

Berührungslos sicher?

Wie sicher sind Transponder-Karten? Experten referierten bei einem Seminar in Frankfurt/Main über die „(Un)Sicherheit berührungsloser Ausweislesetechnik“.

Wissenschaftler der Universität Nijmegen (Niederlande) und – unabhängig davon – Experten aus dem Umfeld des *Chaos-Computer-Clubs* knackten zu Jahresbeginn 2008 den Verschlüsselungs-Algorithmus des RFID-Chips eines weitverbreiteten Kartensystems. Wie gefährlich ist die dadurch entstandene Situation wirklich? Bei einem *Simedia-Forum* am 27. August 2008 in Frankfurt zum Thema „(Un)Sicherheit berührungsloser Ausweislesetechnik“ referierten Experten über diese Problematik.

Chipkarten. Im Bereich der „körperlich-materiellen Identifikationsmerkmalsträger“ (Definition nach DIN 0830-8-1) wurden bei Ausweis- oder Berechtigungskarten Barcode oder Magnetstreifen bis auf untergeordnete Anwendungen abgelöst durch Karten, die einen Chip enthalten, der entweder über Kontakte oder berührungslos ausgelesen werden kann. Wegen der größeren Benutzerfreundlichkeit sowie des Wegfalls der Abnützung von Kontakten geht der Trend zu berührungslos arbeitenden Systemen.

Es handelt sich dabei um bloße Speicher-Chipkarten (Telefonwertkarten), um Prozessor-Chipkarten (SIM-Karten, E-Cash) oder um Prozessor-Chipkarten mit Kryptoprozessor (Smartcards). Von Bedeutung ist dies für die Art, wie sich die Chipkarte gegenüber dem Lesegerät authentifiziert, damit Missbrauch durch Nachbildungen derartiger Karten erschwert oder ver-



Karten, über Kontakte oder berührungslos ausgelesen, haben Barcode und Magnetstreifen abgelöst.

hindert werden. Während eine Speicher-Chipkarte, die einen elektronisch lösch- und wiederbeschreibbaren Speicher (EEPROM) enthält, nur mäßig gesichert ist, enthält eine Prozessor-Chipkarte eine in ihren elektronischen Bauteilen fest verschaltete Sicherheitslogik, über die die Karte angesteuert wird. Der „Hack“ bezog sich auf Karten dieser Bauart, indem der innere Aufbau dieser vorgeschalteten Sicherheitslogik entschlüsselt wurde.

Bei einer Prozessor-Chipkarte mit Kryptoprozessor erfolgt der Verbindungsaufbau zwischen Karte und Leser über in beiden gespeicherte geheime Schlüssel, mit denen in einem wechselseitigen Dialog Zufallszahlen erzeugt werden. Nur diese werden übermittelt; ein Errechnen des Schlüssels durch „Mitlesen“ ist daher prinzipiell nicht möglich; Abhören, Aufzeichnen und Wiedereinspielen bleiben erfolglos.

RFID. Berührungslos arbeitende Systeme bestehen aus einem Lesegerät, das in seinem Umfeld ein elektro-

magnetisches Feld im (Radio-)Frequenzbereich von 125 kHz oder 13,56 MHz aufbaut (Radio Frequency Identification). Geräte im Mikrowellenbereich (2,45 GHz) sind für Zutrittskontrollsysteme in Erprobung. Der – üblicherweise ohne eigene Stromquelle auskommende – Transponder („Tag“) besteht aus einer Antenne, die mit einem Kondensator einen auf die Frequenz des Lesers abgestimmten Schwingkreis bildet, mit nachgeschaltetem Chip, mit dem das Lesegerät in Verbindung tritt. Antenne und Chip sind entweder eingegossen in Anhänger am Schlüsselbund oder am Armband, oder, wie in Zutrittskontrollanlagen zumeist üblich, in Plastikkarten im Scheckkartenformat.

Wenn ein Transponder in die Sendereichweite eines Lesers gelangt, beginnt der Leser bereits die Daten auszulesen – vom Benutzer unbemerkt, von ihm nicht zu beeinflussen und sogar dann, wenn er es gar nicht will (Diebstahlsicherung). „Man kann nicht einmal den Stecker ziehen“, sagte Werner Metterhausen (Von zur

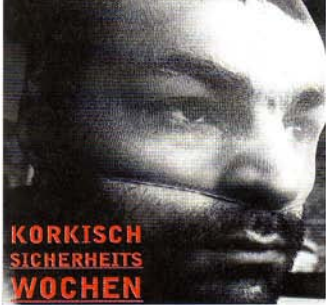
Mühlen'schen GmbH). Schutz bietet lediglich eine metallische Abschirmung des Transponders.

Nach den Normen beträgt die Reichweite 15 Zentimeter (Proximity Coupling nach ISO 14443) bzw. 1,5 Meter (Vicinity Coupling nach ISO15693), doch sind das Mindestwerte, die selbst unter ungünstigen Bedingungen erreicht werden müssen. Die tatsächlich bei einem noch verwertbaren Signal-Rausch-Abstand erzielten Reichweiten liegen im Bereich von etwa vier Metern. Dazu kommt, dass sich ein Lauscher nicht an die genormte Sendeleistung des Lesers halten, sondern diese erhöhen wird.

Das Sicherheitsproblem bei RFID ist die Luftschnittstelle, die „abgehört“ („gesniff“) werden kann. Es gilt, den Transponder (Karte) vor Ausspähen seines Inhalts zu schützen, und den Leser vor Manipulation, die ihm das Vorliegen einer echten Karte vortäuscht.

Wie es möglich ist, einfache Kartensysteme zu überwinden, haben Experten des *Chaos-Computer-Clubs* (CCC) erläutert und vorgeführt. Bei einem Durchleuchten der Karte wird die Antenne des Transponders erkennbar. Aus der Anzahl der Windungen können bereits grobe Rückschlüsse auf die verwendete Frequenz gezogen werden. Dann wird die vom Leser permanent ausgesendete Radiostrahlung aufgefangen – einfache Schaltungen reichen hierfür aus – und mit einem Oszilloskop analysiert. Die in weiterer Folge verwendeten Techniken gehen so weit, dass der aus seiner Umhül-

EINBRUCHSCHUTZ!



**KORKISCH
SICHERHEITS
WOCHE**

Die Zeiten werden unsicherer!!!
Die Einbruchdiebstähle nehmen in den letzten Jahren überdurchschnittlich zu. Sich und sein Eigentum zu schützen, wird in den kommenden Jahren immer wichtiger. Sorgen Sie vor - und informieren Sie sich **GRATIS & UNVERBINDLICH** während der **KORKISCH** Sicherheitswochen. Die Möglichkeiten für effektiven Einbruchschutz sind vielseitig und für jeden leistbar. Von einfachen Funkalarmanlagen, bis zum lückenlosen Sicherheitskonzept.

la **korkisch energie**
SOLAR- UND HAUSTECHNIK
ELEKTRO SANITÄR HEIZUNG TORTECHNIK

Elektro Korkisch - Gerhard Korkisch GmbH, 1130 Wien, Auhofstraße 120 A
Tel.: 01/877 25 25 solar@korkisch.at Fax: 01/877 18 66 www.korkisch.at

Sicherheit(s)-Technik

Sicherheitstüren bieten zuverlässigen Schutz vor:
Einbruch, Lärmbelästigung, Geruchsbelästigung und Zugluft

Geprüft nach ÖNORM B 5338
schnelle, saubere Montage
Topqualität aus Österreich

Gratis Hotline: 0800/50 10 75

BÖHM-MITSCH security systems Intelligent sichern
1070 Wien, Lindengasse 58 / Ecke Zieglergasse

- Ladenbau-Design
- Ladenbau-Konzept
- Display
- Regalsysteme
- Kassentische
- Duftmarketing

Viel Erfolg!

VRANA
Ladenbau GMBH

02745 / 28 28 · www.vrana.at

ZUTRITTSKONTROLLE

lung mit Lösungsmitteln herausgelöste oder -geätzte Chip abgeschliffen wird, um die Grundstruktur der integrierten Schaltkreise zu ermitteln. Ein aufwendiges Verfahren, dessen Ergebnisse sich dann im Internet finden, sodass sich eine Bibliothek ansammelt. Das Endergebnis ist der Bau einer elektronischen Schaltung, die einen auf das Lesegerät zugeschnittenen Transponder emuliert. Bei unverschlüsselten Verbindungen kann es mitunter ausreichend sein, die bei der Kommunikation zwischen Leser und Karte entstehenden Frequenzen z. B. mit einem *I-Pod* aufzuzeichnen und diese dann bei Bedarf wieder abzuspielen. Nach Angaben des *Chaos Computer Clubs* werden der Algorithmus und eventuell auch die restlichen Details zum Angriff noch in diesem Jahr veröffentlicht. Spätestens Ende des Jahres soll es dann auch eine Geräte-Kombination aus Kartenemulator und Lesegerät geben, die ein Klonen einer beliebigen Karte mit zunächst unbekanntem Schlüssel bei kurzem Zugriff auf das Lesegerät erlaubt.

„Mifare-Hack“. Wie bedrohlich ist die durch den „Mifare Hack“ entstandene Situation wirklich? Laut Helmut Gerdemann (DOR-MA Time + Access GmbH) gebe es keine Meldungen darüber, dass Zutrittskontrollsysteme auf diesem Weg überwunden worden seien. Einer der möglichen Gründe dafür könnte sein, dass erhebliches Know-how und Kenntnisse über die Karte erforderlich sind. Dazu kommt, dass die Überwindung der Zutrittskontrolle noch kein risikofreies Begehen von fremden Unternehmen erlaubt.

Bestehen noch andere Sicherheitssysteme, kann die



Werner Metterhausen.



Helmut Gerdemann.

Verwendung eines geklonten Ausweises durchaus erkannt werden, etwa dann, wenn mit einem Ausweis, dessen Träger bereits als anwesend geführt wird, neuerlich Zutritt begehrt wird, oder wenn innerhalb eines Unternehmens verschiedene Sicherheitszonen bestehen, erläuterte Dipl. Ing. Klaus Behling (Von zur Mühlen'schen GmbH). Voraussetzung dafür ist, dass auch das Verlassen des jeweiligen Bereiches registriert wird. Der Angreifer weiß nicht, wie weit seine Berechtigung reicht; er wird die Zutrittsverweigerung auslösen, was durch entsprechende Auswertung der Protokolle erkannt werden kann. Der Angreifer weiß ferner nicht, wo sich der tatsächlich Berechtigte im Unternehmen aufhält; die Auswertung einer Raumzonenüberwachung, die auch das Verlassen eines Bereiches registriert, müsste ergeben, dass jemand, der sich in einem bestimmten Bereich befindet, nicht Zutritt zu einem anderen verlangen kann, ohne den ersten Bereich verlassen zu haben.

Das offene Tragen von Ausweisen, die zudem mit Firmenlogo, Bild und Namen des Inhabers personalisiert sind, erschwert es ferner, sich unbemerkt in einem Unternehmen zu bewegen. Dabei kommt es insbesondere auf das Schriftbild des Ausweises und besonders die Erkennbarkeit des Lichtbilds an. Wenn ferner bei bestehender Organisation bereits zusätzliche Identifizierungsmittel

ZUTRITTSKONTROLLE

tifikationsmaßnahmen wie etwa Abfrage einer PIN oder eine biometrische Identifikation des Ausweisinhabers gefordert werden, ist zumindest soweit Sicherheit gegeben, dass das Problem in Ruhe angegangen werden kann.

Entsteht durch mögliche Klone ein nicht tragbares Sicherheitsrisiko für das Unternehmen, sollte als erste Maßnahme zumindest für sicherheitskritische Bereiche ein Austausch der vorhandenen Leser durch solche mit Tastatureingabe und/oder biometrischer Erkennung veranlasst werden. Dies geht in der Regel ohne großen Aufwand, eine Weiterverwendung der ausgegebenen Karten ist möglich. Diese Nachrüstung überbrückt zumindest die Zeit bis zur Neuinstallation eines Systems. Eine weitere, von Gerdemann aufgezeigte Möglichkeit besteht darin, die schon bei der Herstellung eines Chips in diesem unveränderbar abgelegte Seriennummer und allenfalls weitere systeminterne Merkmale als zusätzliches Identifikationsmerkmal in verschlüsselter Form nachträglich in erfahrungsgemäß zumeist noch verfügbaren Platz des Karten-Chips einzuspeichern und diese durch entsprechend upgegradete Lesegeräte auslesen. Ein Angreifer kann zwar die Seriennummer des Chips des zu klonenden Ausweises leicht auslesen, weiß aber nicht, nach welchem Verfahren diese verschlüsselt wurde. Das Lesegerät wird einen „Signaturfehler“ erkennen, was zu einer entsprechenden Reaktion führen sollte.

Neue Anlagen. Letztlich aber sollte bei aus den 1990er-Jahren stammenden Zutrittskontrollanlagen wegen des technischen Fortschritts ein Systemwechsel

ins Auge gefasst werden. In einem Chip festverdrahtete Algorithmen zur gegenseitigen Erkennung von Transponder und Lesegerät genügen nicht mehr den heutigen Anforderungen. Zu fordern sind Systeme, bei denen der Verbindungsaufbau in Form einer verschlüsselten Datenübertragung erfolgt. Ferner sollten standardisierte Technologien mit hohem Verbreitungsgrad eingesetzt werden, damit der entsprechende Support über eine zu veranschlagende Nutzungsdauer von 10 bis 15 Jahren gesichert ist.

Vor der Installation eines neuen Systems sollte allerdings überlegt werden, welchen Zwecken es dienen soll.

Sollen, neben einer nach Sicherheitsbereichen abgestuften Zutrittsberechtigung, auch die Zeiterfassung, Kantinenabrechnung, Parkraumbewirtschaftung, die Schlösser zu den Umkleeschränken, einbezogen werden? Mit zunehmender Zahl der Aufgaben, die ein solcher Multifunktionsausweis übernehmen soll, steigt der administrative Aufwand.

Die Einführung eines Zutrittskontrollsystems größeren Ausmaßes stellt jedenfalls einen in seiner Komplexität nicht zu unterschätzenden Eingriff in die Organisation eines Unternehmens dar, mit hohen Investitionskosten, die allerdings in Relation zum gesamten Sicherheitskonzept zu sehen sind. Es sind weniger die Kosten für die Karten selbst als jene, die bei der Personalisierung (Beschaffung von Lichtbildern, Einscannen, Bedrucken) sowie der Verwaltung (Ausgabe der Ausweise, Registrierung, Folgekosten durch Verlustmanagement) entstehen, sodass für Ausweise 30 bis 40 Euro pro Stück an Kosten entstehen können.

Kurt Hickisch

Value through Innovation



12 Millionen Menschen weltweit erkranken jedes Jahr an Krebs.

Wir versuchen, diese Krankheit an ihrer Wurzel zu bekämpfen.

www.boehringer-ingelheim.at



Boehringer Ingelheim

Boehringer Ingelheim RCV GmbH & Co KG, Dr. Boehringer-Gasse 5-11, 1121 Wien, Tel. 01/801 05-0*, Fax 804 08 23

Die beste Lösung für jede Wohnung:

SICHERHEITSTÜREN
vom Renovierungsprofi schützen Sie vor unerwünschten Besuchern!



WOHNUNGSEINGANGSTÜREN

TOPIC

- >> Mehr Sicherheit: geprüft nach ÖNORM B 5338
- Widerstandsklasse 2 im Standard
- Widerstandsklasse 3 optional
- >> Durchgangslichte bleibt erhalten
- >> Schutz vor Schall- und Geruchsbelästigung
- >> Einfache und saubere Montage

FensterCitySÜD

A-2331 Vösendorf Ortsstraße 2-4
Tel.: 01/698 72 00 Fax.: 01/698 72 00-20
office@fenstercity.at www.fenstercity.at

TOPIC GmbH, Haus- und Wohnungseingangstüren, A-4152 Sarleinsbach, Altendorferfeld 6
Tel. +43 (0) 7283/82 30-0, Fax: DW -21, E-Mail: topic@topic.at, www.topic.at