Digitale beveiligingen kraken om ze veiliger te maken

Tegenwoordig draait cryptografie niet meer om geheimschriften, zoals een eeuw geleden, maar grotendeels om wiskunde. En die moderne cryptografie beveiligt steeds meer alledaagse toepassingen.

In 2008 kraakten onderzoekers van de Radboud Universiteit Nijmegen de ov-chipkaart. Ze lieten zien hoe ze er gratis mee konden reizen. Maar het probleem was veel groter dan de ov-chipkaart alleen. De chip in deze Nederlandse reizigerskaart, de Mifare Classic, is in ruim een decennium wereldwijd in meer dan een miljard pasjes verwerkt. En daaronder zijn ook toegangspasjes tot overheidsgebouwen en militaire installaties.

Het is een goed gebruik dat wetenschappers na de ontdekking van een beveiligingslek de producent informeren en hem de tijd geven om het product te repareren: zes maanden voor het aanpassen van hardware en zes weken voor software. De Radboud-onderzoekers waarschuwden in 2008 de Nederlandse overheid, de binnenlandse veiligheidsdienst en de fabrikant van de ov-chipkaart, het Nederlandse bedrijf NXP. De paniek was groot. NXP probeerde een wetenschappelijke publicatie van de onderzoekers over het beveiligingslek tegen te houden, maar de rechter oordeelde dat de waarheid van publiek belang was en stond publicatie toe.

Geheime sleutel

Roel Verdult, een van de hackers van toen, en inmiddels gepromoveerd aan de Radboud Universiteit, ziet het als een maatschappelijke taak van onderzoekers van digitale veiligheid om

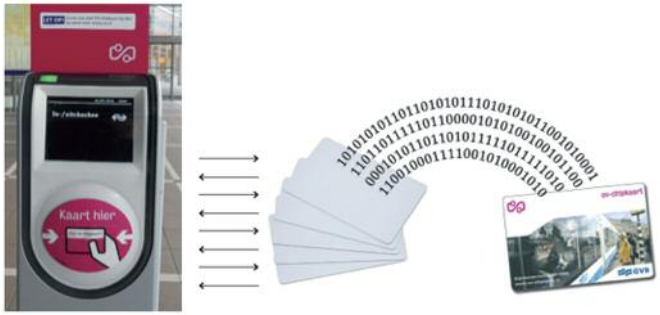
beveiligingen kritisch tegen het licht te houden. “Het is heel moeilijk om een theoretisch bewijs te leveren dat een digitale beveiliging zo-en-zo sterk is”, vertelt Verdult. “Daarom wordt in de praktijk een pragmatische aanpak gekozen. Dit houdt in dat het bij het bouwen van een goed cryptosyteem hoort om ook te proberen het te kraken. Zo kunnen wetenschappers uit allerlei voorgestelde beveiligingen de beste selecteren.”

Zowel het maken als het breken van cryptografische beveiligingen is gebaseerd op wiskunde. Centraal staat een cryptografisch algoritme: een rekenrecept dat geheime digitale sleutels genereert. Een veel gebruikte methode is het uitvoeren van een rekenoperatie op drie getallen: allereerst een bekend getal, bijvoorbeeld het identificatienummer van een kaart, vervolgens een geheime waarde die dient als sleutel, en ten slotte een willekeurig getal dat ter plekke gegenereerd wordt. Hoe moeilijker de sleutel en hoe willekeuriger het getal, des te moeilijker het te kraken is en hoe beter de beveiliging.

In het voorbeeld van de ov-chipkaart werkt het als volgt. Zodra een chipkaart in de buurt van een leesapparaat komt, stuur de kaart een uniek identificatienummer naar de lezer. Met dat nummer genereert de lezer een reeks cryptografische sleutels. Kaart en lezer checken razendsnel via elektromagnetische signalen bij elkaar of ze de geheime sleutel kennen. Als dat het geval is, wordt de reiziger in- of uitgecheckt.

“Het algoritme dat bij de Mifare Classic en dus ook bij de ov-chipkaart werd gebruikt, was al bij het ontwerp onveilig”, vertelt Verdult. “Maar omdat het algoritme geheim werd gehouden, heeft het een tijd geduurd voordat we de ontwerpfouten konden waarnemen. We hebben direct daarna iedereen gewaarschuwd over de bestaande zwakheden. Alhoewel wij de eersten waren die openlijk over de problemen spraken, is het niet onwaarschijnlijk dat deze zwakheden in het geheim al misbruikt werden door anderen.”

Eigenlijk moet het uitgangspunt zijn dat de veiligheid van een cryptosysteem alleen zou moeten afhangen van de sleutel en niet van het algoritme, vindt Verdult. “De willekeurige en geheime getallen worden telkens opnieuw berekend, terwijl het algoritme steeds hetzelfde blijft. Een goed algoritme wordt



niet onveilig wanneer het openbaar is. Sterker nog, iedereen kan dan checken dat het een goed algoritme is. En iedereen kan verbeteringen voorstellen om het nog sterker te maken.”

Nieuwe pas

De aanbevelingen van de onderzoekers voor een sterk verbeterd cryptosysteem werden meteen ter harte genomen door de Nederlandse overheid. Die rolt inmiddels een veilige Rijkspas uit voor de toegang tot ministeries en andere belangrijke gebouwen. Een mooi voorbeeld van het nut van hun werk, zegt Verdult. Maar heel anders ligt het bij de ov-chipkaart. “Daar zijn er eigenlijk alleen wat pleisters geplakt om de beveiliging te verbeteren. Maar in de kern zit nog steeds hetzelfde onveilige Mifare Classic-algoritme. Raar eigenlijk, want zelfs de producent van de Mifare Classic adviseert om de chip niet meer te kopen.”

Na het kraken van de ov-chipkaart in 2008 hoorde je sommige mensen ter verontschuldiging zeggen dat elk systeem te kraken is. Maar Verdult benadrukt dat je die uitspraak nooit van een crypto-onderzoeker zult horen: “Er zijn wel degelijk vele algoritmes die wel veilig zijn. Een bekend voorbeeld is de *Advanced Encryption Standard* (AES), geïntroduceerd in 1998 en na ruim vijftien jaar nog steeds niet te kraken.” Het is de taak van crypto-onderzoekers om uit te zoeken welke algoritmes veilig zijn en bij welke toepassingen ze het beste ingezet kunnen worden.