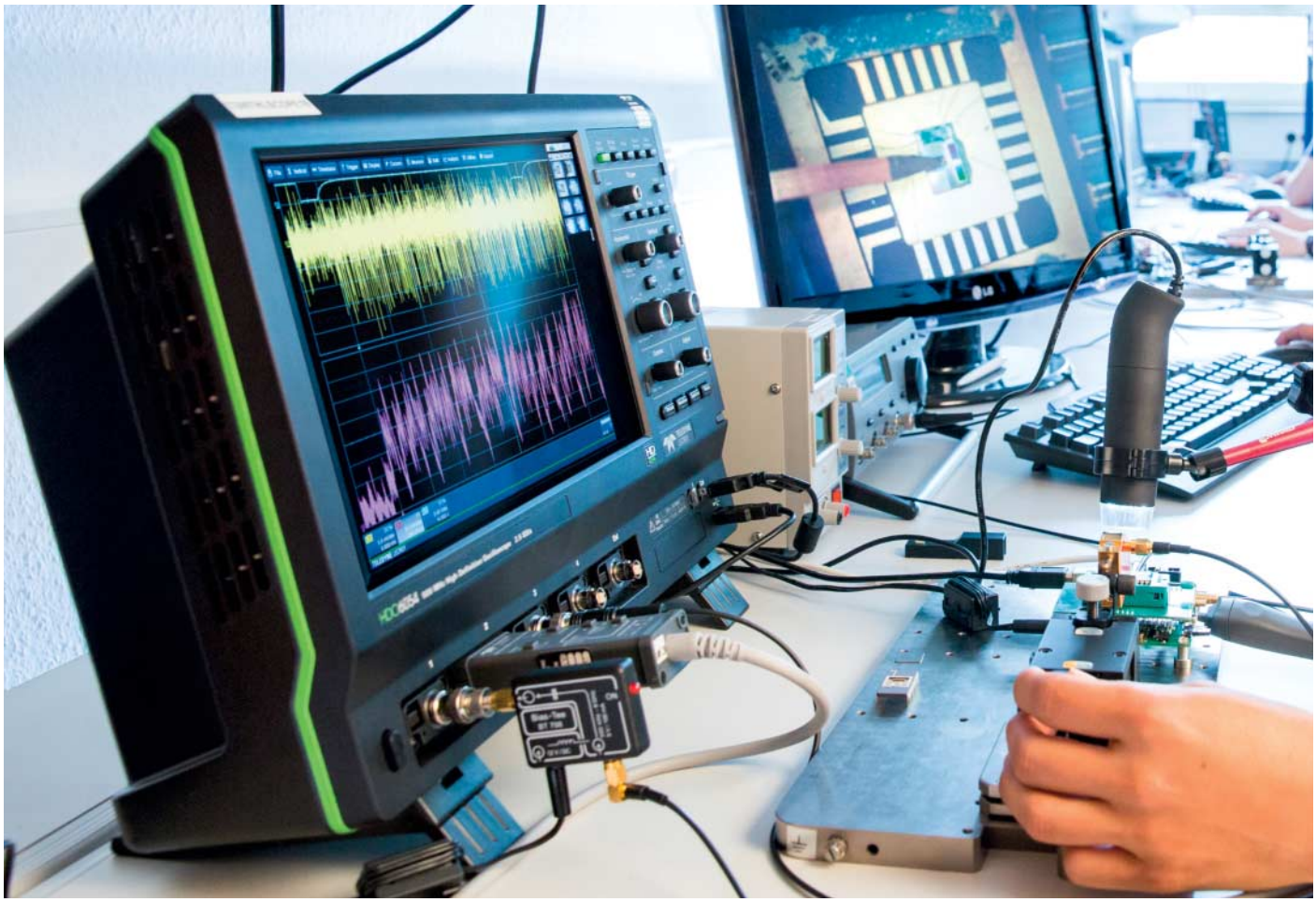

Bild: TÜViT

Unter Chip-Knackern

Sicherheits-Chips im Härtetest: Die „guten Hacker“ von TÜViT

Die Sicherheit von Chips prüft man am besten, indem man sie hackt. Die Spezialisten von TÜViT nutzen dazu empfindliche Messgeräte, Laserpulse und viel Erfahrung.

Von Christof Windeck

So mancher Chip-Entwickler fürchtet sich wohl insgeheim vor den Ideen der rund 50 Experten, die in einem nüchternen Zweckbau im Industriegebiet von Essen-Frillendorf arbeiten. Die Spezialisten des TÜViT traktieren Sicherheits-Chips mit Überspannung und Laserimpulsen, sie messen ihren Stromfluss und elektromagnetische Abstrahlungen. Die professionellen Hacker meinen es jedoch gut: Ihre Tests beweisen, welchen Angriffen die geprüften Chips widerstehen.

Die Sparte TÜViT des TÜV Nord verkauft Hacking als Dienstleistung und verteilt dafür Noten – sprich: Zertifizierungen, welche die Widerstandsfähigkeit des jeweiligen Chips belegen. Nur mit solchen Zertifikaten darf ein Sicherheitschip in kritischen Anwendungen eingesetzt werden: Als Kreditkarte, elektronischer Personalausweis, Smartphone-SIM, Gesundheitskarte, digitaler Fahrschein, Pay-TV-Karte, als TPM in einem Notebook oder als Hardware Security Module (HSM) im Server.

Kein Zutritt!

Chip-Sicherheit ist das Ergebnis vieler Fehler, aus denen die Entwickler lernen. Am Beispiel einer rund zehn Jahre alten SmartCard, die damals unter anderem zum Knacken von Pay-TV-Angeboten beliebt war, demonstrierten die TÜViT-Experten einen typischen Angriff. Dazu wurde die Karte mit einer 16-stelligen Geheimzahl beschrieben, die sie eigentlich sicher speichern sollte. Doch nach zehn Minuten war der Code entschlüsselt: Die Experten ließen die Karte in ihrem Prüfsystem 1000 geschickt gewählte Berechnungen ausführen und maßen unterdessen den Stromfluss. Aus der statistischen Verteilung der protokollierten Stromdaten lässt sich mit genügend Vorwissen das vermeintliche Geheimnis ermitteln.

Moderne SmartCard-ICs sind gegen diesen Angriff gefeit. Bei manchen lassen sich aber auf anderen Wegen Fehler provozieren, etwa durch Veränderung der Betriebsspannung, durch elektromagnetische Störfelder, durch Laserimpulse oder durch Erhitzung. Reproduzierbare Fehler erlauben Rückschlüsse auf die ausgeführ-

ten Berechnungen. Und so kann es wiederum möglich sein, dem Chip Geheimnisse zu entlocken.

Abgelauscht

Mit feinen Sonden messen die „Whitehat“-Hacker elektromagnetische Abstrahlungen des Chips, während dieser rechnet. Die Sonde muss dichter als einen Millimeter an den nur wenige Quadratmillimeter großen Chip heran. Der TÜViT muss dazu kein IC aus der Chipkarte ätzen, sondern bekommt es mundgerecht vom Hersteller serviert. Die Prüfungen finden für gewöhnlich schon während der Entwicklungsphase des Chips statt. Kein Hersteller kann es sich leisten, ein fast fertiges Produkt erst kurz vor der Massenproduktion testen zu lassen.

Die geprüften Chips stecken üblicherweise in Prototypengehäusen, damit die Magnetfeldsonde bequem herankommt. Ihr Messfeld deckt nur 80 bis 150 Quadratmikrometer ab, um einzelne Funktionsbereiche gezielt zu belauschen. Schrittmotoren verschieben den Chip im laufenden Betrieb unter dem Sensor, der Schritt für Schritt dessen Oberfläche abtastet: So entsteht eine Heatmap, die besonders aktive Bereiche enttarnt. Hier bohren die Techniker weiter: Mit dem Mikroskop fokussieren sie Laser auf bestimmte Recheneinheiten. Laserpulse stören deren Transistoren durch fotoelektrische Effekte synchron zum Rechentakt, der bei den modernsten Chipkarten-ICs einige hundert MHz betragen kann.

Die Untersuchungen können mehrere Wochen dauern. Die Auswertung der Ergebnisse braucht Monate. Meistens geht es dabei nicht um komplett neue Chips, sondern um Varianten älterer Designs. Nur etwa alle fünf bis acht Jahre kommen komplett neu entwickelte Sicherheits-Chips auf den Markt, schätzt TÜViT Managing Director Dirk Kretzschmar. Gegenüber bösen Hackern sehen sich die Essener Whitehats im Vorteil: Sie haben Zugriff auf die Baupläne der Chips und den Quellcode ihrer Firmware. Auch deren Analyse gehört zur Prüfung. Jenseits des Horizonts liegt die Bewertung der eigentlichen Krypto-Algorithmen, weil letztere durch die Spezifikationen vorgegeben sind: TÜViT untersucht nur, ob der Algorithmus korrekt implementiert wurde. Deshalb hätte man etwa die im Herbst 2017 veröffentlichte ROCA-Lücke im RSA-Algorithmus mancher TPMs nicht entdecken können.

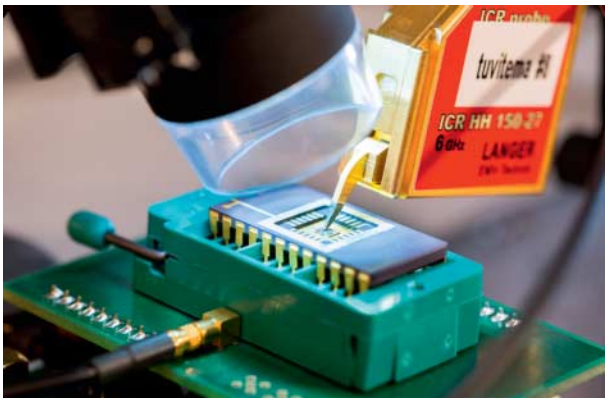

Bild: TÜViT

Der Magnetfeldsensor tastet Punkt für Punkt die Oberfläche des Smart-Card-Chips ab, um den Stromfluss der Rechenwerke zu belauschen.

Die für eine Anwendung nötige Vertrauenswürdigkeit und damit der Preis des Chips richtet sich nach der Art der vermuteten Angriffe und dem Budget. Noch heute, so die TÜViT-Experten, sind in vielen Bereichen relativ leicht angreifbare Chips im Einsatz. Das hängt mit der Langlebigkeit der Produkte und Systeme zusammen, in denen sie stecken, etwa in den Schlüsselkarten für elektronische Schlösser von Hotelzimmern. Pay-TV-Anbieter, die Knackversuche durch gut ausgestattete Handlanger der organisierten Kriminalität befürchten, verwenden besser gehärtete Chips.

Funkende Stromzähler

Der TÜViT prüft nicht nur Sicherheits-Chips, sondern etwa auch die Sicherheit ganzer Rechenzentren oder von Anwendungen und Systemen. Eines der aktuellen Projekte dreht sich in Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) um Datenschutz und sichere Kommunikation von Smart Meter Gateways (SMGW): Das sind die Netzwerk-Module, über die Smart Meter wie digitale Gas- und Stromzähler in Zukunft Verbrauchsdaten senden. Die Zählerdaten dürfen weder manipuliert werden noch in falsche Hände geraten [1].

Den Journalisten, die beim TÜViT hinter die Kulissen schauen – aber nicht fotografieren – durften, gab Dirk Kretzschmar noch einen Hinweise mit: „Wir suchen dringend Bewerber.“ *(ciw@ct.de)* c't

Literatur

[1] Mirko Dölle, Dem Zähler auf die Finger geschaut, Smart Meter mit c't Meterix ablesen, c't 12/2015, S. 46

Sicherheits-Chips

Bezahlfunktionen verlangen ein Secure Element: einen Hardware-Anker, der kryptografische Schlüssel und Zertifikate vor Manipulationen schützt und eine PIN zuverlässig prüft. Der Sicherheitschip erledigt die Krypto-Berechnungen unabhängig vom jeweiligen Computer, Lesegerät oder Bezahlterminal: Viren und Trojaner auf dem Computer kommen nicht an das eigentliche Geheimnis heran. Zunehmende Wartezeiten nach falscher PIN-Eingabe und eine begrenzte Zahl von Fehlversuchen machen kurze, komfortable PINs dermaßen sicher, dass Banken die Haftung in gewissen Grenzen übernehmen. Beim elektronischen Personalausweis speichert der Sicherheitschip biometrische Merkmale – Foto, Fingerabdruck – und gibt sie nur an zertifizierte Lesegeräte heraus. Dazu prüft er wiederum deren Zertifikate.

Sicherheits-Chips enthalten nichtflüchtigen Speicher, einen Prozessorkern und Rechenwerke für Krypto-Algorithmen wie AES und RSA. Ein Sicherheitschip darf sich nicht von Unberechtigten klonen lassen; es darf also nicht möglich sein, die in ihm gespeicherten Geheimnisse auszulesen und etwa in einen anderen, baugleichen Chip zu übertragen.

Für solche Sicherheitsfunktionen gibt es Spezifikationen wie Common Criteria mit den Stufen der Vertrauenswürdigkeit (Evaluation Assurance Level) von EAL 1 bis EAL7, FIPS 140 des US-NIST und EMV für Bezahlkarten – auch drahtlose – der EMVCo-Vereinigung großer Kreditkartenfirmen.