TELEPOLIS

Der erste RFID-Virus wurde präsentiert

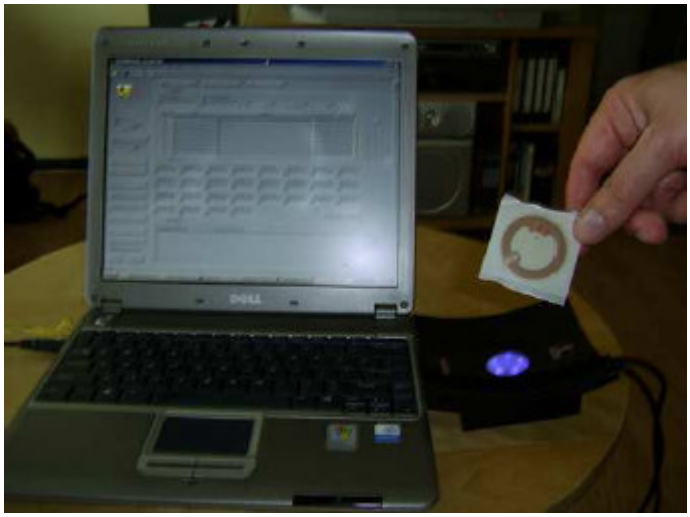
Florian Rötzer *15.03.2006*

Holländische Computerwissenschaftler weisen auf die Manipulationsmöglichkeiten von infizierten RFID-Systemen hin und warnen, dass "die Zeit der RFID-Unschuld" abgelaufen sei

RFID-Chips sind derzeit hoch im Kurs. Die Industrie sieht eine große Palette an Anwendungen, möglichst alle Güter könnten demnächst mit solchen Funkchips ausgestattet sein, die auch in Kleidungsstücke, Eintrittskarten und Ausweise integriert werden. In Haus- und Nutztiere werden sie schon implantiert, auch bereits in Menschen, beispielsweise in Patienten oder Angestellte, die darüber Zugriff auf geschützte Computersysteme erhalten. Datenschützer warnen vor dem dadurch möglichen Ausbau einer flächendeckenden Überwachung und fordern für die Bürger Transparenz, welche Daten auf den Chips gespeichert werden und wer auf sie Zugriff haben soll.

Noch können die Daten von den passiven RFID-Chips nur aus geringer Entfernung gelesen werden. Aber es gibt Bestrebungen, die Reichweiten auch hier größer zu machen (Identifizierung aus der Entfernung (1)). Unverschlüsselt können die Daten von jedem Lesegerät erfasst werden, das sich nahe genug an den Chips befindet. Das Knacken der Verschlüsselung ist nicht sonderlich schwer, wie dies bereits Computerexperten vorgeführt haben (Niederlande: Biometrie-Pass erfolgreich gehackt (2)).

Aber RFID-Chips eröffnen noch eine weitere, bislang kaum diskutierte Möglichkeit: Man kann in sie auch Computerviren einbringen, die wiederum unter bestimmten Bedingungen die Software in den Lesegeräten, aber auch Einträge in den Datenbanken verändern können, mit denen die Lesegeräte verbunden sind. Das würde natürlich die vielbeschworene Sicherheit und Exaktheit etwa der damit erfassten Warenströme beeinträchtigen können.



Der angeblich weltweit erste mit einem Virus infizierte RFID-Chip. Foto: Computer Systems Group

Computerwissenschaftler vom Department of Computer Science der Vrije Universiteit Amsterdam haben nun ein Papier (Is Your Cat Infected With a Computer Virus? (3)) veröffentlicht (siehe auch ihre Webseite: RFID-Virus (4)), in dem sie demonstrieren, wie das Hacken von RFID-Chips möglich wäre. Dazu stellen sie den ersten sich replizierenden RFID-Virus vor. Gleichzeitig weisen sie auf Möglichkeiten hin, wie sich diese besser vor dem Einbringen von Viren schützen ließen. Nach ihrer Ansicht stehen Programme, mit denen beispielsweise ein Buffer Overflow ausgelöst werden kann, um RFID-Würmer und –Viren einzuschleusen, vor der Tür: "RFID-Schadprogramme sind eine Büchse der Pandora, die in den Ecken unserer ‚smarten" Einkaufszentren und Häuser Staub angesammelt hat." Viren oder Würmer seien nur der Anfang, RFID-Phishing oder Wardriving könnten folgen.

Zwar sind die auf RFID-Chips speicherbaren Datenmengen gering – in aller Regel enthalten sie nicht mehr als 1024 Bits -, aber schon in der Middleware gäbe es hinreichend viele Sicherheitslücken, warnen die Wissenschaftler um Andrew S. Tanenbaum. Entsprechendes gelte für die Protokolle und schließlich für die Datenbanken, die zudem ein lohnendes Ziel für Kriminelle wären. Aber schon einfache Befehle wie 'write multiple blocks' (ISO-15693) könnten durch wiederholtes Abrufen zu einem Buffer Overflow führen. Eine andere Lücke wären SQL-Befehle.

Um die theoretischen Möglichkeiten auch praktisch zu zeigen, haben die Wissenschaftler einen RFID-Virus für einen Chip mit 127 Zeichen geschrieben, der Oracle-Programme betrifft. Varianten für andere Programme wollen sie später vorstellen. Allerdings verwendeten sie für ihre Demonstration nicht die kommerzielle Software für die Lesegeräte, sondern ein Programm, das diese repliziert. Der Oracle-SSI-Virus verwendete einen SQL-Befehl, um die Datenbank und schließlich weitere Chips beim Einlesen zu infizieren.

Für die Wissenschaftler jedenfalls ist mit ihrer Demonstration "die Zeit der RFID-Unschuld" abgelaufen. Ein von ihnen vorgestelltes Szenarium für "attraktive" Anwendungen wäre beispielsweise ein Virus in einem RFID-Chip in einem Gepäckstück, das in einem Flugplatz vom Gepäcksystem auf einem Fließband befördert wird. Wird der Code mitsamt dem Virus an einer Verzweigung abgelesen, um das Ziel zu bestimmen, kann er sich auf das ganze System verbreiten und schließlich auch über infizierte Gepäckstücke weitere Flughäfen erreichen. Schmuggler könnten durch die Störung versuchen, ihr Gepäck unter Umgehung der Sicherheitssysteme durchzuschleusen. Man könne aber auch in Kaufhäusern Preise verändern oder andere Identitäten fälschen.

Links

(1) http://www.telepolis.de/r4/artikel/22/22171/1.html
(2) http://www.telepolis.de/r4/artikel/21/21907/1.html
(3) http://www.rfidvirus.org/papers/percom.06.pdf
(4) http://www.rfidvirus.org/index.html

Telepolis Artikel-URL: http://www.telepolis.de/r4/artikel/22/22252/1.html

---