FAQ
Passive NFC-Chips

Antworten auf die häufigsten Fragen

Von Julius Beineke

Energie- und Datentransfer

? NFC funktioniert durch Induktion. Wie geht das? Ist das gefährlich?

! Passive NFC-Chips, also solche ohne eigene Stromversorgung etwa in Aufklebern, Geldkarten oder Plastik-Tags, bestehen aus einem Mikrochip, einem Kondensator und einer Antenne meist in Form einer Metallspule. Hinzu kommt bei beschreibbaren Varianten ein Speicher von derzeit bis zu vier Megabyte Größe.

Die NFC-Lesegeräte – dazu zählen auch NFC-fähige Smartphones – erzeugen ein elektromagnetisches 13,56-MHz-Wechselfeld, wenn man einen passiven Chip auflegt. Dessen Antenne nimmt die Hochfrequenzenergie auf, der Kondensator puffert sie und versorgt den Mikrochip. Um Daten zu übertragen, moduliert das Lesegerät dieses Feld, was der NFC-Chip als Daten interpretiert. Die Übertragungsgeschwindigkeit beträgt je nach Chiptyp 106, 212 oder 424 Kilobit pro Sekunde. Das reicht für Daten wie die Chip-Seriennummer (ID), Systembefehle, Text und kleine Bilder aus. Bluetooth, WLAN & Co. sind schneller – der Clou bei NFC ist jedoch die fast unmittelbare Verbindung und Datenübertragung, ohne eigene Stromversorgung für den Chip.

Gefährlich ist das Ganze nicht – obwohl die Methode dem induktivem Laden ähnelt, wird das Energiefeld so schwach und kurz erzeugt, dass nichts erhitzt. Die geringe Feldstärke bedingt auch, dass NFC nur mit maximal zehn Zentimetern Reichweite funktioniert. Daher auch der Name NFC - Near Field Communication.

Alltagspraxis

? Kann ich mit NFC-Tags kontaktlos bezahlen? Was kann ich noch machen?

! Das geht im Moment nur mit NFC-fähigen Geld- und Kreditkarten sowie Smartphones, die solche Karten simulieren. Dienste dafür kommen in Deutschland langsam in Gang: Apple Pay lässt auf sich warten, Google Pay ist kürzlich in Deutschland gestartet und bereits vielerorts nutzbar. Sparkasse, Postbank und Deutsche Bank bieten ihren Kunden ebenfalls schon Smartphone-Bezahlservices an [1].

Ansonsten sind mit NFC viele Spielereien möglich. Die Chip-IDs werden etwa zu Zugangsschlüsseln für Passwortmanager [2], oder mithilfe von Apps wie Trigger (siehe ct.de/yxnh) zum Auslöser diverser Smartphone-Funktionen. Visitenkarten ersetzt man durch vCards und sichert sie auf NFC-Chips mit beschreibbarem Speicher. Möchte man Kontaktdaten weitergeben: einfach ein Smartphone an den Chip halten, der als Sticker auf einer Papier-Visitenkarte klebt oder in einer Smartcard steckt.

Hat man Lust zu basteln, sind die Möglichkeiten noch vielfältiger. Von NFC-Türschlössern bis zur Smart-Home-Steuerung ist eine Menge drin. Mutige können sich die Chips unter die Haut implantieren lassen und so stets dabei haben [3].

Tracking

? Kann man meinen Chip – und damit mich – tracken?

! Das ist ein alter Mythos. Einzige Tracking-Möglichkeit für passive NFC-Chips: Liest ein Lesegerät eine Chip-ID aus, wird das im System des Lesegeräts protokolliert. Das hat seinen Sinn. Checkt man etwa per Smartcard in ein Fitnessstudio ein, kann der Betreiber das Trainingsverhalten seiner Kunden nachvollziehen; hat er mehrere Studios, kann er ein rudimentäres Bewegungsprotokoll anlegen.

Gelangen jedoch Dritte an diese Logs und die zugehörige Kundendatei, könnten sie Chip-IDs mit ihren Besitzern in Verbindung bringen. Das ließe Schlüsse auf deren Verhalten und Bewegungen zu. Kritisch kann das werden, wenn man eine Chip-ID an mehreren Stellen nutzt – etwa ein und dieselbe zum Einstempeln auf der Arbeit und zum Öffnen des heimischen NFC-Türschlosses. Wer dann an Logs aller Lesegeräte gelangt, kann viel über die Chip-Besitzer erfahren. GPS-Verfolgung oder dergleichen geht jedoch nicht.

Sicherheit

? Sollte ich sensible Daten auf NFC-Chips speichern?

! NFC-Chips sind klein und praktisch, technisch betrachtet allerdings nicht sehr sicher. Sensible Daten sollte man nur mit großer Vorsicht darauf speichern.

Hat man einen beschreibbaren NFC-Chip, kann man dessen Schreibzugriff oft per Passwort sichern oder sogar endgültig unterbinden – gespeicherte Daten lassen sich dann nicht mehr verändern, nur auslesen. Letzteres kann aber jeder, der mit einem Lesegerät lange genug in Reichweite kommt. Hier liegt wiederum eine Sicherheitsstärke von NFC: Die meisten Chips lassen sich aus maximal drei bis vier Zentimetern auslesen. Stecken sie als Smartcard im Portemonnaie oder als Implantat unter der Haut, kann die Reichweite auf unter einen Zentimeter schrumpfen. Wer heimlich auslesen will, muss dann schon sehr nahe herankommen. Um etwa Bankkarten gerade in Anbetracht kontaktloser Bezahlmöglichkeiten zu schützen, gibt es signalstörende Hüllen oder Schutzkarten (siehe ct.de/yxnh).

Laufende Datenübertragungen können Dritte mit passendem Equipment mitschneiden. Sogenanntes Eavesdropping ist bei Funksignalen wie NFC nicht gänzlich vermeidbar. Banken, deren Apps mit NFC arbeiten, verschlüsseln aus diesem Grund üblicherweise Daten vor der Übertragung. Diese Sicherheitsvorkehrungen sind allerdings nicht inhärenter Teil von NFC. Bei so schwachen Signalen wie denen passiver NFC-Chips ist die Abhörreichweite aber üblicherweise ohnehin auf unter einen Meter begrenzt.

(jube@ct.de)

Literatur

[1] Jan-Keno Janssen, Stefan Porteck, Appbezahlen: Smartphone-Bezahl-Apps im Test, c't 16/2018, S. 68

[2] Julius Beineke, Funkey: Passwortmanager unter Android mit NFC aufschließen, c't 11/2018, S. 148

[3] Julius Beineke, Handtenne: NFC-Implantat: Ein Selbstversuch, c't 1/2018, S. 108

Apps und Videos zu NFC: ct.de/yxnh