“We moeten softwaremakers veel kritischer volgen”

Kuzien 75, juni 2003, p.15-17.

‘Smartcardprofessor’ Bart Jacobs. Jarenlang vertoefde de selfmade computerhobbyist in de krochten van de fundamentele logica. Tot hij Java ontdekte, en vooral: de chipkaart. Die baande de weg tot zijn KUN-hoogleraarschap (‘Beveiliging en correctheid van programmatuur’) waarvoor hij onlangs zijn inaugurele rede uitsprak. Een pleidooi voor transparante software. “Een nieuw inzicht is leuk, maar het telt pas echt als je de juistheid ervan glashard kunt aantonen.”

Tekst: Paul van Laere
Fotografie: Gerard Verschooten

“Are you really the same guy?” Het wordt professor Bart Jacobs nog regelmatig op verbaasde toon gevraagd. Is hij echt dezelfde Jacobs die vier jaar geleden het standaardwerk *'Category logic and type theory*' publiceerde, zeshonderd pagina's zware kost, in een weinig toegankelijke uithoek van de wiskunde. En dan nu bezig met computerbeveiliging en *smartcards*?
Hij is het echt. Bijna tien jaar beet hij zich vast in een uiterst fundamenteel onderwerp, de type- en categorietheorie. Een mathematische niche die, zoals Jacobs het veelzeggend uitdrukt, “binnen de wiskunde en informatica als redelijk moeilijk en abstract wordt gezien.” Maar geleidelijk verschoof hij de bakens. En plots was daar die wetenschappelijke workshop in Portugal, waar de smartcard zijn pad kruiste. Onmiddellijk besefte Jacobs dat zijn toenmalig onderzoekswerk perfect was toegesneden op de kleine Java-programmaatjes in de jongste generaties chipkaarten.
Sindsdien vertoeft hij in de woelige wereld van de slimme elektronische kaarten, waar de commerciële adem immer voelbaar is. En waar nieuwe technologie bestaande wetgeving op de tocht zet, of omgekeerd. Ooit kon slechts een enkele ingewijde zijn werk volgen maar het laat zich nu aan iedere leek uitleggen. En bij elke computer- of pasjesfraude staan de media voor zijn deur. Is al dat intelligente plastic wel afdoende beveiligd?
Dat kan tegenvallen. Jacobs pakt er zijn laptop bij, voorzien van een kaartlezer. “Die zijn gewoon te koop, je moet er alleen wat software voor schrijven.” De chippas van de interviewer verdwijnt in de laptop en even later verschijnen saldo, rekeningnummer en de laatste vijf betalingen, inclusief plaats van transactie, op het scherm. “Toch niet zo heel goed afgeschermd”, luidt het droge commentaar van Jacobs.

Professionele hackers
De hoogleraar kan nog meer trucs met de chippas uithalen - niet het saldo wijzigen overigens - maar ziet die liever niet publiek gemaakt. Het verzoek symboliseert hét grote verschil met zijn vroegere research, waarvan hij de resultaten zonder restricties kon openbaren. De samenwerking met smartcardbedrijven blijkt een aparte ervaring. “Ze vragen ons de programma’s op hun chipkaart tegen het licht te houden, maar je krijgt tevens een ‘Non Disclosure Agreement’ (NDA) voorgelegd, die inhoudt dat je over de resultaten niks mag zeggen of publiceren. Het is al voorgekomen dat we in zo’n programma fouten ontdekten. Behoorlijk pijnlijk, die kaart was al verkocht. Maar dat mag ik niet naar buiten brengen, daar kunnen ze me op aanspreken. Ik doe dat liever niet, zo’n NDA ondertekenen. Maar soms ontkom je er niet aan, omdat het de enige manier is om achter waardevolle informatie te komen.”
Fabrikanten houden hun beveiligingsmethoden zoveel mogelijk voor zich, zegt Jacobs. ”Je krijgt slechts stukjes van de puzzel, net genoeg om aan de slag te kunnen. Ook daarover moet je onderhandelen. En natuurlijk proberen we op eigen houtje achter de geheimen van zo’n kaart te komen. Professionele hackers, zo mag je ons wel noemen.”

Een onderzoeker voor wie de fijne kneepjes verborgen blijven en die zijn mond moet houden wanneer hij desondanks iets interessants ontdekt. Zo schetst Jacobs zijn tragisch lot in zijn rede 'De computer de wet gesteld'. Geen reden echter om het hoofd in de schoot te leggen. Integendeel. "Het is heel belangrijk dat relatief onafhankelijke clubs als de onze, de industrie op de vingers kijkt. Er worden nu bijvoorbeeld proeven gedaan met elektronisch verkiezingen. Stemmen vanaf je eigen computer. Dat systeem wordt door een bedrijf gebouwd. Die kunnen wel beweren dat het systeem veilig is, maar is dat echt zo? Daarvoor is het goed dat er iemand kritisch meekijkt en druk op de ketel houdt. Dat helpt rampzalige fouten te voorkomen."

Leuk knutselwerk

Met zijn duw- en trekwerk aan smartcards lijkt de 39-jarige Jacobs terug bij zijn eerste experimenteerfase op zijn Apple II als middelbare scholier. Jacobs herinnert zich dat de radio wekelijks een computerprogramma uitzond. Letterlijk. "Fantastisch was dat. Een uur lang piepjes en bliebjes, die ik dan op een cassettebandje opnam."

Die hobby-achtige sfeer rond computers trok hem richting een klassieke exacte studie - aanvankelijk natuurkunde, na een half jaartje ingeruild voor de wiskunde. "Dat kostte minder tijd en combineerde beter met mijn studie filosofie die ik parallel deed. Je kon toen net informatica studeren, maar dat vak beschouwde ik destijds als leuk knutselwerk, niet als echte wetenschap."

Jacobs dook in de logica, op het snijvlak van wiskunde en filosofie. "Redeneerregels die universeel geldig zijn, los van de empirie, dat heeft een zekere charme." De grootste charme ligt in het waterdichte bewijs. "Een nieuw inzicht is leuk, maar het telt pas echt als je de juistheid ervan glashard kunt aantonen. Het is een kick als je dat rond krijgt."

Na zijn promotie vertoefde Jacobs een jaar in Cambridge. "Qua wetenschap fantastisch, maar er was veel snoeverij. Iedereen voerde zogenaamd geen klap uit, alsof het ze allemaal kwam aanwaaien. En ondertussen keihard werken. Erg individualistisch ook. Nou speelt wiskundig onderzoek zich grotendeels af *'in the privacy of your own mind*.' Aan het bureau met pen en papier, sommetjes maken. Daar heb ik geen moeite mee. Maar elkaar de loef afsteken ligt me niet, ik werk liever samen. Ook in mijn huidige groep probeer ik een sfeer van saamhorigheid te creëren."

Na Cambridge was Jacobs twee jaar verbonden aan de Universiteit van Utrecht, waar hij een groot deel van zijn eerder genoemde boek schreef. Tijd voor iets anders, dacht Jacobs, en hij vertrok naar het Amsterdamse Centrum voor Wiskunde en Informatica (CWI) om zich te verdiepen in de semantiek van programmeertalen, in het bijzonder Java. "Toen was dat nog een tamelijk onbekende taal. Pas later is Java populair geworden vanwege de internettoepassingen."

Met een eervolle KNAW-positie keerde Jacobs in 1996 terug naar Nijmegen, waar hij verder opschoof in de richting van het toegepaste werk. "Ik ging zogenaamde stellingbewijzers gebruiken. Dat zijn een soort logische zakjapanners, waarmee je een klein computerprogramma helemaal kunt doorlopen. Wij behoorden tot de eersten die stellingbewijzers loslieten op Java-programmaatjes. Onze houding was: *let's push the technology*. Kijken hoever we komen."

Een heel eind, zo zou blijken. Met dank aan de workshop in Lissabon waar Jacobs mensen uit de chipkaart-industrie ontmoette. "Die bleken naarstig op zoek naar technieken om de Java-programma's op hun kaarten te verifiëren op correctheid. Precies waar wij mee bezig waren."

Jacobs rook zijn kans. "Dit is een '*killer application'*,' zei ik tegen mijn groep. "Wanneer je gedegen wetenschappelijk werk kunt verbinden aan een duidelijke toepassing, ben je binnen. Dan kun je het spel tegenover subsidiegevers en universiteit spelen zoals het moet." En dat deed Jacobs. Hij werd coördinator van een Europees smartcard-project en zag tevens een NWO-aanvraag gehonoreerd. De onderzoeksgroep groeide van drie naar zeven man.

Digitale assertiviteit

Door de contacten met smartcardproducenten verschoof de aandacht van correctheid naar beveiliging. Werkt het programma ook goed als het aangevallen wordt? Jacobs: “Voor dat soort security-onderzoek heb ik een PIONIER-voorstel geschreven, wat ook is aangenomen. Toen was het helemaal bingo. We werken nu met twaalf mensen, bijna allemaal extern gefinancierd.”
De Nijmeegse successen bleven niet onopgemerkt. Zo kreeg Jacobs van het CWI het aanbod om daar een nieuwe groep op te zetten. De Nijmeegse tegenzet - een hoogleraarschap - wist Jacobs echter binnenboord te houden. “In Nijmegen blijven had mijn voorkeur. Op het CWI is meer tijd voor onderzoek, maar er zijn geen studenten die voor verfrissing zorgen. En onze groep is hier geworteld, het is een heel gedoe om met zijn allen te verhuizen.”
Voor een hoogleraar gaat de deur wat sneller open, ervaart Jacobs. “Je wordt serieuzer genomen, binnen en buiten de universiteit. Het maakt meer indruk in de media. Al moet ik juist daarom extra op mijn woorden passen. Met een kop als: ‘Hoogleraar vindt telebankieren slecht beveiligd’, zou ik een hoop gedonder krijgen.”
Toch gebruikt Jacobs het podium van zijn inaugurele rede om een aantal hartenkreten te ventileren. Over het voorstel tot een nieuwe Auteurswet bijvoorbeeld, die publicaties over zwakke plekken in digitale beveiligingssystemen verbiedt. “Stel dat wij in de kopieerbeveiliging van een nieuw soort DVD’s een fout ontdekken. Volgens de nieuwe wet zijn we strafbaar als we dat openbaar maken. Dat vind ik maf. Bovendien werkt het op termijn averechts. In Amerika bestaat al langer zo’n wet. Met als gevolg dat het onderzoekers op gebied van computer security zich eerder afwenden. Dan heb je jezelf aardig in de nesten gewerkt. Zo ver moeten we het niet laten komen.’
Jacobs spoort ook de consument aan tot digitale assertiviteit. “Computertechnologie dringt steeds dieper ons leven binnen. Aan de kwaliteit en betrouwbaarheid mogen we hoge eisen stellen. Er moet een soort keurmerk voor software komen. En garanties, net als bij andere producten. Hoe vaak gebeurt het niet dat een programma vastloopt en je weer naar dat bekende blauw scherm zit te staren? Eigenlijk ongelooflijk dat iedereen dat accepteert en softwareproducenten nog nooit aansprakelijk zijn gesteld voor geleden schade. De softwaremakers moeten veel kritischer gevolgd worden. Daar wordt uiteindelijk iedereen beter van.”

Kader

Alles op één kaart?

Geen mens zonder een portemonnee vol plastic kaartjes. Om geld te tappen, het parkeren te betalen, bonuspunten of airmiles te incasseren, of gewoon ergens binnen te komen. Het slimst zijn de chipkaarten, of smartcards, herkenbaar aan het goudgele vlakje, waaronder zich een minuscuul computertje bevindt. Zo gauw het kaartje in een lezer wordt geschoven – een automaat in de muur bijvoorbeeld - gaat via het gele contactvlak een elektrisch stroompje lopen en begint het kaartbrein te werken.
Bij de eerste generatie kaarten, waartoe de huidige giro- en bankpassen behoren, behelst dat brein niet meer dan wat geheugen en enkele commando’s, ingebrand in machinetaal. Het computertje van de nieuwste kaarten bevat echter kleine programmaatjes, veelal in Java geschreven. Jacobs: “Ook de SIM-kaarten in mobiele telefoons draaien vaak op Java-programma’s. Zo’n kaart kan ingewikkelder functies aan, en is anderzijds makkelijker en flexibeler te programmeren.”
In theorie zou één kaart volstaan voor een reeks van toepassingen. Paspoort, treintickets, bioscoopbon, credit card, alles op dezelfde kaart. “Voor de consument natuurlijk aantrekkelijk, maar of al die betrokken partijen zich laten verenigen op een stukje plastic, is nog de vraag. Zelfs binnen één sector blijkt dat al moeilijk, zie de mislukte onderhandelingen over de zorgpas. Maar er komen ongetwijfeld experimenten met gecombineerde functies, bijvoorbeeld een bankpas die

tevens als openbaar vervoerskaart dienst doet. De Java-chipkaart wordt slimmer en veelzijdiger, dat is zeker.”