Information Security for South Africa, Johannesburg, South Africa, 12-14 August 2014

Social engineering attack framework

Francois Mouton [1], Mercia M. Malan[2, 3], Louise Leenen [1] and H.S. Venter[2, 3]

1Defence Peace Safety & Security, Council for Industrial and Scientific Research Pretoria, South Africa
E-mail: moutonf@gmail.com, lleenen@csir.co.za
2University of Pretoria, Information and Computer Security Architecture Pretoria, South Africa
E-mail: malan747@gmail.com
3University of Pretoria, Department of Computer Science Pretoria, South Africa
E-mail: hventer@cs.up.ac.za

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 the human element is thus a weak link. A social engineering attack targets this weakness by using various manipulation techniques in order to elicit sensitive information. The field of social engineering is still in its infancy stages with regards to formal definitions and attack frameworks. This paper proposes a social engineering attack framework based on Kevin Mitnick's social engineering attack cycle. The attack framework addresses shortcomings of Mitnick's social engineering attack cycle and focuses on every step of the social engineering attack from determining the goal of an attack up to the successful conclusion of the attack. The authors use a previously proposed social engineering attack ontological model which provides a formal definition for a social engineering attack. The ontological model contains all the components of a social engineering attack and the social engineering attack framework presented in this paper is able to represent temporal data such as flow and time. Furthermore, this paper demonstrates how historical social engineering attacks can be mapped to the social engineering attack framework. By combining the ontological model and the attack framework, one is able to generate social engineering attack scenarios and to map historical social engineering attacks to a standardised format. Scenario generation and analysis of previous attacks are useful for the development of awareness, training purposes and the development of countermeasures against social engineering attacks.