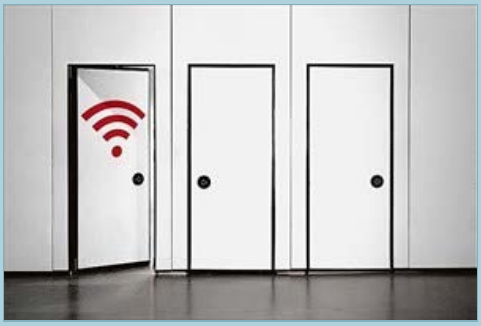
Türöffner ins Internet der Dinge

ALOIS PUMHÖSEL
17. Jänner 2014, 18:26



vergrößern 800x533

foto: corbis; bildbearbeitung: thomas korn

Die Vernetzung schreitet voran. Die kontaktlose Datenübertragung auf kurze Distanz via NFC soll im kommenden "Internet der Dinge" die eine oder andere Tür öffnen.

Kontaktloses Zahlen mit der Bankomatkarte ist nur ein erster Schritt: Die Datenübertragung per NFC-Chips soll in Zukunft auch Haustüren öffnen oder Informationen aus Zahnspangen auslesen

Die Haustür ist verschlossen. Der Wohnungsinhaber zückt das Smartphone und hält es an das Schloss. Das Handy baut eine verschlüsselte Datenverbindung zum Schließmechanismus auf. Wenn ein gültiger Zugangsschlüssel auf das Schloss übertragen wird, wird es entsperrt. Ist am Handy kein Schlüssel vorhanden, fragt die entsprechende App am Server nach, ob es für den Handynutzer eine Zugangsberechtigung für das Schloss gibt, das selbst offline ist.

MEHR ZUM THEMA
APP: Professionelle App-Entwicklung gesucht?
Werbung

Geht es nach Markus Minichmayr, tritt künftig auf diese Art ein mit NFC-Chips ausgerüstetes Smartphone an die Stelle konventioneller Metallschlüssel. Der Mitbegründer des Wiener Softwareunternehmens Phactum glaubt, dass sich das Öffnen privater Haustüren via Near Field Communication "mittelfristig durchsetzen" werde. Mit seinen Kollegen hat er "Tapkey" entworfen, eine, wie er sagt, sehr einfache Möglichkeit, mithilfe des Funkübertragungsstandards den alten Haustürschlüssel sicher zu ersetzen. "Das System minimiert die Hürden für die Benutzer und funktioniert sofort", sagt Minichmayr.

Möglich wird das, weil sich die NFC-Zutrittskontrolle mit einem bestehenden Account eines Internetdienstleisters wie Google oder Twitter verbinden lässt. Tapkey benutzt etwa eine Google-ID, über die fast alle Nutzer eines NFC-fähigen Android-Smartphones verfügen, zur Authentifizierung, erklärt Minichmayr. "Eine zentrale Identität ist komfortabler und sicherer, als weitere Passwörter anzulegen oder Zugangsdaten per E-Mail zu verschicken", ist der Unternehmer überzeugt. Phactum sucht derzeit nach Hardwarepartnern, um Tapkey, für das unter anderem Mittel der Wiener Förderagentur Zit lukriert wurden, umzusetzen. Noch 2014 soll das NFC-Schloss auf den Markt kommen. Bisher schließt es nur eine Tür in der

Die automatische Zutrittskontrolle bei Wohnungstüren und das Einchecken im Hotel per Handy, das mit Systemen wie Tapkey möglich wird, ist eine von vielen Anwendungsfällen, für die NFC im Rahmen des vielbeschworenen "Internet der Dinge" eingesetzt werden soll. Der Funkstandard für die kontaktlose Übertragung von Daten über wenige Zentimeter soll künftig auch Konzertkarten und Öffi-Tickets aufs Handy verbannen, die Identifikation von Fracht im Logistikbereich erleichtern und Kaffee- und Waschmaschinen mit Firmwareupdates versorgen.

Vernetzte Zahnspange

Sogar Zahnspangen werden bereits mit NFC-Chips

ausgestattet, um zu prüfen, wie oft sie vom Patienten tatsächlich getragen wurden. Bankomatkarten werden in Österreich seit 2013 mit NFC ausgeliefert, die das kontaktlose Bezahlen kleiner Beträge an entsprechenden Terminals im Handel ermöglichen. Zuletzt sorgte ein Standard-Bericht über eine Sicherheitslücke für Aufregung, die zulässt, dass man per Smartphone-App Informationen über Transaktionen auslesen kann.

An der Verbesserung von Sicherheit und Leistungsfähigkeit zukünftiger NFC-Technologien wird auch in heimischen Forschungslabors gearbeitet. Im NFC Research Lab an der FH Hagenberg in Oberösterreich arbeitet etwa Josef Langer an Chips, die höhere Übertragungsraten zulassen.

Bisher dient NFC in vielen Fällen zur Identifizierung und zur Initiierung eines Kommunikationsvorgangs, erklärt der Forscher. Die Kommunikation selbst, etwa der Austausch von Fotos zwischen zwei Handys, erfolgt dann über Bluetooth oder WLAN.

NFC verfügt zurzeit nur über geringe Datenraten von wenigen 100 Kilobit/Sekunde. Wollte man auf diese Art ein Foto verschicken, läge die Übertragungsdauer im Minutenbereich. "Wenn in den Reisepässen der Zukunft aber Foto und Fingerabdruck per NFC abrufbar sein sollen, müssen größere Datenmengen in kürzerer Zeit versendet werden", sagt Langer.

Nicht einfach: Denn für einen Kommunikationsvorgang muss im NFC-Chip, der selbst über keine Stromversorgung verfügt, Energie induziert werden. Ein ausgesendetes Magnetfeld, das etwa eine Bankomatkarte durchdringt, wird dank der Antenne am Kartenrand in ein paar Milliwatt Energie umgewandelt - genug, um den Chip für kurze Zeit mit Strom zu versorgen. "Je schneller die Datenübertragung, desto schlechter ist aber die Energieübertragung", erklärt Langer.

Die Forscher versuchen, durch die Optimierung von Signalverarbeitungsalgorithmen aus der Zwickmühle zu kommen. "Wir müssen intelligente Filter bauen, um die tatsächlichen Signale vom Rauschen zu trennen." Ziel des von der Forschungsförderungsgesellschaft FFG und den Research Studios Austria geförderten Forschungsprojekts ist es, eine Testplattform für ein schnelleres NFC-Lesegerät zu etablieren, auf dem verschiedene Anwendungen ausgeführt werden können.

Ein Internet der Dinge erfordert die Entwicklung von ganzheitlichen Konzepten, bei denen die Sicherheit von Anfang an mitgedacht wird. Werner Haas von Joanneum Research in Graz koordiniert das Projekt SeCoS (Secure Contactless Sphere), das im Rahmen des Comet-Programms von Verkehrs- und Wirtschaftsministerium unterstützt wird. Seit 2013 arbeitet er mit seinen Kollegen an einer Plattform, die Alltagsgegenstände in einem automatisierten Zuhause sicher vernetzt.

Hochwertige Kryptografie

NFC werde zur Identifikation im eigenen Haus genauso wie an der Stromladestelle für das Elektroauto dienen, glaubt Haas. Bei Smartphones und Tablets, die als multifunktionale NFC-Kommunikatoren verwendet werden, muss etwa sichergestellt werden, dass Schadsoftware die Verschlüsselung nicht knacken kann. "Um an den Schlüssel zu kommen, werden etwa die Ausführungszeiten von Algorithmen, der Stromverbrauch oder die elektromagnetische Strahlung gemessen", sagt Haas.

"Verwendet man etwa nur eine 58-Bit-Verschlüsselung, lässt sich relativ leicht auf den Schlüssel zurückschließen. Mit höherwertiger Verschlüsselung wird das wesentlich schwieriger."

Aber auch die beste Verschlüsselung bei der Übertragung hilft nichts, wenn die Daten dann am Server im Klartext abgespeichert werden. Die Datensicherheit müsse bei allen beteiligten Komponenten gewährleistet sein. Und auch beim Menschen. Denn: Nicht alles ist mit Technologie machbar, sagt Haas. "Wenn Sie einkaufen gehen, und die 500er schauen aus dem Börsel, ist die Wahrscheinlichkeit, dass Sie überfallen werden, auch größer, als wenn sie aufpassen." (Alois Pumhösel, DER STANDARD, 15.1.2014)

Zum Thema

- Smartphone-App liest Bankomatdaten aus
- "Eine kleine Lücke kann schon ausreichen"