Foto: PCS

Viele Firmen setzen bei der Zugangskontrolle auf RFID-Karten.

RFID-Karten-Hack: Na und?

Von Stephan Speth, Leiter Marketing und neue Geschäftsfelder PCS Systemtechnik GmbH

Das erfolgreiche Hacken von RFID-Karte hat viele Anwender verunsichert. So mancher fragte sich, ob derartige Karten überhaupt für Sicherheitsanwendungen eingesetzt werden können. Dabei sollte man nicht übersehen, dass die echten Sicherheitsprobleme auf ganz anderen Gebieten liegen.

Im Jahr 2008 gelang es der holländischen Universität Dutch Radbound University Nijmegen und dem Chaos Computer Club, den Mifare classic RFID-Chip zu hacken. Die Meldung ging nicht nur durch die

Fachpresse, sondern auch durch die allgemeine Presse: Der Verschlüsselungs-Algorithmus der „Mifare classic“ RFID-Chipkartentechnik sei geknackt. Mit den veröffentlichten Ergebnissen vom Chaos Computer Club (CCC) in Berlin, der University of Virginia und der Zeitschrift ct könnten jetzt Kriminelle mit entsprechendem Fachwissen grundsätzlich Mifare classic Zutrittskarten klonen. Also der absolute Sicherheitsgau?

Nach der ersten Aufregung hat sich die Situation zwar wieder normalisiert und in Fachkreisen weiß man, dass der Aufwand zum Hacken einer Karte in den meisten Fällen in keinem Verhältnis zum erwarteten Gewinn steht. Chinesische Spezialisten haben schon vor mehreren Jahren Mifare classic-Karten geknackt und mit diesem Wissen gefälschte Karten produziert. Bemerkt wurden die gefälschten Karten durch die schlechte Qualität beim Lesen. Der Vorfall wurde jedoch nicht in der Presse publiziert. Die Aufmerksamkeit in der breiten Öffentlichkeit erreichte erst der Chaos Computer Club, der Erfahrung besitzt, wie man in der Presse derartige Fakten – und damit auch sich selbst – in Szene setzen kann.

Mit der Veröffentlichung Ende Dezember 2009, dass jetzt auch Legic prime-Karten gehackt seien, ist das Thema wieder auf die Tagesordnung von vielen Firmen gekommen. Der CCC will das Hackverfahren derzeit nicht veröffentlichen. Er verwies darauf, dass auch RFID-Karten von HID und Atmel unsicher seien. Auffällig ist der süffisante Hinweis, das Hacken von HID-Smartcards lohne sich gar nicht, da diese Karten mit jedem Proxmark3 auslesbar seien, und das teuerste Teil einer einfachen Nachbaukarte die verwendeten AAA-Batterien wären. Man kann also davon ausgehen, dass alle Karten mit der Technologie aus den 90er Jahren ähnlich „unsicher“ sind.

Ablauf des Hackens und Voraussetzung

Der Aufwand zum Klonen der Mifare classic-Karten (und wahrscheinlich auch von Legic prime-Karten) ist zwar derzeit noch sehr hoch, aber mit viel Fleiß und der entsprechenden Bauanleitung für einen Karten-Emulator aus dem Internet zu bewerkstelligen. Auch wenn das Verfahren zum Klonen von Mifare-Karten nicht in allen Details komplett veröffentlicht wurde, ist der Ablauf in aller Kürze wie folgt:

- Über eine spezielle Antenne wird von einem Mifare classic-Leser ein verschlüsselter Datenblock gelesen und auf einen Laptop kopiert.
- Ein Entschlüsselungsprogramm (zum Beispiel aus dem Internet) generiert aus diesen Daten den konkreten Projektschlüssel.
- Mit der gleichen Laptop-Antenne-Kombination wird „im Vorbeigehen“ der Inhalt einer Original Mifare classic-Zutrittskarte, die sich beispielsweise in der Ja-

ckentasche eines Mitarbeiters befindet, ausgelesen.
- Zusammen mit dem Schlüssel kann die Mifare classic-Karte geklont werden.

Ein Klonen der Karte ist folglich nur möglich, wenn das entsprechende Fachwissen und die dazu notwendige Hardware vorhanden ist, und zudem der Täter einen ungehinderten Zugang zu der betreffenden Original Zutrittskarte hat.

Die wahren Probleme

Anwender, die heute Mifare classic, Legic prime oder ähnliche Karten alter Technologie für die Zutrittskontrolle einsetzen, sollten nicht einfach blind in neue und sicherere Technologien investieren wie Mifare DESFire EV1 oder Legic advant. Viel wichtiger ist es, zuerst einmal ganz nüchtern für ein Unternehmen das tatsächliche Gefahren-Potential zu definieren.
- Wie wahrscheinlich ist es, dass überhaupt jemand versucht, unbemerkt auf das Firmengelände oder in ein Gebäude zu gelangen?
- Wie wahrscheinlich ist es, dass er dazu den Weg des Klonens einer RFID-Karte geht, oder gibt es einfachere Wege (Aufbrechen einer Hintertür, Diebstahl einer Karte), die zum gleichen Ziel führen?
- Wie weit kommt ein Krimineller mit einer geklonten Zutrittskarte? Gibt es innerhalb der Firma noch weitere Sicherheits-Hürden, die er überwinden müsste?

Bemerkenswert ist hierbei, dass das Sicherheitsbewusstsein bei Anwendern sehr unterschiedlich ausgeprägt ist, sei es nun aus Unwissenheit oder weil man letzten Endes mehr auf die Kosten als auf die tatsächliche Sicherheit achtet. Seit vielen Jahren sind Millionen RFID-Zutrittskarten im Einsatz, die als Read-Only-Karten (Miro) lediglich eine Seriennummer besitzen. Das Auslesen der Seriennummer von diesen Karten ist ohne großes Spezialwissen durchführbar und die Herstellung von Kopien ist mit Mitteln möglich, die man im Elektronik-Versandhandel leicht erwerben kann. Obwohl diese Karten somit wesentlich weniger sicher als beispielsweise Mifare classic-Karten sind, werden sie bedenkenlos benutzt.

Entsprechende Systeme bieten große Elektronik-Versandhäuser an und werden auf Grund ihres sehr günstigen Preises nicht nur in Privathaushalten eingesetzt. Und trotzdem: sie sind immer noch sicherer als ein klassisches Sicherheitsschloss, das Fachleute in Sekundenschnelle öffnen.

Was sind nun klassische Fehler und Fehlverhalten, die jede noch so sichere Zutrittskarte zur Farce macht?

Offene Hintertür

Immer wieder gern zitiert und noch viel öfter „praktiziert“: Neben

dem abgesicherten Haupteingang gibt es auf dem Firmengelände Fenster und Nebeneingänge, die offen stehen oder in die ohne große Nachfrage Personen eingelassen werden, obwohl man sie nicht kennt. Das mangelnde Sicherheitsbewusstsein vieler Mitarbeiter ist eines der größten Probleme in einer Firma. Die oberste Prämisse sollte sein, die Mitarbeiter zu sensibilisieren und regelmäßig zu schulen. Das hilft mehr als jede neue Karte.

Lässiger Umgang mit Zutrittskarten

Auch Kriminelle arbeiten möglichst effizient und vermeiden unnötigen Aufwand. Die kriminelle Energie, eine Original-Zutrittskarte zu stehlen, ist wesentlich geringer als eine RFID-Karte heimlich zu klonen. Warum also den komplizierten Weg gehen, wenn man auch mit einfacheren Mitteln zum gleichen Ziel kommt? Auf einer Kundenveranstaltung hat ein Kriminalbeamter aus Frankfurt die treffende Anmerkung gemacht, dass er in Frankfurt Imbissbuden kennt, an denen Kriminelle einem in der Mittagspause die Zutrittskarte entwenden, damit einbrechen und die entwendete Karte dem Mitarbeiter vor Ende seiner Pause wieder in die Tasche stecken, ohne dass er etwas bemerkt. Das mag zwar etwas drastisch ausgedrückt sein, aber in der Praxis ist das immer noch viel wahrscheinlicher als das Hacken einer Karte.

Firmen mit wirklich hohen Sicherheitsanforderungen wie Kernkraftwerken arbeiten beispielsweise mit zwei verschiedenen Zutrittskarten. Eine dient dem Zutritt zum Gebäude, die zweite Karte dem Zutritt zum Hochsicherheitsbereich. Diese Karte darf grundsätzlich nicht das Firmengelände verlassen und wird bei Nichtgebrauch sicher im Tresor aufbewahrt. Bei Einhaltung solch strikter Sicherheitsvorschriften hilft auch der beste Hack nichts.

Fehlendes zweites Merkmal

Wer sicher sein will oder muss, dass Personen mit einer geklonten

Foto: PCS

Mit den entsprechenden Daten lassen sich Klone von Zutrittskarten erstellen.

Zutrittskarte keinen Zutritt zu einem Gebäude erlangen können, muss zuerst einmal sicherstellen, dass auch mit einer verlorenen, einer gestohlenen oder einer unberechtigterweise weitergegebenen Original-Zutrittskarte Missbrauch vermieden wird. Für diesen Fall ist nach VdS Richtlinie 2358 (ZKA Klasse C) der zusätzliche Einsatz eines zweiten Identifikationsmerkmals zwingend vorgeschrieben, wie eine zusätzliche PIN oder ein biometrisches Merkmal (Fingerprint, Handflächenvenenerkennung etc.). Dieses zweite Merkmal kann bei weniger hohen Sicherheitsanforderungen auch nur temporär eingesetzt werden, beispielsweise am Wochenende oder beim Zutritt außerhalb der üblichen Arbeitszeit.

Der zweite Schritt

Erst, wenn man bei den oben genannten Punkten seine Hausaufgaben erledigt hat und immer noch ein Problem mit der Karte hat, kann man sich in einem zweiten Schritt Gedanken über den Einsatz von alternativen Karten machen. Mittlerweile gibt es RFID-Verfahren wie Mifare DESFire EV1 oder Legic advant, die wesentlich sicherer sind als die frühere Generation und die sich zumindest in absehbarer Zeit nicht hacken lassen. Karten mit Microcontroller (sogenannte Smartcard-Chips), bei denen der Microcontroller mit einem hochsicheren Betriebssystem den Speicher verwaltet (JP = Java Plattform), besitzen zusätzliche Sicherheits-Features, die vom BSI zertifiziert sind, und die eine außerordentlich hohe Hürde darstellen. Derartige Chips werden beispielsweise in elektronischen Reisepässen eingesetzt. In jedem Fall muss sichergestellt sein, dass man auch wirklich die Sicherheitsfeatures einsetzt und nicht nur kauft. In der Tat gibt es Firmen, die bei einer Mifare DESFire-Karte nur die Seriennummer verwenden und damit diese hochsichere Karte auf das Sicherheitsniveau einer RO-Karte herunterziehen.

Eines ist klar: Das Wettrennen ist eröffnet, die Sicherheitsmechanismen werden in Zukunft noch ausgefeilter. Industrie und Hacker werden mit immer größerem Aufwand versuchen, dem anderen zu beweisen, dass man besser ist. Ob das unbefugte Kopieren von Karten in der täglichen Praxis ein tatsächliches Sicherheitsproblem darstellt, oder alles nur eine rein akademische Relevanz besitzt, wird sich erst noch zeigen müssen. Für einfache Zutrittskarten mag man das bezweifeln, bei Kreditkarten und Ausweisen mit RFID-Chip sieht die Sache natürlich völlig anders aus. Ein absoluter Schutz ist technisch unmöglich. Man kann und muss aber die Schwelle erhöhen, der notwendig wird, einen Schutzmechanismus zu überwinden und damit das Verhältnis von Aufwand und Nutzen so ändern, dass es für Kriminelle nicht mehr lukrativ ist. ■