Der RFID-Sicherheitsexperte Chris Paget hat in einem Praxistest gezeigt, wie einfach es ist, die vom US-Außenministerium ausgegebenen neuen Passport Cards aus der Ferne auszulesen und zu klonen. Paget machte sich dazu seit Ende Oktober 2008 bekannte Schwachstelle in der Implementierung der verwendeten RFID-Karten zunutze. Zum Auslesen benutzte er eine Motorola-RFID-Antenne und einen RFID-Leser von Symbol für rund 250 US-Dollar, womit er eine Reichweite von rund 10 Metern erreicht haben will. Die Ausrüstung verstaute er nebst Laptop und selbst geschriebener Software in seinem Auto und ging auf RFID-Jagd.

Innerhalb von 20 Minuten will er zwei RFID-Tags in Passport Cards unbemerkt ausgelesen haben – ohne Wissen der Besitzer. Bei den ausgelesenen Daten handelte es sich nur um eine Seriennummer, die zwar keine persönlichen Informationen enthalte, allerdings mit einer Datenbank des Department of Homeland Security (DHS) verknüpft ist und etwa bei Grenzübertritten geprüft wird. Die Seriennummer lässt sich in handelsübliche RFID-Karten zurückschreiben. Nach Meinung der Bürgerrechtsvereinigung American Civil Liberties Union sei dies der erste Schritt, um elektronische Pässe zu fälschen.

Paget hat damit erfolgreich demonstriert, was Forscher von RSA bereits Ende des vergangenen Jahres herausgefunden und veröffentlicht hatten. Demzufolge verfügen die Passport Cards über keine Anti-Cloning-Funktion, wie sie etwa das DHS gefordert hat.

In den USA sollen rund 750.000 Personen eine RFID-Karte für Reisen zwischen den USA, Mexico, Canada, den Karibischen Inseln und den Bermuda-Inseln besitzen. Keine Gültigkeit haben die ID-Karten indes für Reisen per Flugzeug ins US-Ausland.

Auch die neuen elektronischen Führerscheine (Enhanced Drivers Licence, EDL) lassen sich auf die gleiche Weise auslesen und klonen. EDLs bieten etwa Washington und New York State an. Nach Meinung von Paget ließen sich mit dem großflächigen Erfassen von RFID-Tags Bewegungsprofile erstellen.

Die zuständigen Behörden sehen jedoch kein Problem. Mit den ausgelesenen Daten könne man wenig anfangen. Zudem seien die Karten mit Schutzhüllen versehen, die das ungewollte Auslesen verhindern sollen. Auch dies hatten die RSA-Forscher aber bereits vergangenes Jahr bemängelt: Trotz Hülle war es möglich, die Seriennummer auszulesen.

Quelle: heise.de