Near Field Communication
Research Lab
Hagenberg

University of Applied Sciences

Dissertation

Doktoratsstudium der
Techn. Wissenschaften

Angefertigt am Institut für
Computational Perception

Beurteilung:
Dr. Josef Scharinger
Dr. René Mayrhofer

Security Issues in Mobile NFC Devices

Michael Roland
NFC Research Lab Hagenberg
University of Applied Sciences Upper Austria

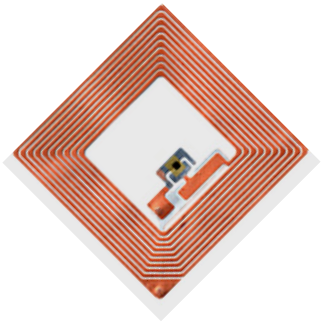
21. März 2013, Rigorosum, JKU Linz

This work is part of the project "4EMOBILITY" within the EU program "Regionale Weltbewerbsfähigkeit OÖ 2007–2013 (Regio 13)" funded by the European regional development fund (ERDF) and the Province of Upper Austria (Land Oberösterreich).

Agenda

- Was ist NFC?
- Motivation & Zielsetzung
- Forschungsfragen
- Überblick über die wesentlichen Ergebnisse
- Software-basierte Relay-Attacke im Detail

Was ist NFC?



- Near Field Communication
  - kontaktlose Übertragung über kurze Distanzen
  - Basis: RFID & Smartcards
  - Standardisiert in ECMA, ISO, NFC Forum
- NFC-Gerät kann
  - kontaktlose Chipkarten/NFC-Tags lesen
  - mit anderen NFC-Geräten kommunizieren
  - selbst als kontaktlose Chipkarte verwendet werden
- Typische Anwendungen
  - Vorgänge rund um das Mobiltelefon einfacher gestalten
    - Zugriff auf interaktive Inhalte durch einfache Berührung eines Objekts
    - Enabler für Bluetooth, Wi-Fi, …
  - NFC-Mobiltelefon ersetzt vorhandene Chipkarten
    - Payment, Ticketing, Access Control

Motivation

- NFC in vielen neuen Smartphones integriert
- Immer mehr NFC-Anwendungen verfügbar
- Dennoch viele Vorurteile gegen NFC
  - Unsicher, gefährlich, …
  - Unterstützt Betrug & Identitätsdiebstahl
- Bekannte Sicherheitsrisiken bei NFC
  - Manipulation von NFC-Tags
    - ungewollte Aktionen, Phishing, Mehrwert-SMS
  - „Virtueller Taschendieb“
    - Zugriff auf Kreditkarten, Zutrittskarten, … im Vorbeigehen
  - Abhören der Kommunikation
    - auch aus größerer Distanz!

Zielsetzung

- Beurteilung des aktuellen Stands der Sicherheit von NFC im Mobiltelefon
- Finden neuer Angriffsszenarien
- Lösen gefundener Sicherheitsprobleme

Forschungsfragen

- What are the strategies that NFC uses to provide security and privacy for its current applications?
- Are these measures adequate for the current applications?
- What are NFC's main unresolved security and privacy issues?
- What steps are necessary to make NFC a reliable and secure technology?

Ergebnisse im Überblick

- Fokus auf NFC-Tags und Secure Element
- NFC-Tags
  - Schutz der Daten durch digitale Signatur (Spezifikation: NFC Forum)
  - Spezifikation lässt Infrastruktur hinter Signatur offen
    → Definition einer Public-Key Infrastructure für NDEF-Signatur
    - Aussagekraft von Zertifikaten?
    - Verknüpfung von Zertifikaten mit signierten Inhalten?
    - Gültigkeitsdauer von Signaturen & Zertifikaten?
  - Spezifikation erfüllt Ziele einer digitalen Signatur (Integrität & Authentizität) nicht
    - Header-Information teilweise nicht signiert
    - Datensemantik trotz Signatur veränderbar

    → „Record Composition Attack“
  - Privatsphäre-Problem durch Verwendung von URLs in Signatur-Record
    - Angreifer kann Nutzungsinformationen zu NFC-Tags erhalten
    - Angreifer kann beliebigen HTTP GET-Request im Kontext des Benutzers ausführen

Ergebnisse im Überblick

- Secure Element
  - Sicherheitsniveau vergleichbar mit dem herkömmlicher (kontaktloser) Smartcards
  - Mobiltelefon bringt zusätzliche Vorteile
    - Verwaltung der Anwendungen im laufenden Betrieb
    - Interaktion durch Tastatur & Display
  - Analyse verschiedener Secure Element APIs
    - Gemeinsamkeit: Mobiltelefonbetriebssystem (am Applikationsprozessor) verwaltet Zugriffskontrolle

    → Unsichere Komponente regelt Zugriff auf sichere Komponente

    → Annahme: Apps können Schutz des Betriebssystems aushebeln
  - Neue Angriffsszenarien möglich
    - Denial-of-Service durch Schutzmechanismen in SE-Anwendungen
    - Relay-Attacke durch App mit Internetanbindung statt physischer Nähe zu SE
  - Relay-Attacke erfolgreiche gegen existierende Anwendung eingesetzt

    → Google Wallet

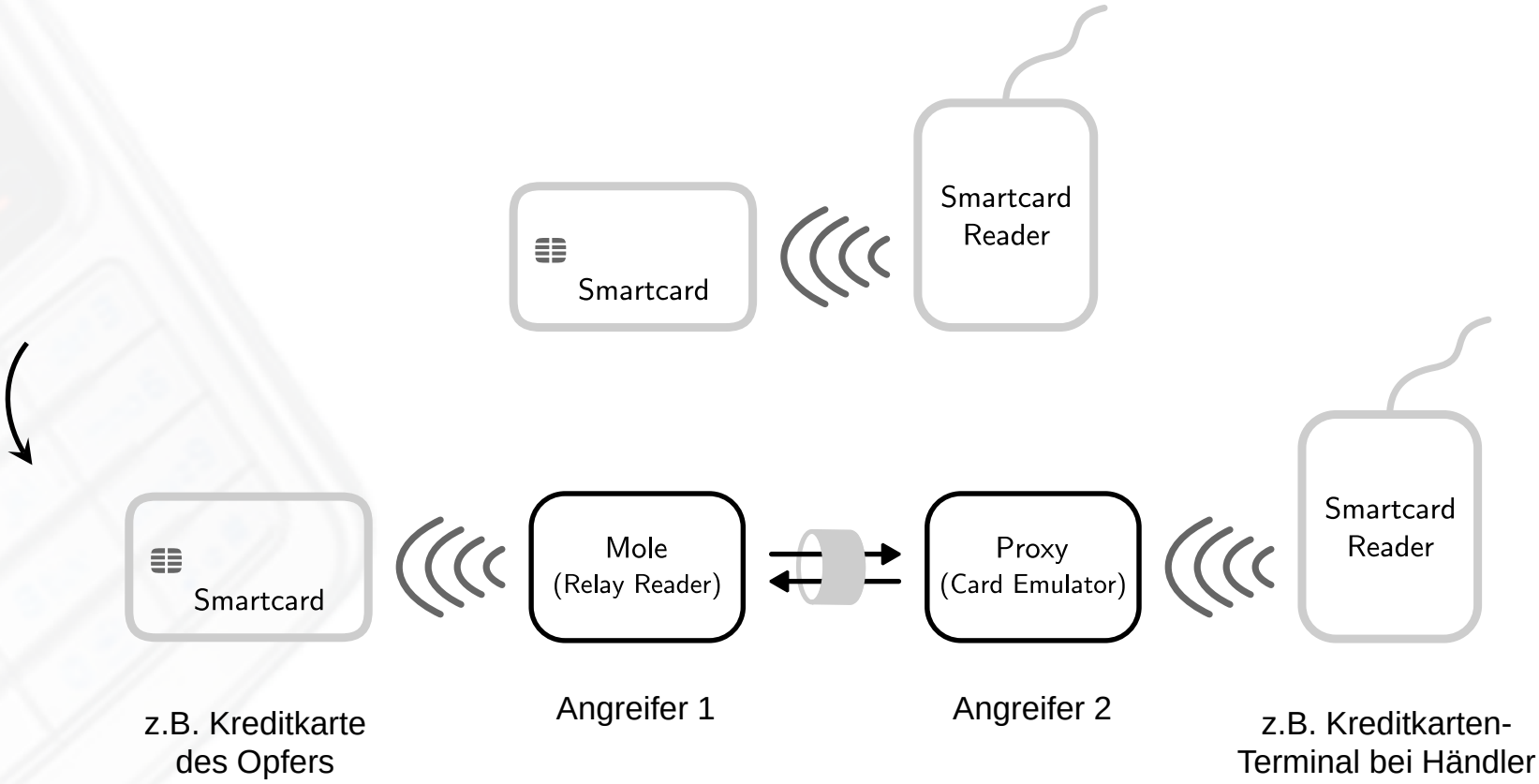
Ergebnisse im Überblick

- Schlussfolgerungen
  - Bei der Standardisierung von NFC wurde lange Zeit kaum Fokus auf Sicherheit gelegt

    → Vorwiegend Reaktion auf Schwachstellen & Angriffe
  - Sicherheitskonzepte vorhanden

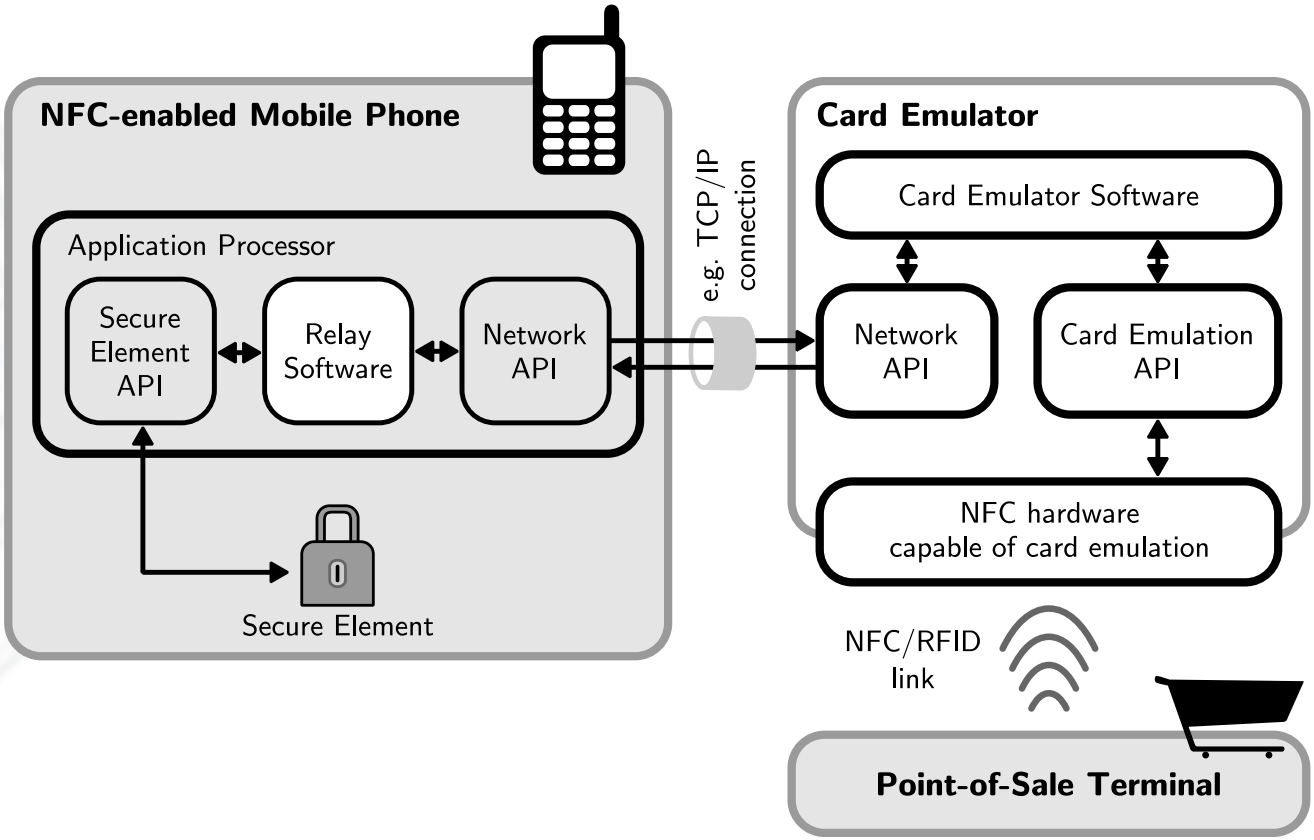
    → Teilweise aber nicht wirksam

Relay-Attacke: Beispiel

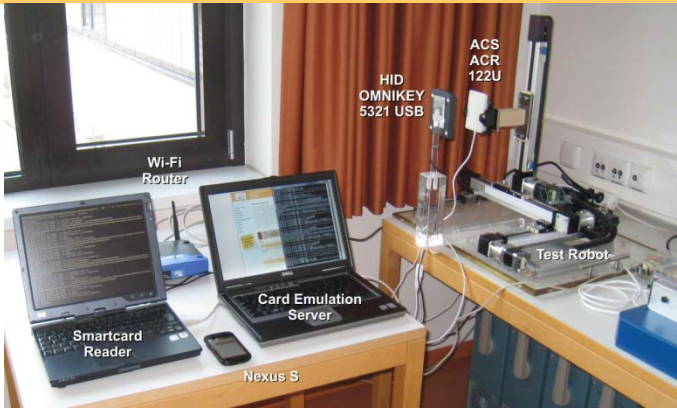


Neuer Ansatz: Software-basierte Relay-Attacke

- Angreifer 1 wird durch App am Mobiltelefon ersetzt



Verifikation



- Vergleichsmessungen mit Testaufbau
  - Gegenüberstellung der Verögerungszeit
    - direkte Kommunikation
    - Relay über Wi-Fi
    - Relay über Internet
  - Zusätzliche Verzögerung pro Befehl:
    - Wi-Fi: 110 – 210 ms
    - Internet: > 200 ms, Peak bei 300 ms, 44% der Messungen < 1 s
  - Relay ist signifikant langsamer aber erfüllt Anforderungen der involvierten Protokolle

Verifikation

- Test an existierender Anwendung: **Google Wallet**
  - MasterCard PayPass (standard Kreditkarten-Protokoll)
- Relay App
  - Android App
  - Google Wallet wird vor Transaktion entsperrt
- Card Emulator
  - Python Applikation
  - ACR 122U
  - Notebook
- POS terminal
  - Hypercom Artema Hybrid
    ViVOtech ViVOpay 5000


H-Ä-N-D-L-E-R-B-E-L-E-G

Testterminal
OPP B50

Terminal-ID 54183583
TA-Nr 000219 BNr 0062

Kartenzahlung
MasterCard

EUR 1,00

PAN 5430[redacted]0[redacted]7[redacted]
EMV-AID A0000000041010
VU-Nr 158632721
AIDPara 0100000002
Genehmigungs-Nr 735259
Datum 20.02.12 17:18 Uhr

Zahlung erfolgt

==========
AS-Proc-Code = 00 914
00
Capt.-Ref.= 0010
AID59: 714487
==========

BITTE [redacted]N

Mögliche Gegenmaßnahmen

- Striktere Timeouts
  - Nachteil: Cloud-basierte Lösungen funktionieren nach dem selben Prinzip wie die Relay Attacke und werden somit ebenfalls verhindert
  - Nachteil: Bei guter Netzwerkverbindung könnten Transaktionen trotzdem funktionieren
- PIN-Code/2-Factor-Authentication
- Internal-Mode für Payment-Applets deaktivieren
  - Applikationen am SE können erkennen über welche Schnittstelle sie angesteuert werden (kontaktlos oder aus App)
  - Nachteil: Einer der wesentliche Vorteile des Secure Elements ist, dass es auch aus Apps heraus genutzt werden kann (z.B. sichere Bezahlung mit Kreditkarte über Mobiltelefon-Webbrowser)

Fragen?

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 "4EMOBILITY" 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).