94–100. doi:10.1145/1290958.1290968. <http://doi.acm.org/10.1145/1290958.1290968>.
Jahankhani H. The behaviour and perceptions of on-line consumers: risk, risk perception and trust. Int J Inf Sci Manage 2012;7(1):79–90.
Janczewski L, Fu L. Social engineering-based attacks: model and New Zealand perspective, in: Computer Science and Information Technology (IMCSIT), Proceedings of the 2010 International Multiconference on, 2010, pp. 847–53. doi:10.1109/IMCSIT.2010.5680026.
Jetten J, Hornsey MJ, Adarves-Yorno I. When group members admit to being conformist: the role of relative intragroup status in conformity self-reports. Pers Soc Psychol Bull 2006;32(2):162–73. doi:10.1177/0146167205279904.
Jodeit M, Johns M. USB device drivers: a stepping stone into your kernel, in: Computer Network Defense (EC2ND), 2010 European Conference on, 2010, pp. 46–52. doi:10.1109/EC2ND.2010.16.
Kieseberg P, Leithner M, Mulazzani M, Munroe L, Schrittwieser S, Sinha M, et al., QR code security, in: Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, MoMM '10, ACM, New York, NY, USA, 2010, pp. 430–5. doi:10.1145/1971519.1971593. http://doi.acm.org/10.1145/1971519.1971593.
Kingsley Ezechi A. Detecting and combating malware [Master's thesis]. University of Debrecen, Hungary; 2011. http://hdl.handle.net/2437/105305.
Krombholz K, Hobel H, Huber M, Weippl E. Social engineering attacks on the knowledge worker, in: Proceedings of the 6th International Conference on Security of Information and Networks, SIN '13, ACM, New York, NY, USA, 2013, pp. 28–35. doi:10.1145/2523514.2523596. http://doi.acm.org/10.1145/2523514.2523596.
Laribee L. Development of methodical social engineering taxonomy project, Msc, Naval Postgraduate School, Monterey, California; 2006.
Lenkart JJ. The vulnerability of social networking media and the insider threat new eyes for bad guys [Master's thesis]. Naval Postgraduate School, Monterey, California; 2011. http://calhoun.nps.edu/public/handle/10945/5562.
Long J. No tech hacking: a guide to social engineering, dumpster diving, and shoulder surfing. Syngress; 2011.
Lott AJ, Lott BE. Group cohesiveness, communication level, and conformity. J Abnorm Soc Psychol 1961;62(2):408–12. doi:10.1037/h0041109.
Major SDA. Social engineering: hacking the wetware! Inf Secur J Global Persp 2009;18(1):40–6. doi:10.1080/19393550802623214.
Mitnick KD, Simon WL. The art of deception: controlling the human element of security. Indianapolis: Wiley Publishing; 2002.
Mohd Foozy F, Ahmad R, Abdollah M, Yusof R, Mas'ud M. Generic taxonomy of social engineering attack, in: Malaysian Technical Universities International Conference on Engineering & Technology, Batu Pahat, Johor, 2011, pp. 1–7.
Mouton F, Malan M, Venter H. Development of cognitive functioning psychological measures for the SEADM, in: Human Aspects of Information Security & Assurance, Crete, Greece, 2012, pp. 40–51.
Mouton F, Malan MM, Venter HS. Social engineering from a normative ethics perspective, in: Information Security for South Africa, Johannesburg, South Africa, 2013, pp. 1–8. doi:10.1109/ISSA.2013.6641064.
Mouton F, Leenen L, Malan MM, Venter H. Towards an ontological model defining the social engineering domain. In: Kimppa K, Whitehouse D, Kuusela T, Phahlamohlaka J, editors. ICT and society, vol. 431 of IFIP advances in information and communication technology. Springer Berlin Heidelberg; 2014. p. 266–79.
Mouton F, Malan MM, Leenen L, Venter H. Social engineering attack framework, in: Information Security for South Africa, Johannesburg, South Africa, 2014, pp. 1–9. doi:10.1109/ISSA.2014.6950510.
Mouton F, Leenen L, Venter HS. Social engineering attack detection model: SEADMv2, in: International Conference on Cyberworlds (CW), Visby, Sweden, 2015, pp. 216–23. doi:10.1109/CW.2015.52.
Mouton F, Malan MM, Kimppa KK, Venter H. Necessity for ethics in social engineering research. Comput Secur 2015;55:114–27. <http://dx.doi.org/10.1016/j.cose.2015.09.001>, <http://www.sciencedirect.com/science/article/pii/S0167404815001224>.
Nohlberg M. Securing information assets: understanding, measuring and protecting against social engineering attacks [Ph.D. thesis]. Stockholm University; 2008.

Noy NF, McGuinness DL. Ontology development 101: a guide to creating your first ontology, Technical report ksl-01-05, Stanford Knowledge Systems Laboratory; 2001.
Peltier TR. Social engineering: concepts and solutions. Inf Syst Secur 2006;15(5):13–21. doi:10.1201/1086.1065898X/46353.15.4.20060901/95427.3. <http://www.tandfonline.com/doi/pdf/10.1201/1086.1065898X/46353.15.4.20060901/95427.3>, <http://www.tandfonline.com/doi/abs/10.1201/1086.1065898X/46353.15.4.20060901/95427.3>.
Rao U, Nayak U. Social engineering. In: The InfoSec handbook. Apress; 2014. p. 307–23.
Salem O, Hossain A, Kamala M. Awareness program and AI based tool to reduce risk of phishing attacks, in: Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, 2010, pp. 1418–23. doi:10.1109/CIT.2010.254.
Schrittwieser S, Frühwirt P, Kieseberg P, Leithner M, Mulazzani M, Huber M, et al., Guess who's texting you? Evaluating the security of smartphone messaging applications, in: Network and Distributed System Security Symposium, 2012, pp. 1–9.
Simon HA. Models of man; social and rational. Oxford, England: Wiley; 1957.
Stasiukonis S. Social engineering, the usb way (June 2006) URL: <http://tonydye.typepad.com/main/files/HO05-DarkReading.doc>; [cited 2015.08.13].
Symantec Security Response, Francophoned? a sophisticated social engineering attack (January 2014) URL: <http://www.symantec.com/connect/blogs/francophoned-sophisticated-social-engineering-attack>; [cited 2014.02.24].
Tam L, Glassman M, Vandenwauver M. The psychology of password management: a tradeoff between security and convenience. Behav Inf Technol 2010;29(3):233–44. doi:10.1080/01449290903121386. <http://dx.doi.org/10.1080/01449290903121386>, <http://dx.doi.org/10.1080/01449290903121386>.
Tetri P, Vuorinen J. Dissecting social engineering. Behav Inf Technol 2013;32(10):1014–23.
Thornburgh T. Social engineering: the "dark art", in: Proceedings of the 1st annual conference on Information security curriculum development, InfoSecCD '04, ACM, New York, NY, USA, 2004, pp. 133–5. doi:10.1145/1059524.1059554. http://doi.acm.org/10.1145/1059524.1059554.
Workman M. A test of interventions for security threats from social engineering. Inf Manage Comput Secur 2008;16(5):463–83.
Zeltser L. Malware infection that began with windshield fliers (February 2009) URL: <https://isc.sans.edu/diary/5797>; [cited 2014.02.24].

Francois Mouton is a senior information warfare researcher at the Council for Scientific and Industrial Research (CSIR) with expertise in the fields of social engineering, mobile security and digital forensics. Francois graduated with an M.Sc. Computer Science, in the field of digital forensics, from the University of Pretoria in 2012. During his M.Sc. degree he also completed all the undergraduate BA Psychology modules due to his passion in the field of social engineering. He is currently pursuing his PhD Computer Science, with a main focus on social engineering, at the University of Pretoria. He has (co)authored several international publications, mainly on topics of digital forensics readiness and social engineering. Francois is currently leading the development on mobile security related projects within the CSIR.

Dr Louise Leenen is a Senior Researcher in the Cyber Defence research Group at the Council for Scientific and Industrial Research (CSIR), South Africa. She holds a PhD Computer Science (in Constraint Programming) from the University of Wollongong in Australia. Her research focus is on artificial intelligence applications in the defence environment, cyber defence and ontology development. She is the Chair of the IFIP Working Group 9.10 on ICT in War and Peace.

Prof H.S Venter has established an international research reputation in digital forensics, information privacy, computer-based trust and information security management. Over the past 8 years, Prof Venter has been focusing mainly on digital forensic research. Prof Venter is the research group leader for the Information and Computer Security Architectures (ICSA) research group at the University of Pretoria, where he supervises more than 30 honours, masters and doctoral students.