Kryptografie und Kryptoanalyse eingebetteter Systeme

Kurzfassung der Dissertation

Dipl.-Ing. Thomas Eisenbarth
Lehrstuhl eingebettete Sicherheit

Schon jetzt ist ein Großteil der Geräte des täglichen Bedarfs mit Rechenkapazität ausgestattet, so dass bereits heute mehr als 98 % aller hergestellten Prozessoren in eingebetteten Anwendungen verwendet werden. Aus der immer stärkeren Vernetzung eingebetteter Systeme resultiert die mögliche Verwundbarkeit dieser Systeme. Angriffe, die bisher nur gegen PCs ausgeführt wurden, können plötzlich gegen verschiedenste Systeme wie Autos, Fahrkarten oder sogar Herzschrittmacher ausgeführt werden. Gleichzeitig ist das Sicherheitsbewusstsein sowohl bei den Nutzern als auch bei den Herstellern dieser Systeme deutlich geringer als im PC-Bereich. Hierdurch werden Daten- und Kommunikationssicherheit zu Schlüsseleigenschaften eingebetteter Systeme. Da eingebettete Systeme normalerweise in großen Stückzahlen vertrieben werden, sind Kosten für Entwickler solcher Systeme von großer Bedeutung. Deshalb müssen Sicherheitslösungen für eingebettete Systeme günstig und effizient sein.

Der erste Teil dieser Arbeit untersucht Alternativen zu den vorherrschenden asymmetrischen Kryptosystemen wie RSA und ECC, deren Sicherheitsannahmen eng verwandt sind. Wird eine Sicherheitslücke in einem der vorherrschenden Verfahren aufgedeckt, werden mit hoher Wahrscheinlichkeit die meisten auf asymmetrischer Kryptografie basierender Systeme mit einem mal unsicher. Deshalb werden zwei alternative Signaturverfahren und ein asymmetrisches Verschlüsselungsverfahren aus der Familie der *Post-Quantum Kryptosysteme* untersucht. Die Sicherheit dieser Systeme beruht auf anderen Sicherheitsannahmen, so dass diese Systeme bei einer Sicherheitslücke in einem der vorherrschenden Verfahren gute Alternativen darstellen.

Der Hauptaugenmerk der Arbeit liegt auf den Implementierungsaspekten dieser Verfahren, die im Gegensatz zur vorherrschenden Meinung ähnliche oder sogar bessere Leistungsmerkmale aufweisen als die gängigen Verfahren. Zu den vorgestellten Lösungen gehört eine skalierbare Softwareimplementierung des Merkle-Signaturverfahrens, die auf kostengünstige Mikrocontroller abzielt. Des weiteren wird für Signaturen in Hardware ein Framework zur Implementierung einer Gruppe von Signaturverfahren, die auf multivariaten quadratischen Gleichungen beruhen, vorgestellt. Abhängig vom gewählten Verfahren dieser Gruppe zeigen multivariate Signaturen im Hinblick auf den Flächenverbrauch und den Durchsatz bessere Eigenschaften als elliptische Kurven. Das McEliece Verschlüsselungssystem ist ein alternatives Verfahren, von dem lange geglaubt wurde dass es auf eingebetteten Plattformen nicht implementerbar sei aufgrund der enormen Schlüsselgrößen. In dieser Arbeit wird gezeigt dass durch die vorgestellten Methoden nicht nur die Implementierung ermöglicht wird, sie sogar vergleichbare Leistungsmerkmale wie die gängigen Verfahren erreichen.

Der zweite Teil dieser Arbeit untersucht Methoden zur effizienten Analyse der Seitenkanalresistenz von eingebetteten Implementierungen. Durch die Anwendung von Simulationsmethoden wird die Möglichkeit zur Evaluation von Logistilen und Schaltungskonzepten gezeigt. Durch diese Methoden wird eine bisher unentdeckte Schwachstelle in MDPL und iMDPL, also Logikstilen, die bis jetzt als seitenkanalresistent galten, aufgedeckt. Des weiteren wird ein neuentwickelter Angriff auf die KeeLoq-Chiffre vorgestellt. Durch das Anwenden dieses Angriffs auf Keeloq-basierte Funktüröffnersysteme werden die möglichen Gefahren der Seitenkanalangriffe für eingebettete Systeme demonstriert. Hierdurch werden die Schwierigkeiten der praktischen Anwendung der Seitenkanalanalyse in einem black-box Szenario hervorgehoben und Lösungen aufgezeigt.

Abschließend werden fortschrittliche Techniken der Seitenkanalanalyse angewendet um nur durch die Messung seines Stromverbrauchs den Programmablauf eines Mikrocontrollers zu rekonstruieren. Die vorgestellten generischen Methoden können auf Mikrocontrollerplatformen angewendet werden um einen Disassembler mit einer annähernd optimalen Codeerkennungsrate zu bauen.

Schlagworte

Kryptographie, Assymetrische Kryptografie, Software, Hardware, Eingebettet, Sicherheit, Seitenkanalanalyse, Stromprofilanalyse, Disassembler.