Timo Kasper, David Oswald, Christof Paar

Seitenkanalanalyse kontaktloser SmartCards

Berührungslose RFID-Technologie wird weltweit für verschiedenste sicherheitsrelevante Anwendungen wie den Identitätsnachweis oder Bezahlvorgänge eingesetzt. Nach der Aufdeckung von Schwachstellen im kryptografischen Schutz der „ersten Generation" kontaktloser SmartCards hoffte man auf die mit sicheren Chiffren versehenen Nachfolger. Der Beitrag zeigt die Anfälligkeit kontaktloser SmartCards für Seitenkanalangriffe am Beispiel des Mifare DESFire MF3ICD40.

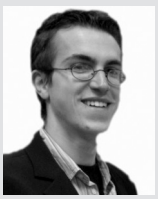
Einleitung

Sie sind mittlerweile allgegenwärtig und fast jeder benutzt sie nahezu täglich, ohne bewusst darüber nachzudenken – die Rede ist von kontaktlosen SmartCards, kleinen Prozessoren, die über eine Funkschnittstelle berührungslos kommunizieren und zugleich ihre Betriebsspannung beziehen.

Die technischen Vorteile der zugrunde liegenden RFID-Technologie (*Radio Frequenz Identifikation* [Fin03]) sind offensichtlich: Da die Lesegeräte (*Reader*) die Energie zur Verfügung stellen, entfällt die Notwendigkeit für eine wartungsanfällige Batterie. Dank der drahtlosen Kommunikation werden außerdem keine Kontakte benötigt, die bei längerem Einsatz unweigerlich abnutzen und verschmutzen – ein auf den ersten Blick unscheinbares Problem, das dennoch (z. B. Fehlfunktionen bei kontaktbasierten EC-Karten) früher oder später zum Ärgernis oder gar Verhängnis werden kann. Die Funktechnologie bringt neben technischen Vorzügen auch neuen Komfort in etablierten Anwendungen mit sich, z. B. das bargeldlose Bezahlen durch Wedeln der Handtasche oder Geldbörse vor dem Lesegerät, ohne die Karte heraussuchen zu müssen.

Dipl. -Ing. Timo Kasper

Wiss. Mitarbeiter am Lehrstuhl für Embedded Security Ruhr-Universität Bochum (HGI)
E-Mail: Timo.Kasper@rub.de
Dipl.-Ing.



David Oswald

Wiss. Mitarbeiter am Lehrstuhl für Embedded Security, Ruhr-Universität Bochum (HGI)
E-Mail: David.Oswald@rub.de

Prof. Dr.-Ing. Christof Paar

Inhaber des Lehrstuhls für Embedded Security, Ruhr-Universität Bochum (HGI)
E-Mail: Christof.Paar@rub.de

1 Anwendungen

Längst sind die im ISO 14443-Standard [Int01] spezifizierten kontaktlosen SmartCards die Grundlage einer Vielzahl von Systemen. Sie ersetzen zunehmend das klassische, „papierbasierte" Monatsticket im öffentlichen Nahverkehr, dienen als elektronische Zahlungsmittel und regeln in vielen Firmen die Zugangskontrolle. Dazu kommen hoheitliche Anwendungen wie der elektronische Reisepass (ePass) und der zuletzt vermehrt in den Fokus der Öffentlichkeit gerückte neue Personalausweis (ePA) – auch hier bilden kontaktlose SmartCards den Vertrauensanker und bestimmen damit das Sicherheitsniveau.

So vielfältig wie die Einsatzgebiete sind die mittlerweile verfügbaren Produkte: Während in weniger sicherheitskritischen Bereichen oft nur eine einfache Kennziffer zur Identifizierung gespeichert wird, verfügen die neuesten Generationen über zahlreiche kryptografische Funktionen. Ein moderner ePass oder ePA verwendet beispielsweise Triple-DES und elliptische Kurven in komplexen, mehrstufigen Authentifizierungsprotokollen [BSI10].

2 Sicherheitsrisiken

RFID-basierte, kryptografische SmartCards sind fraglos auf dem besten Weg, Bestandteil nahezu aller alltäglich genutzten sicherheitsrelevanten Systeme zu werden – sei es als Schlüssel, Geldbörse oder Identitätsnachweis. Dementsprechend rücken Sicherheitsfragen mehr und mehr in den Vordergrund. Doch welche Risiken entstehen im Bereich von RFID-Systemen und was sind mögliche Angriffsziele?

Dabei ergibt sich zunächst eine grundlegende Unterscheidung zwischen Bedrohungen für den Nutzer auf der einen und für den Systembetreiber auf der anderen Seite. Aus Sicht des Benutzers steht der Schutz der oft personenbezogenen gespeicherten Daten im Vordergrund. Schließlich lässt sich der Zugriff auf eine Karte im Fall von funkbasierter Kommunikation niemals vollständig rein physikalisch kon-

trollieren, so dass das unbemerkte Auslesen eines Chips – wenn keine Schutzmechanismen vorhanden sind – aus einiger Entfernung durchaus realistisch ist [Han06, BSI08]. Zudem kann auch finanzieller Schaden für den Nutzer entstehen, man denke hier nur an die elektronische Variante des Taschendiebstahls, bei der der Dieb vollständig unbemerkt z. B. eine Kopie einer kontaktlosen Kreditkarte anfertigt [KSP10].

Weitaus größer ist diese Gefahr aus Sicht des Systembetreibers: Wenn Schwachstellen einem Angreifer die Manipulation oder Duplizierung („Klonen") von Karten ermöglichen, kann je nach Anwendungsgebiet ein erheblicher (finanzieller) Gesamtschaden entstehen. Ebenso gravierend sind die Auswirkungen im Fall von Identifikations- und Zugangskontrollsystemen. Da angesichts der vermeintlich sicheren Technologie oft auf eine zusätzliche Kontrolle von optischen Echtheitsmerkmalen verzichtet wird, ist eine geklonte SmartCard ein rein technisch kaum erkennbarer „Zweitschlüssel". Und dass bei elektronischen Ausweisen Fälschungssicherheit an erster Stelle steht, bedarf wohl kaum einer Erwähnung.

3 Rückblick

Um die mit kontaktlosen SmartCards in der Praxis verbundenen Sicherheitsprobleme zu verstehen, lohnt ein Blick in die Geschichte der Produkte der „ersten" Generation. Karten wie Mifare Classic oder Legic Prime bildeten seit Mitte der neunziger Jahre (mangels Alternativen) die Grundlage für nahezu alle RFID-basierten Bezahl- und Zugangskontrollsysteme. Gemein ist diesen Chips, dass die Sicherheit auf proprietären und geheim gehaltenen Chiffren beruht, d. h. die eingesetzten Verschlüsselungsverfahren nie einer öffentlichen und objektiven Evaluierung durch die internationale Forschergemeinschaft unterzogen wurden. Es kam wie es kommen musste: Nachdem es Forschergruppen 2008 bzw. 2010 gelang, die Chiffren durch Untersuchung der Hardware zu „reverse-engineeren", fanden sich innerhalb weniger Monate gravierende mathematische Schwachstellen sowohl in Mifare Classic [NESP08, Cou09] als auch in Legic Prime [PN09].[1] Auf diesen Produkten basierende Systeme können heute innerhalb weniger Minuten mit minimalem Aufwand und Know-How geknackt werden.

Neue Anwendungen setzen daher vermehrt auf moderne Produkte, die mathematisch starke Chiffren wie Triple-DES, AES, RSA oder ECC bereitstellen. Das Risiko, Opfer von klassischen kryptoanalytischen Angriffen zu werden, ist dadurch überschaubar, beißen sich doch weltweit schon seit Jahrzehnten zahllose Forscher mehr oder weniger erfolglos die Zähne an diesen Verfahren aus. Zwar kann nie ausgeschlossen werden, dass unerwartet eine moderne Chiffre zu Fall gebracht wird – dennoch ist die Wahrscheinlichkeit dafür sehr gering, ganz abgesehen davon, dass selbst dann noch sichere Alternativen zu Verfügung stünden.

4 Sicherheit in Theorie und Praxis

Dennoch sind, wie so oft im Leben, nicht alle Gefahren gebannt und jegliche Probleme gelöst. Neue Angriffsmethoden nutzen aus, dass jede mathematisch noch so sichere Chiffre physikalisch implementiert werden muss und damit für einen Angreifer beobachtbar wird. Über einen Seitenkanal, wie z. B. die Stromaufnahme oder die elektromagnetische Abstrahlung eines Mikroprozessors, lassen sich daher ggf. Rückschlüsse auf interne Abläufe in den Schaltkreisen des analysierten Geräts ziehen. In der Folge können, trotz ungebrochener mathematischer Sicherheit des Verfahrens, Geheimnisse wie kryptografische Schlüssel oft in Minuten extrahiert werden.

Das Prinzip der Seitenkanalanalyse ist vergleichbar mit dem Vorgehen eines Tresorknackers, der mit einem Stethoskop auf das mechanische Klicken der Zahnräder hört, um die richtige Kombination zum Öffnen des Safes zu finden. Durch Beobachtung des Schall-Seitenkanals erspart sich der Dieb das mühsame Durchprobieren aller möglichen Kombinationen und kann den korrekten Öffnungscode wesentlich schneller ermitteln. Bei einem Siliziumchip hilft ein Stethoskop wenig (obwohl es tatsächlich akustische Angriffe gibt [ST]); zum Auffangen des elektrischen Seitenkanals dient ein Oszilloskop, während ein handelsüblicher PC, der die aufgenommenen Signale statistisch auswertet, an die Stelle des Tresorknackers tritt. Belauscht werden also nicht die Geräusche einer Mechanik, sondern das Umschalten der zahllosen Transistoren auf dem Chip, die durch ihre Verschaltung den Verschlüsselungsalgorithmus umsetzen. In Abhängigkeit von den verarbeiteten Daten (z. B. Null oder Eins) ist der Leistungsverbrauch, der aus dem Stromverbrauch oder der elektromagnetischen Abstrahlung abgeleitet werden kann, grundsätzlich verschieden.

Die Seitenkanalanalyse ist ein junges Forschungsfeld. Erst kurz vor der Jahrtausendwende publizierten Forscher die Konzepte [KJJ99], die heute die Grundlage für die meisten Veröffentlichungen in diesem rasch wachsenden Gebiet bilden. Zwar war die Beobachtung, dass elektronische Schaltungen auswertbare Signale abstrahlen, in Militär- und Regierungskreisen schon seit dem Ende des zweiten Weltkriegs bekannt (z. B. im lange geheimen TEMPEST-Programm [NSA07]), doch wurde dabei der statistische Trick übersehen, der die Seitenkanal-Analyse heute zu einer universellen Gefahr für kryptografische Geräte macht.[2]

In der Kryptologie bewährt sich seit langem ein Wechselspiel zwischen den Disziplinen der Kryptografie, die kryptografische Verfahren erfindet, und der Kryptoanalyse, also dem Brechen von Verschlüsselungsverfahren. Indem die von Kryptoanalysten gefundenen Schwachstellen in den Algorithmen oder modellierten Systemen von Kryptografen geschlossen werden, können langfristig sichere Verfahren entwickelt werden. Ein Verfahren wird schließlich genau dann als (höchstwahrscheinlich theoretisch) sicher angesehen, wenn es seit langer Zeit veröffentlicht ist und kein Forscher eine Sicherheitslücke entdecken konnte.

Für den praktischen Einsatz einer solchen theoretisch sicheren Chiffre wird diese in einer elektrischen Schaltung realisiert und in ein Gesamtsystem integriert. In dieser Umgebung treten neue Angriffsvektoren und Schwachstellen auf, die in der reim mathematischen Betrachtung nicht berücksichtigt wurden. Beispielsweise erlauben physikalische Angriffe wie Fehlerinjektionen, Seitenkanalanalysen und Reverse-Engineering häufig, die geheimen Schlüssel aus mathematisch unknackbaren Verfahren zu extrahieren.

Entsprechend ist für die Entwicklung sicherer Produkte in der Praxis ein Wech-

1 Siehe auch Fox, Die Mifare-Attacke, DuD 5/2008, S. 348-350.

2 Mehr zu Seitenkanalanalysen siehe Kasper/Kasper/Moradi/Paar, in diesem Heft.

selspiel zwischen Sicherheitsanalysen und anschließenden Verbesserungen erforderlich, um ein hohes Schutzniveau zu erreichen – diesmal jedoch in der realen Welt und nicht der des mathematischen Spielplatzes.

Die Veröffentlichungen über Angriffe auf konkrete Implementierungen von Kryptografie blieben lange Zeit weitgehend theoretischer Natur, nachdem viele Hersteller ihre Produkte scheinbar ausreichend abgesichert hatten. Die reale Bedrohung erschien überschaubar – fast zehn Jahre nach den ersten Publikationen zu Seitenkanalanalysen gab es kein bedeutendes kommerzielles System, das mit dieser Methode gebrochen wurde.

Im Jahr 2008 wurde schließlich ein erster praxisnaher Seitenkanalangriff auf das KeeLoq-System[3] vorgestellt [Eis08], das in zahlreichen Garagen- und Türöffnern zum Einsatz kommt. Seitdem ist ein Trend in der Wissenschaft erkennbar, auch kommerzielle Produkte praktischen Sicherheitsanalysen, insbesondere im Hinblick auf physikalische Angriffe zu unterziehen. Nur so können der Aufwand möglicher Angriffe abgeschätzt, vorhandene Sicherheitsrisiken aufgezeigt und frühzeitig durch Gegenmaßnahmen behoben werden, bevor Schaden durch Kriminelle entsteht.

Dass sich dieser Trend zu mehr Praxisrelevanz fortsetzt, verdeutlicht auch die vorliegende Analyse. Die Autoren hoffen, damit einen positiven Beitrag zur korrekten Bewertung und zukünftigen Verbesserung der Sicherheit der untersuchten Produkte zu leisten und gleichzeitig den Anwender für mögliche Systemschwächen zu sensibilisieren.

Der im Folgenden vorgestellte Seitenkanalangriff zielt auf moderne kontaktlose SmartCards mit integrierter Triple-DES-Verschlüsselung und ermöglicht die (auf mathematischem Weg unmögliche) vollständige Extraktion der kryptografischen Schlüssel innerhalb weniger Stunden.

5 Seitenkanalanalyse von Mifare DESFire

Im Blickpunkt der Sicherheitsanalyse steht Mifare DESFire MF3ICD40, eine kontaktlose SmartCard, die oft als sichere Alternative zur gebrochenen Mifare Classic empfohlen wird. Der Chip verfügt über eine Implementierung von Triple-DES, die sowohl zur Authentifizierung zwischen SmartCard und Reader (zwecks Echtheitsprüfung) als auch zur Datenverschlüsselung (Schutz der Benutzerdaten) dient.

Aufgrund der geringen Stückkosten (im Bereich von einem Euro), der Anpassungsfähigkeit an verschiedene Anwendungen und nicht zuletzt der aus theoretischer Sicht starken Kryptografie hat die Karte weite Verbreitung gefunden. Neben großen Systemen mit zehntausenden Nutzern im öffentlichen Nahverkehr (z. B. in Prag und San Francisco) wird Mifare DESFire in diversen kleineren Installationen z. B. als elektronisches Zahlungsmittel oder zur Zugangskontrolle eingesetzt.

Die Sicherheit beruht dabei zunächst auf der Geheimhaltung des 112-bit-Triple-DES-Schlüssels. Wird dieser bekannt, kann ein Angreifer Karten auslesen, manipulieren und klonen. Schutzmaßnahmen auf Systemebene können die Konsequenzen zwar auch in diesem Fall durchaus wirksam abfedern und den Schaden minimieren (mehr dazu am Schluss dieses Beitrags); nichtsdestoweniger eröffnet die Extraktion des Schlüssels einem Angreifer zahlreiche Möglichkeiten, das Sicherheitskonzept ins Wanken zu bringen.

Das genaue Risiko hängt natürlich vom Einzelfall und der Sensitivität der Anwendung ab, unabhängig davon gilt jedoch die Aussage: Das schwächste Glied bestimmt zunächst die Sicherheit des Gesamtsystems.

5.1 Messumgebung

Nach der recht ausführlichen Diskussion der Historie und möglicher Risiken – die dem tieferen Verständnis der Tragweite der im Folgenden vorgestellten Methode dient – folgt nun der konkrete Ablauf der Seitenkanalanalyse von Mifare DESFire-Karten.

Anders als bei kontaktbasierten SmartCards ist der genutzte Seitenkanal dabei nicht unmittelbar der Stromverbrauch, sondern das elektromagnetische Feld in der Umgebung der Karte. Der Grund für diesen Ansatz liegt in der kontaktlosen Übertragung der Betriebsenergie – um die Stromaufnahme direkt zu messen, wäre ein nachträglich feststellbarer und ggf. zerstörerischer invasiver Eingriff in die Karte erforderlich. Im Gegensatz dazu kann die Messung des elektromagnetischen Feldes mit einer in der Nähe des Chips der Karte positionierten Messsonde komplett *nicht-invasiv* erfolgen und hinterlässt damit keine im Nachhinein forensisch auswertbaren Spuren.

Allerdings ergibt sich ein RFID-spezifisches Problem: Die Kommunikation und Energieübertragung erfolgt über ein vom Reader erzeugtes Feld mit einer Frequenz von 13.56 MHz, das zunächst wie ein Störsignal wirkt und jede Ad-Hoc-Analyse zum Scheitern verurteilt – die winzige informationstragende Abstrahlung des Chips ist um mehrere Größenordnungen geringer und geht daher völlig im Störsignal unter.

Trotzdem lässt sich der elektro-magnetische Seitenkanal nutzen: Der Trick liegt hier in der Entwicklung spezieller Filterschaltungen, die die auswertbaren Signalanteile vom störenden Feld trennen. Das Prinzip gleicht dem eines normalen analogen Radioempfängers, der auf den speziellen Frequenzbereich von kontaktlosen SmartCards angepasst ist. Nachdem das gewünschte Seitenkanal-Signal isoliert wurde, erfolgt eine Verstärkung, bevor ein PC-basiertes Oszilloskop die analogen Werte digitalisiert und zur anschließenden Auswertung speichert.

Bezogen auf den bereits bemühten Vergleich mit einem Tresor entspricht die Messsonde dem Stethoskop, Filterschaltung und Verstärker einem geübten Gehör, und der PC ersetzt die Auswertung der Signale im Gehirn des Diebes.

5.2 Statistische Auswertung

Ist der Seitenkanal einmal entdeckt, wird wiederholt auf der SmartCard eine Verschlüsselung mit Triple-DES angestoßen und das gefilterte elektromagnetische Feld gemessen – im konkreten Fall der DESFire wiederholt man diesen Vorgang ca. 250.000 Mal. Auch wenn diese Zahl auf den ersten Blick enorm erscheint (zum Klonen eines KeeLoq Funktüröffners genügen ca. zehn Stromkurven), können die notwendigen Messungen in wenigen Stunden durchgeführt werden, da jede Verschlüsselung nur wenige Millisekunden in Anspruch nimmt.

An dieser Stelle sei erwähnt, dass es unvermeidbar ist, die Verschlüsselungsfunktionalität von außen wiederholt abrufbar zu machen: Sie ist elementarer Bestandteil des ersten Schrittes einer jeden Authentifizierung, sprich erst nach Ausführung

3 Siehe auch Eisenbarth/Kasper/Paar, Sicherheit moderner Funktüröffnersysteme, DuD 8/2008, S. 507-510.

der Chiffre kann die SmartCard feststellen, ob sie mit einem potentiellen Angreifer spricht. Eine Zählung der Fehlversuche mit Sperrung (ähnlich der PIN-Eingabe am Geldautomaten) ist zwar vorstellbar, würde jedoch die Wartungsanfälligkeit der Karten drastisch erhöhen bzw. ihre Lebensdauer verringern, denn im Gegensatz zu kontaktbasierten Karten sind Fehler aufgrund der störanfälligen Funkverbindung an der Tagesordnung, sodass Sperrungen langfristig den häufigen Austausch von Karten erfordern würden.

Die abschließende statistische Auswertung der gemessenen Signale erfolgt „offline" durch Analyse der aufgenommenen Messkurven am PC, ohne dass weiter ein physikalischer Zugang zur Karte erforderlich ist. Zu Beginn ist die Analyse mühsam und erfordert viele Experimente, da außer der verwendeten Chiffre nichts über die tatsächliche Umsetzung der Verschlüsselung auf der Karte bekannt ist. Ist einmal die interne Realisierung verstanden – was in der Praxis Monate geduldigen Ausprobierens in Anspruch nimmt – steht der Extraktion eines Triple-DES Schlüssels aus DESFire MF3ICD40-Karten nichts mehr im Wege. Im Labor der Autoren wurde der Vorgang inzwischen vollständig automatisiert: Nach Einlegen einer beliebigen DESFire MF3ICD40-Karte wird der gesuchte Schlüssel vom PC nach ca. einem Tag preisgegeben. Die Reproduzierbarkeit unserer Methoden wurde anhand verschiedener kommerzieller Systeme verifiziert.

Alles, was der Angreifer benötigt, ist temporärer Zugang zur SmartCard, um die beschriebenen Messungen durchzuführen. Entweder wird dazu die Karte eines Opfers für beschränkte Zeit entwendet, oder – was in der Praxis der wahrscheinlichere Fall ist – erfolgt die Attacke durch einen Insider. Im Fall von Zahlungssystemen oder elektronischem Ticketing ist schließlich jeder Nutzer ein potentieller Angreifer mit vollem Zugriff auf mindestens eine Karte. Die Motivation ist ebenso klar, man denke hier an das „Aufladen" einer Kreditkarte oder die Fälschung einer kostspieligen Monatsfahrkarte. Im Extremfall sind mafiaartige Strukturen vorstellbar, die das Klonen von kontaktlosen SmartCards in ein lukratives Geschäft verwandeln könnten.

5.3 Aufwand

Zur Extraktion des 112-bit-Schlüssels aus einer Mifare DESFire MF3ICD40 sind einige Stunden für Messungen erforderlich, die anschließende Datenauswertung hat einen ähnlichen Zeitaufwand. Anzumerken ist, dass die Analyse der Messdaten in diesem Beispiel auf einem handelsüblichen PC ausgeführt wird – schnellere Hardware kann die für die Auswertung benötigte Zeit erheblich reduzieren.

Die Dauer der Messungen wird hingegen wesentlich von der Kommunikation mit der SmartCard bestimmt, die erheblich länger dauert als der eigentliche Verschlüsselungsvorgang. Dennoch ist eine Reduktion des benötigten Messzeitraums möglich, wenn verbesserte Auswertungsmethoden mit einer geringeren Anzahl von Wiederholungen (statt der erwähnten 250.000) entwickelt würden. Wie bei jeder Sicherheitslücke gilt: Wenn die prinzipielle Machbarkeit nachgewiesen ist und ausreichende Motivation für Angreifer besteht, sind weitere Verbesserungen bezüglich der Effizienz der Angriffe sehr wahrscheinlich.

Doch schon in der aktuellen Form ist die Schlüsselextraktion von einem Angreifer in realistischer Zeit und mit geringem Budget umsetzbar. Die Kosten für die benötigten Gerätschaften bewegen sich im Bereich von einigen tausend Euro. Mit dem erforderlichen Ingenieurswissen lässt sich ein geeigneter Messplatz [KOP10] nachbauen und die in den entsprechenden Veröffentlichungen [OP11] detailliert beschriebene Vorgehensweise reproduzieren.

5.4 Gegenmaßnahmen

Damit stellt sich die Frage, wie sich auf verwundbaren kontaktlosen SmartCards basierende Systeme wirkungsvoll vor einem solchen Seitenkanalangriff schützen lassen.

An erster Stelle sei hier empfohlen, stets auf die aktuellste Produktgeneration zurückzugreifen – so bietet NXP, der Hersteller der DESFire MF3ICD40, mittlerweile den Nachfolger DESFire EV1 an, dessen zahlreiche Gegenmaßnahmen zum Schutz vor Seitenkanalanalysen im Rahmen einer EAL-Zertifizierung evaluiert und getestet wurden. Auch wenn die Zertifizierung natürlich niemals alle (ggf. noch nicht entdeckten) Angriffsmöglichkeiten abdecken kann, garantiert sie trotzdem ein mehr als gutes Sicherheitsniveau – und so sind bislang keine Angriffe gegen DESFire EV1 bekannt.

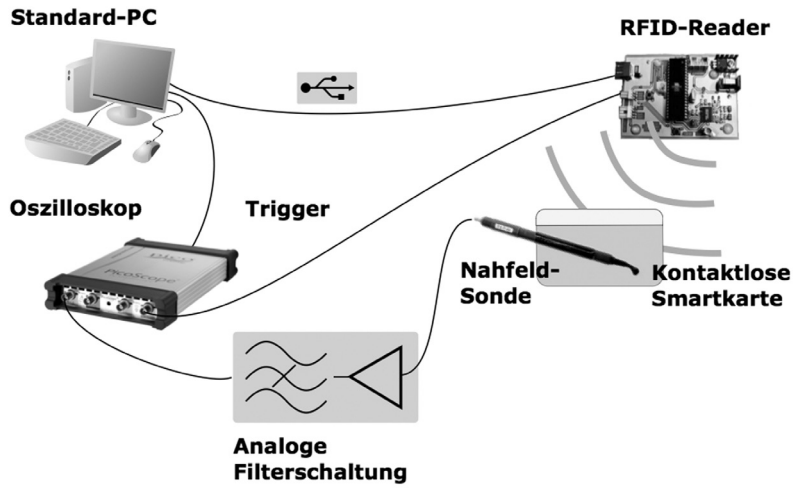
Darüber hinaus ist auch dann noch nicht alles verloren, wenn eine Seitenkanalschwachstelle vorliegt. Man bedenke hier, dass nur die auf der konkret analysierten Karte vorhandenen Schlüssel ermittelt werden können. Wenn folglich jede Karte im System über einen individuellen, „diversifizierten" Satz von Schlüsseln verfügt, kompromittiert die Extraktion dieser Schlüssel genau eine Karte. Im Klartext: Für den Zugriff auf eine weitere Karte im System muss der Mess- und Auswerte-Vorgang komplett wiederholt werden.

Eventuell können Duplikate der ausgelesenen Karte erstellt werden – diese können jedoch häufig durch geeignete Maßnahmen auf Systemebene identifiziert und gesperrt werden.

Älteren RFID-Systemen wurde der Verzicht auf kartenindividuelle Schlüssel oft zum Verhängnis. Da alle SmartCards den gleichen Schlüssel benutzten, fiel mit einem erfolgreichen Angriff auf eine Karte das gesamte Sicherheitssystem. Heute weiß man um dieses Problem und es gibt effiziente Möglichkeiten, die Schlüsselverteilung zu realisieren – dennoch finden sich noch immer kommerzielle Anwendungen, in denen dieser eigentlich vermeidbare, fatale Fehler gemacht wird [KSP10].

Als weitere Maßnahme im Hintergrundsystem empfiehlt sich das Führen sogenannter Schattenkonten. Dabei existiert eine geschützte Datenbank, in der alle schützenswerten Informationen (z. B. Geldbeträge, Zugangsrechte usw.) abgelegt sind, um mit den auf den SmartCards gespeicherten Daten abgeglichen zu werden. Damit lassen sich Manipulationen erkennen, führen sie doch zu Inkonsistenzen zwischen Schattenkonto und Karte. Im Rahmen von automatischen, routinemäßigen Prüfungen fällt die fehlende Übereinstimmung unmittelbar auf. In Reaktion kann der Sachverhalt weiter untersucht und die betroffene SmartCard vorläufig gesperrt werden. In Erweiterung dieses Prinzips lassen sich zusätzliche Ebenen schaffen, die nahezu jede Art der Manipulation und Duplikation fast unmöglich machen, einen guten Überblick gibt hier [NPR10].

Abbildung 1 | Typischer Messaufbau für die Seitenkanalanalyse kontaktloser SmartCards mit RFID-Reader, Oszilloskop und analogen Filterschaltungen.



6 Quo vadis, Sicherheit?

Eine vollständige Entwarnung kann jedoch nie gegeben bzw. 100-prozentige Sicherheit nicht erreicht werden. Mit verbesserten Produkten werden auch die Methoden der Angreifer besser. Dementsprechend ergibt sich auch für hardwarebasierte Sicherheit mehr und mehr eine Situation wie im Bereich von Software, in dem die stetige Bedrohung aus dem Internet durch Viren, Trojaner u. ä. längst alltäglich geworden ist.

Glücklicherweise lässt sich aus zuvor gemachten Fehlern lernen: Während die Sicherheitsproblematik von Seiten der Betriebssystementwickler lange ignoriert wurde, sind sich viele Hersteller von Hardwareprodukten (also z. B. kontaktlosen SmartCards) der möglichen Angriffsvektoren bewusst und reagieren frühzeitig auf aufkommende Schwachstellen und Angriffsmethoden.

Und auch die Einschätzung von Sicherheitsanalysen in der akademischen Welt entwickelt sich weiter. Während Software-Sicherheit lange zu Unrecht nicht als ernstzunehmendes Forschungsthema angesehen wurde und „Hacker“ als grundsätzlich kriminell galten, ändert sich die Wahrnehmung hier zusehends. Gerade auf dem Gebiet der Analyse und insbesondere des Schutzes von Hardwarekomponenten existiert eine aktive internationale Forschungsgemeinde, die öffentlich auf mögliche Schwachstellen hinweist, bevor andere sie unerkannt und böswillig ausnutzen können.

Literatur

[BSI08] Bundesamt für Sicherheit in der Informationstechnik. Messung der Abstrahleigenschaften von RFID-Systemen, Version 2.05. Technical report, 2008. https://www.bsi.bund.de/ContentBSI/Themen/Elekausweise/rfid/MarsStudie/marsstudie.html

[BSI10] Bundesamt für Sicherheit in der Informationstechnik. TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents. Technical Guideline TR-03110, V. 2.05 https://www.bsi.bund.de/DE/Themen/ElektronischeAusweise/elektronischeausweise_node.html

[Cou09] Nicolas Courtois. The Dark Side of Security by Obscurity - and Cloning MiFare Classic Rail and Building Passes, Anywhere, Anytime. In SECRYPT, pages 331–338. INSTICC, 2009.

[Eis08] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M. T. M. Shalmani. On the Power of Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme. In CRYPTO 2008, volume 5157 of LNCS, pages 203-220. Springer.

[Fin03] Klaus Finkenzeller. RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification. John Wiley and Sons, 2nd edition, 2003.

[Han06] Gerhard P. Hancke. Practical Attacks on Proximity Identification Systems (Short Paper). In IEEE Symposium on Security and Privacy 2006. http://www.cl.cam.ac.uk/~gh275/SPPractical.pdf

[Int01] International Organization for Standardization (ISO). ISO/IEC 14443: Identification Cards - Contactless Integrated Circuit(s) Cards - Proximity Cards – Part 1-4, 2001. www.iso.ch

[KJJ99] P. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In CRYPTO 99, volume 1666 of LNCS, pages 388-397. Springer, 1999.

[KOP10] Timo Kasper, David Oswald, and Christof Paar. A Versatile Framework for Implementation Attacks on Cryptographic RFIDs and Embedded Devices. Volume 10 of Transactions on Computational Science, LNCS 6340, pages 100–130. Springer, 2010.

[KSP10] Timo Kasper, Michael Silbermann, and Christof Paar. All You Can Eat or Breaking a Real-World Contactless Payment System. In Financial Cryptography 2010, volume 6052 of Lecture Notes in Computer Science, pages 343–350. Springer.

[NESP08] Karsten Nohl, David Evans, Starbug, and Henryk Plötz. Reverse-Engineering a Cryptographic RFID Tag. In USENIX Security Symposium, pages 185–194, 2008.

[NPR10] Karsten Nohl, Henryk Plötz, and Andreas Rohr. Establishing Security Best Practices in Access Control. 2011. http://www.srlabs.de/pub/acs

[NSA07] National Security Agency (NSA) TEMPEST: A Signal Problem. Declassified September 2007 http://www.nsa.gov/public_info/_files/cryptologic_spectrum/tempest.pdf

[OP11] David Oswald and Christof Paar. Breaking Mifare DESFire MF3ICD40: Power Analysis and Templates in the Real World. In CHES 2011, to appear.

[PN09] Henrik Plötz and Karsten Nohl. Legic Prime: Obscurity in Depth. 2009. http://events.ccc.de/congress/2009/Fahrplan/attachments/1506_legic-slides.pdf

[ST] Adi Shamir and Eran Tromer. Acoustic cryptanalysis: On nosy people and noisy machines. http://cs.tau.ac.il/~tromer/acoustic/