2016 IEEE International Conference on Big Data (Big Data), 5-8 December 2016, Bethesda, MD, USA

Reverse engineering smart card malware using side channel analysis with machine learning techniques

Hippolyte Djonon Tsague ; Bheki Twala

Abstract:

From inception, side channel leakage has been widely used for the purposes of extracting secret information, such as cryptographic keys, from embedded devices. However, in a few instances it has been utilized for extracting other information about the internal state of a computing device. In this paper, we exploit side channel information to recover large parts of the Sykipot malware program executed on a smart card. We present the first methodology to recover the program code of a smart card malware by evaluating its power consumption only. Besides well-studied methods from side channel analysis, we apply a combination of dimensionality reduction techniques in the form of PCA and LDA models to compress the large amount of data generated while preserving as much variance of the original data as possible. Among feature extraction techniques, PCA and LDA are very common dimensionality reduction algorithms that have successfully been applied in many classification problems like face recognition, character recognition, speech recognition, etc. with the chief objective being to eliminate insignificant data (without losing too much information) during the pre-processing step. In addition to quantifying the potential of the created side channel based disassembler, we highlight its diverse and unique application scenarios.