Anschrift

Datum: 07.04.2008
Unser Zeichen: JE
Unsere Tel. Nr.: 089/ 42735-0
Unsere Fax Nr.: 089/ 42735-111
Ihre Zeichen:
Ihre Nachricht:
Ihre Tel. Nr.:
Ihre Fax Nr.:

Sicherheitsaspekte MIFARE

Sehr geehrter Kunde,

nach Auswertung der uns vorliegenden Informationen (erstes NXP Statement, NXP Statement 12.3.08, Chiptease c't 2008 Heft 8, Radboud Universiteit Nijmegen 08-33A v. 12.3.2008, www.nxp.com, CCC '07 MIFARE SECURITY), können wir Stand heute folgendes zur Einschätzung der Lage beitragen.

Von welcher Technologie ist die Rede?

Betroffen ist der MIFARE Standard classic in der 1k und 4k Variante. Durch Abtragen einzelner Schichten eines Chips, wurde die Verschlüsselungslogik (Crypto-1) ermittelt. Weiterführend wurde die Verschlüsselung zwischen Karte und Leser analysiert. Dazu waren und sind Hardware, Tools und spezielles Know-how notwendig.

Welche Auswirkungen kann dies haben?

Für den ungünstigsten Fall, können damit Karten dupliziert und/oder der Dateninhalt einzelner Sektoren verändert werden. Nach den uns vorliegenden Informationen sind die Chipseriennummer (UID), Herstellerangabe, und Herstelldatum davon ausgenommen. Diese Daten wurden noch nicht angegriffen da diese in einem festen Bereich liegen. Die UID ist innerhalb der Hersteller eindeutig.

Wie kann ein Missbrauch bei kopierten Karten festgestellt werden?

Unsere Systeme führen mit jeder Einzeltransaktion auch einen Vorgangszähler (VGZ) mit. Wird eine Mifare dupliziert, kann dies über einen Sonderbericht, der nach eklatanten Vorgangszählersprüngen auswertet, festgestellt werden. Es gibt in diesem Fall zwei gleiche Karten, mit gleicher Kartennummer, die in den Start- und Endsalden Auffälligkeiten aufweisen. Bei Verdachtsfällen, kann die Karte über eine Sperrdatei für weitere Bezahlvorgänge gesperrt werden.

Ist eine Datenmanipulation möglich?

Eine Manipulation ist nur mit tieferem Verständnis und genauer Kenntnis

- über den Segmentaufbau (an welchem Byte steht welche Information),
- über Anzahl und Position der Spiegelspeicher
- über den Algorithmus der Checksummen Bildung

möglich.

Diese aufgeführten Mechanismen sind geschützt. Eine Manipulation ohne diese Kenntnisse, würde also mit hoher Wahrscheinlichkeit nicht ohne Fehler stattfinden. Eine Plausibilitätsprüfung während dem Bezahlvorgang weist diese Karte sofort ab.

Sollten alle Hürden überwunden sein, und z.B. gezielt ein Euro Betrag „korrekt“ manipuliert worden sein, dann ist dies bei einem Vergleich durch das mitgeführte Schattenkonto auf der Datenbankseite (doppelte Buchführung) im Nachhinein feststellbar

Gibt es zusätzliche Sicherheitsmaßnahmen?

Automaten Seitz erstellt ein Sicherheitsupdate. Die UID wird in eine erweiterte Identitäts- und Plausibilitätsprüfung involviert. Ein entsprechendes Update liegt in KW 17 vor.

Eine zusätzliche Verschlüsselung der Daten auf der Karte wird integriert werden. Der Termin für dieses Upgrade wird noch bekannt gegeben.

Welche weiterführende Empfehlung gibt es?

Die jüngere und modernere MIFARE DESFire Technologie hat einen höheren Sicherheitsstandard wie die classic Variante. Verschlüsselungsmechanismus, Tiefe und Anzahl der Schlüssel sind weitergehend. Die Karte selber beinhaltet einen Prozessor, welcher z.B. autark Spiegelspeicher führt. Die seit 7/2005 ausgelieferten Leser von Automaten Seitz sind in der Regel bereits jetzt elektrisch kompatibel.
Für die Umstellung auf diese Technologie, muss über unseren Service eine entsprechende Konfiguration am Leser und ein Upgrade vorgenommen werden. Die MIFARE DESFire Leser verhalten sich abwärtskompatibel. D.h. classic Medien funktionieren auch mit MIFARE DESFire Lesern und Software. Dies ermöglicht eine schrittweise Umstellung auf MIFARE DESFire Medien. Bis jetzt wurde die MIFARE DESFire Technologie nicht angegriffen.

Die von NXP angekündigte MIFARE plus Technologie soll als Erstversion im vierten Quartal 2008 verfügbar sein. Wir beobachten diese Technologie und sobald nähere Informationen für Integratoren zur Verfügung stehen, werden wir sehr schnell und ernsthaft eine Aufnahme in unser Portfolio prüfen.

Zusammenfassung

Eine massive und akute Bedrohung oder unauffällige Massenmanipulation sehen wir im Moment nicht. Dazu sind zusätzliche Hardware und spezielles, tiefes Know-how notwendig. Angriffe und Manipulationen auf das System können wir nicht ausschließen. Das Hintergrundsystem von Automaten Seitz bietet aber zusätzliche Sicherheiten und Prüfungsmöglichkeiten. Allerdings empfehlen wir als Vorsichtsmaßnahme den Einsatz des Updates/Upgrades.

Mittelfristig sollte der Umstieg auf neuere Technologie wie MIFARE DESFire oder ggf. MIFARE plus in Betracht gezogen werden.

Mit freundlichen Grüßen

AUTOMATEN SEITZ GmbH

Geschäftsführerin
Andrea Seitz-Maier

Technischer Leiter
ppa. Joachim Egelhof