Proceedings of the 16th Information Security South Africa 2017, Johannesburg, South Africa, 23 November 2017

Benchmarking a Mobile Implementation of the Social Engineering Prevention Training Tool

Francois Mouton
Marcel Teixeira
Thomas Meyer

Abstract:

As the nature of information stored digitally becomes more important and confidential, the security of the systems put in place to protect this information needs to be increased. The human element, however, remains a vulnerability of the system and it is this vulnerability that social engineers attempt to exploit. The Social Engineering Attack Detection Model version 2 (SEADMv2) has been proposed to help people identify malicious social engineering attacks. Prior to this study, the SEADMv2 had not been implemented as a user friendly application or tested with real subjects. This paper describes how the SEADMv2 was implemented as an Android application. This Android application was tested on 20 subjects, to determine whether it reduces the probability of a subject falling victim to a social engineering attack or not. The results indicated that the Android implementation of the SEADMv2 significantly reduced the number of subjects that fell victim to social engineering attacks. The Android application also significantly reduced the number of subjects that fell victim to malicious social engineering attacks, bidirectional communication social engineering attacks and indirect communication social engineering attacks. The Android application did not have a statistically significant effect on harmless scenarios and unidirectional communication social engineering attacks.