Vlnr. Wouter Teepe, Gerhard de Koning Gans en Roel Verdult

De kwajonge

Nijmeegse onderzoekers ontmantelden dit voorjaar de Mifare Classic: de chip die is ingebouwd in onder andere de ov-chipkaart. *Radboud Magazine* keek mee op de afdeling Digital security van hoogleraar Informatiebeveiliging Bart Jacobs. “Je moet je bewust zijn van de macht die je als informaticus hebt.”

gens van Jacobs

Het geheim van de afdeling Digital security

Tekst: Ilse Schuurmans | Fotografie: Bert Beelen

Wouter Teepe: “Wil je een leuk detectivescenario? Ik pleeg een moord en kloon de ov-chipkaart en eventuele toegangspassen van een andere mogelijke verdachte. Dan kan ik hém naar de plaats van delict laten reizen. Als diegene dan ook nog een motief heeft, hangt ’ie.”
Peter van Rossem: “Gelukkig is ons rechtssysteem niet zo simpel.”
Teepe: “Je hóópt het! Je hoopt het.”

De jongens van de afdeling Digital security, de groep van hoogleraar Informatiebeveiliging Bart Jacobs, vertrouwen niet zomaar alles. “Dat zullen we nog wel eens zien!” is het motto als ergens geroepen wordt dat een systeem waterdicht is. De groep haalt regelmatig het nieuws met onderzoek naar het biometrisch paspoort, digitaal stemmen, smartcards, internetbankieren en rekeningrijden, met als absolute hoogtepunt de ontmanteling van de ov-chipkaart eerder dit jaar.

Het is 8 mei 2008. Een doodgewone donderdag in het kantoor van de kerngroep die verantwoordelijk was voor het chiponderzoek. Een zestal centraal opgestelde werktafels met daarop acht computers. Vanochtend draaien er twee. Rond de tafels zitten postdocs Wouter Teepe, het gezicht uit de media, en Peter van Rossum, het wiskundig brein op de achtergrond. Daarnaast scriptiestudent Gerhard de Koning Gans. Samen met student Roel Verdult, die later zal komen, zijn zij verantwoordelijk voor het nodige monnikenwerk – anderhalf jaar stug doorprogrammeren – dat voorafging aan het gezamenlijke eurekamoment.

De jongens van Bart Jacobs zijn er inmiddels wel klaar mee, met die chip, al praten ze er nog steeds met plezier over. Zeker wanneer dat ene moment wordt teruggehaald. Wouter Teepe, een lange wat studentikoze man met verbaasde ogen achter een rechthoekige bril, zet voor: “Die eerste keer dat Roel binnenkwam en riep: ‘Hij is stuk, hij is stuk!’, dat was echt mazzel. Vanaf dat moment zijn we er gericht met z’n allen naar gaan kijken.”
Gerhard de Koning Gans, een rustige jongen met opvallende lichte ogen, kijkt op van zijn computer: “Toen kwamen de ideeën heel snel.”
Peter van Rossum, guitig gezicht, snor, vaalgrijs shirt: “Elke dag was er wel een nieuw idee over hoe de versleuteling in elkaar zou kunnen zitten.”
Wouter: “Vooral op maandag.”

Dat de maandagen zo vruchtbaar zijn, komt omdat er vrijdags het nodige werk mee naar huis wordt genomen. Uit veiligheidsoverwegingen niet in de tas, maar in het hoofd. Zo bleef Peter van Rossum malen over de structuur van de encryptiemethode. "Dat was inderdaad een weekendje. Je kunt de computer álles laten uitproberen, maar dan ben je heel lang bezig. Je kunt ook met wat slimme berekeningen in één keer een aantal opties uitsluiten. Ik had op den duur zo'n slimmigheid te pakken. Dat hebben we die maandag meteen uitgeprobeerd.”
Wouter: “Dat was een mooi staaltje teamwork. Eén persoon zat bij het scherm, één had een kladblok, één stond bij het whiteboard en één drukte op een knopje. De eerste persoon noemde het getal. Hop, streepje in blok, streepje op bord, enzovoort. Toen we na een aantal blokjes code een bepaald mechaniek herkenden, wisten we dat we goed zaten.
Peter: “Er bleken een paar zwakheden in de code te zitten, waardoor we op een redelijk efficiënte manier de sleutels konden achterhalen. Dat hoort nooit te kunnen, ook niet bij een systeem waarvan je weet hoe het werkt. Later bleek het achterhalen van de sleutels nog efficiënter te kunnen.”

Wouter: “Dat hadden we van tevoren allemaal niet bedacht.”
Peter: “We hadden ook kunnen concluderen dat het allemaal heel goed in elkaar zat en dat de chip veilig was.”
Wouter (tegen de interviewster): “Dan had jij hier waarschijnlijk niet gezeten.”

Rekeningrijden

Al aan de telefoon had Bart Jacobs op de gevoeligheid van de materie gewezen. Zijn groep werkt graag mee met een publicatie maar er mag geen enkel technisch detail naar buiten worden gebracht. Hun werk ligt vooral politiek gevoelig. “We kunnen veel mensen voor het hoofd stoten, maar ons vak is simpelweg om te kijken of de chip werkt. Dat punt is nu wel gemaakt.”
Het is één uur, lunchtijd. In de felle zon tegen de achterkant van het Huygensgebouw vindt de groep een plaats. Onder de boterham en ciabatta's gezond informeert Jacobs naar Flavio Garcia, een promovendus die ook aan het project bijdroeg, maar vandaag niet aanwezig is omdat hij morgen promoveert. De Argentijn is nogal zenuwachtig. Jacobs is bezorgd: “Kun je hem niet even pingen?”

Na de lunchpauze gaan er extra computers aan. Er wordt getikt en naar beeldschermen getuurd. Zonder van de schermen op te kijken, discussiëren de groepsleden over het bericht dat de Zwolse politie op de A50 alle nummerborden opslaat om criminelen op te sporen. Al snel volgen alternatieven, waarbij niet iedere onschuldige burger die voorbij komt hoeft te worden gefotografeerd. Als Peter vertelt over de ambitie van de groep om een oplossing te creëren voor het fraudegevoelige internetbankieren, vliegen de technische een-tweetjes over en weer, waarbij verschillende opties worden afgecheckt en vervolgens in één zin weer verworpen.
Wat is hun geheim? Jacobs filosofeert over verklaringen voor de bijzondere kracht van de Digital security-groep. Het doorzettingsvermogen van Roel en Gerhard, de verscheidenheid in technische expertise, de wiskundige kennis van Peter, en de grote interesse in de maatschappelijke gevolgen. “Als informaticus ben je eigenlijk een sociaal architect. Hoe een systeem wordt gebouwd, is niet alleen iets van de digitale wereld. Het is van direct maatschappelijk belang hoe iets werkt. Neem het rekeningrijden. De informatie over wie waar en wanneer rijdt, komt allemaal bij de overheid terecht. Het zou veel privacyvriendelijker kunnen. Door de info in de auto zelf te laten en van daaruit de individuele rekening te genereren en versturen. Wil je dat de overheid op elk moment weet waar jij je bevindt? Iedereen doet daar vrij gemakkelijk over, maar met het overdragen van die informatie spreek je in feite je vertrouwen uit in elke toekomstige regering.”

Het aandeel van studenten in het toch precaire onderzoek is onbedoeld groot. Volgens Roel Verdult “omdat we toevallig op iets groots stuitten”. Jacobs bevestigt dit. "Bij informatica moet er af en toe monnikenwerk worden verricht. Daar vragen we vaak studenten voor.
Roel en Gerhard bleken ontzettend veel geduld en doorzettingsvermogen te hebben. Ze hebben zich diep ingegraven in de details en echt fantastisch en nauwkeurig werk afgeleverd. Uit veiligheidsoverwegingen hebben we de studenten bij medewerkers op de kamer gezet. Die kamers konden namelijk op slot. Dat had een positief effect op de samenwerking. Het onderzoek is daardoor in een stroomversnelling gekomen.”
En dat heeft de groep bepaald geen windeieren gelegd.
Jacobs: “Door de kick van het onderwerp en de onderlinge synergie heeft de groep bijzonder goed gedraaid. Goede wetenschap kun je net als kunst niet plannen of afdwingen. Je kunt er hooguit de voorwaarden voor scheppen. Ik hecht aan een sfeer van creatieve anarchie. Niet onverschillig, maar met onderlinge betrokkenheid, waarbij mensen elkaar op hun resultaten aanspreken.”
Ook Wouter Teepe noemt de samenwerking met Roel en Gerhard gelijkwaardig. “De kracht van deze groep is juist dat er niet met machts- en gezagsverhoudingen is gespeeld. Iedereen neemt elkaar in alle opzichten serieus. Natuurlijk hebben wij wat meer kennis en ervaring. Maar mijn mening is niet meer doorslaggevend omdat ik medewerker ben.”
Een andere verklaring voor het succes van de groep is dat Jacobs naar eigen zeggen “een goede neus voor maatschappelijk relevante ontwikkelingen” heeft. “Er is terecht een zeker wantrouwen gegroeid of het belang van het individu wel veilig is.” Hij lijkt even na te denken. “Ik denk dat we dat hier allemaal wel iets rebels hebben. Een typische vraag die mensen in onze groep stellen is: hoe kan iemand die fout wil, een systeem misbruiken?”
Niet lang daarvoor had Teepe hetzelfde gezegd: “Je zocht toch het geheim van onze groep, hè? Kwajongensmentaliteit. Als je wilt testen hoe goed een kogelvrij vest is, moet je in de huid kunnen kruipen van iemand die daar een kogel doorheen wil jassen.” Jacobs wil dat beeld nuanceren. Hij wil niet het imago aan zijn broek van een bijeengeraapte hackersclub. Natuurlijk lopen er jongens tussen die thuis dingen proberen. Maar daar heeft hij duidelijke afspraken over gemaakt. “Ik vind dat je je bewust moet zijn van de macht die je als informaticus hebt. En van de grenzen die je daarbij stelt. Die moet je zelf trekken. Soms ga je daar net even overheen. Dat maakt het ook wel weer spannend.”■

‘Als informaticus ben je eigenlijk een sociaal architect. Het is van direct maatschappelijk belang hoe iets werkt’


Links: Peter van Rossum