



Near Field Communication Security

Michael Roland

28. Mai 2014 • Mobile Marketing Innovation Day • Wien



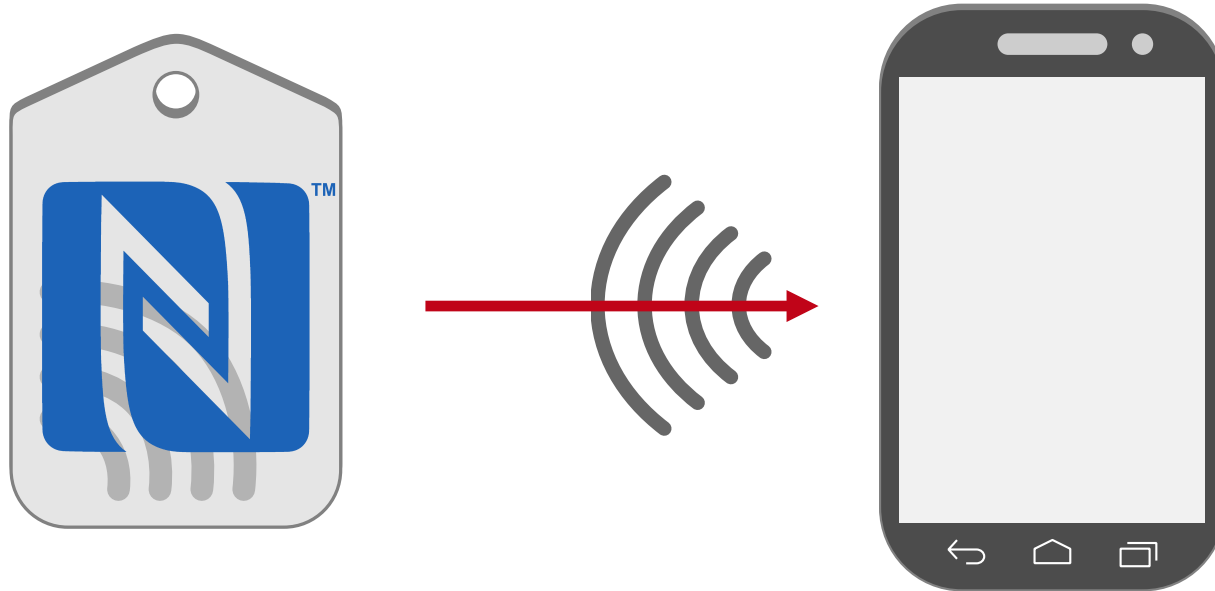
This work is part of the project “High Speed RFID” within the EU program “Regionale Wettbewerbsfähigkeit OÖ 2007–2013 (Regio 13)” funded by the European regional development fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).



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

Was leistet NFC im Smartphone?

Tagging



- NFC-Tags: Interaktive Inhalte auf Smartphone bringen
 - ▶ URLs, sendebereite SMS, Visitenkarten, ...
- Vergleichbar mit QR-Codes, aber
 - ▶ Robuster
 - ▶ Einfacher bedienbar

Was leistet NFC im Smartphone?

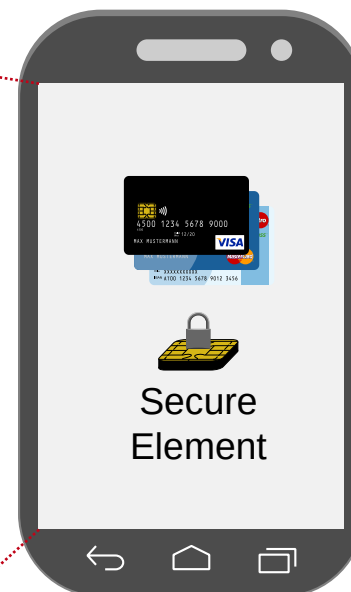
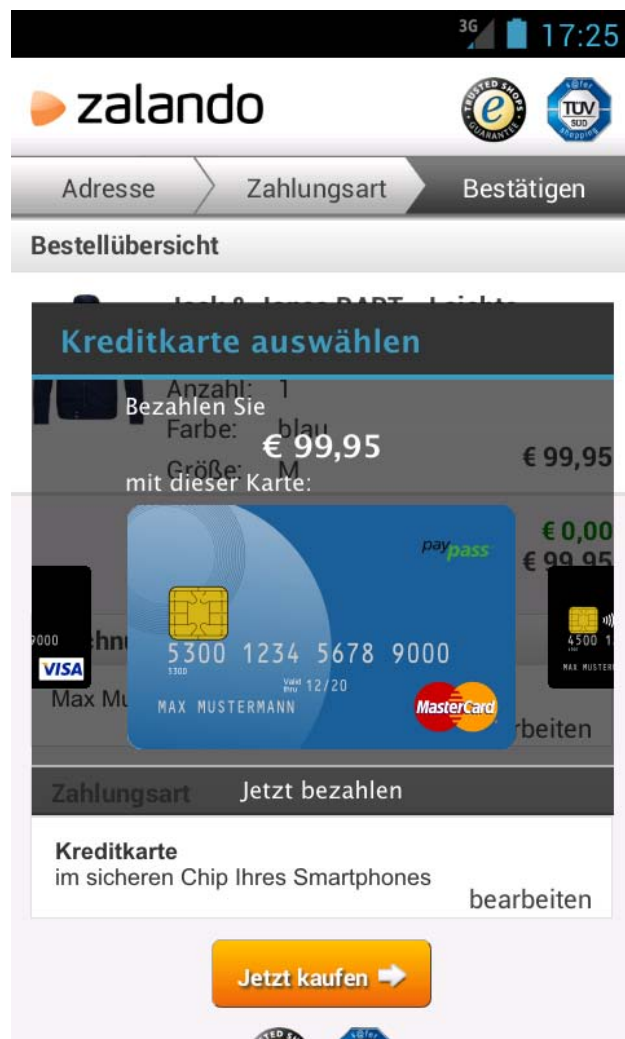
Smartphone als NFC-Chipkarte



- Funktionalität von NFC-Chipkarten kommt ins Smartphone
 - ▶ Secure Element: Emulation durch sicheren Smartcard-Chip
 - ▶ Host-based Card Emulation: Emulation durch App
- Payment, Ticketing, Zutrittssysteme, Kundenkarten
 - ▶ Smartphone (überall) einsetzbar wo es jetzt schon NFC-Karten gibt
 - ▶ ABER: nicht jede Karte kann vom Smartphone emuliert werden

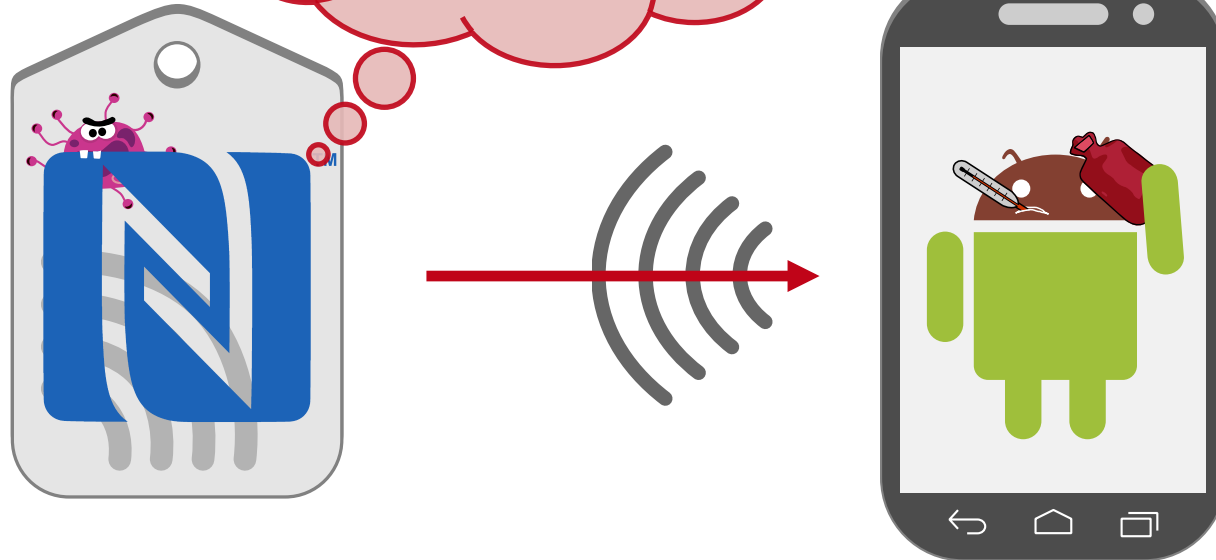
Was leistet NFC im Smartphone?

Sicheres In-App Payment



- Karten im Secure Element direkt für In-App Payment nutzen
- *Karten-gestützte* Transaktionsautorisierung
 - ▶ im mobilen Webbrowser
 - ▶ in Apps

Tagging Sicherheit?



- Manipulation / Austausch / Überkleben von NFC-Tags
 - ▶ Phishing / Pharming / Clickjacking
 - ▶ SMS an teure Mehrwertnummern
 - ▶ Installation von Schadsoftware
 - ▶ ...

Smartphone als NFC-Chipkarte

zusätzlicher Schutz

- Mobiltelefon als Benutzerschnittstelle der virtuellen Karte
 - ▶ Karte aus- und einschalten
 - zusätzliche PIN-Eingabe möglich
 - ▶ aktuelle Transaktion anzeigen
 - ▶ Liste der letzten Transaktionen anzeigen
 - ▶ Prepaid-Karten mit integrierter Lademöglichkeit



NFC-Kreditkarten-Transaktion

Wie funktioniert das?



Liste der verfügbaren
Payment-Applikation anfordern

MasterCard-Applikation auswählen

Applikations-Konfiguration anfordern

Kartendaten (lt. Konfiguration) anfordern

Transaktionsdaten an Karte senden und
digitale Signatur anfordern

```
--> 00A404000E...
<-- 6F2C840E32...
--> 00A4040007...
<-- 6F298407A0...
--> 80A8000000A...
<-- 7716820219...
--> 00B2010C00...
<-- 701A571367...
--> 00B2020C00...
<-- 70535F2403...
--> 00B2030C00...
<-- 701B314A01...
--> 00B2011400...
<-- 7081BC8F01...
--> 00B2021400...
<-- 700C0F4702...
--> 00B2041400...
<-- 7081C19F46...
--> 00B2012400...
<-- 702B8E0C00...
--> 80AE500042...
<-- 7781B29F27...
```

Karte unterstützt „MasterCard“

Applikationsparameter

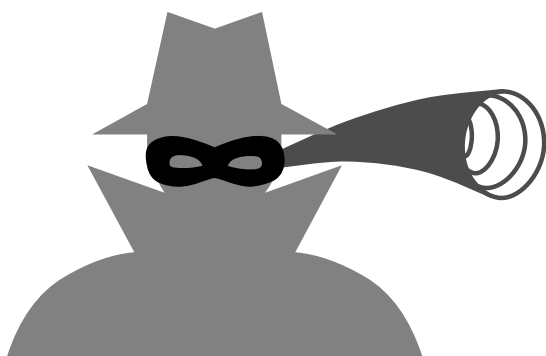
Konfigurationsparameter

Kartendaten

digitale Signatur über Transaktions-
und Kartendaten

NFC-Kreditkarte: mögliche Angriffe

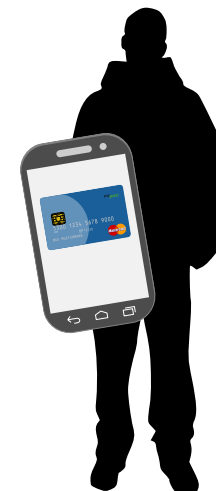
Eavesdropping



- NFC = Funkübertragung
 - ▶ Kommunikation nur über wenige Zentimeter
 - ▶ ABER: Mithören auch über *mehrere Meter* hinweg möglich
- Informationen über Karte und aktuelle Transaktion ausspähbar
 - ▶ z.T. personenbezogene Daten:
Kartenummer, Ablaufdatum, bezahlter Betrag, ev. Quick-Guthaben, ...
 - ▶ **Nicht übertragen:** geheime (Signatur-)schlüssel
 - Daten reichen **nicht** aus um weitere Kartentransaktionen durchzuführen oder Kartenkopie zu erstellen

NFC-Kreditkarte: mögliche Angriffe

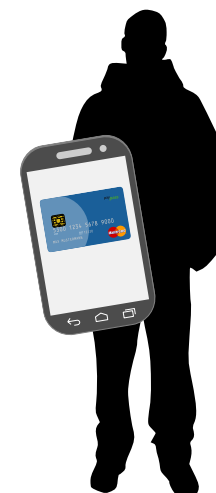
Skimming



- Entfernung zwischen Angreifer und Opfer
 - ▶ Mit Smartphone: max. wenige Zentimeter
 - ▶ Mit Speziallesegerät: 1-2 Meter möglich
- Kartendaten frei auslesbar
 - ▶ Karte im Smartphone: Kartenemulation **ausschaltbar**
 - ▶ z.T. personenbezogene Daten
Kartenummer, Ablaufdatum, ev. Transaktionslog, ev. Quick-Guthaben, ...
 - ▶ **Nicht auslesbar:** geheime (Signatur-)schlüssel
 - Daten reichen **nicht** aus um später Kartentransaktionen durchzuführen oder Kartenkopie zu erstellen

NFC-Kreditkarte: mögliche Angriffe

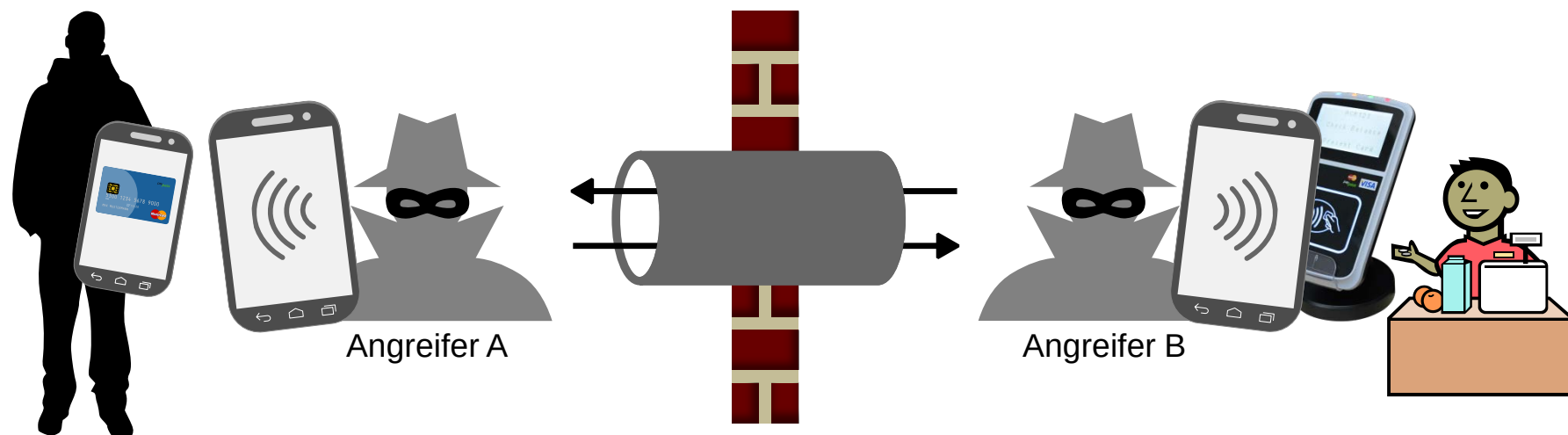
Abbuchen im Vorbeigehen



- Skimming mit echtem Bezahlterminal
 - ▶ Karte ist nur „Schlüssel“ zum Konto
 - ▶ Geld kann nur auf Händlerkonto gebucht werden
 - ▶ Angreifer über Händlervertrag leicht identifizierbar
- Andere Bezahlssysteme
 - ▶ ???

NFC-Kreditkarte: mögliche Angriffe

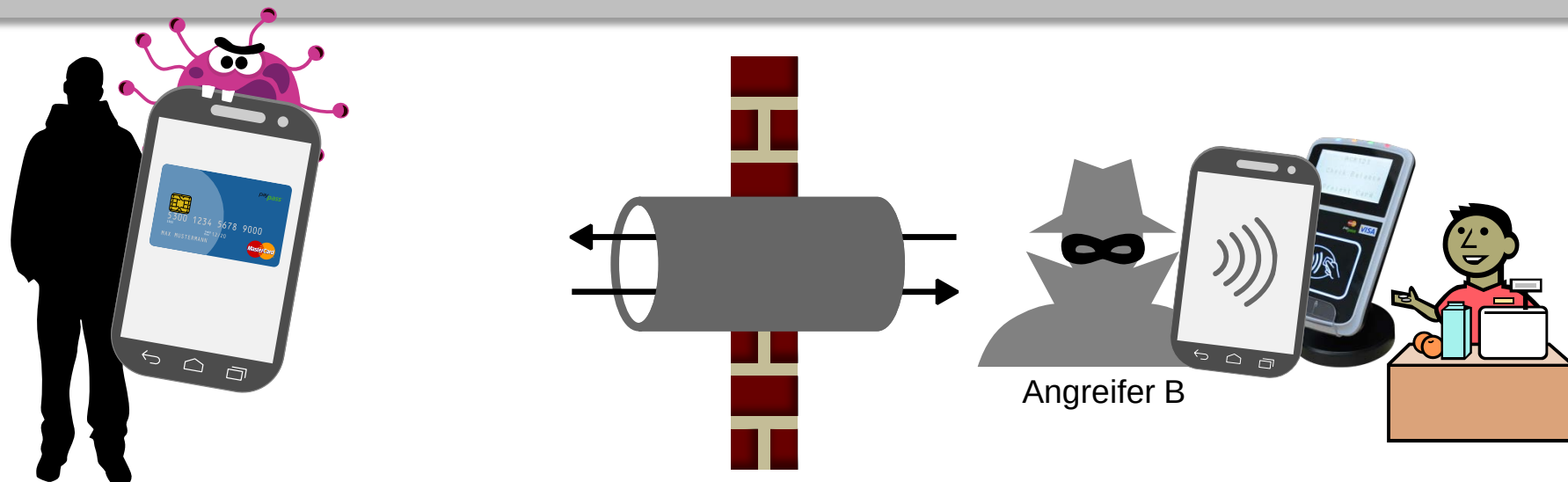
Relay



- Zwei Angreifer notwendig
 - ▶ Angreifer A mit Lesegerät in Reichweite von Opfer
 - ▶ Angreifer B bezahlt an Kasse
- Hürden für Angreifer
 - ▶ Angreifer A und B müssen *zeitgleich* arbeiten
 - ▶ Kontaktlostransaktionen (ohne PIN) auf Kleinbeträge beschränkt
 - ▶ typ. keine Barbehebungen möglich

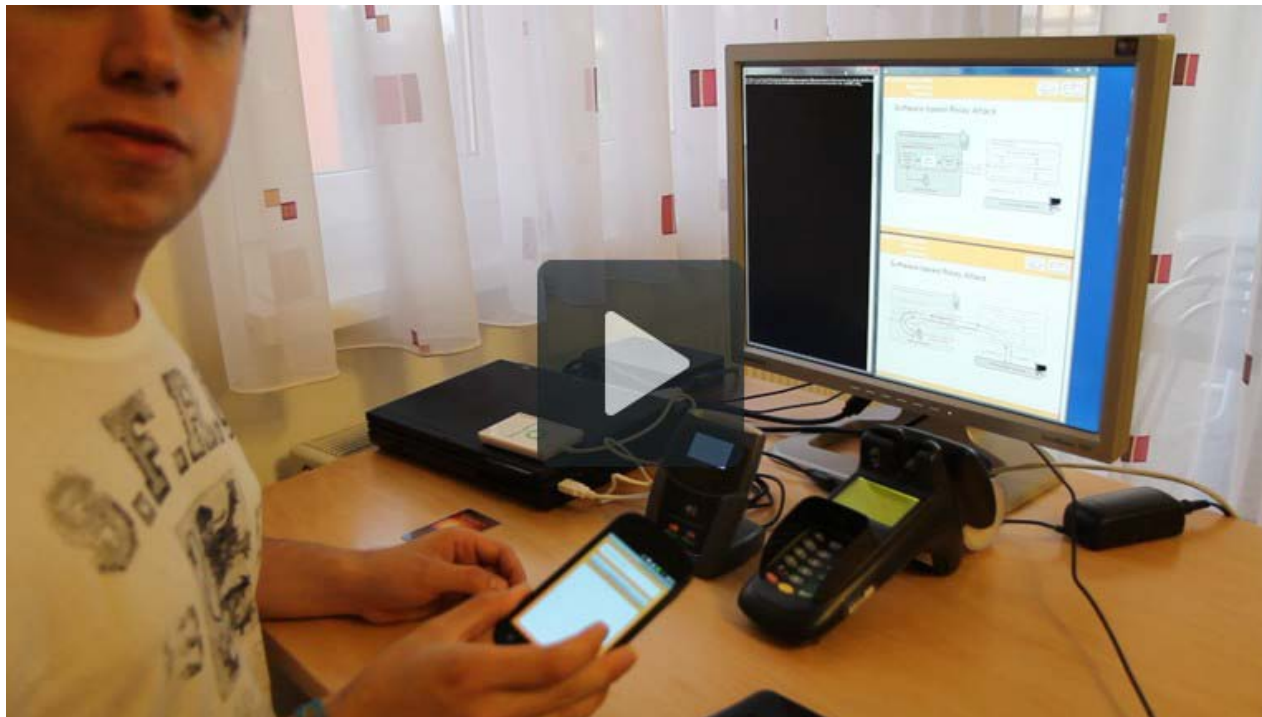
NFC-Kreditkarte: mögliche Angriffe

Software-basiertes Relay



- Nur ein Angreifer (B) an der Kasse notwendig
 - ▶ Statt Angreifer A greift App (Malware) auf virtuelle Karte zu
- Smartphone-System potentiell unsicher (im Vgl. zu Smartcard-Chip)
 - ▶ Schadsoftware könnte Zugriff auf virtuelle Karte erlangen
- Secure Element: Schutzmaßnahmen durch *gutes* Softwaredesign bedingt möglich
 - ▶ virtuelle Karten nur für NFC-Schnittstelle freigeben (Zugriff durch Apps blockieren)
 - ▶ ABER: sicheres SE-basiertes In-App Payment wird dadurch unmöglich
- Host-based Card Emulation: ???

Google Wallet Relay Attack



http://youtu.be/_R2JVPJzufg

Applying Relay Attacks
to Google Wallet
(M. Roland et al.;
NFC 2013)



Dr. Michael Roland

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

[michael.roland \(at\) fh-hagenberg.at](mailto:michael.roland@fh-hagenberg.at)

