EC-Karten Unsicherheit

Vortrag: *Andy Mueller Maghun* <andy@ccc.de>

Bericht: *Kai Herings*

EC Karten sind in mehrfacher Hinsicht ein beliebtes Ziel von Attacken jeglicher Art, weil sie so weit verbreitet sind und weil sie sehr "wertvolle" Daten enthalten. Sie wurden Mitte der 80er Jahre eingeführt. Mit ihnen war es zum ersten Mal möglich, an verschiedenen Geldinstituten Geld abzubuchen. Technisch hatte sich folgendes getan: Die Kundenkarten enthielten nur einen Institutskey, mit dem es nicht möglich war, bei einer anderen Bank Geld abzuheben. Um dies zu ändern, wurde zu dem mit 56 Bit verschlüsselten Institutskey ein zweiter aufgesetzt, der sogenannte Poolkey, der in drei verschiedenen Ausfertigungen auf der Karte vorhanden war. Wenn der Automat erkennt, daß die eingeschobene Karte keine institutseigene Karte ist, verwendet er den Poolkey, wenn der Automat nun den Poolkey verwendet hat, bekommt er ein anderes Ergebnis, als er mit dem Institutskey errechnet hätte. Jetzt kommt ein sogenannter Offsetwert ins Spiel, der auch auf der Karte gespeichert wurde, dieser wird dann zu dem errechneten Wert addiert und ergibt den selben Wert, als hätte man den Institutskey. Um sich gegen das Plündern von EC-Karten zu schützen, gibt es zwei Verfahren. Einen Fehlbedienungszähler: Bei dem sogenannten Offline-Verfahren, wird auf der Karte notiert, wie oft die PIN der Karte falsch eingegeben wurde und der Automat zieht die Karte nach 3maliger Falscheingabe ein. Mit einem Kartenlesegerät kann man dies umgehen, indem man den Fehlbedienungszähler, welcher frei zugänglich ist, zurücksetzt. Beim Online-Verfahren wird mit einer Backlist überprüft, ob diese Karte ungültig ist; wenn das der Fall ist, wird sie ebenfalls eingezogen.

Die Systemschwächen: Die zwei direkten Systemschwächen sind, daß man den Fehlbedienungszähler zurücksetzen kann und so damit unendlich viele Möglichkeiten hat, die PIN zu erraten, was sich nicht als so schwierig erweist, wie es den Anschein hat. Denn die 2. Sicherheitslücke bezieht sich auf die PIN selber. Es gibt nicht, wie es einleuchtend wäre, 10^4 Möglichkeiten, sondern:

1. Keine PIN fängt mit 0 an

2. Es gibt keine doppelten Zahlen hintereinander

3. Die PIN wird von Hexadezimal auf Dezimal konvertiert, wobei A wieder 1 ist Wenn man alle diese Faktoren einrechnet, hat man noch ein Chance von 1:64, die PIN zu erraten. Andere Möglichkeiten, eine EC-Karte zu hacken: Die anderen Möglichkeiten, an die PIN für eine Karte zu kommen, sind zum Teil wirklich simpel oder auch viel kniffliger als das Rateverfahren. Viele Karteninhaber gehen zu sorglos mit ihren PINs um und schreiben sie z.B. sogar mit einem Stift auf die Karte. Die meisten Kriminellen loggen den Datenverkehr zwischen Karte und Automaten mit und spionieren mit Minikameras die PIN aus. Eine andere, ebenso effektive Methode ist es, die Emissionen des Automaten abzuhören. Die unverfrorenste Methode ist es aber, einen eigenen "Automaten" aufzustellen und nach der PIN Eingabe ihn die Karte unter einer dubiosen Fehlermeldung wieder auswerfen zu lassen.

Die Entschlüsselung des Pool-Keys: Den 56Bit Schlüsssel kann man mit verschiedenen Methoden knacken: 1. Pool-Key Berechnung - in einem Rechenzentrum 2. Pool-Key Berechnung - DES-Knacker Selbstbau 3. Automatendiebstahl, MM-Modul-Recycling

Das MM-Modul ist ein im Automaten eingebautes, gepanzertes Modul, in dem die Entschlüssellung stattfindet. Dieses Modul zerstört sich selbst, wenn Licht hineinfällt oder es länger als 15 Minuten keinen Strom hat.

Sicherheitsmaßnahmen: Inzwischen gibt es ein neues Verfahren, alle Karten sind nun mit 128 Bit verschlüsselt, und Auszahlungen erfolgen nur noch, wenn der Automat online ist. Die Banken behaupten, daß dadurch die Kartenbetrügereien drastisch zurückgegangen sind.