Social Engineering from a Normative Ethics Perspective

F Mouton
Defence, Peace, Safety and Security
Command, Control and Information Warfare
Council for Scientific and Industrial Research
Pretoria, South Africa
Email: moutonf@gmail.com

M M Malan
Information and Computer Security
Architecture Research Group
University of Pretoria
Pretoria, South Africa
Email: malan747@gmail.com

H S Venter
Department of Computer Science
University of Pretoria
Pretoria, South Africa
Email: hventer@cs.up.ac.za

***Abstract*—Social engineering is deeply entrenched in both computer science and social psychology. Knowledge on both of these disciplines is required to perform social engineering based research. There are several ethical concerns and requirements that need to be taken into account whilst performing social engineering research on participants to ensure that harm does not come to the participants. These requirements are not yet formalised and most researchers are unaware of the ethical concerns whilst performing social engineering research. This paper identifies several ethical concerns regarding social engineering in public communication, penetration testing and social engineering research. This paper discusses the identified ethical concerns with regards to two different normative ethics approaches namely utilitarianism and deontology. All of the identified ethical concerns and their corresponding ethical perspectives are provided as well as practical examples of where these formalised ethical concerns for social engineering research can be utilised.**

***Index Terms*—Consequentialism; Deontology; Ethical Concerns; Ethics; Penetration Testing; Public Communication; Social Engineering; Social Engineering Research; Utilitarianism;**

I. Introduction

Social engineering, in the context of this paper, refers to various techniques that are utilised to obtain information through the exploitation of human vulnerability in order to bypass security systems [1]. As clearly stated by various authors, the human element is the 'glitch' or vulnerable element within security systems [2], [3], [4]. It is the basic 'good' human-natured characteristics that make people vulnerable to the techniques used by social engineers, as it activates various psychological vulnerabilities that could be used to manipulate the individual into disclosing the requested information [5].

Many individuals are unaware of the extent to which these techniques can be used in an attack. These individuals may not even realise that they were a victim of such an attack or they do not believe that they will ever be a victim. The majority of the public do not realise the value of some information that they willingly disclose and the impact of social consequences if this information is used maliciously. The social engineer is dedicated to researching various aspects and gathering information from various sources.

On the other end of the spectrum, the individual may believe that they will not fall prey to such an attack, as they will be able to recognise such an attack. However, the social engineer is a skilled human manipulator, preying on human vulnerabilities using various psychological triggers that could foil human judgment [6].

Social engineering attacks can have unintended after-effects on the victim. The after-effects can be so severe that it may, for example, lead to suicide. There are several ethical concerns related to social engineering attacks, and consequences of such attacks may be minimised if the right actions are taken after the attack.

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

These non-malicious attacks are categorised into three different environments in which these attacks can happen. The three environments defined for this paper is public communications such as radio and television, penetration testing and social engineering research.

Social engineering attacks performed in one of these environments are not intended to cause harm to the victim or to use information gathered in the attack maliciously.

This research is important in the computer science domain as social engineering is a computer science field with a very strong cross disciplinary relation to social psychology [7], [8], [6]. Computer science researchers are not always aware of all the ethical concerns whilst dealing with human participants in a research study. It is for these reasons that research is conducted on the ethics regarding social engineering in order to simplify the ethical constraints for a computer scientist.

The remainder of the paper is structured as follows. Section II provides a background about both social engineering and ethics. Section III introduces three chosen environments in which social engineering attacks can be performed. Section

IV lists and describes different social engineering ethical concerns framed in scenarios from each environment. Section V discusses the ethical concerns from section IV in terms of two ethical perspectives. Section VI provides the reader with practical examples of where these social engineering ethical concerns can be utilised and Section VII concludes this paper with a summary and future work.

II. Background

The following section is divided into two subsections. Subsection A gives a background on social engineering and social engineering attacks. Subsection B discusses ethics according to two main approaches to normative ethics.

A. Social Engineering

According to Mitnick & Simon [1], 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, indicating the psychological aspect of social engineering.

Various psychological vulnerabilities and triggers, used by social engineers, have been identified, which aim to influence the individual's emotional state and cognitive abilities in order to obtain information. To successfully defend against these psychological triggers, the individual will need to have a clear understanding of these triggers in order to recognise each during a social engineering attack. There are several psychological vulnerabilities, the most common ones are defined as: strong affect, overloading, reciprocation, diffusion of responsibility and moral duty, integrity and consistency, authority and finally deceptive relationships [9], [10], [3], [11].

These triggers could be used to perform a social engineering attack on an unsuspecting victim, which could lead the victim to experience a sense of discomfort, whether just an uneasiness or even anxiety, as all these attacks prey on the victim's psychological vulnerabilities. One would expect that a victim would be able to use these clues of discomfort to detect that he is being targeted by a social engineering attack. However, this is the ideal and not reality, as the human reasoning and decision-making process is extremely complex, and prone to error.

B. Ethics

This paper focuses on two main approaches to normative ethics: Utilitarianism and deontology [12]. Normative ethics is the 'right' and the 'wrong' of interpreted social behaviour [13]. The main difference between these two perspectives is the way a moral dilemma is approached, and not necessarily the consequences of it.

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

1) 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 [12]. 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 [14]. 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 consequence 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 [15].

2) Deontology: Unlike the previous approaches, deontology focuses on the adherence to the rules of the world in order to measure whether the action is right or wrong. It is also known as 'duty' or 'obligation'-based ethics [16]. Deontology focuses on the ethical act and some deontologists believe that there are universal rules regarding right and wrong behaviour [14]. Deontology protects the individual more than it protects the community[14]. Deontologists live in a world of moral rules, such as [16].

- 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" [17] is followed. It is ethical if the individual is doing a morally right action, regardless of the consequenses [16].

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, irrespective of their consequenses, for the most part. 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 in the case where 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.

III. SOCIAL ENGINEERING ENVIRONMENTS

This paper focuses on three main environments in which social engineering can be performed. The three environments are 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.

The following subsections describe each of the three environments.

A. Public Communication

This environment is where communication is made to the public 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.

B. Penetration Testing

This environment is where social engineering penetration testing is performed. Social engineering penetration tests are designed to mimic attacks that actual malicious social engineers will use to steal ones data [18]. This can include attacks over the phone or the internet, but also onsite, doing a "break-in" to 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 it is 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.

C. Social Engineering Research

Social engineering research is another 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 a part of research. Social engineering research is a large environment and can also encapsulate both scenarios in 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 which 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 providing informed consent. The intent of this research is not to harm the participant, although the participants may be required to be unaware that they are participating in social engineering research. The reason informed consent from the participant is not provided is because the participants will act differently if they aware that he is participating in social engineering research and this may provide inaccurate results.

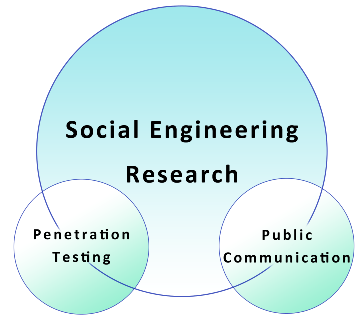

Fig. 1. Overflow of Environments

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.

IV. SOCIAL ENGINEERING ETHICAL CONCERNS

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

In each of these scenarios a single ethical concern, directly relating to the specific scenario and environment, is provided. 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 following subsections list all of the ethical concerns and the specific scenario in which to frame them from the different environments.

A. Public Communications

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

1) Radio prankster scenario: This scenario uses a radio prankster from a South African radio station, Highveld Stereo, Darren 'Whackhead' Simpson [19]. 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 which 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 in order 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 of 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 to 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?*

2) Con artistry scenario: The final scenario from the public communications scenario is related to con artists on television. There are several con artists on television who give audience members false hope by playing on their emotions. An example of this is Marietta Theunissen from "Die ander kant" (The other side) [20]. She allows participants to "speak" to their deceased relatives. She 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 in order 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 weapon. The individuals want to believe that they have just spoken to their deceased family members and therefore the psychics can easily manipulate these people into believing that they have indeed spoken to their deceased family members.

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 they will believe that the phrase is aimed at them 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.

The ethical concern for this scenario is as follows: *Is it ethical when information gathering techniques are used 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.

B. Penetration Testing

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

1) 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.

The receptionist's duty involves helping customers, to the best of her ability, while the customer is in the reception area of the organisation.

The penetration tester enters the reception area as a customer. While waiting for a scheduled appointment, the penetration tester takes out his laptop and realises that he has no network access. He sees that there is a network access point which he can potentially utilise in order to connect his computer to the internet as well as 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 is not aware of the dangers involved in providing access to the network and it is also not against company policy to assist customers in the reception area, thus she agrees 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?*

2) Penetration test reporting scenario: This scenario deals with the information that is required for the penetration tester's report which is sent back to the organisation.

When an employee is susceptible to a specific penetration test, the employee's details can potentially be recorded. The employer may request a full detailed report which consists of all employee names that 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 in order to reduce the vulnerability. This may not be the right action as the employee may be doing his or her job correctly or the employee was not trained to be able to identify social engineering attacks.

The solution to the problem is rather to train the employee to be able to correctly identify social engineering attacks. This employee already has been subjected to a social engineering penetration test and he or she will be much more vigilant than a new employee who has never heard of social engineering before. If the solution from management is to replace the employee it might be detrimental to the employee if his name is recorded in the penetration testing report.

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

This concludes the social engineering penetration testing environment. The following section deals specifically with scenarios unique to social engineering research as both this section and the previous section has scenarios which could also occur in social engineering research.

C. *Social Engineering Research*

1) Awareness research and debriefing scenario: In this scenario it is required to measure, using social engineering research, how susceptible a group of participants would be to social engineering attacks. In order to test whether a person is susceptible to social engineering, it is required to perform social engineering techniques or provide social engineering examples to the participant.

In the case where the participants are susceptible to these techniques or examples, the participants can feel as they were fooled or tricked during the experiment. This can lead to the participants doubting the decisions they make and also make them feel like they are gullible to fall prey to the tactics.

In most of these cases when testing social engineering awareness, the general consensus is that several participants will fall prey to these types of social engineering attacks. The social engineering attacks that are tested during such an experiment will test whether the individuals will be overly helpful or accommodating. It is common human nature to be both helpful and accommodating to other individuals and thus it is not necessarily wrong to fall prey to a social engineering attack.

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

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

2) Informed consent scenario: This scenario requires the participants to provide informed consent for a specific research scenario and then be subjected to another social engineering based research scenario.

It is required to fool the participant 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, it is required that the participants are not 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 is going to subjected to, is not doing it to be malicious or harmful to the participant. The researcher is only trying to limit any bias that a participant might have to the specific field and to ensure accurate experiment results from the participant.

The ethical concern for this scenario is as follows: *Is it ethical to mislead a participant when it comes to informed consent as it is required in order to get accurate results from the social engineering research experiment?*

This concludes the section on all of the ethical concerns regarding social engineering. All of the different ethical concerns that have been identified in this section are now discussed from the point of view of each of the different ethical approaches to normative ethics.

V. 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 utilised to answer these questions. The two different normative approaches that will be used are the utilitarianism perspective and deontological perspective.

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

1) Utilitarianism: The majority of the public gained entertainment from this scenario, which outweighs any consequences there may be on the victim of the attack. From a utilitarian perspective, this is ethical as the joy and laughter of the majority outweighs the humiliation of the victim.

2) Deontology: The social engineer gained delegated permission to perform the social engineering techniques, however, permission was not granted from the victim self. There was also trickery and lying involved in performing the social engineering attack which are against the moral rules of deontologists. From a deontological perspective, this is unethical.

B. *Is it ethical when information gathering techniques are used to provide participants with false information and to exploit them for either financial gain or fame?*

1) Utilitarianism: In this scenario the con artist gains either fame or fortune through utilising social engineering techniques. The rest of the world do not gain anything from this, not even the victims who believes their happy with their false hope. The only individual who gains anything from this is the con artist. This is thus unethical from a utilitarian perspective.

2) Deontology: The social engineer exploited and lied to the victim which breaks several moral rules. From a deontological perspective, this is unethical.

C. *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?*

1) Utilitarianism: Reporting on the successful penetration test can cause the employee to bare consequences, however, 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.

2) Deontology: The outcome of the penetration test is that it was successful. From a deontological perspective it is required to both report on the social engineering penetration test and 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, this is ethical.

D. Is it ethical to provide the name of the employees who were susceptible to the penetration tests in the report to an authoritative figure even though there may be consequences to the employees?

1) Utilitarianism: The employee can be either trained or dismissed to avoid future vulnerabilities for the organisation. This will lead to a better future for the organisation as a whole. As the organisation is now more aware of what vulnerabilities exists within the organisation, the organisation can perform an informed decision to plan for the future. Since this benefits the majority of the organisation, according to the utilitarian perspective, it is ethical.

2) Deontology: Assuming the case where 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 employee names as the focus is on the rule that the penetration tester will provide a report with full details.

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

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

1) Utilitarianism: Research is needed even if the 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 a utilitarian perspective, any research that is performed to better the greater whole of society is seen as ethical.

2) Deontology: Social engineering awareness testing has the ultimate goal to trick participants into answering the questions wrongly. As deontology has a rule that participants should not be lied to or tricked during research, this will be seen as unethical.

From a deontological perspective, any research that requires that the participants should be lied to or tricked is deemed as unethical.

F. Is it ethical to mislead a participant when it comes to informed consent as it is required in order to get accurate results from the social engineering research experiment?

1) Utilitarianism: The social engineering research experiment may be harmful to the participant if informed consent was given for a different research experiment. In some scenarios accurate results can only be gained if the participant is unaware that they are partaking in the research. Participants may behave differently if they are aware that they are forming part of a social engineering research experiment. It is important to limit the bias that the participant would have towards the social engineering research experiment to ensure the most accurate results from the experiment.

Since accurate results are required to improve society as a whole and this also outweighs the harm that can possibly be done to the participant, this action is seen as ethical from a utilitarian perspective.

2) Deontology: Informed consent was not given by the participant for participating in the social engineering research experiment. Since this breaks one of the social engineering research rules it can already be seen as unethical. The participant may also feel bad for being tricked since the participant is not aware that he or she is participating in a social engineering research experiment.

From a deontological perspective, it is unethical as the participant is fooled into participating in a research experiment that the participant did not sign up for.

To summarise this section, the following three tables lists 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 I
ETHICAL CONCERNS IN PUBLIC COMMUNICATION

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

TABLE II
ETHICAL CONCERNS IN PENETRATION TESTING

	Utilitarianism	Deontology
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
Is it ethical to provide the name of the employees who were susceptible to the penetration tests in the report to an authoritative figure even though there may be consequences to the employees?	Yes	Yes

TABLE III
ETHICAL CONCERNS IN SOCIAL ENGINEERING RESEARCH

	Utilitarianism	Deontology
Is it ethical to perform social engineering awareness research and how should the participant be debriefed?	Yes	No
Is it ethical to mislead a participant when it comes to informed consent as it is required in order to get accurate results from the social engineering research experiment?	Yes	No

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

VI. PRACTICAL EXAMPLES FOR THE ETHICAL CONCERNS

This paper has now provided one with six different ethical concerns and how one would reason about these ethical concerns from the different ethical perspectives. This section provides the reader with two practical examples where this research can now be utilised.

The following sections discuss practical examples where this research can be utilised such as ethical committees and ethical guideline for penetration testers.

A. Ethical committees

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

This research can be used as a tool by any ethical committee in order 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 certain ethical concerning questions in order to determine whether a single action in social engineering is ethical or not.

As an example, a student comes to the ethical committee and this student wants to conduct social engineering based research that is specific to a certain organisation. He also wants to research the effects social engineering attacks may have on the organisational structure of the organisation. The table of ethical concerns allows one to easily determine the major ethical concerns which 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 two different ethical perspectives and how they are addressed in terms of social engineering. From the table one can clearly see that if the ethical committee examines project proposals based on a utilitarianism perspective more projects will be approved than when examining the same project proposals from a deontological perspective.

B. Ethical guideline for penetration testers

Penetration testers often have to decide whether a certain penetration test would be deemed to be ethical or not [21]. Also, form the scenarios that were provided, there were more scenarios 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.

This research allows social engineering penetration testers to have a good guideline in order to measure their applicable social engineering penetration tests. The table can also assist the penetration testers when it comes to ethical concerns when reporting on a certain successful infiltration. It is important to the penetration testers that they report their information in an ethical manner as they may potentially have a major impact on an employee's life if the employee is dismissed due to the penetration testing report.

The penetration testers will also benefit from having the different ethical perspectives on each of the different ethical concerns. Having the different ethical perspectives allows the penetration tester to examine the ethical concern with the different perspectives in order to make an informed decision about their actions.

The next section of this paper now concludes the work by providing a summary of the ethical concerns of social engineering, how this research can be utilised in a practical example and future work.

VII. CONCLUSION

Social engineering is deeply entrenched in both computer science and social psychology. Knowledge on both of these disciplines is required to perform social engineering based techniques. As all of these techniques are ordinarily performed on human participants, the ethical impact that social engineering has on the participants needs to be considered. There are several ethical concerns and requirements that need to be taken into account whilst performing social engineering research on participants to ensure that harm does not come to the participants.

The problem is that these requirements are not yet formalised and most researchers are unaware of the ethical concerns whilst performing social engineering research. This paper addressed this problem by first providing the reader with a thorough background on both social engineering and the two main ethical perspectives from the normative ethics approaches.

The paper provides three environments in which social engineering can occur. These environments are public communication, penetration testing and social engineering research. As the social engineering research environment is such a broad environment it can also contain scenarios of both public communication and penetration testing. Each of the three environments is subdivided into several different scenarios applicable to each of these environments.

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

Each of the ethical concerns that are proposed is measured against each of the two different ethical perspectives namely utilitarianism and deontology. Each ethical concern is answered by utilising all of the ethical perspectives.

This paper also provides practical examples where this research can be used. Some of the practical examples include that the research can be utilised as a tool for ethical committees as well as an ethical guideline for penetration testers.

Further research can be performed to explore any other practical examples where this research can potentially be utilised. This research can also be further developed to be training material to teach both university level students and penetration testers about social engineering and the ethical concerns regarding social engineering. More ethical perspectives should be examined, such as virtue ethics, in order to provide a more thorough investigation of the ethical concerns regarding social engineering.

REFERENCES

[1] K. D. Mitnick and W. L. Simon, *The art of deception: Controlling the human element of security*. Wiley, 2001.

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

[3] K. Mitnick and W. Simon, "The art of intrusion: the real stories behind the exploits of hackers, intruders & deceivers," 2005.

[4] J. W. Scheeres, "Establishing the human firewall: reducing an individual's vulnerability to social engineering attacks," DTIC Document, Tech. Rep., 2008.

[5] G. L. Orgill, G. W. Romney, M. G. Bailey, and 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*. ACM, 2004, pp. 177–181.

[6] F. Mouton, M. Malan, and H. Venter, "Development of cognitive functioning psychological measures for the seadm," 2012.

[7] M. Bezuidenhout, F. Mouton, and H. Venter, "Social engineering attack detection model: Seadm," in *Information Security for South Africa (ISSA), 2010*. IEEE, 2010, pp. 1–8.

[8] S. Granger, "Social engineering fundamentals, part i: hacker tactics," *Security Focus, December*, vol. 18, 2001.

[9] A. N. Chantler and R. Broadhurst, "Social engineering and crime prevention in cyberspace," 2006.

[10] D. Gragg, "A multi-layer defense against social engineering," *SANS Insitute Reading Room*, 2002.

[11] M. Workman, "A test of interventions for security threats from social engineering," *Information Management & Computer Security*, vol. 16, no. 5, pp. 463–483, 2008.

[12] L. N. Gowdy, "Normative ethics," http://www.ethicsmorals.com/ethicsnormative.html, accessed May 18, 2013.

[13] G. Harman, "Moral philosophy meets social psychology: Virtue ethics and the fundamental attribution error," in *Proceedings of the Aristotelian society*. JSTOR, 1999, pp. 315–331.

[14] D. Knights and M. OLeary, "Leadership, ethics and responsibility to the other," *Journal of Business Ethics*, vol. 67, no. 2, pp. 125–137, 2006.

[15] BBC, "Consequentialism," http://www.bbc.co.uk/ethics/introduction /consequentialism_1.shtml, accessed May 19, 2013.

[16] ——, "Duty-based ethics," http://www.bbc.co.uk/ethics/introduction/ duty_1.shtml, accessed May 19, 2013.

[17] L. Alexander and M. Moore, "Deontological ethics," in *The Stanford Encyclopedia of Philosophy*, winter 2012 ed., E. N. Zalta, Ed., 2012.

[18] SocialEngineer.org, "Social engineering penetration testing," https://www.social-engineer.com/social-engineer-pentesting/, accessed May 18, 2013.

[19] TVSA, "Darren "whackhead" simpson," http://www.tvsa.co.za/actorprofile.asp?actorid=5107, accessed May 18, 2013.

[20] other world's tomorrow, "Marietta theunissen," http://www.otherworldstomorrow.com/index.php?q=con,58,Marietta_ Theunissen, accessed May 15, 2013.

[21] Social-Engineer.org, "Social engineering past, present and future 2010," 2010. [Online]. Available: http://www.social-engineer.org/episode-010-social-engineering-past-present-and-future/