Mittwoch, 15. März 2006 16:58 Alter: 1 Tage

Viren per RFID-Chip

Tanenbaum demonstriert Angriffsmöglichkeiten

Die RFID-Chips, die in Zukunft Barcodes überflüssig und Reisepässe drahtlos auslesbar machen sollen, können theoretisch zur Verbreitung von Viren verwendet werden. Dies konnten Melanie Rieback, Bruno Crispo und Andy Tanenbaum nun erstmals demonstrieren .

Bedenken gegen die Funkchips werden gerne damit zerstreut, dass die RFID-Tags selbst meist sehr simpel sind, nur ausgelesen oder nur gezielt von einem RFID-Reader modifiziert werden können. Die Auslesegeräte selbst sind Angriffsziel in dem nun vorgestellten Szenario. Weist der Reader bzw. die auf ihm laufende Software Sicherheitslücken auf, müßten diese mit speziell modifizierten RFID-Chips ausgenutzt werden können - wie auch beispielsweise ein Browser durch modifizierte Webseiten dazu gebracht werden kann, eigentlich nicht zur Ausführung bestimmten Code auszuführen statt anzuzeigen. Beim Ausgelesenwerden manipulieren die Chips den Reader dahingehend, dass der Input aus dem manipulierten RFID-Chip ausgeführt wird.

Durch diesen Code könnte ein Reader dazu gebracht werden, dass er die kompromittierenden Daten anschließend auf jeden Chip schreibt, der mit ihm gescannt wird und auf dem dieser Schreibvorgang möglich ist. Diese könnten ihrerseits weitere RFID-Lesegeräte infizieren.

Die praktische Umsetzung wurde mit einem eigens programmierten Reader demonstriert, in welchem ein Bug platziert wurde, der eine SQL-Injection ermöglichte. Die Verbreitung eines passenden Schadcodes konnte anschließend reproduziert werden.

Ob solche Bugs in RFID-LEsegeräten existierten, wäre bislang noch offen, die Wahrscheinlichkeit spreche jedoch dafür, so Ed Felten in seinem Blog . Die bisherigen Erfahrungen mit Computern und Internet wiesen darauf hin, dass auch bei sorgfältiger Programmierung esolche Lücken auftauchen. Die Schlußfolgerung: RFID-Systeme müßten weitaus sorgfältiger und sicherer designed werden als ursprünglich angenommen.

Korrupt

Neuste Board-Kommentare:

nathan west schrieb am 16.03.2006 14:47:

Halte die Möglichkeit auch für absolut realitätsfern, und jeder der sich mit RFID beschäftigt müsste sehen, wie albern das ist. *Natürlich* sind ein paar Vorhaben auf Basis von RFID-Technik von ...

rolve schrieb am 16.03.2006 16:09:

kein programm, welches irgendeinen input verarbeitet, ist sicher.

Links:
Proof of Concept (pdf)
Ed Felten