Cloning Credit Cards

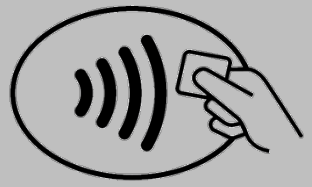
Michael Roland

17. Dezember 2013 • Hacking Night • Hagenberg

This work is part of the project "High Speed RFID" within the EU program "Regionale Wettbewerbsfähigkeit OÖ 2007–2013 (Regio 13)" funded by the European regional development fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).

NFC Research Lab Hagenberg • www.nfc-research.at
A research group of the University of Applied Sciences Upper Austria

EMV Contactless



- Standard für Kredit-/Debit-Karten mit Kontaktlosschnittstelle
  - Nicht einzelnes Protokoll, sondern Sammlung verschiedener Bezahlsysteme
- Basiert auf ISO 14443
  - 13.56 MHz, induktive Kopplung
  - Kompatibel zu NFC

VISA
V PAY
Visa payWave
AMERICAN EXPRESS
express pay
MasterCard
paypass
Maestro
UnionPay 银联
Quick 闪付Pass
JCB
J/Speedy

MasterCard PayPass

- 2 Protokolle für Kontaktlostransaktionen
  - EMV
  - Mag-Stripe
- EMV-Mode
  - EMV-Protokoll (“Chip & PIN”) über Kontaktlosschnittstelle
- Mag-Stripe-Mode
  - (erweitertes) Magnetstreifen-Protokoll über Kontaktlosschnittstelle
    - Kompatibel zu Magnetstreifen-Back-End-Systemen

Wie funktioniert eine PayPass-EMV-Transaktion?

Liste der verfügbaren Payment-Applikationen anfordern

--> 00A404000E...
<-- 6F2C840F32...
--> 00A4040007...
<-- 6F298407A0...

Karte unterstützt MasterCard Credit

MasterCard-Applikation auswählen

--> 80A8000002...
<-- 7716820219...
--> 00B2010C00
<-- 701A571367...

Applikationsparameter
(Applikationsname, bevorzugte Sprache, …)

Applikationskonfiguration anfordern und Transaktion starten

--> 00B2020C00
<-- 70535F2403...
--> 00B2030C00
<-- 701D9F4A01...

Konfigurationsparameter
(unterstützte Protokolle, …)

--> 00B2011400
<-- 7081BC8F01...

Kartendaten (lt. Konfiguration) anfordern

--> 00B2021400
<-- 709C9F4703...

Kartendaten

--> 00B2041400
<-- 7081C19F46...

Transaktionsdaten an Karte senden und digitale Signatur anfordern

--> 00B2012400
<-- 702B8E0C00...
--> 80AE500042...
<-- 7781B29F27...

digitale Signatur über Transaktions- und Kartendaten

Karten- und Transaktionsdaten bei PayPass EMV

- Statische Kartendaten
  - Daten sind frei lesbar und werden unverschlüsselt übertragen
  - Kartennummer (Primary Account Number, PAN)
  - Gültigkeitsdaten
  - Land in dem Karte ausgestellt wurde
  - Währung in der die Karte abgerechnet wird
  - Liste der Daten zur Berücksichtigung bei der digitalen Signatur
  - Protokoll über die letzten Transaktionen
  - öffentlicher Schlüssel/Zertifikat des Kartenherausgebers und der Karte
  - geheimer Schlüssel der Karte *(nicht auslesbar)*
- Dynamische Daten
  - Daten werden unverschlüsselt übertragen
  - Betrag, Währung, Datum, Uhrzeit, Art, … der Transaktion
  - Länderkennung, Art, … des Terminals
  - Zufallszahl, Transaktionszähler, digitale Signatur

Wie funktioniert eine PayPass-Mag-Stripe-Transaktion?

Liste der verfügbaren Payment-Applikationen anfordern

--> 00A404000E...
<-- 6F2C840E32...
--> 00A4040007...
<-- 6F298407A0...

Karte unterstützt MasterCard Credit

MasterCard-Applikation auswählen

--> 80A8000002...
<-- 7716820219...
--> 00B2010C00...
<-- 70759F6C02...

Applikationsparameter
(Applikationsname, bevorzugte Sprache, …)

Applikationskonfiguration anfordern und Transaktion starten

--> 802A8E8004...
<-- 770F9F6102...

Konfigurationsparameter
(unterstützte Protokolle, …)

Kartendaten (lt. Konfiguration) anfordern

Kartendaten für Mag-Stripe

Zufallszahl an Karte senden und Autorisierungscode anfordern

Autorisierungscode (Card Verification Code, CVC3) und Transaktionszähler

Karten- und Transaktionsdaten bei PayPass Mag-Stripe

- Statische Kartendaten
  - Daten sind frei lesbar und werden unverschlüsselt übertragen
  - Kartennummer (Primary Account Number, PAN)
  - Gültigkeitsdaten
  - gemeinsamer Schlüssel zwischen Karte und Herausgeber *(nicht auslesbar)*
- Dynamische Daten
  - Daten werden unverschlüsselt übertragen
  - Zufallszahl, Transaktionszähler, Autorisierungscode (unabhängig vom Transaktionsinhalt)

PayPass: EMV vs. Mag-Stripe

- EMV-Mode
  - Asymmetrische Kryptographie
  - Signatur über statische Kartendaten und Transaktionsdaten
  - Terminal kann Signatur selbst prüfen („Offline“)
  - Unterstützung von EMV-Mode optional (Ausnahme: Europa)
- Mag-Stripe-Mode
  - Symmetrische Kryptographie
  - Keine Integritätsprüfung der statischen Kartendaten
  - Autorisierungscode
    - Kein Bezug zu den Transaktionsdaten (Betrag, …)
    - Nur „Vorhandensein“ der Originalkarte kann überprüft werden
    - Nur Kartenherausgeber kann Gültigkeit eines Transaktionscodes bestätigen („Online“)
  - Alle Karten und Terminals unterstützen PayPass Mag-Stripe
    - Rückwärtskompatibilität mit älteren/ausländischen Terminals bzw. Karten
    - Ausnahme: Maestro-Karten (z.B. Bankomatkarte) können **nur** EMV-Mode!

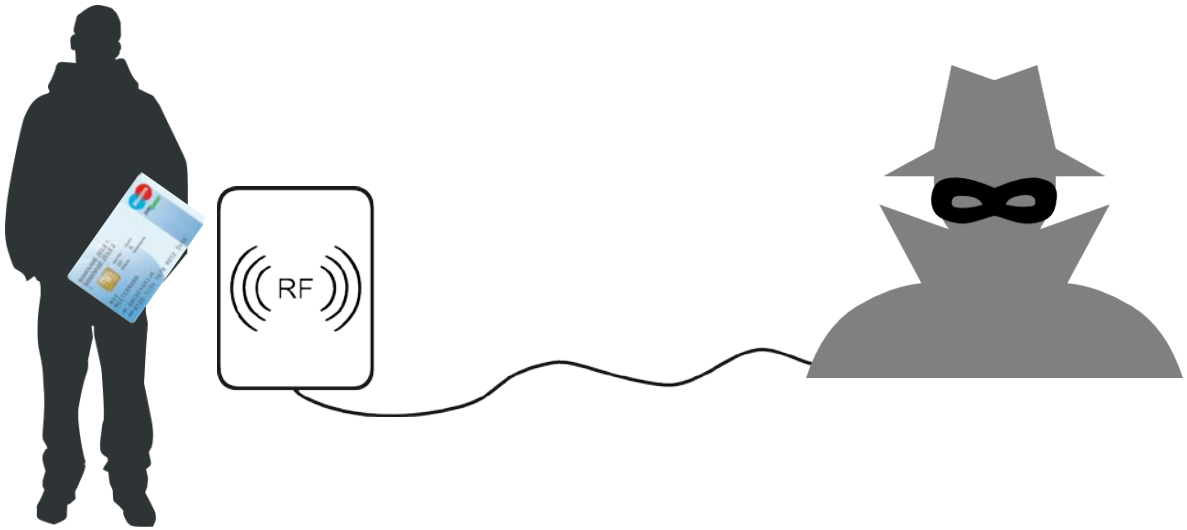
Möglichkeiten zum Kopieren von Karten

- Eavesdropping
  - Mithören von Transaktionen
- Skimming
  - Auslesen von statischen Daten
- Skimming mit Pre-play
  - Vorberechnen von Transaktionsdaten

Eavesdropping

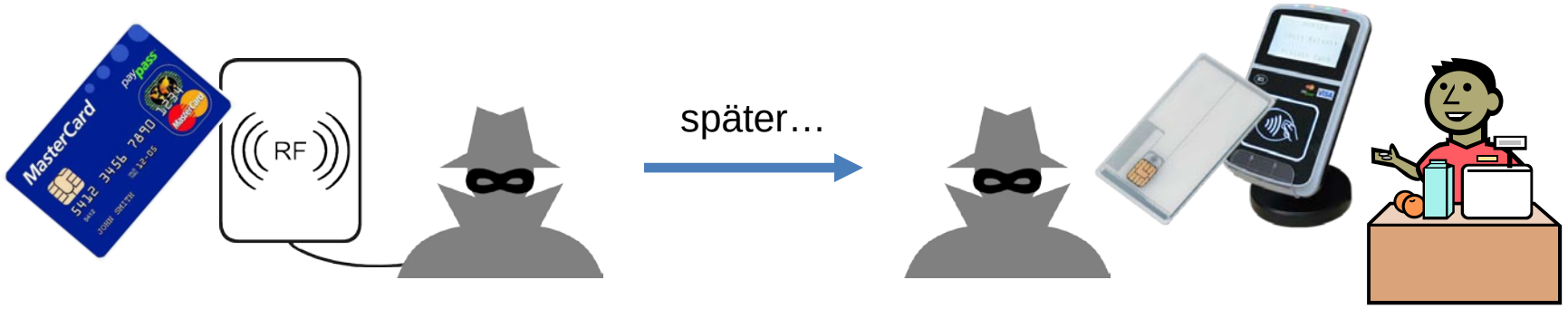
- NFC = Funkübertragung
  - Kommunikation nur über wenige Zentimeter
  - ABER: Mithören auch über mehrere Meter hinweg möglich
- Angriff
  - Informationen über Karte und aktuelle Transaktion ausspähen
  - Daten auf neue Chipkarte oder Magnetstreifenkarte speichern
    - Chipkarte: geheime Schlüssel fehlen
    - Magnetstreifenkarte: Magnetstreifenautorisierungscodes fehlen
    - Daten reichen im Allgemeinen **nicht** aus um weitere Kartentransaktionen durchzuführen oder funktionsfähige Kartenkopie zu erstellen (Ausnahme: einige Onlinebezahlsysteme)

Skimming



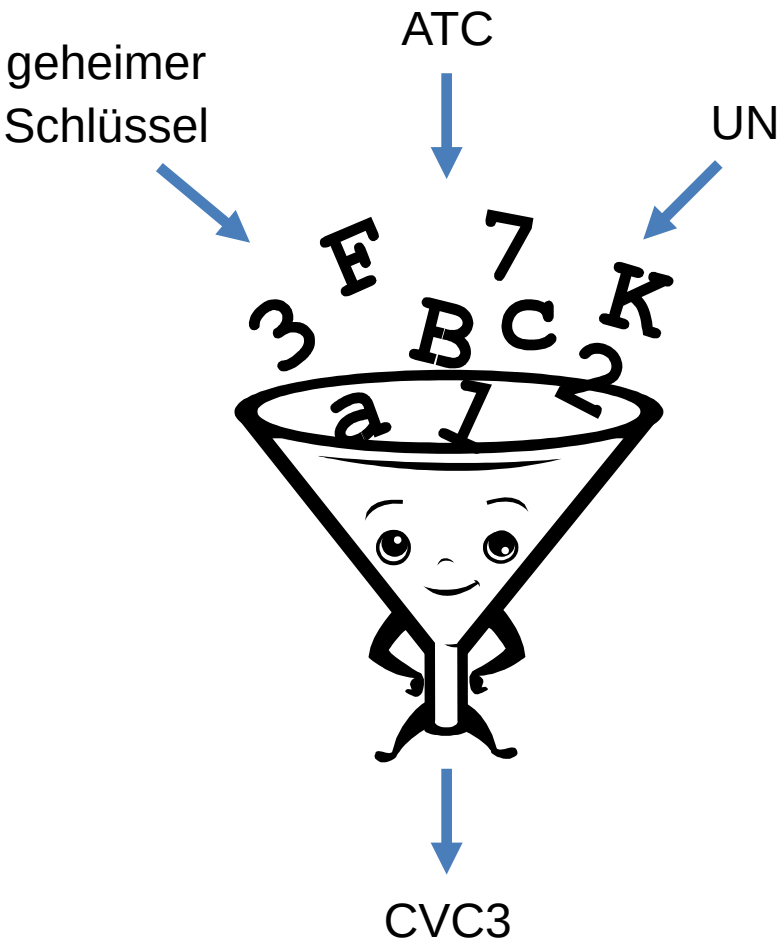
- Kartendaten frei auslesbar
- Angriff
  - Kartendaten auslesen
  - Daten auf neue Chipkarte oder Magnetstreifenkarte speichern
    - Chipkarte: geheime Schlüssel fehlen
    - Magnetstreifenkarte: Magnetstreifenautorisierungscodes fehlen
    - Daten reichen im Allgemeinen **nicht** aus um weitere Kartentransaktionen durchzuführen oder funktionsfähige Kartenkopie zu erstellen (Ausnahme: einige Onlinebezahlsysteme)

Skimming mit Pre-play



- Angriff
  - Statische Kartendaten auslesen
  - EMV-Mode: digitale Signatur für Transaktionsdaten vorausberechnen
  - Mag-Stripe-Mode: dynamische Transaktionscodes (CVC3) vorausberechnen
  - Daten auf neue Chipkarte speichern
- Problem
  - EMV-Mode: digitale Signatur ist abhängig von
    - Transaktionsdaten (Betrag, Datum, Uhrzeit, …)
    - Zufallszahl (von Terminal generiert)
    - Transaktionszähler (fortlaufender Zähler auf Karte)
  - Mag-Stripe-Mode: Transaktionscode ist abhängig von
    - Zufallszahl (von Terminal generiert)
    - Transaktionszähler (fortlaufender Zähler auf Karte)

Transaktionscode (CVC3) bei PayPass Mag-Stripe



- geheimer Schlüssel
  - Sicher im Chip gespeichert und nicht auslesbar
  - CVC3 kann nur mit Originalkarte generiert werden
- ATC = Application Transaction Counter
  - Im Chip gespeichert und wird bei jedem Transaktionscode erhöht
  - Schutz vor Mehrfachnutzung von CVC3s (Re-play)
- UN = Unpredictable Number
  - Vom Terminal erzeugte „Challenge“
  - Schutz vor Vorausberechnung von CVC3s (Pre-play)

Pre-play trotz Unpredictable Number

- Für Pre-play-Angriff müsste UN voraussehbar sein
- UN bei PayPass Mag-Stripe:
  - UN ist 4-Byte-Feld
    - 2^{32} (~4.3 Milliarden) mögliche Werte
    - Vorausberechnung kaum möglich
  - UN verwendet BCD-Codierung
    - 100 Millionen mögliche Werte
    - ~43 Mal weniger als in 4 Byte Platz hätte
    - Vorausberechnung dennoch kaum möglich
  - Anzahl der Stellen der BCD-codierten Zahl vom Kartenherausgeber vorgegeben
    - Typisch: 2-3 Ziffern
    - 3 Ziffern: 1000 mögliche Werte
    - ~4.3 Millionen Mal weniger als in 4 Byte Platz hätte
    - **Vorausberechnung von 1000 Codes in ca. 1 Minute möglich**

Einschränkungen

- ATC-Sequenz
  - CVC3s können nicht mehrfach verwendet werden
  - Transaktion mit höherem Transaktionszähler führen dazu, dass ältere CVC3s (niedrigerer ATC) ungültig werden
  - ATC hat Obergrenze (≤ 65535): Ist Grenze erreicht wird Karte unbrauchbar!
- Mag-Stripe-Mode
  - Pre-play funktioniert nur mit PayPass Mag-Stripe (UN bei EMV-Mode nutzt vollen Wertebereich)
  - Maestro (Bankomatkarte) verwendet kein PayPass Mag-Stripe
  - Wenn Karte und Terminal EMV-Mode unterstützen wird auch EMV-Mode verwendet
    - Angriff funktioniert also nur wenn entweder Terminal oder Karte nur das Mag-Stripe-Protokoll unterstützen
    - *Lösung: Downgrade*

Downgrade

- Statische Kartendaten so manipulieren, dass Karte für Terminal wie reine PayPass Mag-Stripe Karte aussieht
- Unterstützung für EMV-Mode ist einzelnes Bit in den Konfigurationsdaten der Karte (Application Interchange Profile)
- Keine Integritätsprüfung der Konfigurationsdaten durch Terminal
- **Downgrade: Bit auf der Kartenkopie nicht setzen**
  - Kartenherausgeber könnte diesen Fall bei der Freigabe der Transaktion erkennen
  - Test wird in der Praxis jedoch derzeit nicht durchgeführt

Angriff im Überblick

- Kartendaten lesen
  - Android NFC-App (auf Galaxy Nexus)
  - Statische Kartendaten lesen
  - EMV-Mode-Bit verändern
  - 1000 CVC3s vorausberechnen
    - Ein Code für jeden mögliche Zufallszahl
    - Damit kann mindestens eine Transaktion durchgeführt werden
  - Performance
    - ~1000 Codes/Minute mit Galaxy Nexus
    - Einige Karten lassen sich nicht gut lesen

- Karten-Klon erstellen
  - Java Card Applet auf leerer Smartcard
    (alternativ: Emulation mit Android HCE)
  - Applet simuliert Funktionalität einer PayPass-Kreditkarte
    - Statische Kartendaten mit Daten der Originalkarte befüllbar
    - Liste aus vorausberechneten UN + ATC + CVC3 Datensätzen
    - Klon liefert ersten Datensatz mit der vom Terminal gesendeten UN

Workarounds & Limits

- Erkennung: Mag-Stripe vs. EMV-Mode
  - Kartenherausgeber bekommt Information über
    - Unterstützte Protokolle des Terminals
    - Für Transaktion verwendetes Protokoll
  - Kartenherausgeber hat Information, ob Karte das EMV-Mode-Protokoll unterstützt
  - Kartenherausgeber könnte Downgrade-Angriff (EMV-Mode-Karte wird auf EMV-Mode-Terminal im Mag-Stripe-Mode verwendet) erkennen und Transaktionen ablehnen
- Wertebereich von UN maximieren
  - Anzahl der Ziffern wegen Mag-Stripe-Backend-System begrenzt
  - Eine Zusätzliche Ziffer würde die notwendige Zeit für den Preplay-Angriff verzehnfachen
  - 4 Ziffern: 10 Minuten → Pre-play kaum noch möglich!
  - Kartenherausgeber sollte Anzahl der Stellen von UN maximieren
- Einschränkungen bei Kontaktlostransaktionen
  - PIN-los in Österreich auf € 25 beschränkt
  - Keine Bargeldbehebungen möglich

Demo

http://youtu.be/VlAwxUs1ZFo

Cloning Credit Cards – A combined pre-play and downgrade attack on EMV Contactless (M. Roland, J. Langer; WOOT 2013)

Dr. Michael Roland

Research Associate, NFC Research Lab Hagenberg
University of Applied Sciences Upper Austria

michael.roland (at) fh-hagenberg.at

This work is part of the project "High Speed RFID" within the EU program "Regionale Wettbewerbsfähigkeit OÖ 2007–2013 (Regio 13)" funded by the European regional development fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).

NFC Research Lab Hagenberg • www.nfc-research.at
A research group of the University of Applied Sciences Upper Austria