Een kat en muisspel zonder einde

20 augustus 2012

Dr. ir. Erik Poll staat niet zozeer bekend als beveiliger, maar eerder als professioneel kraker. ‘Om iets te kunnen beveiligen, moet je eerst weten waar de zwakke plekken zitten.’ Binnen Sentinels werkte hij aan de beveiliging van smartcards, en aan een systeem dat software lekdicht maakt.

Poll was samen met dr. Jaap-Henk Hoepman projectleider van het Sentinels-project JASON. Dit heeft een platform opgeleverd waarmee je door een compleet softwaresysteem heen beveiliging kunt aanbrengen, legt hij uit. ‘Niet door een paar regels code op het laatste moment als toeter of bel toe te voegen, maar door integraal verweven met de code op de juiste plekken de juiste beveiliging aan te brengen.’ Fouten in software zijn snel gemaakt, zegt hij. ‘Meestal ontstaat een lek in een enkele regel code. Gewoon over het hoofd gezien door een programmeur. Met Jason kun je na completering van de code aangeven op welke fronten het systeem beveiligd moet zijn en wie waar toegang toe moet krijgen. Het platform integreert dan de benodigde code op de juiste plaatsen.’

Dr. ir. Erik Poll, projectleider van JASON en betrokken bij PINPASJC

Binnen het Sentinels-project werkte Poll nauw samen met het bedrijfsleven. ‘Bij Jason was het bedrijf Chess IT betrokken. Dat bedrijf is gespecialiseerd in betaalterminals, denk aan parkeerautomaten en dergelijke. Wij hebben gekeken hoe je zoiets zou moeten beveiligen. Hoe zorg je ervoor dat die automaten niet gehackt worden en zo bijvoorbeeld persoonsgegevens van bankpassen kunnen lezen?’ Om een goede samenwerking te bewerkstelligen, zaten onderzoekers van de universiteit een dag in de week bij Chess.

Kraak haalt nieuws

In het tweede project waar Poll bij betrokken was, PINPASJC, werd gewerkt aan de beveiliging van chipkaarten, zoals die bijvoorbeeld worden gebruikt in

chipknips, ov-chipkaarten en paspoorten. Dit soort systemen beveiligen is een aparte tak van sport. Zo kwam de Digital Security onderzoeksgroep van de Radboud Universiteit, waar Poll werkt, in het nieuws toen de ov-chipkaart en meer recentelijk autosleutels gekraakt werden. ‘Je moet nu eenmaal eerst heel hard proberen om zoiets te kraken, dan weet je pas hoe je het moet beveiligen.’

Er bestaat nog veel verwarring over de veiligheid van dit soort contactloze smartcards, zegt Poll. ‘Mensen zijn vooral bang dat je ze op een afstand zou kunnen uitlezen.’ Maar die angst in ongegrond, stelt hij. ‘Je kunt die dingen alleen uitlezen als je op dertig centimeter afstand staat met een enorme antenne.’ Je moet pas echt gaan uitkijken als aanvallers fysiek toegang krijgen tot zo’n chip. ‘In een lab gaan ze hem dan strippen en uitzoeken hoe alles werkt.’

Daar zijn verschillende methoden voor. ‘Vijftien jaar geleden kon je aan het energieverbruik van zo’n kaart zien of er een 0 of een 1 geschreven wordt.’ En wat kan een onverlaat met die kennis? ‘Terwijl de software draait, verandert hij op het juiste moment de spanning. Van 5 volt naar 2, 5 volt bijvoorbeeld. De software draait dan door, maar kan even geen enen schrijven. Zo kan een kwaadwillende heel specifiek een 1 in een 0 veranderen. Als je dat op het goede punt doet, denkt een betaalsysteem bijvoorbeeld dat er een pincode is ingevoerd, terwijl dat helemaal niet het geval is.’

Laser schieten

Die simpele methode werkt niet meer zo goed. Door slimmere hardware zijn die energiepieken redelijk nietszeggend geworden. Maar aanvallers zitten ook niet stil. ‘Een modernere manier is door met een laser op een chip te schieten. Die chips bevatten inmiddels meerdere controles, dus je moet wel twee of drie keer hetzelfde doen om de chip een gewenste bewerking te laten uitvoeren.’ Ook tegen die aanvallen is een beveiliging mogelijk. ‘Denk aan een hardware-oplossing: je zet een extra lichtsensor op de chip. Zodra iemand de bovenste laag eraf haalt of met lasers gaat schieten, schakelt de chip zichzelf uit. Op softwareniveau zijn goedkopere mogelijkheden, bijvoorbeeld door een programma de belangrijkste operaties te laten controleren. Daar werken wij met name aan.’

Security is een kat-en-muisspel zonder einde, zegt Poll. ‘De aanvallen worden slimmer. Dan moet de verdediging slimmer worden. En dat noopt de aanvaller weer tot innoveren.’ Binnen Nederland is er inmiddels een berg expertise opgebouwd om de verdediging te versterken. Sentinels is een van de katalysatoren die de afgelopen jaren het vakgebied hebben versneld, zegt Poll. ‘Zo’n programma trekt mensen aan, ook uit het buitenland. Security wordt een steeds groter probleem met steeds ingewikkeldere vragen. Gelukkig is er een stevige gemeenschap in Nederland die ze kan oppakken.’

Foto: Sjoerd van der Hucht Fotografie
Tekst: Sonja Knols, IngenieuSe