IT-Architekturen und Sicherheitskonzepte für eine generische Interpreter-Plattform für mobile NFC-Geräte

Michael Roland
FH Oberösterreich, Campus Hagenberg, Austria

31. Mai 2011, JKU Linz

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).

Inhalt

- Zusammenfassung vom letzten Mal
  - Ziele der Arbeit
  - Was ist NFC
  - Sicherheitsrisiken bei NFC-Anwendungen
  - erste Ergebnisse
- Status-Update zu bisherigen Ergebnissen
- Nächstes Zwischenziel

Ziele der Arbeit

- Evaluierung vorhandener Sicherheitskonzepte für Mobiltelefonsysteme
- Evaluierung von Sicherheitsrisiken für NFC-Anwendungen
- Erstellung einer Toolbox mit sicherheitsrelevanten Funktionen für NFC-Anwendungen
  - mit Fokus auf eine generische Interpreter-Plattform

Was ist NFC?

- kontaktlose Übertragungstechnologie (Basis: RFID & Smartcards)
- NFC-Gerät kann kontaktlose Chipkarten/Tags lesen, mit anderen NFC-Geräten kommunizieren und selbst als kontaktlose Chipkarte verwendet werden
- typische Anwendungen:
  - Payment, Ticketing, Loyalty
    - NFC-Mobiltelefon ersetzt vorhandene (kontaktlose) Chipkarten
  - Smart Poster
    - Zugriff auf interaktive Inhalte durch einfache Berührung eines Objekts mit einem NFC-Gerät/Mobiltelefon
  - Enabler für andere Kommunikationstechnologien
    - Bluetooth, WiFi, Wireless USB

Sicherheitsrisiken bei NFC-Anwendungen

- Verwendung manipulierter NFC-Tags
  - Phishing
  - ungewollte Nutzung von teuren Mehrwertdiensten (SMS, …)
  - Einschleusen von Schadcode
- „virtueller Taschendieb“
  - unbemerkter Zugriff auf das SE (z.B. im Vorbeigehen)
  - Abbuchung von Kleinstbeträgen
  - Nutzung von Tickets, Berechtigungen bei Zutrittssystemen (z.B. durch Relay-Attacke)
- Angriffe durch „fremde“ Mobiltelefonapplikationen
  - Phishing oder Abhören von PINs, Kennwörtern, …
  - Verfälschung von Statusinformationen (z.B. Anzeige eines falschen Geldbetrags bei SE-Transaktionen)

Analyse der Signatur-Spezifikation für Daten auf NFC Tags

- Signatur-Spezifikation
  - Entwickelt & veröffentlicht vom NFC Forum
  - Ziel: Schutz der Daten auf NFC Tags vor ungewollter Manipulation
- Ergebnisse
  - Digitale Signatur würde prinzipiell die notwendigen Anforderungen erfüllen aber die Umsetzung ist mangelhaft
  - Es werden nur Datenfelder signiert; für den Inhalt maßgebliche Header bleiben unsigniert
    - Datensemantik im Nachhinein veränderbar ohne Signatur zu verändern!
  - Die Spezifikation lässt die Zertifizierung der Signaturen offen
    - Keine Kriterien für das Vertrauen in signierte Daten definiert!

[1] M. Roland et al.: Digital Signature Records for the NFC Data Exchange Format
[2] M. Roland et al.: Security Vulnerabilities of the NDEF Signature Record Type

Update zur Signatur-Spezifikation

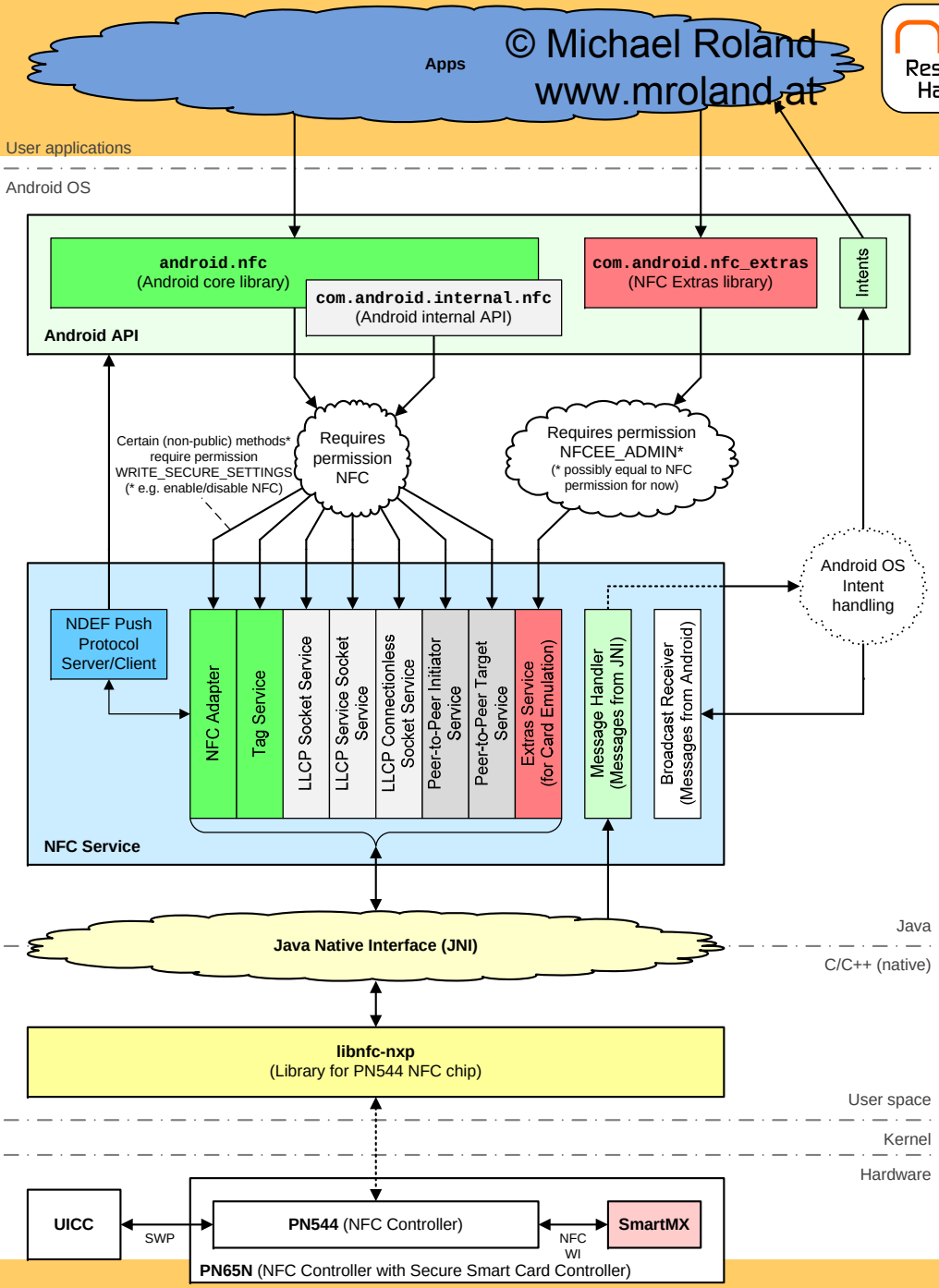
- Ergebnisse wurden an das NFC Forum übermittelt
  - Wird beim nächsten Member-Meeting (Mitte Juni) diskutiert
- Ergebnisse wurden am NFC Congress und auf der WIMA präsentiert

Nächstes Zwischenziel

- Untersuchung der Möglichkeiten zum Authentisieren von Benutzern und Mobiltelefonapplikationen gegenüber dem Secure Element
  - Generelle Möglichkeiten
    - PIN / Kennwort
    - Biometrische Merkmale
    - Smart Card
  - Absicherung des Vorgangs
    - Abhörsicherheit der PIN-Eingabe, …
    - Fälschungssichere Eingabemasken
    - Schutz vor Schadprogrammen
    - Notwendigkeit eines Trusted Execution Environment für das Mobiltelefon

Android & NFC

- Dezember 2010: erstes Android-NFC Handy (Nexus S)
- Seither: Fokus auf Android-Plattform
  - Open Source
  - offen für Veränderungen/Ergänzungen
  - Zugriff auf Source Code erleichtert Analyse der NFC-Funktion und deren Sicherheit
  - Aber: einige bekannte Schwachstellen die in Android 2.3.4 noch nicht behoben wurden
    - Angreifer kann Rechte von System-Diensten oder sogar root-Rechte erlangen (Privilege-Escalation durch grundlegende Designfehler im Sicherheitskonzept von Android)



Analyse des NFC-Stack von Android

- Verfügbare Funktionalität
  - Reader/Writer-Mode
    - Zugriff auf kontaktlose Chipkarten/NFC Tags
  - Kommunikationsprotokoll zum einfachen Datenaustausch zwischen zwei Android NFC-Handys (NDEF Push Protocol)
    - Vollständige Peer-to-Peer-Kommunikation noch nicht in öffentlicher API enthalten
  - Versteckte Bibliothek zum Zugriff auf das integrierte Secure Element
    - 1. Schritt in Richtung Google Wallet
    - Nur internes Secure Element wird unterstützt (kein Zugriff auf UICC)
    - Implementierung hat noch einige Stabilitätsprobleme
    - Zugriff nur durch Apps mit spezieller Berechtigung

Angepasste Firmware für das Nexus S

- Ziel: offene Plattform für weitere Untersuchungen
- Einfacherer Zugriff auf Funktionalität, die noch nicht in öffentlicher API enthalten ist
- Umfangreichere Secure Element Unterstützung
  - Aktivierung des SmartMX (internes Secure Element) und der UICC als kontaktlose Chipkarte
  - Zugriff auf den Smartcard-Chip SmartMX über Android Apps

Erste Ideen/Erkenntnisse

- Komplexe Smartphone-Betriebssysteme bieten zusätzliche Angriffsflächen
  - Schwachstellen zur Privilege-Escalation (root-Rechte)
  - Laufend neue Schwachstellen
- Gerade bei Payment-Anwendungen wird die Plattform „Mobiltelefon“ weitgehend als sicher vorausgesetzt
  - Falsche Annahme

Schwachstelle: Mobiltelefon

- Bei Betrachtung der Sicherheit von Secure Element Anwendungen besteht bisher die Annahme, dass die selben Sicherheitsrisiken wie bei kontaktlosen Chipkarten bestehen
  - d.h. ein Angreifer kann nur in unmittelbarer Nähe zum Telefon seinen Angriff durchführen (z.B. Relay-Attacke)
- Bei bisherigen NFC-Mobiltelefonen (Low-End-Geräte)
  - interner Zugriff auf das Secure Element ist nur mit vertrauenswürdigen Apps (gesichert durch digitale Signatur + Zertifikat) möglich
  - Schutzmechanismen des Betriebssystems lassen sich nur sehr schwer umgehen

Schwachstelle: Mobiltelefon

- Gerade bei Smartphones gilt diese Annahme nicht mehr
  - Beispiel Android: Jede Anwendung kann durch Ausnutzung von Schwachstellen root-Rechte erhalten (und in Folge uneingeschränkt auf das gesamte System zugreifen!)
- Konsequenzen:
  - Jede Anwendung kann unbemerkt Keylogger, … installieren
    - vgl.: „besondere“ Schutzfunktion beim neuen Google Wallet (NFC Payment Anwendung) ist eine PIN-Eingabe am Mobiltelefon
  - Jede Anwendung kann mit dem Secure Element kommunizieren

Auswirkungen von freiem Zugriff auf SE

- Secure Element ist zwar durch Zugriffsschlüssel geschützt
- Aber:
  - Die Komponente zum Installieren/Löschen von Anwendungen im SE haben einen besonderen Zugriffsschutz:
    - Nach 10 fehlgeschlagenen Authentisierungsversuchen wird die Komponente irreversibel deaktiviert (bereits installierte Anwendungen bleiben weiter verfügbar)
    - Ermöglicht Denial-of-Service gegen das Secure Element (Card-Emulation ist dann nur mehr eingeschränkt nutzbar!)
  - Für eine Relay-Attacke ist keine unmittelbare Nähe zwischen Angreifer und Telefon mehr notwendig
    - Statt einem NFC-Lesegerät wird einfach eine App verwendet, die die Kommunikation zwischen einem Chipkartenemulator (verbunden mit dem Payment-Terminal) und dem Secure Element über das Internet tunnelt

Michael Roland
Research Associate, NFC Research Lab Hagenberg
FH Oberösterreich, Campus Hagenberg, 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).