Information Security for South Africa Conference (ISSA2017), 16-17 August 2017, Sandton, Johannesburg, South Africa

Underlying Finite State Machine for the Social Engineering Attack Detection Model

Francois Mouton, Alastair Nottingham, Louise Leenen, H.S. Venter

ABSTRACT:

Information security is a fast-growing discipline, and relies on continued improvement of security measures to protect sensitive information. In general, human operators are often highly susceptible to manipulation, and tend to be one of the weakest links 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 with respect to formal definitions, attack frameworks, examples of attacks and detection models. In order to formally address social engineering in a broad context, this paper proposes the underlying finite state machine of the Social Engineering Attack Detection Model (SEADM). The model has been proven to successfully thwart social engineering attacks utilising either bidirectional communication, unidirectional communication or indirect communication. Proposing and exploring the underlying finite state machine of the model allows one to have a clearer overview of the mental processing performed within the model. While the current model provides a general procedural template for implementing detection mechanisms for social engineering attacks, the finite state machine provides a more abstract and extensible model that highlights the interconnections between task categories associated with different scenarios. The finite state machine is intended to help facilitate the incorporation of organisation specific extensions by grouping similar activities into distinct categories, subdivided into one or more states. In addition, it facilitates additional analysis on state transitions that are difficult to extract from the original flowchart based model.