NFC - Near Field Communication

Johanna Sacher

Basics

- internationaler Kommunikationsstandard, der es zwei Geräten – oder einem Gerät und einem NFC-Tag – ermöglicht Daten auszutauschen [6]
- und zwar drahtlos
- Trick dabei: Geräte müssen sehr nah beieinander sein (max. 10 cm)
- basiert auf **Radio-Frequency Identification-Technologie (RFID):** [9]
  - Daten können kontaktlos über Radiowellen gelesen werden
  - zwei Komponenten: Transponder (RFID-Tag) und Lesegerät
  - Funktionsweise:
    - Lesegerät erzeugt elektromagnetisches Feld und sendet so ein Signal an die Antennen des Transponders [6]
    - die leiten das Signal weiter und der Transponder schickt die angeforderten Daten über das gleiche Feld zurück
    - funktioniert auch über große Distanzen (je nach Transponder bis zu 100 m) und durch verschiedene Materialien hindurch (aber nicht durch Metalle!) [6]
    - je nach Tag können große Datenmengen gespeichert oder die Tags sogar neu beschrieben werden
    - Tags sind sehr robust ggü. Umwelteinflüssen [6]
  - Verwendung (u.a.): [6]
    - Diebstahlsicherung v. Waren
    - Chips für (Haus-) Tiere, Menschen, Autos u.ä.
    - bargeldlose Zahlung
    - Schlösser

Funktion

- das besondere an NFC: hat ein spezielles Koppelungsverfahren nach internationalem Standard (ISO 14443-2, 14443-3, 18092, 21481) [7]
- Transponder/NFC-Tag besteht aus einem Speicherchip mit einer aufgerollten Antenne rund herum [2], [12]
- Datenübertragung geschieht über elektromagnetische Induktion [6]
- Datenübertragungsrate: max 424 kBit/s [6]
- Frequenz: 13.56 MHz
- funktioniert nur über kurze Strecken hinweg, max. 10 cm (nach ISO Standard und lt. NFCForum)

⇒ keine Konkurrenz für Bluetooth oder WLAN [6]

⇒ Alternative zu Bar- oder QR-Codes, da größere Speicherkapazität [6]

- Geräte müssen nur aneinander gehalten werden, sonst keine Anmeldung oder Authentifizierung notwendig
- Übertragungsarten: [2]
  - passiv (aktives Lesegerät und passiver NFC/RFID-Tag, der seine Energie aus dem vom Lesegerät erzeugten elektromagnetischen Feld bezieht)
  - aktiv (Verbindung zwischen zwei aktiven Geräten)
- Verbindungsmodi für NFC-Devices: [8]
  - Tag Reader/Writer: NFC Tags lesen/neu beschreiben
  - Peer-to-Peer: zwei Geräte miteinander verbinden, um Daten auszutauschen
  - Card Emulation: Gerät verhält sich wie SmartCard, z.B. für Tickets, kontaktlose Zahlung, oder um Schlösser zu öffnen

Anwendungen

- Idee: [6]
  - Paarung der Geräte erfolgt durch den Nutzer (automatische Authentifizierung)
  - erneute Authentifizierung je nach Anwendung
  - Mitlesen soll weitgehend ausgeschlossen werden
  - Smartphone soll als Lesegerät verwendet werden können
- Häufige Anwendungen [6], [2]:
  - Bargeldlose Zahlung
  - E-Tickets
  - Onlinebanking
  - Zweifaktor-Authentisierung
  - Smartposter
  - Steuerung des Smartphones über NFC-Tags
  - Übertragung von Bluetooth- und WLAN-Authentifizierungsdaten
  - Schlüssel (viel für Autos, Hotels, Universitäten u.ä.)
  - Campus Karten (z.B. Thoska)
- neuere Anwendungsgebiete: Smart Home, IoT (z.B. Türschlösser) [6]

Sicherheit

- Sicherheit hängt von den Einstellungen des Lesegeräts/Smartphones ab [6]
- Schutz der Privatsphäre ist nur gesichert, wenn NFC deaktiviert ist [6]
- geringe Reichweite bietet einen gewissen Schutz, aber eben nicht zuverlässig [6]
- Handy weg = Schlüssel weg [6]
- mögliche Angriffe:

- **Phishing:** sensible Daten eines ahnungslosen Users durch social Engineering erlangen [5]
  - ⇒ Nutzt Naivität der User aus, z.B. Geldversprechen
  - ⇒ social engineering: z.B. Marketing; psychologische Manipulation anderer, um eigene Ziele zu erreichen [1]
- **Skimming:** unauthorisiertes Lesen von Daten (z.B. einer Kreditkarte)
  - ⇒ z.B. um sie zu speichern und vor Lesegerät wieder "abzuspielen"; möglich mit jedem Lesegerät, das nah genug ist (siehe NFCProxy oder NFCGate)
- **Eavesdropping/Lauschen:** Daten abgreifen, die zwischen zwei (oder mehr) Geräten ausgetauscht werden [10]
  - ⇒ passive Devices sind immun gegen Eavesdropping, solange sie nicht mit Energie versorgt werden (durch ein Lesegerät z.B.) [10]
  - ⇒ sobald sie aber Energie erhalten, senden sie Daten und sind angreifbar [10]
  - ⇒ auch vulnerable ggü. Skimming, da sie keine Sicherung enthalten (können) [10]
- **Relay-Attacke:** die "Distanz" für NFC wird durch das Zwischenschalten von zwei NFC-Geräten "erhöht"; ein Gerät liest den Transponder, das andere wird vom Reader gelesen, während die beiden Geräte z.B. über einen Server verbunden sind (s. Tool siehe NFCProxy oder NFCGate). So werden die Daten auch über große Distanz zum Lesegerät übertragen.

⇒ selbst verschlüsselte Daten abzuhören lohnt sich, da sie offline noch entschlüsselt werden können [10]

- in allen drei Fällen merkt der User meist nicht, dass er angegriffen wurde, bis tatsächlich ein Schaden entsteht [10]

NFC Tools für Android

- **NFC Reader:** liest verschiedene Tags aus, die bei aktiviertem NFC-Mode ans Smartphone gehalten werden. Mit Scanhistorie, Inhalt kann kopiert werden
- **NFC TagInfo:** sehr detailierter Scan der öffentlich zugänglichen Daten, Scanhistorie, Quick Scan/Full Scan
- **NFC Tools:** NFC-Tags lesen und beschreiben/programmieren (z.B. um das Smartphone damit zu steuern)
- **NFCProxy:** Vermitteln von Transaktionen zwischen NFC-Karte und Reader: [11]
  1. Karte (z.B. Kreditkarte) scannen, Daten speichern und vor einem Lesegerät wieder "abspielen" ⇒ Lesegerät akzeptiert Smartphone als gültige Karte
  2. oder mit zwei Geräten: Eins als Proxy, eins als Relay, Relay wird auf Karte gelegt und liest sie aus, Proxy wird vor den Reader gehalten (siehe Relay Attacke)
- **NFCGate:** für Relay-Attacken; Lauschangriffe; Karte lesen, Daten speichern und vor Reader wiederholen [4], [3]

References

[1] R. J. Anderson. *Security Engineering: a guide to building dependable distributed.* 2nd ed. Wiley, Indianapolis, 2003.

[2] CONGSTAR. *NFC - Near Field Communication.* URL: `https://www.congstar.de/handys/technik-news-trends/nfc/`. (accessed: 19.04.2019).

[3] Max Maaß David Wegemer. *NFCGate*. URL: https://github.com/nfcgate/nfcgate. (accessed: 19.04.2019).

[4] Max Maaß David Wegemer. *NFCGate - NFC security analysis with smartphones*. URL: https://www.youtube.com/watch?v=PSbfRvzmUII. (accessed: 19.04.2019).

[5] R. Dhamija, J. D. Tygar, and M. Hearst. *Why phishing works. In Proceedings of the SIGCHI conference on Human Factors in computing systems*. 2006.

[6] Wikipedia - Die freie Enzyklopädie. *Near Field Communication*. URL: https://de.wikipedia.org/wiki/Near_Field_Communication. (accessed: 17.04.2019).

[7] Fakir. *Unterschied RFID und NFC – Eine kurze Erklärung*. URL: https://www.fakir.it/unterschied-rfid-und-nfc-eine-kurze-erklaerung/. (accessed: 19.04.2019).

[8] NFC Forum. *NFC - What it does*. URL: https://nfc-forum.org/what-is-nfc/what-it-does/. (accessed: 20.04.2019).

[9] RFID Grundlagen. *RFID*. URL: https://www.rfid-grundlagen.de/. (accessed: 19.04.2019).

[10] Stephen J. Jones. *Access Granted: On the Security of Near-Field Enabled Keycards*. 2014. URL: https://www.researchgate.net/publication/324898033_Access_Granted_On_the_Security_of_Near-Field_Enabled_Keycards.

[11] nfcproxy. *NFCProxy*. URL: https://sourceforge.net/projects/nfcproxy/. (accessed: 19.04.2019).

[12] nfc-tag-shop. *Was ist NFC*. URL: https://www.nfc-tag-shop.de/info/. (accessed: 22.04.2019).