Kurzfassung

Über Effiziente Praktische Seitenkanal-Kryptanalyse

Verbesserte Implementierungen, Neue Methoden, Anwendungen und Praxisrelevante Angriffe

Autor: Timo Bartkewitz

In dieser Arbeit legen wir besonderes Gewicht auf die Effizienz der Seitenkanal-Kryptanalyse. Zuerst demonstrieren wir wie die Laufzeit der wichtigsten Analysewerkzeuge, der Korrelationsbasierten Analyse (CPA) und der profilierenden Seitenkanalanalyse, besser bekannt als Template Angriffe (TA), mit Hilfe der kosteneffizienten CUDA Plattform erheblich gesteigert werden kann. Überraschenderweise hat man sich wissenschaftlich wenig mit hocheffizienten Werkzeugen auseinandergesetzt, obwohl es dringenden Bedarf in der Praxis gibt. Mit Teil II dieser Arbeit möchten wir den Fokus auf die Untersuchungen unserer vorgeschlagenen Implementierungen legen, mit welchen die Laufzeiten von mehreren Stunden auf wenige Sekunden reduziert werden können. Zweitens untersuchen wir neue Ansätze der profilierenden Seitenkanalanalyse. Diese Art der Analyse ist sicherlich die mächtigste, da sie auf realen statt modellbasierten Daten arbeitet. Der Forschungszweig des maschinellen Lernens kann für deutliche Verbesserungen adaptiert werden, wurde jedoch wenig dahingehend untersucht. In Teil III dieser Arbeit präsentieren wir zwei neue Methoden, die einige Gemeinsamkeiten jedoch auch einige Unterschiede aufbieten, sodass sich Prüfergebnisse in einem vollständigeren Bild zeigen lassen. Im Einzelnen ermöglicht die eine Methode die Trennung der zu profilierenden Information bei gleichzeitigem Verwerfen von kontraproduktiven Informationen. Die andere Methode nutzt die zu profilierende Information optimal aus, in dem sie deren Unbestimmtheit auf ein Minimum reduziert. Beiden Methoden ist gemein, dass sie eine eigene Datenraumreduktion bereitstellen, der eine wichtige Rolle bei der profilierenden Seitenkanalanalyse zukommt. Darüber hinaus schlagen wir in Teil IV eine Seitenkanalanwendung zum Schutz geistigen Eigentums (IP) vor. Sicherlich hat dies keinen Anteil an Prüfungen, jedoch steigt der Bedarf an Werkzeugen, die mögliche Fälschungen von IT Sicherheitsprodukten entlarven können. In Teil V beschäftigen wir uns tiefergehend mit praktischer Seitenkanal-Kryptanalyse, indem wir praktische Attacken durchführen, die uns die kompletten kryptographischen Schlüssel eines AES und eines DES Koprozessors gewinnen lassen. Diese Koprozessoren sind auf einem gehärteten Sicherheitsmikrokontroller implementiert, der Anwendung in einer, in Deutschland weit verbreiteten, EC Karte findet.