Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Social engineering attack examples, templates and scenarios

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

[a] Command, Control and Information Warfare, Defence, Peace, Safety and Security, Council for Scientific and Industrial Research, Pretoria, South Africa
[b] Department of Computer Science, University of Pretoria, Pretoria, South Africa

ARTICLE INFO

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

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

ABSTRACT

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

© 2016 Elsevier Ltd. All rights reserved.

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

http://dx.doi.org/10.1016/j.cose.2016.03.004
0167-4048/© 2016 Elsevier Ltd. All rights reserved.

1. Introduction

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

The "art" of influencing people to divulge sensitive information is known as social engineering and the process of doing so is known as a social engineering attack. There are various definitions of social engineering and also a number of different models of social engineering attack (Åhlfeldt et al., 2005; Culpepper, 2004; Hadnagy, 2010; Hamill et al., 2005; Kingsley Ezechi, 2011; Lenkart, 2011; Mitnick and Simon, 2002; Mouton et al., 2012, 2014; Nohlberg, 2008; Thornburgh, 2004). The authors considered a number of definitions of social engineering and social engineering attack taxonomies in a previous paper, *Towards an Ontological Model Defining the Social Engineering Domain* (Mouton et al., 2014), and formulated a definition for both social engineering and social engineering attack. In addition, the authors proposed an ontological model for a social engineering attack. They defined social engineering as "the science of using social interaction as a means to persuade an individual or an organisation to comply with a specific request from an attacker where either the social interaction, the persuasion or the request involves a computer-related entity" (Mouton et al., 2014).

Although the ontological model contains all the components of a social engineering attack, it fails to depict temporal data such as flow and time (Noy and McGuinness, 2001). Due to this shortcoming, the authors developed a social engineering attack framework that expands on Kevin Mitnick's social engineering attack cycle (Mitnick and Simon, 2002; Mouton et al., 2014). The social engineering attack framework depicts the logical flow of a social engineering attack (Mouton et al., 2014). This framework refers to the components in the ontological model but focuses on the process flow – starting at the point at which an attacker initially thinks about gaining sensitive information from some target, up to the point of succeeding in the goal of gaining this information (Mouton et al., 2014).

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

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

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

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

2. Defining social engineering attacks

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

Download English Version:

https://daneshyari.com/en/article/456423

Download Persian Version:

https://daneshyari.com/article/456423

Daneshyari.com