Der Knackpunkt ist der Stromverbrauch: Ein Oszilloskop misst den Strom, während der Chip Verschlüsselungsoperationen durchführt.

Volle Breitseite

Pay-TV, Autotür oder Firmengelände – Zugang gewähren uns Smartcard oder Chip. Fraunhofer-Forscher testen die Sicherheit dieser eingebetteten Systeme und arbeiten an neuen Sicherheitsvorkehrungen.

Text: Stefanie Heyduck

Ein Alltag ohne Computer? Unvorstellbar. Nicht nur Arbeitsplatz und Heimnetzwerk werden von Rechnern gesteuert, selbst in EC-Karten, Smartcards, Mobiltelefonen und Autoschlüsseln sind winzige, komplexe Computersysteme am Werk – in der Fachsprache Embedded Systems, eingebettete Systeme, genannt. Auf ihren Chips sind persönliche Informationen, Zugangsberechtigungen oder Geldbeträge gespeichert – sensible Informationen.

Kriminelle haben ein lukratives Geschäft daraus gemacht, Informationen zu klauen und zu verkaufen. Besonders Anbieter von Pay-TV sind betroffen. Jeder Kunde erhält eine verschlüsselte Smartcard, mit der er sich an seiner Settop-Box ausweist und die Bezahlsender freischaltet. Gelingt es Kriminellen, nur einen dieser Schlüssel zu knacken, lässt sich die Karte kopieren und vielfach weiterverkaufen. Dem Anbieter entstehen Schäden in Millionenhöhe. Auch durch die steigende Vernetzung beispielsweise im Auto werden Viren, Würmer und Trojaner in naher Zukunft zum Problem für Hersteller.

Knackpunkt: Seitenkanal

In einem modernen Hardware-Labor untersuchen Forscher vom Fraunhofer-Institut für Sichere Informationstechnologie SIT die Sicherheit von eingebetteten Systemen. Am Standort Garching bei München testen, evaluieren, analysieren und entwickeln sie neue Sicherheitsmethoden. »Mit dem nötigen Aufwand lässt sich alles knacken – trotz starker Schlüssel«, erklärt Dr. Vitaly Ocheretny, Wissenschaftler am SIT. Ist der Aufwand jedoch zu hoch, lohnt es sich für die Kriminellen nicht, den Code zu hacken. Der kryptographische Algorithmus einer Karte beruht meist auf einem komplexen mathematischen Problem, das sich mit viel Rechenleistung und Zeit entschlüsseln lässt. »Sogar ein neuer Rechner würde mehrere Jahre brauchen, um alle wahrscheinlichen Ziffernkombinationen durchzuprobieren«, sagt Ocheretny. Deshalb setzen die Schlüsseldiebe auf eine neue Strategie: die Seitenkanalangriffe. Um einen kryptographischen Algorithmus auszuführen, benötigt der Chip eine bestimmte Zeit und verbraucht eine bestimmte Menge Energie. Diese Informationen haben auf den ersten Blick mit dem Sicherheitssystem nichts zu tun, helfen aber den Hackern, die Karte zu knacken.

»Wenn im amerikanischen Pentagon etwas passiert war, hat das die Presse dadurch erfahren, dass mehr Pizzalieferanten als üblich auf das Gelände fuhren«, beschreibt Dr. Frederic Stumpf, Bereichsleiter Embedded Security, das Phänomen des Seitenkanalangriffs. Im Labor erforschen die SIT-Wissenschaftler, wie Smartcards oder eingebettete Systeme sich verhalten, wenn man versucht, einen Schlüssel anzusprechen und ob eine Sicherheitslücke auftaucht.

Ocheretny untersucht den Stromverbrauch eines Chips, um dadurch den Schlüssel zu extrahieren. Ein Oszilloskop misst den Strom, während der Chip Verschlüsselungsoperationen durchführt. Hinterher geben die Messergebnisse Stück für Stück den kompletten Schlüssel preis.

Präziser und schneller ist die Technik, um die elektromagnetische Abstrahlung des Chips zu messen. Hier wird nur an einem bestimmten Punkt gemessen – genau dort, wo im Chip auf den Schlüssel, die PIN oder einen Geldbetrag zugegriffen wird.

Die kostspieligste Attacke ist der Fehlerangriff. Punkt für Punkt beschießt ein Laser das winzige Rechnersystem, um beispielsweise eine Leitung auf einer EC-Karte zu manipulieren. Dies kann dazu führen, dass die Überprüfung der PIN nicht mehr reibungslos funktioniert und eine falsche PIN akzeptiert werden würde. Mit dem Laser lässt sich der Mikrorechner auch nach Informationen abtasten, um Daten zu überschreiben oder zu verändern – zum Beispiel ließe sich so der Betrag auf einer Geldkarte beliebig erhöhen.

Während sich große Konzerne, die eingebettete Systeme in ihre Produkte einbauen, in der Regel ein eigenes Testlabor leisten, sind kleinere Firmen auf externes Know-how angewiesen. »Wir machen nicht nur angewandte Forschung, sondern stellen auch kleinen und mittelständischen Unternehmen unsere Leistungen zur Verfügung. Für Kunden führen wir Seitenkanalangriffe aus, erkennen Fehler und entwickeln Werkzeuge für neue Angriffsarten. Letzteres mit dem Ziel, dass Kunden ihre Hardware selbst auf Herz und Nieren prüfen können«, erklärt Stumpf. Die Experten arbeiten außerdem eng mit Branchengrößen wie Infineon und Giesecke & Devrient zusammen. Weitere Aufgaben sind: Sicherheitsstudien zu erstellen, Risiko- und Verwundbarkeitsanalysen durchzuführen sowie neue Technologien zu evaluieren. ■

Das Fraunhofer SIT in München

Cloud-Computing, eingebettete Systeme, Produktpiraterie oder aber auch vernetzte kritische Infrastrukturen stellen die Sicherheitsforschung vor ständig wachsende Herausforderungen. Im neuen Institutsteil des Fraunhofer SIT am Standort München arbeiten mittlerweile über 50 Mitarbeiterinnen und Mitarbeiter. Im Spannungsfeld zwischen wirtschaftlichen Erfordernissen, Benutzerfreundlichkeit und Sicherheitsanforderungen entwickeln sie Konzepte, Methoden, Werkzeuge und Lösungen, die für den jeweiligen Einsatzzweck am besten geeignet sind. Durch das neu aufgebaute Testzentrum in München stehen Testlabore zur Verfügung, um Sicherheits- und Zuverlässigkeitstests in erster Linie von Hardware, aber auch von Software-Komponenten und -Anwendungen, sowie Funktions-, Interoperations- und Konformitätstests durchzuführen.