ICT and Society

IFIP Advances in Information and Communication Technology Volume 431, 2014, pp 266-279

Towards an Ontological Model Defining the Social Engineering Domain

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

1 Defence Peace Safety & Security, Council for Industrial and Scientific Research, Pretoria, South Africa

Moutonf@gmail.com, lleenen@csir.co.za

2 University of Pretoria, Information and Computer Security Architecture Research Group, Pretoria, South Africa

Malan747@gmail.com

3 University of Pretoria, Computer Science Department, Pretoria, South Africa

Hventer@cs.up.ac.za

Abstract

The human is often the weak link in the attainment of Information Security due to their susceptibility to deception and manipulation. Social Engineering refers to the exploitation of humans in order to gain unauthorised access to sensitive information. Although Social Engineering is an important branch of Information Security, the discipline is not well defined; a number of different definitions appear in the literature. Several concepts in the domain of Social Engineering are defined in this paper. This paper also presents an ontological model for Social Engineering attack based on the analysis of existing definitions and taxonomies. An ontology enables the explicit, formal representation of the entities and their inter-relationships within a domain. The aim is both to contribute towards commonly accepted domain definitions, and to develop a representative model for a Social Engineering attack. In summary, this paper provides concrete definitions for Social Engineering, Social Engineering attack and social engineer.