Auf dem Finanzplatz Schweiz werden jeden Tag bis zu zwei Millionen Überweisungen im Wert von rund 100 Milliarden Schweizer Franken zwischen den Banken getätigt. Die Sicherheit jeder einzelnen Transaktion hat oberste Priorität. Ein Forschungsinstitut der HSR macht es Cyber-Kriminellen nun noch schwerer, das Transaktionssystem zu knacken.

Hacken für den Finanzplatz Schweiz

Willi Meissner, Redaktion

HSR Forscher Roman Willi vom IMES Institut für Mikroelektronik und Embedded Systems sitzt konzentriert über einer Platine. Er hat ein sensibles Strom-Messgerät an einem unscheinbaren Chip angelegt und kann so kleinste Spannungsveränderungen sehen. Eine hohe Spannung ist eine 1. Eine niedrige Spannung ist eine 0. 00011010100000011101000… So ähnlich, nur mit 3072 Nullen und Einsen, sehen die Zahlenreihen aus, auf die es Willi abgesehen hat: Der Schlüssel für die elektronische Unterschrift einer Bank. Wer den Schlüssel kennt, kann auch die Unterschrift fälschen. Ein Krimineller könnte auf diesem Weg mit der Identität einer Bank Überweisungen tätigen – zum Beispiel auf sein eigenes Konto.

Schnelle Sicherheit durch Hardware

Wenn Banken im Minutentakt Millionenbeträge überweisen, wollen sie sehr sicher sein, dass jede Transaktion ohne Risiko abläuft. Dafür müssen sie auf die Firma SIX Interbank Clearing vertrauen, die das Transaktionssystem des Schweizer Finanzplatzes betreibt. Neben fast allen Schweizer Banken arbeiten auch viele ausländische Banken mit dem System. Bei bis zu zwei Millionen Überweisungen pro Tag muss das SIX-System nicht nur sicher, sondern auch schnell sein. Diese Anforderungen stellt SIX mit einer kombinierten Hard- und Software-Infrastruktur sicher. Speziell entwickelte Hardware kann Daten schneller verarbeiten als Software. Dieses Hardware Security Modul (HSM) wird von der Schweizer Firma Securosys (www.securosys.ch) produziert.

«DAS FORSCHUNGSPROJEKT MIT DER HSR ERMÖGLICHT SECUROSYS, VERSCHLÜSSELUNGSSYSTEME IN ZUKUNFT NOCH SICHERER ZU MACHEN.»

Monatelange Datenjagd

Für das KTI-geförderte Forschungsprojekt von HSR und SIX haben die beiden HSR Forscher Roman Willi und Dorian Amiet mehrere Monate lang «gegeneinander» gearbeitet. Ein Kern-Element der Securosys-Hardware sollte so sicher wie möglich werden: Der Chip, in dem die Authentifizierung der Überweisungen verarbeitet wird. Zwar ist der Chip selbst vor unbefugtem physischem Zugriff geschützt. Aber sicher ist sicher.

Die Rollenverteilung für die Arbeit am Chip: Dorian Amiet programmiert den Chip möglichst sicher, Roman Willi versucht in der Rolle des kriminellen Hackers, den Schlüssel für die elektronische Bank-Unterschrift auszulesen. «Irgendwann war es unter vertretbarem Zeitaufwand nicht mehr möglich, den Schlüssel auszulesen», sagt Willi. Auch Securosys-CTO/CSO Andreas Curiger zieht ein positives Fazit: «Das Forschungsprojekt mit der HSR ermöglicht es Securosys, Verschlüsselungssysteme in Zukunft noch sicherer zu machen.»

Learning by hacking

Am Anfang war es für Willi noch verhältnismässig machbar, an den Schlüssel zu kommen. Sowohl mit einem Strom-Messgerät, wie auch durch das Messen der Magnetfelder um den Chip. Denn im Chip der Hardware werden endlos lange Zahlenreihen aus 1 und 0 verarbeitet. Willi fand heraus, bei welcher Spannung eine 1 verarbeitet wird und konnte so 0en und 1en unterscheiden und abspeichern – solange bis der Schlüssel komplett war.

Konzentriert sucht Roman Willi in einem abgeschirmten Raum nach kleinsten Veränderungen im Stromfluss – sein Ziel: die digitale Unterschrift einer Bank.

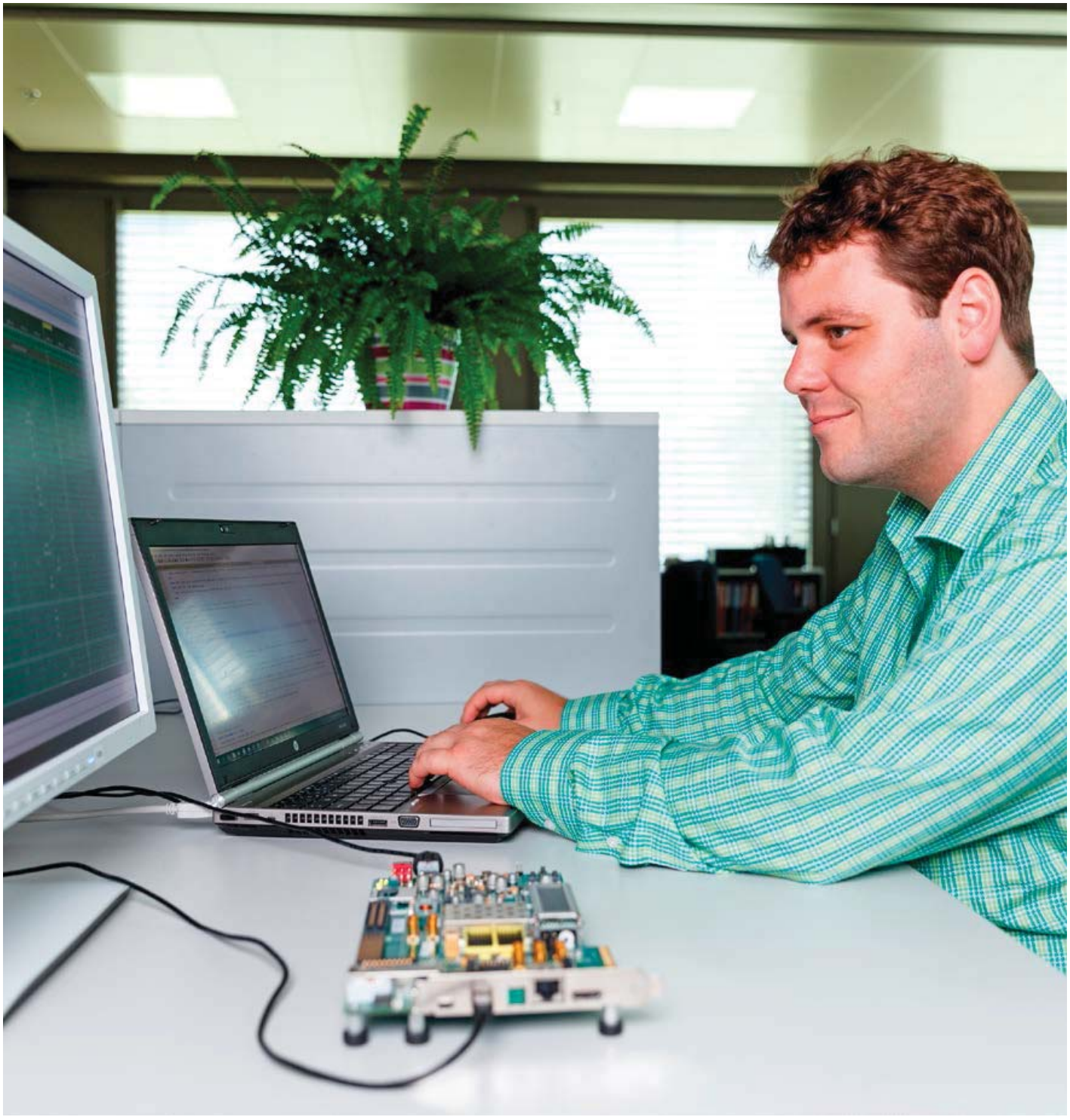
Amiet liess daraufhin bei jeder Null «sinnlose Daten» mitproduzieren, um die Spannung an jene bei den Einsen anzugleichen. Willi konnte die Nullen und Einsen nicht mehr zu unterscheiden. Jedoch: Die Müll-Daten wurden auf dem Chip nicht gespeichert, die echten schon. Um weiterzukommen, musste Willi also mittels Filtertechniken und Korrelationen die echten Daten herausfiltern und konnte so den klaren Schlüssel wieder auslesen.

Nächste Runde. Amiet speichert die Müll-Daten ebenfalls ab. Willi findet aber heraus: Der Strom für die falschen Daten nimmt auf dem Chip einen anderen Weg als die echten Daten, sie werden damit unterscheidbar.

Das gemeinsame Gegeneinander geht weiter. Sogar einen magnetisch abgeschirmten Raum des ICOM Institut für Kommunikationssysteme nutzte Willi, um noch die letzten physischen Methoden zum Auslesen des Schlüssels auszureizen. Bis zu dem Punkt, als sich beide IMES Forscher einig sind: Mit heute verfügbarer Technik lässt sich der Schlüssel nicht mehr innert ausreichender Frist knacken. Amiet formuliert es so: «Mit mathematischen Methoden müsste man länger auf den richtigen Schlüssel warten, als die Erde noch existiert.»

Vielversprechender könnte dagegen ein Angriff mit neuer, heute noch nicht verfügbarer Technologie sein. Das IMES befasst sich bereits mit einem Folgeprojekt, um Kriminellen auch in Zukunft einen Schritt voraus zu sein: Sie wollen die Schlüssel gegen Angriffe mit Quanten-Computern wappnen, obwohl diese um ein vielfaches leistungsfähigeren Supercomputer heute noch gar nicht verfügbar sind. ■

paul.zbinden@hsr.ch



Dorian Amiet muss die Verschlüsselungs-Hardware nochmals neu programmieren – Roman Willi hat Amiets Methode erfolgreich knacken können.