

Erster Mensch mit Computervirus infiziert
<http://www.heise.de/tp/blogs/3/147695>

Britischer Wissenschaftler warnt vor Manipulationsmöglichkeiten mit infizierten RFID-Systemen

Bericht von Thomas Pany 26.05.2010

In Großbritannien, an der [Universität von Reading](#), hat sich [Dr. Mark Gasson](#) den Titel als "[erster Mensch, der mit einem Computer-Virus infiziert ist](#)" verschafft.



Dazu hat sich **Gasson** einen überarbeiteten RFID-Chip in die Hand implantiert, wie er sonst zur Identifizierung von Tieren verwendet wird. Im Code des Chips hatte er einen Virus eingebaut. Das RFID-Implantat des Forschers aus der [Cybernetic Intelligence Research Group](#) war mit Lesegeräten verbunden, die an Zugängen an Universitätsräumen installiert bzw. in seinem Mobil-Telefon eingebaut sind. Zudem war es - wie bei den mit RFID-Tags bestückten Tieren - möglich, ihn anhand des Implantats zu identifizieren, zu orten und seine Wege zu verfolgen. **Gasson** gelang es, mit dem manipulierten Chip die Lesegeräte zu [infizieren](#):

"Der infizierte Chip steckte das Hauptsystem an, das mit ihm kommunizierte. Wären noch andere Geräte mit dem System verbunden, hätte sich der Virus auch dorthin übertragen."

Genauere Details will **Gasson** erst bei der Anfang Juni angesetzten Konferenz [IEEE International Symposium on Technology and Society](#) in Australien verraten. Das Prinzip dürfte jedoch dem gleichen, was der

Informatikprofessor Andrew S. **Tanenbaum** zusammen mit anderen schon 2006 vorstellte.

In dem [Paper](#) mit dem Titel "Is Your Cat Infected with a Computer Virus?" führte **Tanenbaum** vor, wie man RFID-Systeme via Buffer-Overflow mit Schadprogrammen infizieren kann (siehe dazu ausführlicher: [Der erste RFID-Virus wurde präsentiert](#) und [Katze mit Computervirus](#)).

Ein Jahr lang habe er dieses Implantat getragen, so **Gasson**, er habe sich so sehr daran gewöhnt, dass er es als Teil seines Körpers empfunden habe. Umso mehr habe in der Blick in eine mögliche Zukunft erschüttert. Dass er die erste Person, die mit einem Computer-Virus infiziert ist, sei, [schildert](#) er als aufregende Erfahrung und gleichzeitig als schockierend, "weil das Implantat so intim mit mir verbunden ist, aber die Situation potentiell außer Kontrolle ist".

"Ich glaube, wir müssen zur Kenntnis nehmen, dass unser nächster evolutionärer Schritt wahrscheinlich bedeutet, dass wir teilweise Maschinen werden, wenn wir danach trachten, unsere Möglichkeiten auszuweiten. Tatsächlich könnten wir herausfinden, dass es einen deutliche sozialen Druck gibt, der solche Implantat-Technologie fördert. Entweder weil es eine soziale Norm wird wie zum Beispiel Mobil-Telefone oder weil wir benachteiligt sind, wenn wir das nicht tun. Wir sollten uns aber bewusst sein, welche neuen Bedrohungen dieser Schritt zur Folge haben kann."

Die einzelnen in dem Bericht eingearbeiteten LINKS aufgelistet:

<http://www.reading.ac.uk/> - University of Reading

<http://www.reading.ac.uk/sse/about/staff/m-n-gasson.aspx> - School of Systems Engineering - Dr. Mark **Gasson**

<http://www.reading.ac.uk/about/newsandevents/releases/PR281590.aspx> - englischer Text - Could humans be infected by computer viruses? - 26.5.2010

<http://www.reading.ac.uk/cirg/> - Cybernetic Intelligence Research Group (CIRG)

<http://www.ieeessit.org/> - The IEEE Society of Social Implications of Technology
The IEEE-SSIT International Symposium on Technology and Society will be held June 7-9, 2010, in Australia!

<http://www.rfidvirus.org/papers/percom.06.pdf> -
Is Your Cat Infected with a Computer Virus?
Melanie R. Rieback Bruno Crispo Andrew S.

Tanenbaum

Vrije Universiteit Amsterdam

Computer Systems Group

De Boelelaan 1081a, 1081 HV Amsterdam,
Netherlands

fmelanie,crispo,astg@cs.vu.nl



Katze mit Computervirus:

<http://www.heise.de/security/meldung/Katze-mit-Computervirus-110494.html>

News-Meldung vom 15.03.2006 15:07

Katze mit Computervirus

Meldung vorlesen und MP3-Download

Mit Hilfe einer Datenbank für ausgelesene Informationen lassen sich RFID-Transponder, wie sie auch zur Markierung von Haustieren benutzt werden, als Gastgeber für Virensoftware missbrauchen. **Andrew Tanenbaum**, der Erfinder des Betriebssystems Minix, hat auf der IEEE Conference of Pervasive Computing in Pisa gleich mehrere Angriffsszenarien zur drahtlosen Datenerfassung per RFID beschrieben. Wie der gebürtige US-Amerikaner

auch auf einer Website der freien Universität Amsterdam darlegt, könnte zum Beispiel ein böswilliger Hacker einen RFID-markierten Artikel regulär im Supermarkt erstehen und den darauf angebrachten Transponder anschließend durch einen von ihm selbst programmierten ersetzen. Schmuggelt er die Ware mit der manipulierten Auszeichnung zurück in den Laden und legt sie erneut zur Bezahlung vor, kann er Supermarkt-Software, die sonst nur digitale Preisschildchen übers RFID-Lesegerät auswerten muss, mit schädlichem Code füttern.

Um die Machbarkeit solcher Attacken zu beweisen, hat **Tanenbaum** einen Virus für RFID-Middleware des Anbieters Oracle geschrieben, der mit gemeinhin verfügbaren 128 Byte an Transponder-Memory auskommt. Einmal in die Datenbank eingebracht, entpuppt sich der Transponder-Inhalt als so genannter Quine – ein Programm, das seinen eigenen Quelltext ausgibt – und vermag sich in der Datenbank zu replizieren. Auf diesem Weg ist auch die Infektion weiterer Transponder vorstellbar. Ähnliche Szenarien bauen auf die reiskorngroßen RFID-Tags, die hierzulande das Identifizieren entlaufener Haustiere erleichtern sollen und die typischerweise von Tierärzten oder Tierheimen kodiert und injiziert werden, daher der Titel von **Tanenbaums** Vortrag (PDF-Datei).

Der Professor beschreibt auch andere Techniken, mit denen man ein RFID-System in der Theorie sabotieren kann, etwa einen Wurm, der sich per Internet auf die RFID-Middleware ausbreitet. Seine Anleitung zur Gegenwehr beschränkt sich indes auf eher allgemeine Faustregeln, etwa, dass man unbenötigte Nutzerkonten für RFID-Middleware blockieren und die Software insgesamt mit möglichst begrenzten Nutzerprivilegien betreiben sollte.

<http://www.heise.de/tp/r4/artikel/22/22252/1.html> -
Der erste RFID-Virus wurde präsentiert
lorian 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 ([local] Identifizierung aus der Entfernung). 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 ([local] Niederlande: Biometrie-Pass erfolgreich gehackt).

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 ([extern] Is Your Cat Infected With a Computer Virus?) veröffentlicht (siehe auch ihre Webseite: [extern] RFID-Virus), 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.

Identifizierung aus der Entfernung >>>

<http://www.heise.de/tp/r4/artikel/22/22171/1.html> -

Niederlande: Biometrie-Pass erfolgreich gehackt >>>

<http://www.heise.de/tp/r4/artikel/21/21907/1.html> -



Es muss nicht einmal unbedingt der Staat sein, der schnüffelt (Bild: CCC)

Update: Deutscher und österreichischer Biometrie-Pass ebenfalls unsicher Österreich

<http://futurezone.orf.at/stories/86706/> -

Biometrie-Chips erstmals "gecrackt"

Kategorie: REISEPASS

31.01.2006|Erstellt um 18:13 Uhr

Binnen zweier Stunden haben holländische Spezialisten die schwache Verschlüsselung mit einem gewöhnlichen PC gebrochen. Im österreichischen Innenministerium wird nun überprüft, ob ein derartiger Angriff auch auf die künftigen österreichischen Pässe möglich ist.

Holländische Security-Spezialisten haben Daten aus den Funkchips der neuen Biometrie-Pässe erfolgreich abgezapft und die Verschlüsselung dann binnen zweier Stunden auf einem handelsüblichen PC gecrackt.

Laut einem Bericht des öffentlich-rechtlichen holländischen Senders VARA-TV sind Attacken dieser Art aus einer Entfernung von bis zu zehn Metern möglich. Das ist die maximale Reichweite, durch die der Chip [genannt: "contactless smart card"] mit einem Impuls auf 13, 65 MHz ["skimmed"] ausgelesen werden kann. Realisierbar wird der Angriff ausgerechnet durch jene Daten der maschinenlesbaren Zone im Pass, die ihn sicher gegen Auslesen durch Unbefugte machen sollen.

zu diesem Zeitpunkt sind die Daten zwar noch verschlüsselt aber:

Der geheime Schlüssel, der den Zugang zu den auf dem Chip enthaltenen Daten samt digitalem Passfoto und Fingerabdruck sichern soll, ist nicht sicher, weil bei seiner Erzeugung zu wenig "Randomness" [Zufälligkeit] im Spiel ist. Verschlüsselung nur 35 bit

Gebildet wird der Schlüssel nämlich aus dem Ablaufdatum des Passes, dem Geburtsdatum des Inhabers sowie der Passnummer, die in der Maschinen-Lesezone des Passes enthalten ist. Da die letzte Stelle der Passnummer auch noch aus einer Prüfsumme der anderen Stellen besteht, die holländischen Pässe fortlaufend nummeriert sind und die Verschlüsselung nur 35 bit beträgt, ist hier ein erhebliches Sicherheitsrisiko gegeben.

Solchermaßen ausgelesene Daten könnten nämlich zu Passfälschungen in hervorragender Qualität missbraucht werden. Und in Österreich ...

"Wir wussten seit dem vergangenen Sommer, dass die Kollegen in Holland Probleme mit den neuen Biometrie-Pässen haben." sagte Heinrich Pawlicek, Leiter der Passbehörde im Innenministerium am Dienstag zur futurezone.

Welche Probleme das genau seien, habe man zwar nicht gewusst. Dass es sich nicht um Lappalien handle, sei aber durch das um Monate verschobene Roll-Out-Datum klar geworden.

Die Niederländer hatten ursprünglich vorgehabt, die neuen Pässe Anfang 2006 vor allen anderen EU-Staaten auszugeben, im Sommer 2005 mussten diese Pläne weit nach hinten im Jahr verschoben werden.

Genau um diese Zeit hatten die Security-Spezialisten von Riscure ihr Angriffskonzept erstmals präsentiert, freilich noch ohne Demonstration, wie es nun geschah.

- * Der Bericht von VARA-TV
- * Das Angriffskonzept von Riscure
- * Wie das Auslesen funktioniert
- * Play-Doh trickst Fingerabdruck-Scanner aus

Auch fortlaufend nummeriert

Man müsse nun prüfen, sagt Pawlicek, ob auch die künftigen österreichischen Pässe von einem derartigen Angriff ebenso kompromittiert werden könnten.

Die österreichischen Pässe sind ebenfalls fortlaufend nummeriert und auch die anderen Gegebenheiten wie die Daten in der Maschinenlesezone sind hier gleich.

In Österreich sollen die ersten Biometrie-Pässe mit einem digital auf einem Chip gespeicherten Foto noch in diesem Frühjahr ausgegeben werden.

BM.I - Bundesministerium für Inneres
http://www.bmi.gv.at/cms/BMI/_news/BMI.aspx
<http://www.bmi.gv.at/publikationen/sicherheitspass.asp> - dieser Bericht ist nicht mehr zu finden!?

http://www.bmi.gv.at/cms/BMI_Service/reisepass/start.aspx

Der neue Sicherheitspass mit Fingerabdruck

Seit Juni 2006 können bei den Passbehörden neue Reisepässe beantragt werden.

Die Dokumente entsprechen dem neuesten Stand der Sicherheitstechnik und enthalten einen Chip, auf dem das Passfoto gespeichert ist. Seit 30. März 2009 werden auf dem Chip auch die Fingerabdrücke gespeichert.

Seit dem 15.6.2009 sind keine neuen Kindermiteintragungen mehr zulässig; überdies werden auch neu ausgestellte Kinderpässe mit einem Chip versehen.



http://www.bmi.gv.at/cms/BMI_Service/reisepass/files/FlyerZickZack.pdf

Sehr geehrte Damen und Herren!
Ab 2009 entspricht Ihr neu ausgestellter Reisepass dem modernsten Stand der Sicherheitstechnik.

Der Grund: erstmals werden – zusätzlich zu den bereits bestehenden Sicherheitsmerkmalen – **auch Fingerabdrücke** im Pass gespeichert.

Die Speicherung auf einem im Pass integrierten Chip dient zum Schutz vor unberechtigter Verwendung und Fälschung und gilt als wichtiges Instrument im Kampf gegen Menschenhandel und andere kriminelle Machenschaften. Die Speicherung erfolgt unter strengsten Sicherheitsbedingungen und ermöglicht eine noch eindeutigere Zuordnung des Passes zu seinem Besitzer.

Sie werden Ihren „Hochsicherheitspass“ weiterhin auf der Bezirkshauptmannschaft, dem Magistrat oder der ermächtigten Gemeinde beantragen können. Der Reisepass wird Ihnen wie bisher binnen fünf Arbeitstagen an die von Ihnen gewünschte Adresse zugesandt.

Ihre
Maria Fekter
Bundesministerin für Inneres