2015 International Conference on Cyberworlds

Social Engineering Attack Detection Model: SEADMv2

Francois Mouton_†, Louise Leenen_ and H.S. Venter†

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

Abstract

Information security is a fast-growing discipline, and therefore the effectiveness of security measures to protect sensitive information needs to be increased. Since people are generally susceptible to manipulation, humans often prove to be the weak link in the security chain. A social engineering attack targets this weakness by using various manipulation techniques to elicit individuals to perform sensitive requests. The field of social engineering is still in its infancy as far as formal definitions, attack frameworks, examples of attacks and detection models are concerned. This paper therefore proposes a revised version of the Social Engineering Attack Detection Model. The previous model was designed with a call centre environment in mind and is only able to cater for social engineering attacks that use bidirectional communication. Previous research discovered that social engineering attacks can be classified into three different categories, namely attacks that utilise bidirectional communication, unidirectional communication or indirect communication. The proposed (and revised) Social Engineering Attack Detection Model addresses this problem by extending the model to cater for social engineering attacks that use bidirectional communication, unidirectional communication or indirect communication. The revised Social Engineering Attack Detection Model is further verified using published generalised social engineering attack examples from each of the three categories mentioned.