Vortrag zu NFC in public transport – and elsewhere

Samuel Brack, Christian Steinfeldt

Institut für Informatik
Humboldt-Universität zu Berlin

2012-11-29

Einführung in NFC

Was ist NFC?

NFC („Near Field Communication“) ist Sammlung von Standards zur Kommunikation, die

- kontaktlos
- auf kleiner Distanz (< 10 cm)
- aktive Geräte zulassend
- zu älteren Systemen wie MiFare kompatibel

sind.
NFC wurde 2002 von NXP (ehem. Philips) und Sony entwickelt, Hersteller der RFID-Systeme Mifare und FeliCa. Es besteht Kompatibilität zwischen diesen Systemen.
NFC erlaubt zusätzlich zur Kommunikation zwischen aktivem (Terminal) und passivem (Transponder) Teilnehmer auch die zwischen zwei aktiven Terminals.

Einführung in NFC

Was ist NFC?

- Standardisiert in ISO/IEC 14443, 18092 und ECMA-340 durch das NFC-Forum
- NFC Forum ist eine Industrievereinigung von Firmen, die an NFC interessiert sind und Standards verabschieden, u.a. sind dort Nokia, Samsung, Sony und NXP Mitglied
- Smartcards können „Trägersystem“ von NFC-Transpondern sein
- Durch Kompatibilität zu RFID müssen relativ aufwändige Protokolle implementiert werden
- NFC-Verbindung wird oft nur als Initiationskanal für spätere Verbindungen via Bluetooth/WLAN/... genutzt (geringe Datenrate von max. 424 kbit/s)

Einführung in NFC

Anwendungsarten

Bei NFC werden vier Anwendungsarten unterschieden:

1. Touch and go: Der Benutzer muss sein NFC-Gerät oder Tag in die Nähe des Lesers bringen und kann dann weitergehen. Beispiele: Zugangskontrollen, ÖPNV-Tickets
2. Touch and confirm: Der Benutzer muss die Datenübertragung zusätzlich noch bestätigen. Beispiel: mobile Bezahlsysteme
3. Touch and connect: Aktiv-aktiv-Verbindung zwischen NFC-Geräten, die Daten austauschen. Beispiel: Android Beam
4. Touch and explore: Die NFC-Geräte beherrschen mehrere der vorigen Anwendungsarten und können die gewünschte Funktion durch Nutzerinteraktion auswählen

Einführung in NFC

Übertragungsmodi

Außerdem gibt es drei Betriebsarten, in denen die NFC-Verbindung an sich abgewickelt werden kann:

1. Peer-to-Peer-Modus: Zwei aktive Geräte verbinden sich und tauschen Daten aus. Dabei werden auch zuverlässige Protokolle im NFC-Stack genutzt (LLCP) und die Geräte können beide Daten senden und empfangen.
2. Reader-/Writer-Modus: Kompatibilitätsmodus zu RFID, es wird also von einem aktiven Terminal ein passives Tag angesprochen und die aktive Seite übernimmt sowohl den Verbindungsaufbau, als auch die Stromversorgung (per induktivem Feld).

Einführung in NFC

Übertragungsmodi

3. Card-Emulation-Modus: Ein aktives NFC-Gerät emuliert einen passiven RFID-Tag, um mit einem alten RFID-Lesegerät zu kommunizieren. Im Unterschied zum Reader-/Writer-Modus muss die „passive “ Seite aber nicht mit Strom vom aktiven Teilnehmer versorgt werden.

Einführung in NFC

Hardware

In Mobiltelefonen kann die Verwendung des NFC-Chips durch ein „Secure Element“ abgesichert werden. Dieses ist meist die SIM-Karte (und wiederum durch die PIN gesichert) oder aber ein eigener Chip in Hardware.
Da NFC kompatibel zu RFID ist, müssen aufwändige Kollisionserkennungen vor Beginn der Übertragung durchgeführt werden, was sich negativ auf die Geschwindigkeit auswirkt.

Bezahlsysteme

Zahlungsdienstleister sehen NFC zunehmend als attraktiv an, da

- jeder (potentiell) ein NFC-Gerät in Form eines Telefons herumträgt.
- bestehende RFID-Systeme kompatibel bleiben.
- mobile Bezahlung oftmals umständlich ist.
- Kleinbeträge oftmals nur kompliziert bezahlt werden können.
- sich andere Systeme wie die GeldKarte nicht ausreichend (aus Bankensicht) durchgesetzt haben.

Daher existieren verschiedene Ansätze, NFC in Bezahlsysteme zu integrieren bzw. neue zu schaffen.

Google Wallet

Dieses System ist bisher noch nicht in Deutschland verfügbar.
Idee: Bezahlungen komplett vom NFC-fähigen Smartphone aus durchführbar.

Wie funktionierts?

1. Kreditkartendaten werden im Google-Profil verschlüsselt hinterlegt
2. Beim Einkaufen wird die Wallet-App auf dem Smartphone gestartet und das Smartphone wird an ein Lesegerät gehalten
3. Eventuelle Gutscheine von Google Offers werden eingelöst
4. Bezahlung abgeschlossen, auf dem Telefon erscheint eine Bestätigung

Google Wallet

Wie funktionierts?

Dadurch werden die Kreditkarten des Nutzers durch sein Smartphone ersetzt. Diese Daten sind noch mit einer zusätzlichen PIN absicherbar, auch eine Ferndeaktivierung nach Verlust des Telefons kann vorgenommen werden.
Allerdings kann dieses Verfahren nur dort eingesetzt werden, wo auch Lesegeräte vorhanden sind und in der Praxis kann man seine Kreditkarte dann doch (noch) nicht zu Hause lassen.

Bewertung des Systems

Vorteile

- Keine Herausgabe der vollen Kreditkartendaten an jeden Händler
- Weniger Karten mitzunehmen
- PIN und Fern-Deaktivierung schützt im Verlustfall
- Schnellerer Bezahlvorgang

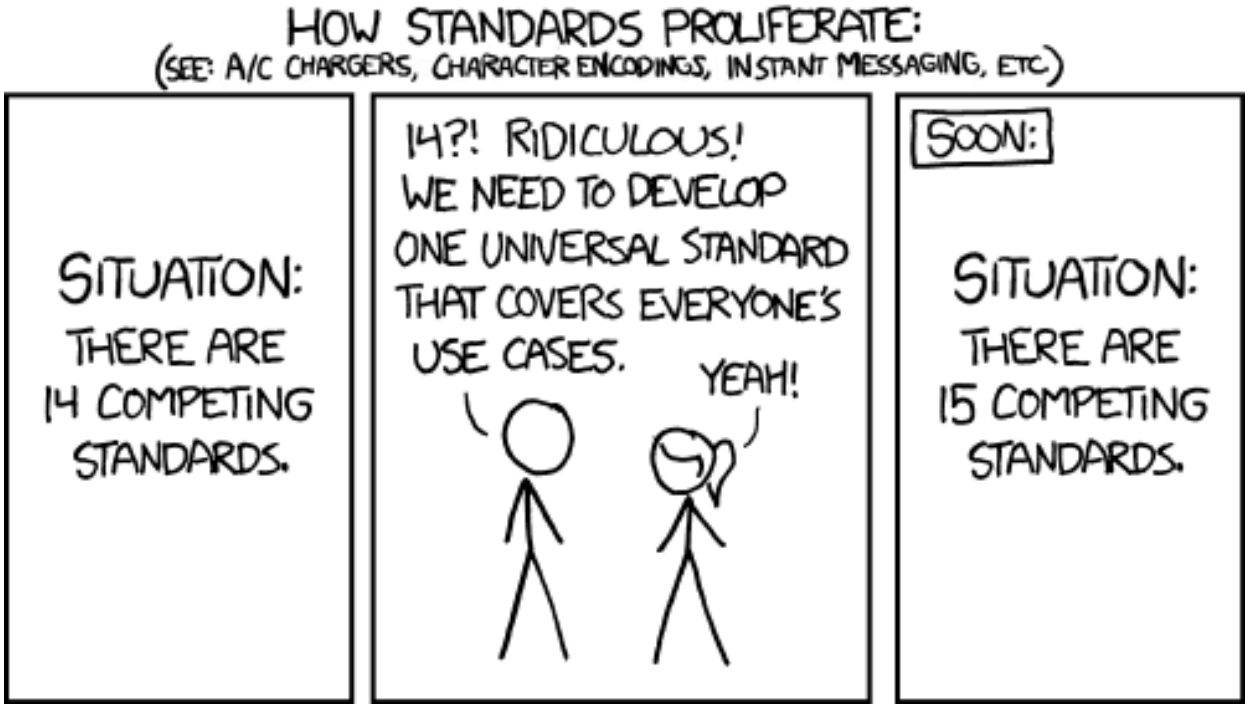
Bewertung des Systems

Nachteile

- Kreditkartendaten landen bei Google
- Transaktionshistorie ebenfalls zentral bei Google
- Unklare Verschlüsselung der Kreditkartendaten (welches Verfahren?)
- Auch die CVC (eigentlich „geheime“ 3-stellige Zahl) wird bei Google gespeichert

Konkurrenzsysteme

Auch Visa, Mastercard, Paypal u.a. haben ähnliche Projekte in Planung.



Umfrage

Wer von euch kennt die GeldKarte?
Und wer nutzt sie?

GiroGo

- Zahlungssystem basierend auf ec-Karten mit NFC-Antenne (Transponder), auf die Prepaid-Beträge aufgeladen werden (max. 200 €)
- Ziel: Vereinfachung der Bezahlung von Kleinbeträgen ($\leq$ 20 €)
- Dazu wird an der Kasse das Geld am Terminal nach Auflegen direkt abgebucht
- Dieser Vorgang passiert ohne Bestätigung des Benutzers, die einzige Rückmeldung ist ein Signal des Terminals(!)
- Beträge $>$ 20 € werden weiter per Chip/Magnetstreifen abgewickelt

GiroGo

- Aufladung erfolgt entweder am Geldautomaten, im Internet mit Chipkartenleser oder „künftig“ auch per Smartphone-App oder aber per Abo-Laden
- Restbetrag kann mit vielen NFC-Geräten ausgelesen werden
- Betreiber sind die Banken (momentan Sparkassen und Volksbanken im Großraum Wolfsburg in einem Pilottest)
- Karte besitzt eindeutige ID und speichert die letzten 15 Transaktionen mit Betrag, Timestamp und Terminal-ID des Händlers unverschlüsselt
- „Händler, die 'Girogo' akzeptieren, greifen auf diese Daten nicht zu. Sollten sie es doch tun, wäre dies ein Verstoß gegen die Nutzungsbedingungen.“- Michael Schlier vom Sparkassenverband Hannover

Bewertung des Systems

Vorteile

- Schnelle Bezahlung an der Kasse
- Benutzer kann anonymer bezahlen als mit ec-Karte
- Integration in bestehendes System der ec-Karten
- Bei Verlust/Diebstahl gehen maximal 200 € verloren

Bewertung des Systems

Nachteile

- Kontaktlose Abbuchung ohne Bestätigung auf Kartenseite
- Unverschlüsseltes Transaktionslog ist ein Datenschutzproblem
- Karte nicht sperrbar, Restbetrag ist bei Verlust weg
- Umständliche Handhabung (Aufladen, Überprüfen ob noch genug Geld vorhanden ist)
- Trotzdem: Karte nötig, keine Integration ins Smartphone

Das System ist also weder komfortabel noch sicher, wird sich also vermutlich kaum über das Betastadium hinaus halten können bzw. ein Nischendasein wie schon die GeldKarte führen.

VBB *fahr*Card

Abbildung : https://lh3.ggpht.com/–7NJkASIqr8/T_cA44xWV8I/AAAAAAAAAJI/bf4Sh5IQiII/s1600/VVB_fahrCard_vorne.jpg

VBB *fahr*Card

Einführung in 2 Stufen:

1. Umstellung der Abos und Jahreskarten (7 Unternehmen mit $\approx$ 320.000 Kunden betroffen)
   - Aufrüstung der Verkaufsstellen
   - nach 2 Tests (09/2011 und 06/2012) im Herbst 2012 angelaufen
2. Unterstützung durch alle 33 VBB-Betriebe und Tarife
   - Verbannung der *Papiertickets*

VBB *fahr*Card – Herausgeberangaben

- Gilt 5 Jahre lang, vereinfachte Tarifwechsel
- Datensparsam; kann an Kundenterminals oder durch Servicepersonal ausgelesen werden
- Seit Juni 2012 *Call a Bike*-Support
- *Verschlüsselung mit höchster Sicherheit basierend auf einem in Deutschland zwischen den Verkehrsunternehmen und Verbünden gemeinsam abgestimmtem Standard.*
- Bewegungsprofile unmöglich, Datenschutz wird eingehalten

VBB *fahr*Card – State of the Art

Zitiert nach `http://kaltreserve.blogspot.de/2012/07/der-erste-monat-mit-meiner-vbb-fahrcard.html`

Habt ihr Erfahrungen mit der *fahr*Card?

(((eTicket Deutschland

- *fahr*Card Teil eines überregionalen Projekts
- Zusammenarbeit von zur Zeit VBB, RMV (Rhein-Main Verkehrsverbund), VVO (Verkehrsverbund Oberelbe) und weiteren
- Standardisierung zu deutschlandweit benutzbaren ÖPNV-Tickets
- Weitere Funktionen (z. B. Carsharing, Fahrradverleih) denkbar
- Gefördert durch Bundesministerium für Verkehr, Bau und Stadtentwicklung

DB *Touch and Travel*

Abbildung : http://img.fotocommunity.com/Bahnhoefe-Gleise/Bushaltestellen/Touchpoint-a18460065.jpg

DB *Touch and Travel* – Einrichtung

- personenbezogene Daten, Adresse, E-Mail, Bankverbindung, Handyidentifikationsnummer
- Bonitätsprüfung durch infoscore ConsumerData GmbH
- Aktivierung der LSB und des Ortungsdienstes zur periodischen Standortbesimmung

DB *Touch and Travel* – Reise

- Check-In durch Ortung, Barcode, Kontaktpunkt oder NFC
- periodische Standortbestimmung alle 5 Min.
  Für NFC über die durchfahrenen Funkzellen
  Sonst LSB und Ortung
- Bei Kontrolle fällt Kontrolldatensatz an
- Abmelden, Günstigster Preis von A nach B bezahlt
- Speicherdauer: 55 Tage (Standortdaten), 12 Monate (Kunden-, Reise- und Abrechnungsdaten)

DB *Touch and Travel* – Probleme

- DB erhält Bewegungsprofil
- Sende- oder Telefonausfälle gleichen schwarz fahren
- Bei Verspätungen werden Ab- und Wiederanmeldung empfohlen
- Man kann die Fahrgastrechte nur bedingt wahrnehmen
- Bei vergessenem Check-Out nach 13 Stunden (bzw. 24 NFC) Accountsperre

SmartCards und SmartPhones

SmartCards sind zur Zeit schon sehr weit im öffentlichen Nahverkehr vertreten. Versuche mit NFC ausgestatteten Handys sind noch selten. Im direkten Vergleich hat sich London weiter für seine *Oyster Card* entschieden. Die Reaktionszeit von 300 ms gegenüber 500 ms bei Telefonen war ausschlaggebend.

NFC kann eine Fahrscheinalternative darstellen, wenn es datensparsam und sicher implementiert ist.

Angriffsmöglichkeiten

Bisher vertrauen wir auf die Nähe und Eindeutigkeit des Lesers.

Was kann passieren, wenn eine dritte Person ins Spiel kommt?

Kommunikation ablauschen

- NFC ist Funk, der leicht mitgehört werden kann
- Besonders bei sicherheitsrelevanten Anwendungen kritisch
- ECEMA Standarts 385/386 bieten Verschlüsselung
  - Keymanagement: Diffie-Hellmann
  - Datenintegrität & -verschlüsselung: 128-Bit AES
- Diese aber nicht in heute verbreiteten Systemen implementiert

Angriffe auf die Datenintegrität

- Denial of Service / Störsignale
- Modifikation
  Erfolgsmöglichkeit hängt von der Amplitudenmodulation, Codierung und dem tatsächlichen Bitwert ab
  ($1 \Rightarrow 0$ ok, wenn $11 \Rightarrow 0$; $0 \Rightarrow 1$ nicht ok)
- Injection
  Einfügen von Nachrichten in einen offenen Kommunikationskanal
  Antwort des Angreifers muss vor der Antwort des Opfers verarbeitet werden

Relay Wiedergabe des Signals über längere Distanzen

Replay Nach dem Abhören einer Kommunikation kann man die gewonnen Daten dem Opfer wieder vorspielen.
Schutz: (Pseudo-)Randomisierte Sessiontokens

Man-in-the-Middle In die direkte Kommunikation *Alice–Hutmacher* schaltet sich als Proxy dazwischen.
Schwachstelle by Design: Keine Möglichkeit zur Verifikation der Echtheit eines NFC-Gerätes

- Implementation: NFC-Proxy
  Relay, Replay und Man-in-the-Middle Attacken auf Visakarten mit 2 Handys.


PUT YOUR HANDS UP
IF YOU HAVE A QUESTION

Quellen

- Josef Langer, Michael Roland – „Anwendungen und Technik von Near Field Communication (NFC) “, Springer Verlag, Berlin 2010.
- C. Dachs - „The intuitive contactless technology becoming reality “ in elektrotechnik&informationstechnik, Heft 12 Dezember 2005/122. Jahrgang, S. 466ff.
- http://www.google.com/wallet/index.html
- http://schooleymitchell.com/blog/google-wallet-raises-security-concerns/
- http://www.girogo.de/
- http://www.spiegel.de/netzwelt/netzpolitik/datenschuetzer-fuerchten-missbrauch-bei-funk-geldkarte-der-sparkasse-a-838470.html
- http://mp-nfc.org/nfc_security_nfc_security_threats.html