Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Necessity for ethics in social engineering research

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

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

ARTICLE INFO

Article history:
Received 10 June 2015
Received in revised form 18 August 2015
Accepted 3 September 2015
Available online 9 September 2015

Keywords:
Consequentialism
Deontology
Ethical concerns
Ethics
Penetration testing
Public communication
Social engineering
Social engineering research
Utilitarianism
Virtue ethics

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.

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 (Mouton et al., 2014). As clearly stated by various authors, the human element is the "glitch" or vulnerable element in security systems (Debrosse and Harley, 2009; Mitnick and Simon, 2002; Scheeres, 2008). 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 (Orgill et al., 2004).

People are usually unaware of the extent to which social engineering techniques can be used in an attack. They may

http://www.social-engineer.co.za/
* *Corresponding author*. Tel.: +27 82 857 5842.
E-mail address: moutonf@gmail.com (F. Mouton).

http://dx.doi.org/10.1016/j.cose.2015.09.001
0167-4048/© 2015 Elsevier Ltd. All rights reserved.

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 are 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 (Mouton et al., 2012).

Social engineering attacks may have unintended aftereffects on the victim. These may be so severe that they may, for example, lead to suicide (Hadnagy, 2012) 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 (Bezuidenhout et al., 2010; Granger, 2001; Mouton et al., 2012). 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

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

2.1. *Social engineering*

According to Mitnick and Simon (2002), 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 (Chantler and Broadhurst, 2006; Gragg, 2002; Mitnick and Simon, 2002; Workman, 2008).

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 (Gowdy, 2013). Normative ethics deals with the "right" and the "wrong" of interpreted social behaviour (Harman, 1999). 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 (Manners, 2008). 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 (Stevenson, 2010), 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 (Knights and O'Leary, 2006).