Abstract

Hassan Shokry El-Dib

QMS: Evaluating the Side-Channel Resistance of Masked Software from Source Code

Many commercial systems in the embedded space have shown weakness against power analysis based side-channel attacks in recent years. Designing countermeasures to defend against such attacks is both labor intensive and error prone. Furthermore, there is a lack of formal methods for quantifying the actual strength of a counter-measure implementation. Security design errors may therefore go undetected until the side-channel leakage is physically measured and evaluated. We show a better solution based on static analysis of C source code. We introduce the new notion of Quantitative Masking Strength (QMS) to estimate the amount of information leakage from software through side channels. The QMS can be automatically computed from the source code of a countermeasure implementation. Our experiments, based on side-channel measurement on real devices, show that the QMS accurately quantifies the side-channel resistance of the software implementation.