Neuartige Anwendungen für Seitenkanalanalysen auf eingebetteten Mikrocontrollern (Kurzfassung)

Daehyun Strobel

Seitenkanalanalysen werden nun schon seit fast 20 Jahren wissenschaftlich untersucht. Im Gegensatz zu einer klassischen Kryptanalyse, bei der eine Chiffre nach mathematischen Schwachstellen untersucht wird, handelt es sich bei der Seitenkanalanalyse um einen Angriff auf die physische Implementierung einer Chiffre. Dabei werden unterschiedliche Informationen analysiert, die von dieser Implementierung ausgehen, und meist mit statistischen Methoden ausgewertet, um einen kryptographischen Schlüssel zu berechnen. Diese sogenannten Seitenkanalinformationen bestehen i.d.R. aus Stromverbrauch, elektromagnetischer Abstrahlung oder Rechenzeit, können aber auch akustische Signale oder andere Quellen beinhalten.

Aufgrund dieser langen Zeit ist es etwas verwunderlich, dass die Forschung bisher fast nur in eine Richtung vorangetrieben wurde: Ein Großteil aller Veröffentlichungen zum Thema Seitenkanalanalyse befasst sich mit dem Angreifen von Implementierungen oder mit entsprechenden Gegenmaßnahmen. Weitere Anwendungsmöglichkeiten von Seitenkanalanalysen wurden hingegen nur selten untersucht. In dieser Arbeit werden Methoden und Algorithmen vorgestellt, die mit Hilfe von Seitenkanälen Informationen über ausgeführte Instruktionen von Mikrocontrollern erlangen. Dadurch eröffnen sich neue Anwendungen, die auf Basis von Mikrocontrollern bisher nicht durchführbar waren. Obwohl die Idee eines „Seitenkanal-Dissamblers“ nicht neu ist, bieten die bis dato veröffentlichten Ergebnisse keine ausreichende Genauigkeit, um praktische Anwendungsfelder zu ermöglichen.

Wir beginnen mit einem Verfahren, das Messungen des Stromverbrauchs analysiert, um Hamming-Gewichte von ausgeführten Opcodes (Instruktionen inklusive Operanden) zu extrahieren. Diese Hamming-Gewichte werden anschließend zu Strings zusammengeführt, wobei die Reihenfolge der ausgeführten Instruktionen beibehalten wird. Es wird gezeigt, wie man mit den auf diese Weise generierten Strings eine bekannte Seitenkanal-Gegenmaßnahme basierend auf zufälligen Delays überwinden kann. Im weiteren Verlauf wird das gleiche Konzept ausgenutzt, um mit Hilfe von String-Matching-Algorithmen Software-Plagiate zu erkennen.

Danach widmen wir uns einem Verfahren, das es ermöglicht auf Basis der Seitenkanalinformationen auf Instruktionen zu schließen. Mit Hilfe von geeigneten Klassifikationsalgorithmen werden hierbei Messungen der elektromagnetischen Abstrahlung eines Mikrocontrollers vorher definierten Instruktionsklassen zugeordnet. Wir erreichen dadurch eine Erkennungsrate von über 95 % auf Testdaten und über 87 % auf realen Code. Im Vergleich zu dem ersten Verfahren, erlaubt die Extraktion der Instruktionen eine genauere Abschätzung bei einer Untersuchung auf Plagiarismus. Die Ergebnisse können ebenfalls zur Erkennung von Chiffren, als Unterstützung beim Debugging oder etwa zur Sicherheitsanalyse verwendet werden.

Ein weiterer wesentlicher Teil diese Arbeit umfasst eine aufwendige Sicherheitsanalyse, die sich von der Thematik der Seitenkanalanalyse abhebt. Wir betrachten ein weitverbreitetes digitales Schließsystem, welches auf einem proprietären Authentifizierungsprotokoll basiert. Für die umfassende Analyse ist es notwendig gewesen, den Ausleseschutz des Mikrocontrollers zu überwinden sowie weite Teile des Protokolls zu rekonstruieren. Hierbei sind eklatante Sicherheitslücken zum Vorschein gekommen, die verschiedene Angriffe zulassen und somit das komplette System gefährden.