Dirk Fox

Die Mifare-Attacke

Eine Kryptoanalyse des verbreiteten Mifare-Chips, der in ca. 85% aller kontaktlosen Chipkarten zum Einsatz kommt, wurde erstmalig auf dem CCC-Jahreskongress am 28.12.2007 vorgestellt. Inzwischen wurden weitere Details bekannt – und der Angriff erheblich verbessert. Mitte April 2008 stellten Forscher der Radboud Universiteit Nijmegen einen Kurzfilm in YouTube ein, in dem sie den erfolgreichen Angriff auf eine Campus-Zugangskarte zeigen.

Hintergrund

Die weltweit verbreitetsten kontaktlosen Chipkarten beruhen auf der Mifare-Technologie, einem *Radio Frequency Identification* (RFID)-Chip mit 1-4 kB EEPROM-Speicher und einer Datenübertragungsrate von 100 kbit/s. Die Mifare-Technologie wurde in den 90er Jahren von der Firma Mikron Gesellschaft für integrierte Mikroelektronik als kontaktloses Ticketsystem für den öffentlichen Nahverkehr („Mikron Fare Systems") entwickelt. Mifare-Chips werden heute von NXP Semiconductors, der Halbleiter-Tochter von Philips (in der die Mikron GmbH 1995 aufging), und von Infineon Technologies hergestellt.

Mifare-Chips kommunizieren mit einem Lesegerät über eine Distanz von bis zu 10 cm auf einer Frequenz von 13,56 MHz. Mifare-Karten kommen ohne eigene Stromversorgung aus. Die für die Kommunikation mit dem Lesegerät und die Rechenoperationen erforderliche Energie erhält die Karte induktiv vom Kartenleser.

Eingesetzt werden Mifare-Chips heute in kontaktlosen Chipkarten und Hybrid-Smartcards. Hauptanwendung war ursprünglich – und ist es auch heute noch zu einem erheblichen Teil – der Einsatz als kontaktloses „Ticket" im öffentlichen Nahverkehr. Aber auch Unternehmen setzen Mifare-Karten für sehr unterschiedliche Anwendungen ein – typisch sind Zeiterfassung, Gebäudezugang und Zahlungsfunktion in Betriebskantinen, oder auch Zimmertüren in Hotels.

Weltweit sind heute mindestens 500 Millionen, nach einigen Quellen sogar bis zu zwei Milliarden Mifare-Karten und etwa 5 Millionen Lesegeräte in Betrieb. Der Anteil von Mifare-Chips am weltweiten Markt für kontaktlose RFID-Karten liegt nach Angaben von NXP bei 85%. Zwei wesentliche Mifare-Chiplinien bietet NXP heute an: Mifare Classic (MF1 IC S50/S70, mit 1 bzw. 4 kByte Speicher), und Mifare DESFire (MF3 IC S40), der die hier beschriebenen Schwächen nicht aufweist, da er statt einer Stromchiffre zur Verschlüsselung die Blockchiffre DES oder 3DES verwendet. Für Ende 2008 ist eine dritte Chiplinie, Mifare Plus angekündigt, die AES-128 für die Verschlüsselung verwenden und eine schrittweise Migration von Mifare Classic ermöglichen soll.

Dirk Fox

Geschäftsführer der Secorvo Security Consulting GmbH und Herausgeber der DuD.
E-Mail: dirk.fox@secorvo.de

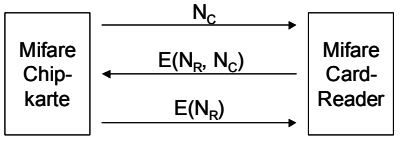
Sicherheitsprotokoll

Die Kommunikation zwischen Mifare-Chipkarte und Lesegerät wird durch eine gegenseitige Authentifikation mit einem Drei-Wege-Protokoll geschützt, das vom Lesegerät eingeleitet wird. Darauf antwortet die Karte mit einer zufälligen Challenge N_C. Das Lesegerät verschlüsselt die empfangene Challenge und eine eigene Zufallszahl N_R und schickt das Ergebnis an die Karte zurück. Letztere entschlüsselt die empfangenen Daten und antwortet mit der verschlüsselten Zufallszahl des Lesegeräts.

Dieses klassische Drei-Wege-Protokoll nach dem ISO-Standard 9798-2 sorgt für eine kryptographisch starke Authentifikation beider Kommunikationspartner, sofern die drei folgenden Bedingungen erfüllt sind:

- der für die Erzeugung der Challenge verwendete Zufallszahlengenerator ist kryptographisch stark, d. h. der Zufallswert ist auch bei Kenntnis aller bereits erzeugten Zufallsbits nicht vorhersagbar,
- der verwendete symmetrische „Systemschlüssel", mit dem die Zufallswerte verschlüsselt werden, und der im Mifare-Chip und in allen Lesegeräten der Anwendung gespeichert ist, ist einem Angreifer nicht zugänglich, und
- das verwendete Verschlüsselungsverfahren ist kryptographisch stark (d. h. nicht gebrochen) und verwendet hinreichend lange Schlüssel (mindestens 80 bit).

Abb. 1 | Authentifikations-Protokoll einer Mifare-Karte [KoHG_08]



Eine Bewertung der Sicherheit des Mifare Classic Chips war bislang nicht möglich, da sowohl der Zufallszahlengenerator als auch der Verschlüsselungsalgorithmus „Crypto-1" vom Hersteller geheim gehalten wurden. Auch die verwendete Schlüssellänge war nicht bekannt.

Grundsätzliche Problematik

Durch die begrenzte Datenübertragungsrate und das Fehlen einer eigenen Energieversorgung sind kryptographischen Ver-

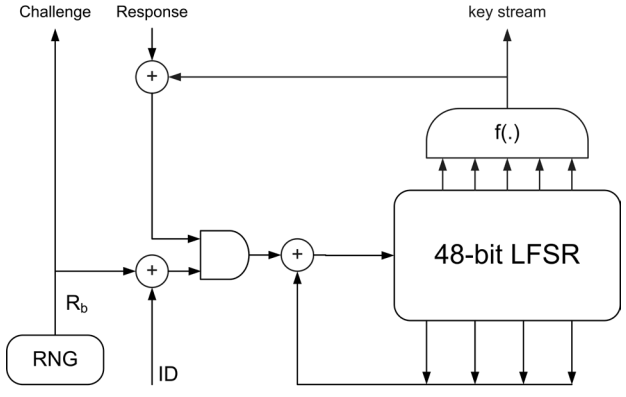
fahren auf RFID-Karten enge Grenzen gesetzt. Insbesondere Systeme wie Mifare Classic, die in den 90er Jahren des vergangenen Jahrhunderts entwickelt wurden, mussten mit sehr begrenzten Möglichkeiten auskommen. Starke kryptographische Verfahren sind auf wenig leistungsfähiger Hardware sowohl rechen- als auch zeitintensiv – beides Eigenschaften, die sich mit der erwünschten kurzen Kommunikationszeit zwischen Lesegerät und Karte und einer geringen Leistungsaufnahme nicht vertragen.

So lässt sich eine echte Zufallsquelle auf einer solchen einfachen Chipkarte nicht realisieren. Daher war der Hersteller auf einen Pseudozufallszahlengenerator angewiesen. Dessen Startwert muss bei der Initialisierung der Karte von außen eingebracht und unauslesbar auf der Karte gespeichert werden. Damit der Pseudozufallszahlengenerator nicht bei jeder Aktivierung der Karte dieselbe Zufallsfolge erzeugt, sollte der Zustand des Generators auf der Karte zwischengespeichert werden. Außerdem muss der Generator kryptographisch stark sein: Auch bei Kenntnis früherer Zufallsbits dürfen zukünftige Ausgaben nicht vorhersagbar sein – ein Kriterium, dass viele Verfahren nur zum Preis der Speicherung eines geheim zu haltenden Schlüssels erfüllen – ein weiterer Angriffspunkt.

In dem Dilemma zwischen hohen Prozessanforderungen und geringer Leistungsfähigkeit der verfügbaren Hardware haben Hersteller in der Vergangenheit immer wieder eine vermeintlich bewährte Kompromissstrategie gewählt: ein kryptographisch schwaches, aber schnelles Verfahren (meist ein linear rückgekoppeltes Schieberegister mit etwas Verschleierungslogik) und „Security by obscurity" – die Geheimhaltung des gewählten Verfahrens.

Diese Strategie ist riskant, da das Nutzervertrauen mit der Aufdeckung des (möglicherweise schwachen) Verfahrens schlagartig verloren gehen kann. Womöglich gingen die Hersteller davon aus, dass die Analyse einer Chipkarte technisch zu aufwändig für eine Kryptoanalyse ist – und das gewählte Verfahren möglicherweise in wenigen Jahren durch leistungsfähigere Hardware ersetzt werden könne.

Abb. 2 | Stromchiffre Crypto-1 und Zufallszahlengenerator [Nohl_08]



Reverse Engineering

Mit Unterstützung der Fachzeitschrift c't rückten Kryptologen und Aktivisten des Chaos Computer Clubs (CCC) dem Mifare-Chip 2007 zu Leibe [KrNP_08]. Sie lösten den Chip mit Azeton aus einer Plastikkarte und analysierten anschließend die Chiparchitektur mit einem optischen Mikroskop (500fache Vergrößerung). Dazu wurden die fünf Chip-Lagen mit einem Spezialschleifgerät Stück für Stück abgeschliffen und mit einer im Mikroskop eingebauten Digitalkamera fotografiert.

Vereinfacht wurde die Analyse dadurch, dass die Kryptologen zu Recht ein linear rückgekoppeltes Schieberegister hinter dem Verschlüsselungsalgorithmus „Crypto-1" vermuteten. Daher konnte man die Analyse auf den Chip-Bereich konzentrieren, in dem eine größere Häufung von Flip-Flops auftrat. Da die Entwickler der Mifare-Chips keine Obfuscation-Techniken verwendet hatten, um die Chip-Logik zu verschleiern – eine Methodik, die im Smartcard-Design heute üblich ist – ließ sich die Analyse der Chipstruktur durch Mustererkennung weitestgehend automatisieren.

Kryptoanalyse

Die Chip-Analyse lieferte die Erkenntnis, dass es sich bei Crypto-1 tatsächlich um ein linear rückgekoppeltes Schieberegister (LFSR) von 48 bit Länge handelt, bei dem jedes Schlüsselstrombit aus jeweils 20 Bit des Schieberegisters über eine einfache Filterfunktion f(·) gewonnen wird (siehe Abb.). Geladen wird das Schieberegister bei der Initialisierung mit dem 48-bit-Schlüssel des Systems, d. h. alle Karten und Leser einer Anwendung arbeiten mit demselben Systemschlüssel. Kennt man diesen Schlüssel, kann man Mifare-Karten für diese Anwendung klonen.

Mit Hilfe des Open-Source-RFID-Lesers OpenPCD und des Kartensimulators OpenPICC, beides Projekte des CCC Berlin, konnten weitere Erkenntnisse über die Arbeitsweise der Stromchiffre gewonnen werden.

So erleichtern neben dem für heutige Anwendungen mit 48 bit viel zu kurzen Systemschlüssel zahlreiche Schwächen in der Sicherheitsarchitektur des Mifare-Chips einen Angriff. Insbesondere wird bei der Initialisierung der Karte das LFSR, das als Zufallszahlengenerator dient, automatisch mit einem in allen Mifare-Chips identischen Startwert vorbelegt. Der „Zufallswert" ist damit vorhersagbar – und damit eben nicht mehr zufällig. Er bildet nicht nur die Challenge, die während des Authentifikationsprotokolls an das Lesegerät geschickt wird, sondern geht, XOR-verknüpft mit der Karten-ID, in das LFSR für die Verschlüsselung ein.

Durch Mängel in der statistischen Unabhängigkeit der Eingaben von den Ausgaben der Filterfunktion f(·) können 12 der 48 Schlüsselbits sehr leicht gewonnen werden. Die restlichen 36 bit lassen sich vergleichsweise schnell durch eine Brute-Force-Analyse (durchprobieren aller verbleibenden Schlüssel) bestimmen. Noch eleganter geht es mit einer erst kürzlich publizierten algebraischen Analyse, d. h. der Auswertung eines Gleichungssystems über GF(2), die den kompletten Schlüssel in nur 200 Sekunden auf einem PC liefert – und als Eingabe lediglich ca. 50 Schlüsselstrom-Bits benötigt [CoNO_08].

Angriffsszenarien

Mit den nun bekannten Schwächen des Crypto-1-Algorithmus lassen sich Mifare Classic Karten in wenigen Minuten analysieren und anschließend beliebig klonen. Das birgt unterschiedliche Gefahren für die verbreitetsten Anwendungen von Mifare Classic RFID-Karten:

- **Zahlungsmittel**: Debit-Karten zur Zahlung in Kantinen oder an Automaten können unberechtigt aufgeladen werden. Der dadurch verursachte Schaden ist jedoch begrenzt, solange die Höhe des Debit-Wertes limitiert ist und nur ein Bruchteil der Nutzer Fälschungen vornimmt. Missbrauch kann in Systemen mit Lade-Terminals meist durch die Führung von Schattenkonten aufgedeckt werden (höhere Ausgaben als Aufbuchungen).
- **Zeiterfassung**: Das Ein- und Ausbuchen mit einer geklonten Karte verursacht Fehlbuchungen. Ein Nutzen für einen Angreifer lässt sich dabei nicht konstruieren; falsche Buchungen lassen sich zudem vergleichbar leicht wieder korrigieren.
- **Gebäudezugang**: Kritisch ist allerdings die Möglichkeit zu bewerten, dass Unberechtigte mit geklonten Karten Zugang zu Gebäuden oder bestimmten Räumlichkeiten erhalten. Hier kann der Schaden beträchtlich sein, z. B. beim Eindringen in Hotelzimmer oder Unternehmen.

Damit besteht kurzfristig die größte Bedrohung bei Zugangssystemen. Gegenmaßnahmen bei Bezahlsystemen sind erst dann unvermeidlich, wenn eine nennenswerte Zahl von gefälschten Karten zum Einsatz kommt.

Gegenmaßnahmen

Die geschilderten Angriffe erfordern die Simulation einer Authentifikation an einem regulären Lesegerät, um Klartext-Schlüsseltext-Paare zu erhalten. Da könnte es nahe liegen, nach einer bestimmten Zahl abgebrochener Authentifikationsversuche das Lesegerät für eine bestimmte Zeit zu sperren, um einem Angreifer die Arbeit zu erschweren. Wegen der geringen Zahl benötigter Schlüsselbits müsste die Sperrung jedoch schon nach dem ersten Abbruch des Protokolls erfolgen – für „reguläre“ Nutzer, deren Authentifikation z. B. durch zu frühzeitiges Entfernen der Karte vom Lesegerät abbricht, ein unzumutbarer Bequemlichkeitsnachteil. Auch würde ein Angriff nicht verhindert, sondern lediglich der Aufwand für einen Angreifer geringfügig erhöht.

Zudem dürfte das Authentifikationsprotokoll so Hardware-nah realisiert sein, dass eine Sperrung des Lesegeräts bei Protokollabbruch nicht ohne weiteres implementiert werden könnte. In jedem Fall würde eine solche Ergänzung des Authentifikationsprotokolls einen Austausch der Lesegeräte oder zumindest der Firmware erfordern.

Schließlich erfordern die neuesten Angriffe nur noch das einmalige passive Abhören der regulären Nutzung einer unmanipulierten Karte [CoNO_08].

Alternativ können Betreiber auf das seit 2004 verfügbare Mifare DESFire-System wechseln, das nach Angaben von NXP über eine echte Zufallsquelle auf der Karte verfügt und wahlweise mit DES oder 3DES verschlüsselt. Ein solcher Wechsel erfordert jedoch den kompletten Tausch von Karten und Lesegeräten – für große Anwendungen ein inakzeptables Vorgehen. Die von NXP für Ende 2008 angekündigte Weiterentwicklung Mifare Plus soll daher eine schrittweise Migration erlauben. Dabei ist allerdings zu bedenken, dass automatisch auf das schwache Verfahren zurück geschaltet wird, wenn ein ‚alter‘ Leser oder eine ‚alte‘ Karte im Spiel ist.

Scheidet (zumindest kurzfristig) der Wechsel auf eine andere Technologie aus, müssen zusätzliche Sicherheitsmaßnahmen getroffen werden. So bieten Karten mit aufgedrucktem Foto eine zusätzliche Sicherheit, sofern sie kontrolliert werden. Bei Bezahlsystemen helfen Schattenkonten mit einer umgehenden Kartensperrung bei Debit-Überschreitung. Bei Zugangskarten können Gültigkeitsbeschränkungen (Arbeitszeit, Begrenzung auf bestimmte Bereiche) das Risiko mindern. Echten Schutz bieten jedoch nur zusätzliche Sicherheitsmechanismen wie beispielsweise PIN-Pads, die den Zugang erst nach zusätzlicher Eingabe einer von der Karte unabhängigen PIN frei geben.

Bewertung

Die publizierten Analyseverfahren erlauben ein Karten-Kloning mit so einfachen Mitteln, dass auf Mifare Classic basierende Anwendungen als vollständig kompromittiert angesehen werden müssen – bei Anwendungen wie Unternehmens- oder Gebäudezugang wäre eine leere Plastikkarte nahezu ebenso sicher (wiewohl erheblich billiger). Unternehmen sollten zumindest beim Zugangsschutz kurzfristig reagieren und entweder auf eine sichere Technologie wie Mifare DESFire oder Mifare Plus migrieren, oder ergänzende Schutzmaßnahmen (PIN-Pads) ergreifen.

Auch Nutzer der Lösung des schweizer Mitbewerbers Legic sollten sich nicht in Sicherheit wiegen. Die „Legic-Verschlüsselung“, die insbesondere bei Zugangssystemen zur Anwendung kommt, wird vom Hersteller ebenfalls geheim gehalten. Da beide Technologien gemeinsame Wurzeln haben, könnte es nur noch eine Frage der Zeit sein, bis sie dasselbe Schicksal ereilt wie Mifare Classic.

Literatur

[CoNO_08] Nicolas T. Courtois, Karsten Nohl, Sean O'Neil: *Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards*. Cryptology ePrint Archive, 2008/166 http://eprint.iacr.org/2008/166.pdf

[KoHG_08] Gerhard de Koning Gans, Jaap-Henk Hoepman, Flavio D. Garcia: *A Practical Attack on the MIFARE Classic*. eprint arXiv:0803.2285, 03/2008 http://www.scriptworks.nl/gerhard/documents/mifare_weakness.pdf

[KrNP_08] Krissler, Jan; Nohl, Karsten; Plötz, Henryk: *Chiptease – Verschlüsselung eines führenden Bezahlkartensystems geknackt*. c't, Heft 8/2007, S. 80-85.

[Nohl_08] Karsten Nohl: *Cryptanalysis of Crypto-1*. http://www.cs.virginia.edu/~kn5f/Mifare.Cryptanalysis.htm

[NoPl_07] Karsten Nohl, Henrik Plötz (CCC): *Mifare – Little Security despite Obscurity*, Vortrag auf CCC-Kongress 2007, http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html