Necessity for Ethics in Social Engineering Research

Francois Mouton[a,d], Mercia M. Malan[b], Kai K. Kimppa[c], H.S. Venter[d]

[a] *Command, Control and Information Warfare*
Defence, Peace, Safety and Security
Council for Scientific and Industrial Research
Pretoria, South Africa
[b] *Information and Computer Security*
Architecture Research Group
University of Pretoria
Pretoria, South Africa
[c] *Turku School of Economics*
University of Turku
Turku, Finland
[d] *Department of Computer Science*
University of Pretoria
Pretoria, South Africa

Abstract

Social engineering is deeply entrenched in the fields of both computer science and social psychology. Knowledge is required in both these disciplines to perform social engineering based research. Several ethical concerns and requirements need to be taken into account when social engineering research is conducted to ensure that harm does not befall those who participate in such research. These concerns and requirements have not yet been formalised and most researchers are unaware of the ethical concerns involved in social engineering research. This paper identifies a number of concerns regarding social engineering in public communication, penetration testing and social engineering research. It also discusses the identified concerns with regard to three different normative ethics approaches (virtue ethics, utilitarianism and deontology) and provides their corresponding ethical perspectives as well as practical examples of where these formalised ethical concerns for social engineering research can be beneficial.

Keywords: Consequentialism, Deontology, Ethical Concerns, Ethics, Penetration Testing, Public Communication, Social Engineering, Social Engineering Research, Utilitarianism, Virtue Ethics

Email addresses: `moutonf@gmail.com` (Francois Mouton), `malan747@gmail.com` (Mercia M. Malan), `kai.kimppa@utu.fi` (Kai K. Kimppa), `hventer@cs.up.ac.za` (H.S. Venter)
URL: `http://www.social-engineer.co.za/` (Francois Mouton)

1. Introduction

Social engineering — in the context of this paper — refers to the science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity [1]. As clearly stated by various authors, the human element is the 'glitch' or vulnerable element in security systems [2, 3, 4]. The basic 'good' characteristics of human nature make people vulnerable to the techniques used by social engineers, as they activate various psychological vulnerabilities that could be used to manipulate the individual into disclosing the requested information [5].

People are usually unaware of the extent to which social engineering techniques can be used in an attack. They may either fail to realise that they were a victim of such an attack or simply refuse to believe that they will ever be a victim. Most individuals do not realise the value of the information that they so willingly disclose and the impact or social consequences if this information is used maliciously. They do not grasp that the social engineer is dedicated to researching seemingly harmless matters and gathering information from various sources.

At the other end of the spectrum, we find people who believe that they will not fall prey to such an attack, as they will be able to recognise and avoid it. However, the social engineer is a skilled human manipulator who preys on human vulnerabilities by using various psychological triggers that could well foil sober human judgement [6].

Social engineering attacks may have unintended after-effects on the victim. These may be so severe that they may, for example, lead to suicide [7] or other forms of trauma. The ethical concerns related to social engineering attacks, as well as the consequences of such attacks, could well be minimised if the right actions are taken after the attack.

When research in relation to social engineering is conducted on participants, several ethical requirements need to be taken into consideration. The problem is that these requirements have not yet been formalised and most researchers are unaware of the ethical concerns that affect social engineering research. This paper aims to discuss the ethical concerns that need to be taken into consideration when social engineering is performed in a non-malicious fashion.

Non-malicious attacks are categorised according to the three different environments defined for this paper in which attacks may happen, namely public communications (such as radio and television), penetration testing and social engineering research. Social engineering attacks performed in any of these environments are not intended to cause harm to the victim or to make malicious use of the information gathered in the attack.

The current research is important in the computer science domain as social engineering has very strong cross-disciplinary relations with social psychology [6, 8, 9]. Computer science researchers are not always aware of all the ethical concerns while dealing with human participants in a research study. Therefore research needs to be conducted on the ethics regarding social engineering to reduce and simplify the ethical constraints for a computer scientist involved in research.

The remainder of the paper is structured as follows. Section 2 provides a background about both social engineering and ethics. Section 3 introduces three chosen environments in which social engineering attacks can be performed. Section 4 lists and describes different social engineering ethical concerns framed in scenarios from each environment. Section 5 discusses the ethical concerns presented in section 4 in terms of three ethical perspectives. Section 6 provides the reader with practical examples of how this research can be beneficial and Section 7 contains a summary and suggests future research work.

2. Background

The next section is divided into two subsections. Subsection 2.1 gives some background information on social engineering and social engineering attacks. Subsection 2.2 discusses ethics in terms of three main approaches to normative ethics.

2.1. Social Engineering

According to Mitnick & Simon [2], social engineering is defined as the techniques used to exploit human vulnerability to bypass security systems in order to gather information. As indicated by this definition, social engineering attacks imply interaction with other individuals, signifying the psychological aspect of social engineering.

Various psychological vulnerabilities and triggers used by social engineers aim to influence the individual's emotional state and cognitive abilities to obtain information. To successfully defend against these psychological triggers, the individual needs to have a clear understanding of the triggers to recognise them during a social engineering attack. Several psychological vulnerabilities exist, of which the most common ones are defined as strong affect, overloading, reciprocation, diffusion of responsibility and moral duty, integrity and consistency, authority, and deceptive relationships [2, 10, 11, 12].

These triggers could be used to perform a social engineering attack on an unsuspecting victim. The attack could cause the victim to experience a sense of discomfort — perhaps a mere uneasiness or actual anxiety — as all these attacks prey on the victim's psychological vulnerabilities. In an ideal world one would have expected a victim to be able to deduce from these clues of discomfort that he or she is being targeted by a social engineering attack. Unfortunately this does not happen in reality, as the human reasoning and decision-making process is extremely complex, and prone to error.

2.2. Ethics

This paper focuses on three main approaches to normative ethics: virtue ethics, utilitarianism and deontology [13]. Normative ethics deals with the 'right' and the 'wrong' of interpreted social behaviour [14]. The main difference between these three perspectives lies in the way they approach a moral dilemma, and not necessarily in its consequences.

The next section discusses the three different approaches of normative ethics and how each ethical perspective is measured.

2.2.1. Virtue Ethics

Virtue ethics is defined as the ethics that emphasises the virtues, or moral character, of an individual's actions [15]. It focuses more on the character of the individual or the character's traits that guide the individual to his or her actions. 'Virtue', as defined in the Oxford Dictionary [16], is behaviour showing high moral standards and a quality considered morally good or desirable in a person.

In virtue ethics, morality is not measured by the rules and rights of the world. Morality is measured by the classic notion of the character, which includes honesty, fairness, compassion and generosity, to name a few. It focuses on the individual and not on the community [17].

Virtue ethics started in ancient Greece, but was revived as a rival account to deontology and consequentialism and their understanding of morality. Virtue ethics is self-centred and focuses on answering questions such as "How should I live?" and "What type of person should I be?" [18].

As a common test for virtue ethics one needs to ask the question: "Will doing this make me a better (or worse) person?". The truly wise person will know what is right, do what is good, and therefore be happy [19].

To apply virtue ethics to an ethical concern one needs to consider whether the act would be the kind of thing that a virtuous person would do [20]. A virtuous person is someone who displays the ideal character traits, such as always being kind to everyone in all situations because that is their character and not because it is required of them.

Since it is difficult to measure virtue ethics in a social engineering computer science domain, this paper will use both the IEEE code of ethics and the general moral imperatives from the ACM code of ethics. These ethical codes are those that are most well known in the field of computer science research. This paper uses examples that include individuals who do not subscribe to either the IEEE or the ACM code of ethics. The codes, however, exemplify what kinds of codes people who do value virtue ethics would subscribe to. Many of the professional requirements in these codes can be extended to any profession, and only some of them are specific to the ICT field. Thus, for the purposes of this paper, a virtuous person is seen as someone who complies with both the IEEE and ACM code of ethics as provided in the excerpt below.

The IEEE code of ethics [21] states that: *We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world, and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:*

1. *to accept responsibility in making decisions consistent with the safety, health, and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;*
2. *to avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;*
3. *to be honest and realistic in stating claims or estimates based on available data;*
4. *to reject bribery in all its forms;*

5. *to improve the understanding of technology; its appropriate application, and potential consequences;*
6. *to maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;*
7. *to seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;*
8. *to treat fairly all persons and to not engage in acts of discrimination based on race, religion, gender, disability, age, national origin, sexual orientation, gender identity, or gender expression;*
9. *to avoid injuring others, their property, reputation, or employment by false or malicious action;*
10. *to assist colleagues and co-workers in their professional development and to support them in following this code of ethics.*

The ACM code of ethics [22], under the general moral imperatives section, states that: *As an ACM member I will:*

1. *Contribute to society and human well-being.*
2. *Avoid harm to others.*
3. *Be honest and trustworthy.*
4. *Be fair and take action not to discriminate.*
5. *Honor property rights including copyrights and patent.*
6. *Give proper credit for intellectual property.*
7. *Respect the privacy of others.*
8. *Honor confidentiality.*

This paper will use the following guideline in order to perform the test for virtue ethics: The social engineering attack that needs to be performed provides a window through which other people can see the social engineer for who he or she really is [23]. One then needs to examine the action from the perspective of these other people who are able to judge one's character from one's actions in order to measure virtue ethics. In the case where those other people would consider one to be a virtuous person in terms of both ethical codes, the attack will then be seen as ethical according to virtue ethics. The opposite is true if those other people would see one as a bad person for performing the social engineering attack.

2.2.2. Utilitarianism

Utilitarianism is the most common form of consequentialism. As in consequentialism, utilitarianism says that the rightness of an action is determined by the consequences of the specified action. Utilitarianist ethicists measure whether the action is ethical based on the outcomes of the action [13]. This approach involves analysing the impact of the individual's actions and the impact that this action has on the majority of other people.

This can be either for the interest of the individual or for the majority of society [17]. For the purposes of this paper, to test utilitarianism one needs to decide how it affects the majority of society. If the majority of society gains from the consequences, it is ethical, otherwise it is unethical.

To apply utilitarianist ethics to an ethical concern, one needs to consider the consequences of performing a social engineering attack on an individual and anyone else affected by the consequences of this attack. In utilitarianism, the consequences are assessed in terms of people's well-being. If the social engineering attack produces the best overall consequences for the community's well-being and the benefits to the community outweigh the consequence to the victim, then the utilitarian considers it ethically correct [24].

2.2.3. Deontology

Unlike the previous approaches, deontology focuses on adherence to the rules of the world in order to measure whether an action is right or wrong. It is also known as 'duty' or 'obligation' based ethics [25]. Deontology focuses on the ethical act and some deontologists believe that there are universal rules regarding right and wrong behaviour [17]. Deontologists live in a world of moral rules, such as [25].

- It is wrong to kill innocent people
- It is wrong to steal
- It is wrong to tell lies
- It is right to keep promises

To test for deontological ethics, the basic rule "do onto others only that to which they have consented" [26] is followed. It is ethical if the individual is performing a morally right action, regardless of the consequences [25].

To apply deontological ethics to an ethical concern one needs to consider whether a social engineering attack would be conforming to moral rules that seem a priori logically correct. From a deontological perspective, the aforementioned rules need to be adhered to for the most part, irrespective of their consequences. If any part of the social engineering attack does not strictly adhere to the deontological rules, the entire attack can be seen as unethical. The opposite would be true when the social engineering attack adheres to all the deontological rules of the world.

The following section discusses three chosen environments in which social engineering attacks can be performed. It also shows how public communication and penetration testing fit in with social engineering research.

3. SOCIAL ENGINEERING ENVIRONMENTS

As mentioned earlier, this paper focuses on three main environments in which social engineering can be performed, namely public communication, penetration testing and social engineering research. These environments were selected as they provide the broadest base to identify specific scenarios in which social engineering attacks are performed.

Social engineering attacks performed with non-malicious intent are mostly performed in one of these three environments. Research and penetration testing is more focused on the study of social engineering and on using social engineering to help a third party discover vulnerabilities in their system. The public communication environment involves public media where there is a presenter who may utilise manipulation techniques without realising that they amount to a social engineering attack.

The following subsections describe each of the three environments in more detail.

3.1. Public Communication

In this environment, communication with the public occurs through some public communication medium such as radio or television. Social engineering attacks that happen in this environment are normally for the goal of entertaining listeners or viewers. The intent of these attacks is mostly not to harm the victim, although the harm can occur unbeknownst to the presenter. The presenter may be unaware that he or she is performing a social engineering attack. The performed attacks can also have unintended harmful consequences.

3.2. Penetration Testing

In this environment, social engineering penetration tests are performed, which are designed to mimic attacks that actual malicious social engineers will use to steal data [27]. This can include attacks over the phone or the internet, but also onsite, by doing a 'break-in' into a physical place. The intent for these tests is not to cause harm, but rather to help improve the security by finding the vulnerabilities in the security system, whether physical or virtual.

The subjects who fall prey to the penetration test can feel guilty that they were not vigilant and this could lead to further personal harm. Management is required to view the penetration test report in an objective manner and not to take action against the employees who fall prey to the attack.

3.3. Social Engineering Research

Social engineering research constitutes a third environment in which social engineering techniques may be required. In this environment, social engineering attacks and social engineering awareness testing can potentially be performed as part of the research. Social engineering research involves a large environment and can also encapsulate the environments of penetration testing and public communication. This overlap of the social engineering research environment is depicted in Figure 1.

Social engineering research consists of several techniques that are required to gain accurate research results. In some of the research scenarios, the participants are required to be subjected to social engineering techniques without being requested to provide informed consent. The intent of this research is not to harm participants, although they may deliberately be kept unaware of their participation in social engineering research. The reason why informed consent from the participant is not provided is because the participants will act differently if they are aware that they are participating in social engineering research and this may provide inaccurate results.

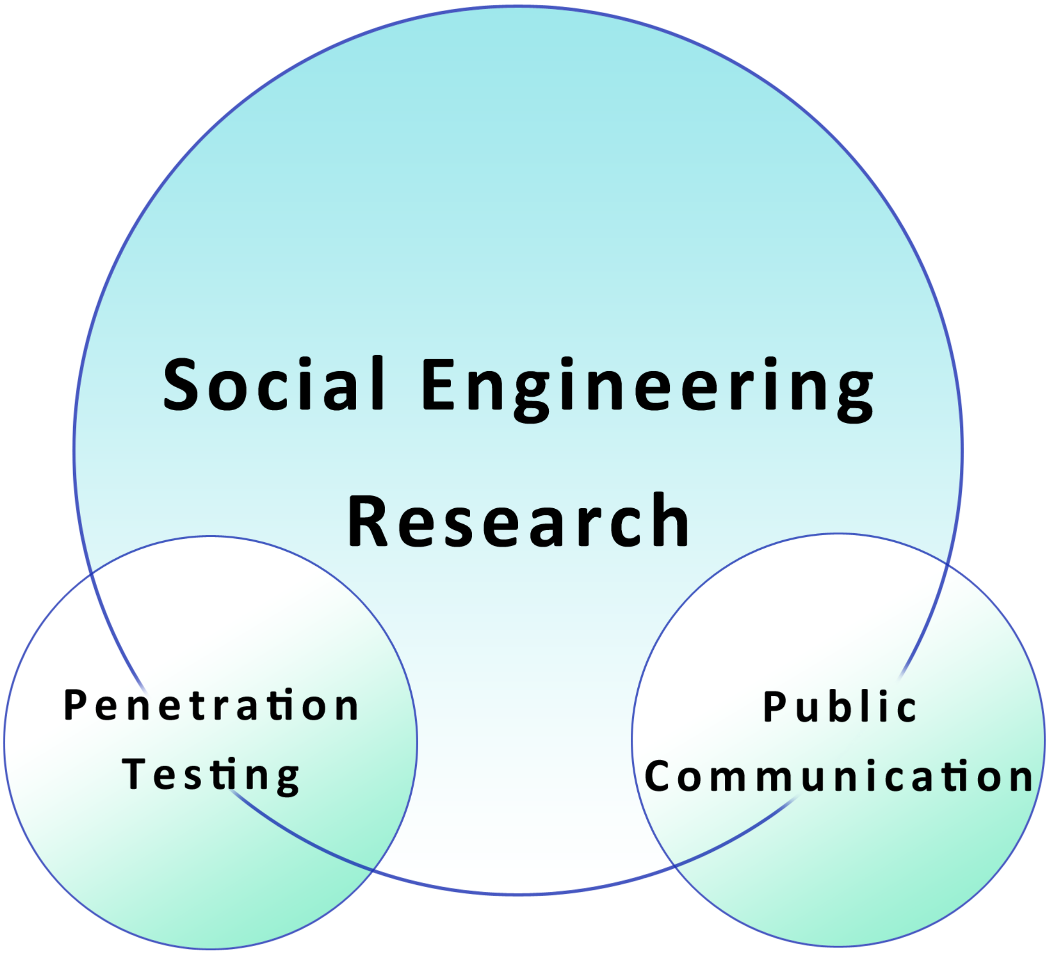

Figure 1: Overflow of Environments

The next section lists some scenarios of social engineering attacks within these three environments. Ethical concerns related to each of the scenarios are also extracted.

4. SOCIAL ENGINEERING ETHICAL CONCERNS

Each of the aforementioned environments allows the researcher to provide several scenarios within context. The goal of the scenarios is to frame the different social engineering ethical concerns and to provide a context in which to examine them.

In each of these scenarios a single ethical concern is provided that relates directly to the specific scenario and environment. Not all of the scenarios adhere to the formal definition of social engineering and have been adapted to highlight the ethical concerns. The goal of this section is to provide the reader with all of the ethical concerns regarding social engineering, whilst providing a scenario in which to frame and later on discuss the ethical concern.

The subsections below list all of the ethical concerns and the specific scenario in which to frame them from the different environments.

4.1. Public Communications

The following scenarios are framed in the social engineering public communications environment.

4.1.1. Royal family scenario

The first scenario is based on an incident concerning the British Royal family [7] when Prince William's wife, Kate, was admitted to hospital. Two Australian DJs phoned the hospital pretending to be Queen Elizabeth and Prince Charles, concerned about Kate's state of health. This prank was broadcasted live on the radio station to the public.

By using social engineering tactics and deceit, the DJs were able to talk their way through the hospital's switchboards and eventually got connected to Kate's personal nurse. Tactics included making noises in the background to simulate the queen's corgis barking. The DJs convinced the nurse to give them information regarding Kate's health status, which the nurse — believing it is the queen and the prince on the phone — gave out freely. The goal of this phone call was to provide entertainment and sensitive information to the radio station's listeners.

The ethical concern regarding this scenario is as follows: *Is it ethical to use social engineering to gain the trust of an individual?*

4.1.2. Radio prankster scenario

This scenario uses a radio prankster from a South African radio station, Highveld Stereo, Darren 'Whackhead' Simpson [28]. Darren is well known for the pranks he pulls on people for radio entertainment. Darren's career as a prankster has been so successful that he has published several audio prank collections discs that are sold all over the world.

In order to arrange a prank by Darren, someone who knows the victim sets up a prank with Darren after which he performs the actual prank. Darren thus has permission from either friends or family of the victim to perform the prank. Darren uses many social engineering techniques to convince the victim of his story, including background noises and different voices. He also gathers information about the person he is pranking beforehand in order to trick the person into believing his story. His intent is not to harm the victims, but to provide entertainment to Highveld Stereo listeners. After each prank, Darren reveals his identity and debriefs the victim.

The ethical concern for this scenario is as follows: *Is it ethical when delegated permission is used to perform social engineering techniques for public comical relief?*

4.1.3. Con artist scenario

The final scenario from the public communications scenarios is related to con artists on television. Several con artists hosting television programmes give audience members false hope by playing on their emotions, for example Marietta Theunissen from "Die ander kant"

(The other side) [29]. She allows participants to 'speak' to their deceased relatives and states her field of work as "Psychic and Clairvoyant Readings, Health and Self-development".

Psychics such as Marietta, and Tarot card readers use psychological methods and information gathering techniques to play on emotions and make people believe they are speaking to their deceased loved ones, or to give them a glimpse into their future endeavours. They trick people into believing these things by using the victim's emotions as a method. The individuals want to believe that they have just spoken to their deceased family members and therefore the psychics can easily manipulate them into believing that they have indeed done that.

General phrases such as "Your grandmother is happy and loves you very much" are used, which can be applicable to almost any individual over a certain age. In the case where the victim has a deceased grandmother, the victim will have an overwhelming emotion and will believe that the phrase is aimed at him or her specifically.

In essence, these con artists give people a sense of false hope by tricking them with social engineering techniques. The intent is not to hurt these people, but to gain money or fame out of it. In reality, however, some people get hurt in the process as they can potentially suffer negative consequences from the advice provided by the con artist.

The ethical concern for this scenario is as follows: *Is it ethical to use information gathering techniques to provide participants with false information and to exploit them for either financial gain or fame?*

This concludes the ethical concerns related to the public communication environment. The following section deals with the penetration testing environment.

4.2. Penetration Testing

The following scenarios are all framed in the social engineering penetration testing environment.

4.2.1. Security guard scenario

This scenario describes a physical on-site penetration test and was adapted from a scenario discussed on a podcast presented by Chris Hadnagy [30]. At some physical location a security guard's duty is to patrol the premises. This involves the guard walking around the building constantly making sure no one gains illegal access to the building.

A penetration tester is hired to try and break into the building. The tester first observes the situation for a bit and finds the exact pattern of the guard patrolling the building. The tester then times the guard's patrol path and observes how much time will be needed to break in from the one side of the building while the guard is patrolling any of the other three sides. The penetration tester then uses lock picks to gain access to the door on one side of the building whilst the guard is correctly patrolling, as his job requires, the other three sides of the building.

The intent of the penetration test is not to cause harm to the security guard, but to provide management with a detailed report on how access to the premises can be gained. The intent of the penetration test is to show the organisation where there are vulnerabilities in their security. The penetration test is not specifically aimed at the single security guard but at the organisation as a whole.

The ethical concern regarding this scenario is as follows: *Is it ethical for the employee to bear the consequences of the successful infiltration, when the actual reason for the successful infiltration is not due to the employee's negligence?*

4.2.2. Generalised human vulnerability scenario

In this scenario a penetration tester is hired with the goal to gather sensitive information from an organisation. The penetration tester chooses an employee as his entry point.

The employee who has been chosen earns a minimum wage and is looked down upon by the general public due to his status. During the penetration test, the social engineer offers the employee a significantly higher sum of money than his or her salary in return for information over which the employee has control. Since the employee needs the money and is attracted to the big amount that is never reflected in his or her salary, the information is given to the penetration tester. The employee is also not necessarily aware of the sensitivity of the information that is given out.

Many people will fall for this type of an attack as the reward that is offered is unreachable by the victim under normal circumstances. If they are offered a sum of money that is significantly higher than their salary or any salary they might ever earn, most people will see it as an opportunity and ignore the danger in it. In the rare case where the victim sees the opportunity as dangerous, it should also take little convincing from a skilled social engineer to get the victim to cooperate.

The ethical concern regarding this scenario is as follows: *Is it ethical to exploit a personal weakness of an employee when it is known to be common human nature to fall prey to this type of attack?*

4.2.3. Receptionist scenario

In this scenario, a penetration tester is hired to attempt to gain sensitive information from the organisation. The penetration tester chooses the receptionist as a possible weak link in the organisation as it is the latter's duty to help customers, to the best of his or her ability, while the customer is in the reception area of the organisation.

The penetration tester therefore enters the reception area as a customer. While waiting for a scheduled appointment, he takes out his laptop and realises that he has no network access. He sees that there is a network access point that he can potentially use to connect his computer to the internet, as well as to the network of the organisation.

The penetration tester asks the receptionist if he could just quickly connect his network cable to the network access point as he urgently needs to check his e-mail. The receptionist knows that it is company policy to assist customers in the reception area and is not aware of the dangers involved in providing access to the network. Since there is no company policy regarding who may and may not connect to the network access point, it is agreed that the penetration tester may use the network access point. With access gained to the organisation's network, the penetration tester is now able to hack into the inner network and extract sensitive information as needed.

The ethical concern for this scenario is as follows: *Is it ethical to report a social engineering penetration test as successful when the incident occurred because the employee was correctly performing his or her duty?*

4.2.4. Penetration test reporting scenario

This scenario deals with the information that is required for the penetration tester's report that is sent back to the organisation.

When an employee is susceptible to a specific penetration test, his or her details can potentially be recorded. The employer may request a detailed report listing the names of all employees who were susceptible to these attacks.

The intent of a penetration test is to help the organisation find the vulnerabilities in their security. If the vulnerability is an employee, management might feel the need to get rid of the employee to reduce the vulnerability [30]. This may not be the right action as the employee may be doing his or her job correctly, or perhaps the employee was not trained to identify social engineering attacks.

The solution to the problem is rather to train the employee to correctly identify social engineering attacks. An employee who already has been subjected to a social engineering penetration test will be much more vigilant than a new employee who has never heard of social engineering before. If management decides to keep this employee, it might be detrimental to his or her future career if the employee's name is recorded in the penetration testing report.

The ethical concern regarding this scenario is as follows: *Is it ethical to provide the names of employees who were susceptible to penetration tests in a report to an authoritative figure even though this may have consequences for the employees?*

The above concludes examples from the social engineering penetration testing environment. The next section deals specifically with scenarios unique to social engineering research. Note that the next as well as the previous section is associated with scenarios that could also occur in social engineering research.

4.3. Social Engineering Research

4.3.1. Awareness research and debriefing scenario

In this scenario it is required to measure the level of susceptibility of a group of participants to social engineering attacks by using social engineering research. Testing whether a person is susceptible to social engineering requires that social engineering techniques be applied or that social engineering examples be provided to the participant.

When participants are found to be susceptible to these techniques or examples, they may feel as if they were fooled or tricked during the experiment. This can lead to the participants doubting their own decisions and causing them to consider themselves gullible to fall prey to the tactics.

In most of these cases when social engineering awareness was tested, the general consensus was that participants will easily fall prey to these types of social engineering attacks [31, 32, 33]. The attacks tested during such an experiment will determine whether the individuals involved are overly helpful and accommodating. It is common to human nature to act in a helpful and accommodating manner towards other individuals and thus it is not necessarily inappropriate to fall prey to a social engineering attack.

The effect on the participant can be minimised provided that the participant is correctly debriefed. The debriefing session will include a one-on-one discussion between the researcher and the participant. The participant can then be informed and reassured that it is common human nature to fall prey to certain social engineering attacks.

The ethical concern regarding this scenario is as follows: *Is it ethical to conduct social engineering awareness research and how should the participant be debriefed?*

4.3.2. Informed consent scenario

This scenario requires participants to provide informed consent for a specific research scenario, but then to be subjected to another social engineering based research scenario. The participant must be fooled into thinking that he or she is part of a different study so that the participants will not be biased against social engineering attacks during the experiment.

In order to receive accurate results from the participants during a social engineering based research experiment, they may not be aware of the type of experiment they are subjected to. The test can be framed to be a normal test so that the participants are unaware that they are partaking in a social engineering research experiment.

The researcher, who requests informed consent from the participant for a different research scenario than the one the participant will eventually be subjected to, is not doing it to be malicious or harmful to the participant. The researcher is merely trying to limit any bias that a participant might have against the specific field and to ensure accurate experimental results from the participant.

The ethical concern regarding this scenario is as follows: *Is it ethical to mislead a participant about informed consent when such consent is required to gain accurate results from the social engineering research experiment?*

4.3.3. Sensitive information scenario

In the final scenario, a participant provided informed consent for the specific social engineering based research experiment. However, the researcher goes beyond the information that the participant has provided and gathers additional information to have a better overview of the participant for the sake of the experiment.

The participant who signed up for the social engineering experiment is not aware of the extent to which the researcher will be performing information gathering and social engineering attacks. Since the researcher gathered additional information of which the participant is unaware, the researcher is also unaware of how the participant may react to this additional information.

The information gained from the information gathering experiment might be sensitive or harmful to the participant and it might be unethical of the researcher to reveal this information to the experiment group. The researcher may also misuse the information he has gathered from the participant and appeal to the latter's emotions to manipulate him or her to take part in the experiment.

The ethical concern regarding this scenario is as follows: *Is it ethical during a social engineering research experiment to utilise information about the participant that may be harmful or sensitive to the participant?*

This concludes the section on the ethical concerns regarding social engineering. All those that have been identified in this section will next be discussed from the point of view of the different ethical approaches to normative ethics.

5. ETHICAL CONCERNS AND THE CORRESPONDING ETHICAL PERSPECTIVE

This section discusses each of the identified ethical concerns by examining how the different normative approaches can be used to address these concerns. The three different normative approaches that will be used are the virtue ethics perspective, utilitarianism perspective and deontological perspective.

5.1. Is it ethical to use social engineering to gain the trust of an individual?

5.1.1. Virtue Ethics

When the person performing social engineering is judged, his actions may be seen as negative since he misused his skills set to gain the trust of an innocent victim. For example, the Australian radio presenter did not comply with either the IEEE or the ACM code of ethics, specifically regarding honesty and trustworthiness. He also did not respect the privacy of the British royal family. From a virtue ethics perspective, such behaviour is unethical.

5.1.2. Utilitarianism

In this scenario, the goal of the presenter was to gather information about the royal family for the public's entertainment. The intent was never to harm the nurse, just to gain information. However, in order to gather this information, the presenter used social engineering techniques such as lying and false pretence to mislead the nurse and goad her to give out sensitive information. Thus, social engineering techniques were used to gain the trust of an individual in a deceptive manner. However, when one takes into account the effect on Kate and the royal family, it has to be admitted that since they are public figures, Kate's pregnancy would have been reported in the media in some form or other, sooner or later. The Australian radio presenters were just the first ones to make this information public.

Nevertheless, it is important to note that this is an extreme example as the nurse committed suicide soon after this event. Thus, the verdict would be that had the suicide not happened, the likely utility would have been positive, but if the suicide followed directly from this particular act and its consequences, then the utility was clearly negative. The suicide of the nurse cannot be ignored, as it was the consequence of this specific act and it has to be considered that the same consequences can occur in a similar instance of the ethical question. Hence, from a utilitarianist perspective, this is seen as immoral and thus unethical.

5.1.3. Deontology

Deontology is directly concerned with whether a universal world rule was breached to perform the action. For a deontologist, it is unethical to breach any of the universal moral rules, and thus a deontologist is not allowed to lie or manipulate people. To gain trust in this scenario, lying and trickery were used and several moral rules were broken. From a deontological perspective, this is unethical.

5.2. Is it ethical when delegated permission is used to perform social engineering techniques for public comical relief?

5.2.1. Virtue Ethics

The social engineer received delegated permission to perform the social engineering attack. Even though the social engineer obtained delegated permission, it is not the same as permission from the victim — thus some of the ethical concerns are delegated to the individuals who provided the permission to the social engineer.

The question to ask is whether performing pranks on other people, in other words lying to and intentionally misguiding and misleading them, makes the person performing the prank a more virtuous person. The radio prankster specifically does not avoid injuring the other person's reputation and also does not respect the latter's privacy. Thus, the radio prankster does not comply with the IEEE or the ACM code of ethics and it can be concluded that from a virtue ethics point of view his actions are unethical.

5.2.2. Utilitarianism

The majority of the large public audience gained entertainment from this scenario, which outweighs any consequences that the attack may have had on the targeted individual. From a utilitarian perspective, this is ethical as the joy and laughter of the majority outweighs the minor momentary humiliation of the targeted individual.

5.2.3. Deontology

Although the social engineer gained delegated permission to perform the social engineering techniques, permission was not granted by the victim self. There was also trickery and lying involved in performing the social engineering attack, which go against the moral rules of deontologists. From a deontological perspective, the radio prankster's action was unethical.

5.3. Is it ethical to use information gathering techniques to provide participants with false information and to exploit them for either financial gain or fame?

5.3.1. Virtue Ethics

If this scenario was judged by the outside world, they would not see it as good as the con artist or psychic (social engineer) exploited the victim. The social engineer also provided false information to the victims, which gave them false hope, thus showing the social engineer as a bad person. The con artist did not adhere to the IEEE code of ethics and was not honest and realistic in making claims, as the claims are not based on available data. The con artist also did not comply with the ACM code of ethics as he or she provided unsubstantiated information that may cause the victim harm. Thus, his or her actions were unethical from a virtue ethics point of view.

5.3.2. Utilitarianism

In this scenario the aim of the con artist was to gain fame and/or fortune through utilising social engineering techniques. The rest of the world does not gain anything from his or her actions. Even if the victim gained some false hope from the act, this false hope did not outweigh the clear wrong-doings by the con artist. The only individual who gained anything was the con artist, whose behaviour was seen as unethical from a utilitarianist perspective.

5.3.3. Deontology

The social engineer exploited and lied to the victim, thus breaking or violating several moral rules. From a deontological perspective, this is unethical.

5.4. Is it ethical for the employee to bear the consequences of the successful infiltration, when the actual reason for the successful infiltration is not due to the employee's negligence?

5.4.1. Virtue Ethics

The question here is whether the employee should bear any consequences when he or she was not negligent. The ethical concern thus focuses on the employer, who is the one initiating the consequences.

Does punishing the innocent employee make the employer a more virtuous person? The employer has to accept responsibility for his or her decisions according to the IEEE code of ethics. The employer would be acting unethically if the employee had to bear the consequences of the employer's decisions. The ACM code of ethics requires the employer to be fair and thus no harm may befall the employee due to the employer's decisions. From a virtue ethics perspective, this is unethical, as the employee should not suffer the consequences when he or she was merely following instructions from the employer.

5.4.2. Utilitarianism

The well-being of the employee does not affect the majority of the community. Only the employee is concerned whether there will be any consequences to him or her. If there are any consequences to the employee, these will surely outweigh the consequences to the community, of which there are none. In either case, whether the employee suffers consequences or not, this will still outweigh the consequences to the community. Thus, the harm done to the employee due to the successful infiltration will always be unethical, no matter whether there are consequences to the employee or not. From a utilitarian perspective, such behaviour is unethical.

5.4.3. Deontology

The employee was not negligent and thus does not deserve to suffer any consequences. It is not the employee who is at fault, provided that the employee followed the correct instructions from his or her superior. Any repercussions or consequences for the employee due to the successful infiltration will therefore be unethical from a deontological perspective.

5.5. Is it ethical to exploit a personal weakness of an employee when it is known to be common human nature to fall prey to this type of attack?

5.5.1. Virtue Ethics

It is known to be common human nature to fall for this type of attack. In this specific scenario the attack involves bribing the individual with an offer that is unreachable under normal circumstances. Since the social engineer takes advantage of an already known weakness, this does not make the social engineer a more virtuous person. Moreover, the IEEE code of ethics clearly states to reject bribery in all its forms. The social engineer provides a bribe to the victim and this is unethical according to the IEEE code of ethics. The social engineer is also not acting in an honest and trustworthy manner, which violates the ACM code of ethics. From a virtue ethics perspective, such behaviour is unethical.

5.5.2. Utilitarianism

In the specific penetration testing scenario the employee will be reassured that this is a common human vulnerability and thus the employee will be more vigilant and alerted to this type of attack in the future. If the employee is not unfairly dismissed, this may have further benefit for the organisation as the employee can use the opportunity to educate the rest of the staff to be more vigilant. The employee who was vulnerable to the attack can have a huge positive impact on his organisation by warning others against such an attack. From a utilitarian perspective, the harm done to the employee does not weigh up to the clear advantage he or she might now provide to the organisation through educating other personnel. Due to the eventual huge benefit to the organisation, this action is seen as ethical from a utilitarian perspective.

5.5.3. Deontology

The social engineer misused a common human vulnerability to exploit the victim. Exploiting other humans for personal gain clearly defies several rules of morality. From a deontological perspective, this is unethical as the action broke several rules of morality by tricking and exploiting the employee.

5.6. Is it ethical to report a social engineering penetration test as successful when the incident occurred because the employee was correctly performing his or her duty?

5.6.1. Virtue Ethics

The focus is not on the employee who performed wrongly, but rather on the guidelines and regulations of the organisation that need to be addressed and corrected. The employee did what he thought was required, thus showing good character in accordance with virtue ethics. The guidelines and regulations were followed correctly by the employee and thus the fault lies with the guidelines and regulations, not with the employee. Even though the guidelines and regulations were misused, the employee acted virtuously. Reporting the social engineering penetration test as successful will not harm the employee for performing his or her duties correctly as it will lead to the guidelines and regulations being corrected. The IEEE code of ethics requires the social engineer to be honest and realistic based on available data. Hence it would be ethical for the social engineer to report the penetration test as successful. Similarly, the ACM code of ethics requires the social engineer to report on his findings honestly while avoiding harm to others. From a virtue ethics perspective, such behaviour is therefore ethical.

5.6.2. Utilitarianism

Although reporting on the successful penetration test can cause the employee to suffer consequences, the organisation greatly benefits from it. By seeing the report, the organisation can better their guidelines and regulations so that future penetration tests as well as real attacks will not be successful. From a utilitarian perspective, the benefits of the majority of the organisation outweigh the possible consequences on the employee. Reporting on the successful penetration test is seen as ethical from a utilitarian perspective due to the benefit of the organisation.

5.6.3. Deontology

The outcome of the penetration test is that it was successful. From a deontological perspective it is required to report on the social engineering penetration test and to confirm that the information in the social engineering penetration test report is correct and accurate. In order to oblige to the rules and not be dishonest about the facts, the social engineering penetration test should be reported and accurately so. From a deontological perspective, it is ethical to report the social engineering penetration test as successful.

5.7. Is it ethical to provide the names of employees who were susceptible to penetration tests in a report to an authoritative figure even though this may have consequences for the employees?

5.7.1. Virtue Ethics

The harm to the employee must be pre-empted by the social engineer penetration tester according to the IEEE and ACM code of ethics. The penetration tester should inform the authoritative figure of the correct way to assist the employees and not to harm or punish them for their mistakes. Furthermore, both ethical codes also require the social engineer to report honestly and correctly on all their findings. Since it is required of the social engineer to pre-empt all harm and report honestly and accurately, it is deemed ethical for the social engineer to report fully on all findings, including the names of the employees involved. From a virtue ethics perspective, this is ethical.

5.7.2. Utilitarianism

In this example, it is important to note that the good of society or the good of humankind is the ultimate utilitarian consideration. In the case where training the employee and benefit to the organisation outweigh the dismissal of the employee and benefit to the organisation, the first option constitutes the morally obligatory choice. Since this benefits the majority of the organisation, it is ethical according to the utilitarianist perspective.

5.7.3. Deontology

If it is assumed that the penetration tester is required by management to report the full detail of the penetration test to the organisation, it would be ethically correct to disclose the names of vulnerable employees as the focus is on the rule stating that the penetration tester should provide a report with full details.

From a deontological perspective, such behaviour is ethical as the penetration testing follows the moral rule of full disclosure.

5.8. Is it ethical to conduct social engineering awareness research and how should the participant be debriefed?

5.8.1. Virtue Ethics

From an outside perspective it would be seen as ethical as it is required in research to perform social engineering awareness testing. However, it will only be seen as good if sufficient time is spent on debriefing each of the participants.

The IEEE code of ethics requires the researcher to accept responsibility in making decisions and to avoid harm to others. The ACM code of ethics requires the researcher to contribute to society and human well-being whilst also avoiding all harm to others. Avoiding harm to others entails the adequate debriefing of all participants.

From a virtue ethics perspective, such behaviour is seen as ethical, provided that the researcher ensures that the participant is correctly debriefed to the best of the researcher's ability.

5.8.2. Utilitarianism

Research is always needed even if such research may be harmful to some of the participants. As long as the ultimate goal of the research is to improve society as a whole, it will be seen as ethical from a utilitarian perspective. From such a perspective, any research that is performed to better the greater whole of society is seen as ethical.

5.8.3. Deontology

Social engineering awareness testing has the ultimate goal to pose questions to the participants to determine whether they are susceptible to social engineering. These questions are developed in a way to trick the participant and can thus cause the participant to answer the question in a manner that shows susceptibility. As deontology has a rule that participants should not be lied to or tricked during research, such behaviour will be seen as unethical.

5.9. Is it ethical to mislead a participant about informed consent when such consent is required to gain accurate results from the social engineering research experiment?

5.9.1. Virtue Ethics

Participants are required to give informed consent for the particular research experiment in which they are about to participate. The specific participant might not have given informed consent for an experiment that involves social engineering research. If the participant had been aware of the fact that he or she would be taking part in a social engineering experiment, he or she might have chosen to not form part of the research experiment.

Both the IEEE and ACM codes of ethics require the researcher to be honest with the research participants and thus it is unethical to be dishonest about the informed consent. Informed consent cannot be given by a participant if he or she is being misled.

From a virtue ethics perspective, the participant must be fully aware of the research experiment that he or she is going to be part of. Since informed consent is not given for the social engineering research experiment, it is considered unethical to trick the participant to be part of such experiment.

5.9.2. Utilitarianism

The social engineering research experiment may be harmful to a participant who gave informed consent for a different research experiment. In some scenarios, accurate results can only be gained if the participant is unaware of partaking in the research. Participants may behave differently if they know that they are part of a social engineering research experiment. It is important to limit the bias that the participant would have towards such an experiment to ensure the most accurate results from it.

However, since accurate results are required to improve society as a whole and since they outweigh the harm that can possibly be done to the participant, this action is regarded as ethical from a utilitarian perspective.

5.9.3. Deontology

The participant did not give informed consent for participating in the social engineering research experiment. Since this implies violation of one of the social engineering research rules, such action can already be seen as unethical. The participant may also feel bad for being tricked since he or she was not aware of participating in a social engineering research experiment.

From a deontological perspective, such behaviour is unethical as the participant is fooled into participating in a research experiment that he or she did not sign up for.

5.10. Is it ethical during a social engineering research experiment to utilise information about the participant that may be harmful or sensitive to the participant?

5.10.1. Virtue Ethics

Such information may harm the participant unbeknown to the researcher. The researcher may harm the participant by revealing sensitive information about the participant without intending to do any harm. Both the IEEE and ACM codes of ethics specifically state that the researcher may not cause harm to any of the participants. From a virtue ethics perspective, such action is seen as unethical since the researcher may potentially harm the participant.

5.10.2. Utilitarianism

Research is needed even if the information and method used to perform the social engineering research might be harmful to some of the participants. In this example it is important to note that the good of society or the good of humankind is the final measure or consideration in a utilitarianist approach. Hence, from a utilitarian perspective the research will still be seen as ethical, since the obligatory goal of all research is to improve society as a whole, and this commendable goal outweighs any negative consequences to the participant. The researcher can only perform the act that will most optimally improve society, since (according to the utilitarianist perspective) the best available solution is considered the morally obligatory choice.

5.10.3. Deontology

The participant did not provide informed consent to the researcher to utilise his or her harmful or sensitive personal information during the social engineering research experiment. Since informed consent is required, especially when dealing with harmful or sensitive information, the deontological rules were not followed. From a deontological perspective, such behaviour is unethical.

To summarise this section, tables 1, 2 and 3 list all of the ethical concerns in the three environments and whether they are ethical from the point of view of each of the different ethical perspectives.

Table 1: Ethical Concerns in Public Communication

	Virtue Ethics	Utilitarianism	Deontology
Is it ethical to use social engineering to gain the trust of an individual?	No	No	No
Is it ethical when delegated permission is used to perform social engineering techniques for public comical relief?	No	Yes	No
Is it ethical to use information gathering techniques to provide participants with false information and to exploit them for either financial gain or fame?	No	No	No

Table 2: Ethical Concerns in Penetration Testing

	Virtue Ethics	Utilitarianism	Deontology
Is it ethical for the employee to bear the consequences of the successful infiltration, when the actual reason for the successful infiltration is not due to the employee's negligence?	No	No	No
Is it ethical to exploit a personal weakness of an employee when it is known to be common human nature to fall prey to this type of attack?	No	Yes	No
Is it ethical to report a social engineering penetration test as successful when the incident occurred because the employee was correctly performing his or her duty?	Yes	Yes	Yes
Is it ethical to provide the names of employees who were susceptible to penetration tests in a report to an authoritative figure even though this may have consequences for the employees?	Yes	Yes	Yes

Table 3: Ethical Concerns in Social Engineering Research

	Virtue Ethics	Utilitarianism	Deontology
Is it ethical to conduct social engineering awareness research and how should the participant be debriefed?	Yes	Yes	No
Is it ethical to mislead a participant about informed consent when such consent is required to gain accurate results from the social engineering research experiment?	No	Yes	No
Is it ethical during a social engineering research experiment to utilise information about the participant that may be harmful or sensitive to the participant?	No	Yes	No

The following section provides practical examples on how this research can be utilised.

6. PRACTICAL EXAMPLES WITH REGARD TO THE ETHICAL CONCERNS

This paper has now provided the reader with ten different ethical concerns and how to reason about these ethical concerns from the different ethical perspectives. Three practical examples of where this research can be utilised are suggested next, such as in ethical committees, for teaching ethics in computer security and as an ethical guideline for penetration testers.

6.1. Ethical committees

Ethical committees perform a tedious job which entails verifying that all research performed adheres to several ethical guidelines. For the social engineering field specifically there is no formalised set of rules for measuring the ethical impact of a social engineering attack.

The current research can be used by ethical committees as a tool to measure the ethical impact of social engineering based research. It provides ethical committees with what each of the three different ethical perspectives have to say about each of the different ethical concerns. This research can also be used to answer specific ethical questions and to determine whether a single action in social engineering is ethical or not.

For example, a student approaches the ethical committee and wants to conduct social engineering based research that is specific to a certain organisation. He also wants to research the effects that social engineering attacks may have on the structure of the organisation. The table of ethical concerns (Table 3) allows one to easily determine the major ethical concerns are associated with this research. It also provides both the student and the ethical committee an easier way to measure the ethical viability of the research proposal.

This research can also provide an ethical committee with the three different ethical perspectives and how they are addressed in terms of social engineering. From the tables 1, 2 and 3 one can clearly see that when the ethical committee examines project proposals based on a utilitarianism perspective, more projects will be approved than when the same project proposals were to be examined from a deontological perspective.

6.2. Teaching ethics in computer security

The research can also be utilised to teach computer science students the ethical impact of social engineering in the field of computer security. As social engineering is entrenched in both computer science and social psychology, it is important for computer scientists to understand pertinent ethical concerns when dealing with individuals.

The table of ethical concerns can also be utilised to teach students the difference between the three different normative ethical approaches and how the reasoning of each of the ethical perspectives can be utilised to determine whether an action is ethical or not. It is furthermore important for students to understand the difference between the ethical perspectives and how the ethical measurement of each of these perspectives differs.

Since Table 1 and Table 2 provides practical examples on how to judge whether a social engineering action is ethical or not, it can be expanded for students to focus on other fields within the domains of computer security and computer science.

6.3. Ethical guideline for penetration testers

Penetration testers often have to decide whether a certain penetration test would be deemed ethical or not [30]. Also, among the scenarios provided, there were more that could be taken directly from the penetration testing environment as it is such a difficult environment in which to judge whether a certain action is ethical or not.

The present research provides penetration testers with a good guideline for measuring their applicable social engineering penetration tests. Table 2 can assist the penetration testers when it comes to ethical concerns about reporting on a certain successful infiltration. It is important to them to report their information in an ethical manner as the outcome potentially has a major impact on an employee's life (e.g. if the employee is dismissed due to the results of the penetration testing report).

Penetration testers will also benefit from having available the different ethical perspectives on each of the different ethical concerns. Being informed about the different ethical perspectives allows the penetration tester to examine the ethical concerns with the different perspectives and to make an informed decision about their actions.

The paper concludes the researchers' work by providing a summary of the ethical concerns about social engineering, how this research can be utilised in practice and future work.

7. CONCLUSION

Social engineering is deeply entrenched in the fields of computer science and social psychology. Knowledge of both of these disciplines is required to apply social engineering based techniques. Since all of these techniques are ordinarily performed on human participants, the ethical impact that social engineering has on these participants needs to be considered. Several ethical concerns and requirements need to be taken into account when social engineering research is conducted to ensure that no harm comes to the participants.

The problem is that these requirements have not yet been formalised and most researchers are unaware of the ethical concerns related to social engineering research. This paper addressed this problem by first providing the reader with a thorough background on both social engineering and the three main perspectives derived from the normative ethics approach.

The paper secondly discusses three environments in which social engineering can occur, i.e. public communication, penetration testing and social engineering research. As the social engineering research environment is such a broad environment, it can contain scenarios from both public communication and penetration testing. Each of the three environments is subdivided into several different and applicable scenarios.

These scenarios are used to develop and provide frames in which the ethical concerns regarding social engineering were proposed. Each scenario is associated with a single ethical concern, while each ethical concern has a scenario in which to frame the ethical concern to test whether the action taken is ethical or not.

The ethical concerns that are proposed is measured against each of the three different ethical perspectives, namely virtue ethics, utilitarianism and deontology. Each ethical concern is addressed by utilising all of the ethical perspectives.

This paper furthermore provides practical examples of where this research can be used, for instance as a tool for ethical committees, to teach ethics in computer security, and as an ethical guideline for penetration testers.

Further research should be conducted to explore other practical and potential uses of this research. The findings can be further refined to be used as training material to educate both university level students and penetration testers about social engineering and the ethical concerns regarding social engineering.

References

[1] F. Mouton, L. Leenen, M. M. Malan, H. Venter, Towards an ontological model defining the social engineering domain, in: K. Kimppa, D. Whitehouse, T. Kuusela, J. Phahlamohlaka (Eds.), ICT and Society, Vol. 431 of IFIP Advances in Information and Communication Technology, Springer Berlin Heidelberg, 2014, pp. 266–279.
URL http://dx.doi.org/10.1007/978-3-662-44208-1_22

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

[3] J. Debrosse, D. Harley, Malice through the looking glass: behaviour analysis for the next decade, in: Proceedings of the 19th Virus Bulletin International Conference, 2009.

[4] J. W. Scheeres, Establishing the human firewall: reducing an individual's vulnerability to social engineering attacks, Master's thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio (March 2008).

[5] G. L. Orgill, G. W. Romney, M. G. Bailey, P. M. Orgill, The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems, in: Proceedings of the 5th Conference on Information Technology Education, CITC5 '04, ACM, New York, NY, USA, 2004, pp. 177–181. doi:10.1145/1029533.1029577.
URL http://doi.acm.org/10.1145/1029533.1029577

[6] F. Mouton, M. Malan, H. Venter, Development of cognitive functioning psychological measures for the seadm, in: Human Aspects of Information Security & Assurance, Crete, Greece, 2012.

[7] C. Hadnagy, One royal pwning (December 2012).
URL http://www.social-engineer.org/social-engineering/one-royal-pwning/

[8] M. Bezuidenhout, F. Mouton, H. Venter, Social engineering attack detection model: Seadm, in: Information Security for South Africa, Johannesburg, South Africa, 2010, pp. 1–8. doi:10.1109/ISSA.2010.5588500.

[9] S. Granger, Social engineering fundamentals, part i: Hacker tactics (December 2001).
URL http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactic

[10] A. N. Chantler, R. Broadhurst, Social engineering and crime prevention in cyberspace, Tech. rep., Queensland University of Technology (June 2006).

[11] D. Gragg, A multi-level defense against social engineering, Tech. rep., SANS Institute InfoSec Reading Room (December 2002).

[12] M. Workman, A test of interventions for security threats from social engineering, Information Management & Computer Security 16 (5) (2008) 463–483.

[13] L. N. Gowdy, Normative ethics (May 2013).
URL http://www.ethicsmorals.com/ethicsnormative.html

[14] G. Harman, Moral philosophy meets social psychology: Virtue ethics and the fundamental attribution error, in: Proceedings of the Aristotelian Society, Vol. 99, JSTOR, Wiley on behalf of The Aristotelian Society, 1999, pp. 315–331.

[15] I. Manners, The normative ethics of the european union, International Affairs 84 (1) (2008) 45–60. doi:10.1111/j.1468-2346.2008.00688.x.
URL http://dx.doi.org/10.1111/j.1468-2346.2008.00688.x

[16] A. Stevenson, Oxford Dictionary of English, Oxford reference online premium, OUP Oxford, 2010.
URL http://books.google.co.za/books?id=TaZZSAAACAAJ

[17] D. Knights, M. O?Leary, Leadership, ethics and responsibility to the other, Journal of Business Ethics

67 (2) (2006) 125–137. doi:10.1007/s10551-006-9008-6.
URL `http://dx.doi.org/10.1007/s10551-006-9008-6`

[18] N. Athanassoulis, Virtue ethics (July 2014).
URL `http://www.iep.utm.edu/virtue/`

[19] W. S. Sahakian, M. L. Sahakian, Ideas of the great philosophers, no. 218, Barnes & Noble Publishing, 1966.

[20] H. Simmons, (September 2013).
URL `http://philosophyadvice.net/Guide%20to%20moral%20philosophy.pdf`

[21] IEEE Board of Directors, Ieee policies (August 2014).
URL `http://www.ieee.org/documents/ieee_policies.pdf`

[22] ACM Council, Acm code of ethics and professional conduct (October 1992).
URL `http://www.acm.org/about/code-of-ethics`

[23] ComputingCases, Publicity test (February 2014).
URL `http://www.computingcases.org/general_tools/teaching_with_cases/ethics_tests/publicity_test.html`

[24] BBC, Consequentialism (February 2014).
URL `http://www.bbc.co.uk/ethics/introduction/consequentialism_1.shtml`

[25] BBC, Duty-based ethics (February 2014).
URL `http://www.bbc.co.uk/ethics/introduction/duty_1.shtml`

[26] L. Alexander, M. Moore, Deontological ethics, in: E. N. Zalta (Ed.), The Stanford Encyclopedia of Philosophy, winter 2012 Edition, Stanford, 2012.

[27] C. Hadnagy, Social engineering penetration testing (February 2014).
URL `http://www.social-engineer.com/social-engineer-pentesting/`

[28] D. Simpson, @whackheads (February 2014).
URL `http://twitter.com/WhackheadS`

[29] M. Theunissen, Marietta theunisse biography (January 2013).
URL `http://www.otherworldstomorrow.com/upload/MariettaTheunissenBioJan2013.pdf`

[30] C. Hadnagy, Social engineering: Past, present and future (June 2010).
URL `http://www.social-engineer.org/episode-010-social-engineering-past-present-and-future/`

[31] K. D. Mitnick, W. L. Simon, The art of intrusion: the real stories behind the exploits of hackers, intruders and deceivers., Wiley Publishing, Indianapolis, 2005.

[32] M. Nohlberg, Securing information assets: Understanding, measuring and protecting against social engineering attacks, Ph.D. thesis, Stockholm University (2008).

[33] W. Kearney, H. Kruger, Considering the influence of human trust in practical social engineering exercises, in: Information Security for South Africa, Johannesburg, 2014, pp. 1–6. doi:10.1109/ISSA.2014.6950509.