idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Press release

Ruhr-Universität Bochum
Dr. Josef König
11/03/2011
http://idw-online.de/en/news448967

Research results
Electrical engineering, Information technology
transregional, national

Der perfekte Klon: RUB-Forscher knacken RFID-Chips

Profis halten ein Stethoskop an den Safe, um über das charakteristische Einrasten die richtige Zahlenkombination zu erkennen. Wissenschaftler der Ruhr-Universität Bochum hebeln den Sicherheitsmechanismus einer weltweit genutzten kontaktlosen Chipkartentechnik auf ganz ähnliche Art und Weise aus. Mittels „Seitenkanalanalyse“ können die Forscher vom Lehrstuhl für Eingebettete Sicherheit der RUB Chipkarten klonen, die millionenfach für Sicherheit sorgen sollen.

Der perfekte Klon
RUB-Forscher knacken RFID-Chips
Über das Magnetfeld zum Schlüssel

Profis halten ein Stethoskop an den Safe, um über das charakteristische Einrasten die richtige Zahlenkombination zu erkennen. Wissenschaftlern der Ruhr-Universität Bochum ist es gelungen, den Sicherheitsmechanismus einer weltweit genutzten kontaktlosen Chipkartentechnik auf ganz ähnliche Art und Weise auszuhebeln. Mittels „Seitenkanalanalyse“ können die Forscher vom Lehrstuhl für Eingebettete Sicherheit (Prof. Dr.-Ing. Christof Paar) Chipkarten klonen, die millionenfach für Sicherheit sorgen sollen.

Mathematisch unknackbar

RFID-Chipkarten (Radio Frequency Identification) vom Typ DESFire MF3ICD40 werden häufig in Bezahl- und Zugriffskontroll-Systemen benutzt. Die Sicherheit beruht dabei auf Triple-DES, einer aus rein mathematischer Sicht unknackbaren Chiffre. DESFire-Karten kommen zum Beispiel in den Verkehrsbetrieben von Melbourne, San Francisco und Prag als elektronische Fahrkarten zum Einsatz. Hergestellt werden die Karten von NXP, der im Jahr 2006 ausgegliederten Halbleiter-Sparte von Philips Electronics.

Veränderungen im Magnetfeld

Als Passagier, Mitarbeiter oder Kunde weisen sich Personen aus, indem sie ihre Karte kurz vor ein Lesegerät halten. Für die notwendige Sicherheit soll der Schlüssel im Inneren des integrierten Funkchips sorgen. Doch ebenso wie der Schließmechanismus am Banktresor nicht lautlos funktioniert, hinterlässt auch dieses Verfahren deutliche Spuren. „Wir haben den Stromverbrauch des Chips beim Ver- und Entschlüsseln mit einer kleinen Sonde gemessen“, berichtet David Oswald. Die Veränderungen im Magnetfeld sind so aufschlussreich, dass die Bochumer Forscher den 112-Bit Schlüssel vollständig auslesen konnten.

Geringer Aufwand, großer Schaden

Mit dem Schlüssel lassen sich unerkannt beliebig viele Kopien einer Karte erstellen. Und der Aufwand ist nicht groß: „Für unsere Messungen brauchten wir eine entsprechende RFID-Karte, ein Lesegerät, die Sonde und ein Oszilloskop, mit dem wir den Stromverbrauch beobachten können“, so Oswald. Der reine Materialpreis für das Equipment betrage nur wenige Tausend Euro. Und bei detailliertem Vorwissen zu Aufbau und Charakteristika der Karte liege der Zeitaufwand für einen solchen Angriff bei rund sieben Stunden. Der Hersteller NXP hat die Lücke inzwischen bestätigt und empfiehlt seinen Kunden den Umstieg auf ein neueres Modell.

Nur unzureichend gesichert

Bereits im Jahr 2008 konnten Forscher um Prof. Dr.-Ing. Christof Paar am Lehrstuhl für Eingebettete Sicherheit der Ruhr-Universität mit Seitenkanalanalyse vermeintlich sichere Lösungen unterlaufen. Vor drei Jahren öffneten sich den Wissenschaftlern fremde Autotüren und Garagentore auf scheinbar wundersame Weise. Denn schon hier erwies sich die zum Einsatz kommende KeeLoq RFID-Technologie, der zuvor Hersteller und Kunden blind vertraut hatten, als unzureichend gesichert.

Weitere Informationen

Prof. Dr.-Ing. Christof Paar, Lehrstuhl für Eingebettete Sicherheit, Fakultät für Elektrotechnik und Informationstechnik der RUB, Tel. 0234/32-22994, christof.paar@rub.de

Homepage: http://www.emsec.rub.de

Redaktion: Jens Wylkop

Smartcard: Messung des elektro-magnetischen Feldes