Chipcard-Hacking

Vortrag: *Christian Kahlo, Markus Kuhn* <Darvad@I.am, mgk25@cl.cam.ac.uk>
WWW: http://www.cl.cam.ac.uk/~mgk25/

Bericht: *Dirk Steinhauer* <moose@uni.de>

Früher gab es Kryptoprobleme in dem Sinne nicht, da Großrechner und die entsprechende Software recht simpel durch Hunde, Mauern und Sicherheitsdienste abzuschirmen waren. Heute sieht das Problem ein wenig anders aus, da fast jeder Mensch mittlerweile Chipkarten mit sich rumträgt, sie ihm aber nicht gehören und er eigentlich auch nicht an die Informationen darauf zugreifen können soll. Entsprechend hoch ist der Kryptoaufwand, den die Hersteller dafür betreiben.

Es muß ja z.B. bei Geldkarten sicher gestellt werden, daß nicht einfach Geld erzeugt wird, sondern daß jedes Mal auf der einen Seite etwas abgezogen wird, wenn auf der anderen etwas dazukommt.

Andere Einsatzmöglichkeiten bestehen bei Pay-TV, Kopierschutzsystemen, Funktelefonen (GSM) und vielem mehr.

Es gibt drei verschiedene "Spezies", die sich um die Entschlüsselung dieser Informationen bemühen. Einmal versierte Outsider (Hacker), die nur über Informationen verfügen, die öffentlich zugänglich sind und normalerweise kein spezielles Equipment haben, dann Insider, die in der Firma arbeiten und oft zu vertraulichen Informationen und speziellen Geräten Zugang haben und schließlich Organisationen, die über genügend fachliches Personal, ausreichend Geld und die Möglichkeit, eigens für diesen Zweck Geräte zu entwickeln, verfügen (Mafia, Konkurrenten, Geheimdienste...).

Entsprechend der "Spezies" kann man natürlich auf verschiedene Art versuchen, die Informationen zu bekommen, am einfachsten durch Ausprobieren, bekannte Bugs, Verletzen der Spezifikationen (Temperatur, Ströme, Protokollverletzungen,...) oder protokollieren aller nach außen erkennbaren Informationen, ohne die einzelnen Pakete zu zerstören (siehe Christians Homepage http://www.gsho.notrix.de/).

Sollte man über bessere Ressourcen verfügen, kann man natürlich versuchen, "Reverse Engineering" zu betreiben, d.h. den Chip selbst zu öffnen, jede Lage zu photographieren und dann Wochen über riesigen Photos zu verbringen und die Schaltpläne nachzuvollziehen. Oder man kann mit einem Lasercutter versuchen, die einzelnen Bahnen auf dem Chip freizulegen und dort die Ströme einzeln zu messen, probieren was passiert, wenn eine Leiterbahn getrennt wird, oder natürlich gezielt einzelne trennen (z.B. um Counter oder Verifizierung auszuschalten).

Für mehr Informationen zu diesem Aspekt schaut auf Markus Homepage (http://www.cl.cam.ac.uk/~mgk25/). Bei den Chipkarten gibt es sogenannte "Smartcards", "intelligente" Chipkarten, die über ein asynchrones Protokoll (T=0 bis T=15) kommunizieren und normale "dumme" Speicherkarten, die ein synchrones Protokoll (I2C, 2-wire, 3-wire,...) benutzen. Telefonkarten sind z.B. normale Speicherkarten, die eigentlich nur herunterzählen können, obwohl natürlich beim Übergang auch niedere Bits noch mal hochgesetzt werden müssen.

Die neu gegründete "German Smartcard Hackers Organisation" soll dem Austausch von Informationen dienen, zu Eigenbasteleien und zum Schreiben von Software anregen. Bis jetzt stellte sich allein die Informationsbeschaffung im Netz als wochenlanges Projekt mit anschließendem intensiven Vertiefen in die Materie heraus, was viele potentielle "Entwickler" doch ein wenig abschreckt. In unseren Nachbarländern gibt es da schon seit Jahren viele aktive, nette Menschen.

Natürlich wird man immer wieder gefragt, wie man möglichst schnell Telefonkarten neu aufladen kann, aber wenn man sich mal in die Materie eingearbeitet hat, verliert man solche Illusionen doch recht schnell, da Siemens und die Telekom mittlerweile eine ganze Menge Sicherheitsmerkmale benutzen (erwähnt sei nur der "Stille Alarm"). Da sollte man sich lieber erst mal durch die ISO-Normen lesen und ein bißchen Hintergrund in Mathe und Physik mitbringen, Verstehen welche unterschiedlichen Karten und Protokolle es gibt... viel Spaß am Thema.