Einleitung

Henryk Ploetz und andere haben Informationen herausgegeben, die Angriffe auf MIFARE Classic massiv erleichtern.

NXP versucht diese Publikationen zu verhindern, aber es liegt in der Natur des Internets, dass das wohl kaum klappen wird.

Diese Mitteilung kam kurz nach 2008, kurz nach einem Beitrag über das Reverse Engineering auf dem Chaos Communication Congress.

Was ist MIFARE?

1990er Jahre: Mikron aus Österreich entwickelt das Mikron Fare-collection System - das RFID Chipkarten-System, das heute unter dem Namen MIFARE Classic bekannt ist. Mit diesem System ist es möglich Guthaben und Zugriffsberechtigungen direkt auf der Karte zu speichern und zu ändern ohne einen Server zu brauchen, auf dem die Daten hinterlegt werden.

1995: Das Unternehmen Mikron wurde von Philips aufgekauft und zusätzliche Chips wurden entwickelt.

2006: Die komplette Sparte MIFARE wurde in das Subunternehmen NXP ausgelagert

Lizenznehmer:

- Infineon (als Tochter von Siemens)
- Hitachi
- Gemalto (Anbieter von SIM, EC, Kriedikaten aus den Niederlande. Hält 50% Weltmarktanteil im Chipkarten-Markt)
- andere

MIFARE Produktportfolio

Heute gibt es die 4 Haupt-Kategorien von MIFARE-Chips mit verschiedenen Speichergrößen, Verschlüsselungsalgorithmen und Einsatzzwecken

Ultralight
2001: Ultralight: 64 byte, ISO 14443A, 7 byte ID, Keine Verschlüsselung
-> 2012 erscheint Android-App zum Auslesen und Wiedereinspielen der Daten (Counter wird dadurch zurückgesetzt)
2008: Ultralight C: 1 Key, DES/ 3DES zur Authentifizierung, Purse Functionality

2012: Ultralight EV1: Decrement only

DESFire
Seitenkanalangriff: Messung der elektromagnetischen Abstrahlung.
Laut RUB: ca. 2500 Messungen (7 Stunden) und Equipment für 2000€
-> DESFire EV1 hat DESFire ersetzt

Plus
Im März 2008 hat NXP einen neuen Chip angekündigt ([NXP08b]), der ebenfalls “Mifare

Plus” heisst und einen Zwischenschritt zwischen Mifare Classic und Mifare DESfire EV1 darstellt. Dieses neu vorgestellte Mifare Plus soll (optional) zufällige UIDs, Crypto-1-Verschlüsselung (permanent abschaltbar) und 128 Bit AES-Verschlüsselung enthalten und die Migration von Mifare Classic auf Karten mit dem AES-Algorithmus erleichtern: EineInstallation kann solange mit Crypto-1 betrieben werden, bis alle Lesegeräte/Backend- Systeme AES-fähig sind und alle Karten gegen Mifare-Plus-Karten ausgetauscht wurden. Dann kann der gesamte Betrieb mit einem Schlag auf AES umgestellt und Crypto-1 dauerhaft abgeschaltet werden.

Crypto1 und 128-bit AES
Multi-Sektor Authentifizierung
Proximity Check
Virtual Card

Plus X: unterstütz zusätzlich proximity check und virtua

Speicherlyout -Wie ist so ein Chip aufgebaut?

Schaubild der 1 KByte Karte

16 Sektoren
a 4 Blocks
a 16 Byte

1. Manufacturer-Block

READ-ONLY

UID – Unique ID (7 Byte)
NUID – Not Unique ID (4 Byte)
2010 wurden Karten mit 7 Byte ID angeboten
4Byte -> 2^32 => 4,29 Milliarden IDs / Karten

Verkauft: 2 Milliarden Karten und 25 Millionen Kartenlesegeräte

BCC: Prüfsummme der UID

Herstellerspezifische Daten

1.b. Daten
Guthaben, Name, usw

2. Sektor-trailer
Key A
Key B
Access Control List

ACL – Access Control Lists

In jedem Sektor-Trailer wird gespeichert:
- Jeder Sektor wird durch zwei Keys (Schlüssel A und B) gesichert
    - Pro Schlüssel können verschiedene Rechte vergeben werden, diese werden in den ACLs gespeichert
- ACL: Access Control List
    - read-only Bereich auf der Karte
    - Zugrifssrechte: lesen & schreiben, nur lesen oder gesperrt

Bsp. 1: Key A darf lesen, Key B darf schreiben -> A kann für alle veröffentlicht werden, B bleibt geheim

Bsp. 2: Ermöglicht wiederaufladbare Wertkarten.
Automat enthält Key A, der nur dekrementieren darf – diese Automaten können also ungesichert aufgestellt werden, da ein Dieb mit dem Key nichts anfangen kann.
Kassen mit Inkrement-Recht auf Key B – Kassen müssen geschützt aufgestellt werden.

Bsp. 3: Nicht-wiederaufladbare Wertkarten

Authentisierung – Wie werden die ACLs durchgesetzt?

1. Der Reader bittet um Authentisierung (AUTH1A für Key A, AUTH1B für Key B), die Blocknummer, auf die zugegriffen werden soll muss übergeben werden
2. Die Karte schickt eine challenge nonce NC an den Reader
3. Von hier ab ist die Kommunikation verschlüsselt. Der Reader antwortet auf die challenge mit einer verschlüsselten „reader response AR“ und einer verschlüsselten „reader nonce NR“
4. Wenn die Karte die Antwort, die vom Reader kommt, korrekt entschlüsseln kann, ist bewiesen, dass der Reader den richtigen shared Key hat

-> Danach kann auf die verschlüsselten Blöcke zugegriffen werden und jegliche Kommunikation läuft verschlüsselt ab

MIFARE Classic – PRNG

Pseudo Random Number Generator

- generiert Zufallszahl, die als Nonce verwendet wird
(- Sektor-Key, das Karten Nonce NC, UID, Reader Nonces werden zur Initialisierung des Crypto1 genutzt)
- 16 Bit breites Schieberegister
- 2^16 = 65.536 mögliche Nonces
- Takt laut ISO-14443 105,9 kHz -> 0,62 sec. Bis sich die nonces wiederholen
- Der PRNG wird, kurz nachdem die Karte mit genügend Strom über die Luftschnittstelle versorgt wurde, initialisiert, indem das Shift-Register auf einen festen Wert gesetzt wird (101010 . . .).

Crypto1

Algebraischer Angriff (lösen per Formel):
Nur ein mitgeschnittener IV (Nonce) und 50 Bit Keystream -> 200 sek. Um den vollen 48 Bit Key zu knacken.

Mit 4 IVs -> 12 sek.
Daten Mitschneiden, Keys herausfinden, Klon erstellen -> sollte in wenigen Minuten schaffabar sein.

Replay
Eve hört Nonce der Kare (Nc) + Response des Readers + Befehle (z.B. Increase des Guthabens) ab

Eve berechnet aus dem Nc, wie lange sie nach der Stromzufuhr zur Karte warten muss bis sie das AUTH abschickt um das gleiche Nc zu erhalten.

Eve sendet den mitgeschnittenen verschlüsselten Response (ohne dessen Inhalt zu kennen) an die Karte

Eve sendet den mitgeschnittenen verschlüsselten Befehl an die Karte

Gegenmaßnahme: echter Zufallszahlengenerator

Brute Force
Erwartungswert, falls die Wahrscheinlichkeit für alle Schlüssel gleich ist

Für einen einzigen Key von 2 pro Sektor (insgesamt 16 Sektoren)

Relay
Generischer Angriff, im Prinzip auf jede kontaktlose Kommunikation anwendbar

Gegenmaßnahmen:
- Zeitmessung (Bei MF Classic nicht möglich, mindestens 1ms Zeit zum Weiterleiten)
- Schutzhülle um Karte
- Taste zum Aktivieren der Karte
-> Komfortverlust (auf Niveau von kontaktbehafteten Karten)

Laziness
Default Keys
aus Practical-Attacks_MIFARE-Classic_mht.pdf S. 31 S47

Fahrkarten in Rumänien, Luxemburg und Bulgarien
Studentenausweise und Eintrittskarten in Tschechien

Weakness 2: Same Key for All Cards
The sector that contains the data blocks used for authentication is protected by the same key for all cards issued. It has remained unchanged since the launch of the system. It is the same key in cards for students (for which access rights given should be minimum) and in cards for security sta (for which access rights given should be maximum). This means that the attacker, once she has that key, is able to obtain any victim's identity using the right equipment just by walking past the victim.