30C3: RFID - Überwachung in China, Pannen in Österreich

heise online

Glaub ich nicht… Die US-Bürgerrechtlerin Kate Krauss hat die auf dem 30. Chaos Communication Congress ***(30C3)*** in Hamburg versammelte Hackergemeinde aufgefordert, eine chinesische Ausweiskarte genau zu inspizieren. **Die Smartcard sei mit einem RFID-Chip bestückt, auf dem unter anderem Fingerabdrücke des Trägers, Name und Adresse, Gesundheitszustand, ethnische Herkunft und Zugehörigkeit zu Gewerkschaften oder anderen Organisationen gespeichert seien. Diese Informationen seien mit einer nationalen Datenbank verknüpft.** ***(Anm.: So etwas kann auch jederzeit in einen RFID-, NFC-Chip-Implantat abgespeichert werden! Inzwischen ist die RFID-Chip Technologie viel weiterentwickelt worden als zum Zeitpunkt dieses Artikels.)***

Die chinesische Regierung[1] nutzt den Ausweis Krauss zufolge, um ganze Bevölkerungsgruppen gezielt zu überwachen. Jeder Bürger erhalte im Alter von 16 Jahren eine solche Karte. Darauf gebe es unter anderem Markierungen für "spezielle Mitbürger" und als "gefährlich" eingestufte Individuen – als solche sehe Peking Menschenrechtsaktivisten, Buddhisten, AIDS-Kranke, Prostituierte, Anwälte oder Drogenabhängige an. Insgesamt würden 30 bis 50 Millionen Menschen in China unter besonderer Beobachtung stehen.

Muster einer mit RFID ausgestatteten Ausweiskarte aus China

Polizei und anderen Sicherheitsbehörden stünden spezielle Lesegeräte zur Verfügung, um die Karten aus der Ferne auszulesen, erläuterte die New Yorker Aktivistin. Auch Hotels, Ticketbüros, Gruppen zur "Nachbarschaftsbeobachtung" sowie Internet-Cafés verfügten über Hardware zum Auslesen der Funkchips. Es sei vorgekommen, dass ein Menschenrechtsanwalt nach dem Kauf einer Zugfahrkarte in einen Kleinbus gezerrt und festgesetzt wurde, ähnliches sei einer Prostituierten beim Einchecken in ein Hotel passiert. Verdächtige dürfen in China ohne ordentlichen Prozess bis zu sechs Monate in Gewahrsam genommen werden.

Lesegerät für die chinesischen Ausweiskarten

Eine Vertreterin des AIDS Policy Project berichtete, manche Chinesen hätten erst bei einer Ausweiskontrolle erfahren, dass sie HIV-positiv seien. Das Virus sei vor allem in der Henan-Provinz über einen Blutbankfehler massiv verbreitet worden, den die Regierung habe

[1] Die USA und die EU planen das Ganze gleich als Zwangs-Implantate, **siehe Web** und **US-Gesetzeslink**

totschweigen wollen. Erst eine chinesische Ärztin habe den Skandal als Whistleblowerin publik gemacht.

Von den Hackern aus dem Umfeld des **Chaos Computer Clubs (CCC)**, die RFID-gestützten Pässen und Personalausweisen seit Jahren sehr kritisch gegenüberstehen, erhofft sich Krauss nun zusätzliche Aufklärung über den in China eingesetzten Chip. Noch sei zu wenig darüber bekannt, wie viele Daten darauf gespeichert werden könnten, wie der Abgleich mit externen Datenbanken erfolge und welche Verschlüsselungsverfahren verwendet würden. Eine Chinesin im Publikum, die derzeit in den USA studiert, bot spontan an, ihre Karte als Testobjekt zur Verfügung zu stellen.

Der Wiener Sicherheitsforscher Adrian Dabrowski ist bei der Analyse des Sicherheitssystems einer österreichischen RFID-Karte bereits etwas weiter. Die Karte wird in Wien vielfach zum Öffnen zentraler Türen von Wohn- und Bürohäusern genutzt.

Die Smartcard der österreichischen Firma Begeh soll es Mitarbeitern von Bürogemeinschaften sowie Postboten und der Müllabfuhr erleichtern, in ein Anwesen zu gelangen. Bisher werden dazu Spezialschlüssel verwendet, deren Handhabung umständlich ist. 16 Prozent der Wohn- und Gewerbeanlagen in Wien sollen daher bereits die neue Funklösung einsetzen.

Diese Zutrittsysteme, Schlüsselkarten *(und natürlich auch die Schlüssel-RFID-Implantate)* konnten schon geknackt werden **=> PDF-LINK**.

Dabrowski gelang es nun nach eigenen Angaben, das Begeh-System mit vergleichsweise einfachen Mitteln auszuhebeln. Zunächst habe er sich selbst ein Paket mit einem **RFID-Leser geschickt, der über eine mittlere Reichweite und einen lange laufenden Akku verfügt habe.** Damit habe er im Rahmen der Zustellung eine der Chipkarten *(von der Ferne!)* auslesen können, erklärte der Experte in seinem an die Simpsons erinnernden Vortrag "Treehouse of Horror". Die entsprechenden Daten habe er auf einen gebrauchten, neu programmierbaren **RFID-Skipass mithilfe einer Android-App für NFC-Smartphones aufgespielt** und damit dann 43 Prozent der gesicherten Haustüren öffnen können*(!)*; unter Einsatz eines selbstgebauten Kartensimulators habe er die **Erfolgsquote gar auf 93 Prozent erhöhen können.** *Ist doch schon was!*
(dwi)

Das zeigt wieder, es gibt keine Software, kein System das nicht zu knacken ist. Daher Finger weg von RFID-, NFC-, oder anderen Funk-Chip-Implantaten.