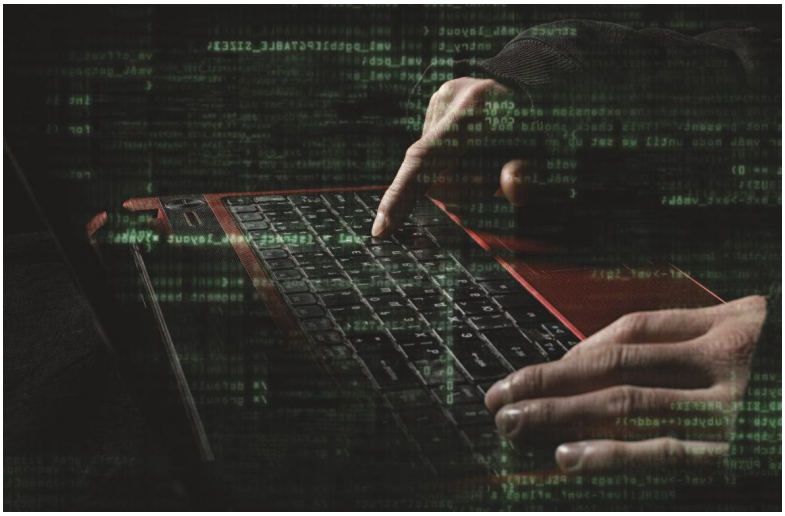
43 Digitale Schutzmechanismen knacken, um sie sicherer zu machen

Heutzutage geht es bei der Kryptographie nicht mehr um Geheimnisse wie noch vor einem Jahrhundert, sondern hauptsächlich um Mathematik. Und dass die moderne Kryptographie immer mehr alltägliche Anwendungen absichert.



Im Jahr 2008 knackten Forscher der Radboud Universität Nijmwegen die OV-Chipkarte. Sie zeigten, wie sie damit kostenlos reisen konnten. Aber das Problem war viel größer als die OV-Chipkarte allein. Der Chip in dieser niederländischen Reisekarte für den ÖPNV, der Mifare Classic, wurde in mehr als einem Jahrzehnt weltweit zu mehr als einer Milliarde Karten verarbeitet. Und dazu gehören auch Zugangsausweise zu Regierungsgebäuden und militärischen Einrichtungen.

Es ist eine gute Praxis für Wissenschaftler, den Hersteller nach der Entdeckung einer Sicherheitsverletzung zu informieren und ihm Zeit für die Reparatur des Produkts zu geben: sechs Monate für die Anpassung der Hardware und sechs Wochen für die Software. Die Radboud-Wissenschaftler warnten 2008 die niederländische Regierung, den internen Sicherheitsdienst und den Hersteller der OV-Chipkarte, die niederländische Firma NXP. Die Panik war groß. NXP versuchte, eine wissenschaftliche Veröffentlichung der Forscher über den Sicherheitsbruch zu verhindern, aber der Richter entschied, dass die Wahrheit von öffentlichem Interesse sei und erlaubte die Veröffentlichung.

Geheimer Schlüssel

Roel Verdult, einer der damaligen Hacker und heute Doktorand an der Radboud Universität, sieht es als soziale Aufgabe von Forschern der digitalen Sicherheit, die Sicherheit kritisch zu untersuchen. „Es ist sehr schwierig, den theoretischen Beweis zu erbringen,

dass die digitale Sicherheit so und so stark ist“, sagt Verdult. „Deshalb wird in der Praxis ein pragmatischer Ansatz verfolgt. Das bedeutet, dass es Teil des Aufbaus eines guten Kryptosystems ist, auch zu versuchen, es zu knacken. Auf diese Weise können die Wissenschaftler aus allen Arten der vorgeschlagenen Schutzmaßnahmen die besten auswählen.“

Sowohl das Erstellen als auch das Brechen kryptographischer Schutzvorrichtungen basiert auf Mathematik. Im Mittelpunkt steht ein kryptographischer Algorithmus: ein Berechnungsrezept, das geheime digitale Schlüssel erzeugt. Eine häufig verwendete Methode ist die Durchführung einer mathematischen Operation mit drei Zahlen: zuerst eine bekannte Zahl, zum Beispiel die Identifikationsnummer einer Karte, dann ein geheimer Wert, der als Schlüssel dient, und schließlich eine Zufallszahl, die an Ort und Stelle generiert wird. Je schwieriger der Schlüssel und je zufälliger die Zahl, desto schwieriger ist er zu knacken und desto besser die Sicherheit.

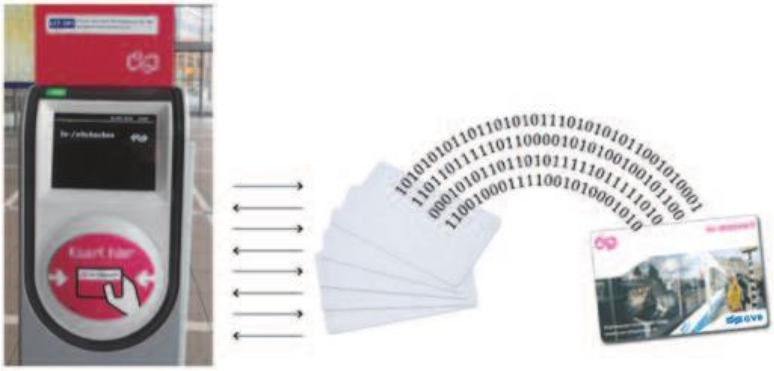
Im Beispiel der OV-Chipkarte funktioniert es wie folgt. Sobald sich eine Chipkarte einem Lesegerät nähert, sendet sie eine eindeutige Identifikationsnummer an das Lesegerät. Mit dieser Zahl erzeugt der Leser eine Reihe von kryptographischen Schlüsseln. Die Karte und das Lesegerät prüfen mit Hilfe elektromagnetischer Signale schnell, ob sie den geheimen Schlüssel kennen. Wenn sie dies tun, wird der Reisende ein- oder ausgecheckt.

„Der Algorithmus, der bei der Mifare Classic und damit auch bei der OV-Chipkarte verwendet wurde, war bereits in der Entwurfsphase unsicher“, erklärt Verdult. „Aber da der Algorithmus geheim gehalten wurde, dauerte es einige Zeit, bis wir die Konstruktionsfehler entdecken konnten. Unmittelbar danach warnten wir alle vor den bestehenden Schwächen. Obwohl wir die Ersten waren, die offen über die Probleme sprachen, ist es nicht unwahrscheinlich, dass diese Schwächen bereits insgeheim von anderen ausgenutzt wurden.“

Eigentlich sollte der Ausgangspunkt sein, dass die Sicherheit eines Kryptosystems nur vom Schlüssel und nicht vom Algorithmus profitieren sollte, meint Verdult. „Die Zufalls- und Geheimzahlen werden immer wieder neu berechnet, während der Algorithmus derselbe bleibt. Ein guter Algorithmus wird nicht unsicher, wenn er öffentlich ist. Tatsächlich kann dann jeder überprüfen, ob es sich um einen guten Algorithmus handelt. Und jeder kann Verbesserungen vorschlagen, um es noch stärker zu machen.“

Neuer Pass

Die Empfehlungen der Forscher für ein stark verbessertes Kryptosystem wurden von der niederländischen Regierung sofort beherzigt. Die Regierung ist nun dabei, einen sicheren nationalen Pass für den Zugang zu Ministerien und anderen wichtigen Gebäuden einzuführen. Ein gutes Beispiel für die Nützlichkeit ihrer Arbeit, so Verdult. Aber bei der OV-Chipkarte sieht die Sache ganz anders aus. „Eigentlich gibt es dort nur wenige Stellen zur Verbesserung der Sicherheit. Aber im Kern gibt es immer noch den gleichen unsicheren Mifare Classic-Algorithmus. Wirklich seltsam, denn selbst der Hersteller des Mifare Classic rät vom Kauf des Chips ab.“



Nach dem Hacken der OV-Chipkarte im Jahr 2008 hörte man einige Leute als Entschuldigung sagen, dass jedes System gehackt werden kann. Aber Verdult betont, dass Sie diese Aussage von einem Kryptoforscher niemals hören werden: „Es gibt viele Algorithmen, die sicher sind. Ein bekanntes Beispiel ist der *Advanced Encryption Standard* (AES), der 1998 eingeführt wurde und nach mehr als fünfzehn Jahren immer noch nicht zu knacken ist.“ Es ist die Aufgabe der Kryptoforscher, herauszufinden, welche Algorithmen sicher sind und in welchen Anwendungen sie am besten eingesetzt werden können.

An der Bergischen Universität Wuppertal gibt es Lernstationen zur Kryptographie, die SpionCamps, siehe https://ddi.uni-wuppertal.de/www-madin//material/spioncamp.html.