

Mifare Karte geknackt!?

Einschätzung und Stellungnahme der InterCard AG Informationssysteme / InterCard GmbH Kartensysteme

Seit vergangener Woche meldet die einschlägige Fachpresse, dass der Verschlüsselungsalgorithmus der Mifare Classic Chipkarte ‚nachvollzogen‘ wurde und somit die Sicherheit der Karte gegen Angriffe von außen zukünftig nicht mehr gewährleistet werden kann.

Aufgrund der ersten Meldung und der jetzt aktuellen Veröffentlichungen haben wir uns der Problematik sofort angenommen und möchten Sie diesbezüglich über den momentanen Status, die Risiken und die von uns geplanten Maßnahmen informieren.

Mifare

Seit den frühen 90er Jahren, in denen die Mifare Classic Chipkarte entwickelt wurde, sind bislang weltweit mehr als 1 Milliarde (man spricht von bis zu 2 Milliarden) Mifare Karten und 5 Millionen Leseeinheiten verkauft und somit in Umlauf gebracht worden. Das Haupteinsatzgebiet sind Bezahl- oder Berechtigungskarten im öffentlichen Nahverkehr sowie Identifikationsanwendungen im Bereich Zutritt.

Die Mifare Chipkarte gehört zur Familie der Speicherchipkarten und besitzt somit keinen Prozessorchip mit Betriebssystem, sondern wird über eine fest in Hardware gegossene Sicherheitslogik angesteuert.

Sicherheitsarchitektur der Mifare Classic

Zur Verschlüsselung der Systemdaten und -informationen wird der geheim gehaltene sogenannte CRYPTO1 Chiffrieralgorithmus eingesetzt, welcher nur mit speziellen NXP Bausteinen umgesetzt und verarbeitet werden kann. Diese Bausteine sind auch in den Mifare Lesemodulen eingebaut. Die Schlüssellänge beträgt 48 Bit, daraus ergeben sich über 280 Billionen Kombinationsmöglichkeiten.

Zum Vergleich wird heute im Bereich der Prozessorchipkarten mit Schlüssellängen von bis zu 168 Bit (10^{50} Kombinationsmöglichkeiten) gearbeitet, welches dann als ausreichend sicher gilt. 10^{50} entspricht in etwa der Anzahl Atome unserer Erde.

Durch immer leistungsfähigere Rechner gelang es in der Vergangenheit immer wieder diverse Sicherheitsstandards zu „knacken“. Dies kann durch die dauernde Weiterentwicklung der Rechenleistung zur Folge haben, dass auch zukünftig weitere Sicherheitsstandards entschlüsselt werden.

Eine Information am Rande: 1976 wurde ein Algorithmus namens DES mit netto 56 Bit als Standard zugelassen. Der Zahlenraum war damit also etwa 1.000 Mal größer als bei Mifare Classic. 1998 wurde er mit einer entsprechend mächtigen Rechenmaschine geknackt, die 88 Milliarden Schlüssel pro Sekunde testen konnte. Er hielt also rund 20 Jahre.

Aktuelle Pressemeldungen – Mifare geknackt!

Die Computer Fachzeitschrift ct (ct 8/2008) hat in Zusammenarbeit mit dem Chaos Computer Club in Berlin und der Universität Virginia ein Verfahren entwickelt, um aus der verwendeten Hardware auf die eingesetzten Rechenvorschrift zu kommen. Der Artikel erschien Anfang letzter Woche (ct 8/2008).

Die Chips wurden auf einer speziellen Maschine Schicht für Schicht abgefräst und von den 5 Lagen wurden über ein Mikroskop entsprechende Digitalaufnahmen angefertigt. Auf diese Weise wurde über die Analyse der Strukturdaten letztlich der Schaltplan des Chips rekonstruiert. Damit liegt also die Rechenvorschrift offen.

Der zweite Ansatz waren Analysen im Bereich der Kommunikation von Karte und Leser. Sie haben gezeigt, dass es a) erhebliche Schwächen im implementierten Zufallszahlengenerator gibt und b), dass Kartenseriennummer und Schlüssel in einem Zusammenhang stehen. Beide Faktoren stellen aus heutiger Sicht Designfehler des Herstellers bzw. der Entwickler dar.

Fazit

Die einfache Struktur der aufgedeckten Rechenregel, voraussagbare Zufallszahlen sowie Zusammenhänge zwischen Karten-ID und Schlüssel lassen einen erfolgreichen Angriff auf die Karte gewissermaßen recht einfach erscheinen.

Die Aussage "Verschlüsselungsalgorithmus Mifare Classic nachvollzogen" muss also im Grundsatz als korrekt bewertet werden !

Mögliche Gefahren!

Prinzipiell können im Bereich von Chipkartensystemen nachfolgende potenzielle Gefahrenquellen identifiziert werden:

1. Die Karten als Zugangskontrollmedium für Zutrittssysteme, d. h. Zutrittsrechte einer legal berechtigten Karte könnten auf eine fremde Karte übertragen werden (Klonen einer Karte). Somit könnten Angreifer illegal Zutrittsrechte erwerben.
2. Die Karte als elektronische Geldbörse, die zur Zahlung von Waren und Dienstleistungen eingesetzt wird. Hier könnte der Angreifer versuchen „künstliches Geld“ auf seine Karte zu laden oder diese Möglichkeit für Dritte zu schaffen.
3. Weitere Identifikationen an: z. B. Zeiterfassungssysteme, PC-Zugang, Bibliothekszugang oder sonstige Identifikationsanwendungen.
4. Bei personenbezogenen Daten auf der Karte ergibt sich i.d.R. insofern keine Gefahr, da die im Chip hinterlegten Daten (Matrikelnummer, Personalnummer, Gültigkeit) oftmals in Klarschrift auf der Karte aufgedruckt sind.

Diese kriminelle Energie könnte zu einem Missbrauch verwendet werden, wodurch wirtschaftliche Schäden entstehen können.

Mögliche Reaktionen

1. Im Bereich Zugangskontrolle lässt sich durch das Implementieren von zusätzlichen Mechanismen die Verwendung von **geklonten Karten** verhindern. Dies kann in Zusammenarbeit mit den Herstellern von Zutrittssystemen ermöglicht werden. Bitte nehmen Sie hierzu Kontakt mit Ihrem Anbieter auf.

Die **InterCard / Intrakey-Lösungen** bieten entsprechende Möglichkeiten. Je nach Alter der Installation können die Systeme nachgerüstet werden.

2. Im Bereich der möglichen Manipulation der Geldbörse muss vorab gesagt werden, dass die Transparenz und Aufbereitung von Bezahlvorgängen/Umsatztransaktionen durch ein sogenanntes Clearingsystem bereitgestellt wird. Dieses System ermöglicht, die durch die Bezahlvorgänge erzeugten Umsätze nach verschiedensten Kriterien auszuwerten und deren Stimmigkeit zu prüfen.

Dieses Konzept kann somit die komplette Einsatzhistorie, vom Aufwerten einer Karte bis hin zu jedem einzelnen Bezahlvorgang, einer jeden Karte nachvollziehen und überwachen.

Auffälligkeiten und Unstimmigkeiten können vom System registriert werden und können dann durch das entsprechende Sperrlistenmanagement dafür sorgen, dass Karten für den weiteren Gebrauch gesperrt und demzufolge an den Terminals abgewiesen werden.

Die von InterCard angebotenen bzw. unterstützten Systeme von tl1 und CashMaster bieten die entsprechenden Möglichkeiten.

Einschätzung allgemein

Bis vor wenigen Tagen hatten wir uns der Analyse des angesehenen niederländischen TNO Instituts angeschlossen, die im Wesentlichen den Wechsel auf eine andere Karte binnen zwei Jahren zusammen mit ein paar kurzfristigeren Ansätzen als ausreichend eingeschätzt hatten.

Für InterCard steht nach den neuesten Informationen aber fest, dass die Mifare Classic in der jetzigen Form schon in sehr viel näherer Zukunft, abhängig vom Einsatzgebiet und der Risikoeinschätzung des jeweiligen Kunden, als nicht mehr ausreichend sicher einzustufen ist.

Vor allem im Umfeld personalisierter Karten ist eine Manipulation mit einem sehr hohen Entdeckungsrisiko verbunden.

Werden anonyme Karten über ec-Aufwerter geladen, sind über die Bankverbindung ebenfalls personenbezogene Daten vorhanden, die bei Auffälligkeiten ggf. zur Verwendung kommen könnten.

Diese Punkte müssen gegebenenfalls in geeigneter Weise publiziert werden, um eine abschreckende Wirkung zu entfalten. Schließlich muss auch unterstrichen werden, dass solche Manipulationen Straftaten darstellen.

Weitere Vorgehensweise

InterCard wird für seine Kunden sehr zeitnah (ca. 4 - 6 Wochen) eine Migrationsstrategie auf eine neue Kartentechnologie ausarbeiten und vorstellen.

Migration

Migration heißt das Schaffen der Voraussetzungen, bestehende Karten parallel zu einer neuen Kartentechnologie zu verarbeiten.

Ziel von InterCard ist, dies soweit als möglich durch Tausch der Lesemodule und Anpassung der Gerätesoftware zu erreichen und so einen weitestgehenden Investitionsschutz für die Kunden zu ermöglichen.

Sie als Kunde legen den Zeitpunkt der Migration in Abhängigkeit Ihrer Risikobewertung fest. Innerhalb der Migration sind Sie völlig frei, den Zeitpunkt des Auslaufens der Altkarten zu bestimmen. Nur im Falle eines massiven betrügerischen Missbrauchs müssten die ‚Altkarten‘ vorzeitig ausgetauscht werden.

Mögliche Folgekartentechnologien

Aktuell befindet sich InterCard bereits im Analyse- und Selektionsprozess der Folgekartentechnologie. Zur Auswahl stehen Kartentechnologien wie z.B. Mifare Plus, Mifare DESFire, Legic Advant oder Sony FeliCa.

Ob es sich um die für Ende des Jahres angekündigte Mifare Plus handeln wird oder eine Mifare DESFire oder um eine ganz andere Familie wie z. B. die Legic Advant oder Sony FeliCa, ist derzeit noch offen. Sie alle bieten die erforderliche Sicherheit.

Bei Mifare Plus handelt es sich um eine Mifare Classic kompatible Karte, die quasi auf Knopfdruck in einen Zustand modernster Sicherheit gebracht werden kann. Die Karte kann sofort voll kompatibel eingeführt werden, sobald dann die Infrastruktur der Geräte entsprechend umgestellt wurde, kann dieses Umschalten stattfinden. Muster sollen im 4. Quartal 2008 erhältlich sein, Preis und Detaildaten sind derzeit noch nicht bekannt.

Mifare Desfire ist eine eingeführte preiswerte und flexible Prozessorkarte mit anerkannter Sicherheitsarchitektur. Eine Variante mit AES Sicherheitslevel, dem heutigen internationalen Standard, soll im zweiten Quartal vorliegen.

Legic Advant aus der Schweiz bietet eine ebenfalls ausreichende Sicherheitsarchitektur eingebettet in eine hoch hierarchische Systemarchitektur.

Eher in Asien verbreitet ist die FeliCa von Sony.

Bei der Auswahl spielen neben dem höchst bewerteten Punkt der Sicherheit unter anderem auch folgende Themen eine Rolle: Leistungsfähigkeit, Flexibilität, Preis, Verbreitung, Migrationsfähigkeit, Implementierungsaufwand in bestehende Hardware und Software.

Die Auswahl der Kartentechnologie wird im Rahmen des Migrationskonzeptes begründet und vorgestellt.

Schutzmaßnahmen für Mifare Classic Systeme

Klonen

Die Mifare Classic besitzt eine fixe vom Chiphersteller vergebene Seriennummer. Sie ist Voraussetzung für die im folgendenden beschriebene Maßnahme.

Für ebenfalls denkbare Kartenemulatoren, also technischen Gerätschaften, die einem Gerät vorgaukeln, eine Karte zu sein, bietet das natürlich keinen Schutz, da Sie in der Lage sind, jede beliebige Seriennummer vorzutäuschen.

In hochsicheren Anwendungen werden neben dem Besitz einer Karte üblicherweise aber weitere Merkmale wie PIN oder biometrische Daten abgefragt, da der Verlust oder Missbrauch einer Karte oftmals nicht unmittelbar bemerkt wird.

Ablauf

Über ein geeignetes Gerät (optimalerweise bereits bei der Kartenpersonalisierung, nachträglich z. B. in entsprechend modifizierten Türlesesystemen, Validierungsterminals, Aufwerter etc.) wird eine spezifische Info auf einen bislang freien Bereich der Karte aufgebracht. Es werden verschiedene Kartenmerkmale kombiniert, verschlüsselt und gespeichert.

Zum Einsatz kommen sichere Verfahren (3DES, AES o.ä.), grob lässt sich der Kodiervorgang so beschreiben:

- Seriennummer der Karte auslesen (SN)
 - Schlüssel K1 erzeugen aus einem Masterkey K0 und kartenspezifischen Daten
 - Kryptogramm M1 über SN bilden mit 3DES-Key K1 und in Sektor X ablegen
-

Die Prüfung läuft dann analog ab: Bilde M1 und vergleiche mit dem in Sektor X hinterlegten Wert.

Buffering

Es können zwar Maßnahmen ergriffen werden, um einfache Aufwertevorgänge mittels komprimierten Schlüsseln zu erschweren. Um solche Hürden zu umgehen, wird das System durch Klonen auf sich selbst angegriffen, dem Buffering.

Ziel eines solchen Angriffs ist, einen regulären Altzustand der Karte herbeizuführen. Nachdem z. B. eine Karte ganz normal auf 50 € aufgeladen wurde, wird ein Abbild der Kartendaten gezogen und konserviert (z. B. auf einem PC). Nachdem der Betrag dann ganz oder teilweise verbraucht wurde, wird der konservierte Zustand wieder hergestellt, d. h., das Abbild wird immer wieder auf die identische Karte zurück geschrieben. Die Karte hat für die verarbeitenden Geräte dann einen für sich betrachtet plausiblen Zustand.

Da die Karte keinen eigenverwalteten Vorgangszähler o. ä. bietet, kann das Wiedereinspielen von Altdateien bei korrupten Schlüsseln nicht verhindert werden. Hierfür hilft allein die Überwachung im Hintergrundsystem, dem Clearing-System (Software zum Verwalten und Auswerten der Zahltransaktionen. In d. R. das Kassensystem im Studierendenwerk).

Empfehlungen von InterCard

Geldbörsensysteme / Kassensysteme

Hier sollte verstärkt die vom Clearing-System angebotene Möglichkeit der Saldenverfolgung genutzt werden, um mögliche Unstimmigkeiten zu entdecken. Die Zahltransaktionen sollten dafür zeitnah in das Clearing-System übertragen werden.

Zutrittssysteme

Je nach Risikoeinschätzung und Einsatz der Zugangssysteme sollte mit dem jeweiligen Anbieter geprüft werden, ob die von InterCard angebotene Möglichkeit für das Nutzen weiterer Kartenmerkmale mit Verschlüsselung etc. realisierbar ist. InterCard unterstützt Sie selbstverständlich in der Kommunikation und Abklärung mit dem jeweiligen Hersteller.

Migration

Nach Vorlage des Migrationskonzeptes durch InterCard stehen wir unseren Kunden für entsprechende Gespräche zur Verfügung. Je nach Bedarf könnte gegebenenfalls eine kurzfristige Nutzertagung angesetzt werden.

Generell sollte das Gesamtsystem mit erhöhter Aufmerksamkeit hinsichtlich Unstimmigkeiten und Auffälligkeiten beobachtet werden. Im Falle von zweifelhaften Transaktionen, Vorgängen etc. steht Ihnen InterCard für Rückfragen jederzeit zur Verfügung.

Links

Hersteller:

<http://www.nxp.com/>

Mifare Homepage:

<http://mifare.net/security/>

Fachzeitschrift ct:

<http://www.heise.de/security/Schwaechen-des-RFID-Systems-Mifare-Classic-bestaetigt--/news/meldung/105315>

Analyse TNO Niederlande:

<http://www.translink.nl/media/bijlagen/nieuws/TNO ICT - Security Analysis OV-Chipkaart - public report.pdf>
