Abstract

Hassan Shokry El-Dib

Quantitative Masking Strength: Quantifying the Power Side-Channel Resistance of Software Code

Many commercial systems in the embedded space have shown weakness against power analysis-based side-channel attacks in recent years. Random masking is a commonly used technique for removing the statistical dependency between the sensitive data and the side-channel information. However, the process of designing masking countermeasures is both labor intensive and error prone. Furthermore, there is a lack of formal methods for quantifying the actual strength of a countermeasure 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. Once the user has identified the sensitive variables, the QMS can be automatically computed from the source code of a countermeasure implementation. Our experiments, based on measurement on real devices, show that the QMS accurately reflects the side-channel resistance of the software implementation.