De computer de wet gesteld

Rede uitgesproken bij de aanvaarding van het ambt van hoogleraar aan de Faculteit der Natuurwetenschappen, Wiskunde en Informatica met als leeropdracht Beveiliging en correctheid van programmatuur op vrijdag 16 mei 2003

Door Bart Jacobs

Fotografie: Dick van Aalst

Vormgeving en opmaak: Nies en Partners bno, Nijmegen

Drukwerk: Janssen Print Nijmegen

ISBN 90 901 6917 2

© Bart Jacobs, Nijmegen, 2003

Niets uit deze uitgave mag worden vermenigvuldigd en/of openbaar worden middels druk, fotokopie, microfilm, geluidsband of op andere wijze dan ook, zonder voorafgaande schriftelijke toestemming van de copyrighthouder.

Mijnheer de Rector Magnificus,
Zeer gewaardeerde toehoorders,

Afgelopen januari en maart hebben velen van ons weer een omslachtige tocht gemaakt naar een of ander plaatselijk stembureau om via een simpele handeling onze stem voor de Tweede Kamer of Provinciale Staten uit te brengen. Wat een gedoe voor de moderne mens! Zou het niet veel gemakkelijker zijn als het uitbrengen van zo'n stem zou kunnen plaats vinden via de mobiele telefoon of via internet, waar ook in Nederland (of daarbuiten)? Dit is handig en bespaart moeite. En wie weet is het opkomstpercentage dan wel hoger. De technische realisatie lijkt geen groot probleem. Het klinkt allemaal aantrekkelijk . . . Of misschien toch niet? Stel u verzendt uw legitieme stem via uw mobieltje, maar krijgt prompt het antwoord dat uw stem niet geaccepteerd wordt omdat u volgens de centrale stemcomputer reeds gestemd heeft! Deze stemcomputer werkt mogelijk niet correct, of misschien heeft iemand zich als u weten voor te doen en uw stem gestolen. Mogelijk heeft deze snoodaard niet alleen uw stem gestolen, maar ook die van vele andere stemgerechtigden en daarmee het resultaat van de verkiezingen weten te bepalen. Chaos, Florida in de polder!

Deze beschrijving van elektronisch stemmen bevat de grote uitdaging waar de moderne informatica mee worstelt. Om te beginnen moeten onze computersystemen steeds opener en flexibeler worden, en willen gebruikers overal en altijd toegang hebben tot de informatie en de besturingstaken van deze systemen. Tegelijkertijd moeten deze computersystemen correct functioneren en goed beveiligd zijn: de integriteit, confidentialiteit en beschikbaarheid van de informatie moet gegarandeerd zijn, en de besturingstaken moeten niet door onbevoegde partijen beïnvloed kunnen worden. Dat is nogal wat.

Ik sta hier voor u met als leeropdracht 'beveiliging en correctheid van programmatuur'. De genoemde combinatie van openheid en veiligheid is van centraal belang in mijn werk. Ik zal het daar uitvoerig over hebben. Zoals bekend, is in het algemeen, buiten de informatica, de laatste jaren het belang van veiligheid en beveiliging sterk toegenomen. In de daarmee samenhangende discussies speelt de informatica een niet onbelangrijke rol. De steeds groeiende ICT infrastructuur gaat ons leven in steeds sterkere mate beïnvloeden, en dient daarbij zorgvuldig ingebed te worden in be-

staande of nieuwe maatschappelijke kaders. Correctheid en beveiliging zijn daarbij voor iedereen van belang. Opzettelijke of abusievelijke fouten in computerprogramma's vormen een groot probleem omdat ze moeilijk detecteerbaar zijn. Ik noem een aantal willekeurige onderwerpen. Elektronische betaling, via chipkaarten, via internet of via de mobiele telefoon; digitale kopieerbeveiliging voor muziek en films; privacy en anonimiteit in communicatie en gegevensopslag; elektronische ondertekening van documenten, met bijbehorende juridische status. Deze ontwikkelingen zijn al verder dan u misschien denkt. Ik noem enkele voorbeelden.

- Er ligt een ontwerpwet ter goedkeuring bij de Eerste Kamer[1] waarin de juridische status van elektronische handtekeningen gelijkgesteld wordt aan die van gewone, welbekende fysieke handtekeningen. Zulke elektronische handtekeningen moeten volgens de wet geplaatst zijn met een "veilig middel". Wat betekent dat?

- De Nederlandse kieswet wordt uitgebreid met een tijdelijke, zogenaamde Experimentenwet, getiteld Kiezen op Afstand[2], teneinde bij de Europese Verkiezingen van 2004 een proef uit te kunnen voeren om het uitbrengen van een stem minder plaatsafhankelijk te maken[3]. Hoe kunnen burgers erop vertrouwen dat hun elektronisch uitgebrachte stem aantoonbaar bijdraagt aan het eindresultaat, maar toch geheim blijft?

- Door de internationale muziek en filmindustrie wordt druk geëxperimenteerd met allerlei beperkingen op het kopiëren van hun producten. Waar zal dat toe leiden? Zullen we straks een netjes gekochte muziekCD nog maar maximaal honderd keer kunnen afspelen? Natuurlijk is het voor informatici een interessante uitdaging om zo'n systeem zodanig te realiseren dat omzeilen van het beveiligingsmechanisme praktisch onmogelijk is. Er ligt een voorstel voor een nieuwe Nederlandse Auteurswet[4] waarin het ondermijnen van zo'n digitaal beveiligingsmechanisme strafbaar gesteld wordt. Deze strafbaarheidstelling is akelig ruim geformuleerd. Maakt dit het werk voor ons informatici gemakkelijker, of juist niet?

Opvallend veel onderwerpen op het gebied van computerbeveiliging kunnen niet goed begrepen worden zonder een juridisch kader. Zo'n kader definieert bijvoorbeeld wat "voldoende veilig" is, en vormt een vangnet voor het geval dat technische of organisatorische beveiligingsmechanismen falen. Ik wil het hier over drie zulke onderwerpen op het snijvlak van informatica en recht hebben, namelijk aansprakelijkheid bij computerprogramma's, certificatie en openheid. Daarmee stel ik mijn technische dagelijkse werk in wijder perspectief.

De computer in de rechtszaal

De laatste tijd zijn er opvallend veel rechtszaken waarin de computer een prominente rol speelt. Vaak krijgen deze juridische geschillen ook de nodige aandacht van de media. Zo berichtte[5] de NRC op haar voorpagina over de (voorlopige) uitspraak in de Verenigde Staten die het bedrijf Microsoft dwingt de programmeertaal Java van concurrent SUN weer standaard in de Windows besturingssystemen op te nemen. Inmiddels is deze beslissing trouwens door een recentere uitspraak weer ongedaan gemaakt. Ook berichtte het NOS journaal niet zo lang geleden over de uitspraak[6] van een Noorse rechter om Jon Jech Johansen, de maker van een programma (DeCSS geheten) om DVDs onder Linux te kunnen afspelen, niet te vervolgen. Het gevoelige punt is dat Johansen hiervoor de kopieerbeveiliging van DVDs had doorbroken. De rechter in Oslo oordeelde dat het hierbij ging om kopiëren voor persoonlijk gebruik. Een gevoelige nederlaag voor de zogenaamde content providers (de film en muziekindustrie). In Amsterdam hebben we op 28 maart 2002 een rechtszaak in hoger beroep[7] gehad tegen de internetdienst Kazaa voor het uitwisselen van films en muziek door internetgebruikers. De rechter oordeelde dat Kazaa niet verantwoordelijk is voor mogelijke inbreuk op het auteursrecht bij zo'n uitwisseling. Deze zaak gaat door naar de Hoge Raad. Andere zaken tenslotte, die ik ter illustratie nog wil noemen, betreffen het niet strafbaar zijn van het verwijderen van zogenaamde SIMlocks op mobiele telefoons[8], en de verplichting door een Nederlandse rechter opgelegd[9] aan het Britse gokbedrijf Ladbrokes om Nederlandse internetgebruikers de toegang te weigeren.

Het gaat hierbij om een nieuwe trend, waarbij de rechter het kader aangeeft waarbinnen de inrichting en het gebruik van computers plaatsvindt. In het algemeen is zo'n kaderstelling door de rechterlijke macht zeer gebruikelijk. Maar het is, meen ik,

een fenomeen van meer recente datum dat wij informatici met zulke jurisprudentie geconfronteerd worden. We zien dat aan onze geliefde computer de wet gesteld wordt. Dit is even wennen binnen de informatica, waar een vrijejongens mentaliteit heel gewoon is. Men is gewend aan vrije toegang tot informatie en aan een grote mate van controle: de informaticus bedient de zelfgemaakte knoppen, en de buitenwereld begrijpt toch niet precies hoe het allemaal werkt. En mocht een en ander uiteindelijk niet geheel volgens eigen plan blijken te verlopen, dan bestaat altijd nog de almachtige *reboot* ingreep, in de vorm van de welbekende toetsencombinatie *control-alt-delete*.

Het is over deze nieuwe ontwikkeling, de aan de computer gestelde wet, dat ik het uitgebreider wil hebben. Ik wil daarbij betogen dat deze kaderstelling een natuurlijke ontwikkeling is, zeker op mijn eigen gebied van beveiliging en correctheid van software, waardoor zich niet alleen nieuwe mogelijkheden maar ook nieuwe gevaren aandienen voor de informatica. Ik heb de indruk dat deze, vaak ingrijpende, juridische aspecten binnen de informatica op dit moment misschien niet voldoende aandacht krijgen. Dat wat ik erover zeg, doe ik niet als jurist (dat ben ik namelijk helemaal niet), maar als informaticus.

Het is goed even op te merken dat er in de andere richting, vanuit de juridische wereld, wel degelijk veel aandacht is voor informatica. Bijna iedere juridische faculteit in Nederland heeft een afdeling die zich ermee bezighoudt. Daarbij wordt gebruikelijk een onderscheid gemaakt tussen "rechtsinformatica" en "informaticarecht". Onder rechtsinformatica verstaat men het vakgebied dat zich richt op de ondersteuning van juridische taken door computers, via gespecialiseerde databases met passende kennis en redeneersystemen. Het gaat daarbij om het ultieme codificeren. Mij is het meer te doen om informaticarecht dwz. om de juridische regels en vraagstukken, die betrekking hebben op het gebruik van computers en computerprogrammatuur, en in het bijzonder om de invloed daarvan op de informatica zelf.

Het is ook goed om ons te realiseren dat computers en computergebruik problematisch zijn binnen de traditionele juridische kaders. Daarbinnen is men gewoon te denken in termen van "zaken", die ofwel roerend- of onroerend kunnen zijn. Een zaak is volgens het Burgerlijk Wetboek[10] een voor menselijke beheersing vatbaar stoffelijk object. De nullen en enen van informatici laten zich moeilijk als "zaak" kwalificeren. Immers, ze zijn zonder moeite willekeurig vaak kopieerbaar en zijn bliksemsnel en grenzeloos transporteerbaar. Juridisch gezien is het niet triviaal dat je bijvoorbeeld iemands PINcode kunt stelen, of iemands harde schijf kunt kopiëren, terwijl die persoon zelf niks kwijtgeraakt is. Wij kunnen ons hier vrolijk over maken, maar de Hoge Raad heeft eraan te pas moeten komen om in deze materie klaarheid te scheppen[11]. De grote charme en uitdaging van het vak informaticarecht is dan ook om de ongrijpbare ingrediënten waarmee een informaticus dagelijks werkt in een precies kader te vatten[12]. Daarbij gaat het niet alleen om de status van informatie (nullen en enen), maar ook om abstractere begrippen als authenticiteit en onloochenbaarheid die binnen computerbeveiliging een grote rol spelen. Daarover eerst meer.

Correctheid, veiligheid en beveiliging

Volgens goed academisch gebruik behoor ik in mijn verhaal aandacht te besteden aan terminologie. Het gaat me vooral om de betekenis en samenhang van de begrippen correctheid, veiligheid en beveiliging. Deze begrippen kunnen in engere zin voor computerprogramma's gebruikt worden, maar ook in bredere zin voor computersystemen en de omgeving waarin ze functioneren. Ik zal de neutrale term 'systeem' gebruiken.

Een systeem heet correct als het doet wat het moet doen. Iets technischer: wanneer het voldoet aan z'n specificatie. Dat wil zeggen dat als de omgeving en de gebruiker zich netjes aan de regels houden, dan doet een correct systeem dat ook. Dit lijkt een voor de hand liggende eigenschap. Echter, het is er een die vaak razend moeilijk te realiseren is voor computersystemen. Programma's zijn vaak zo groot dat ze menselijkerwijs niet meer te overzien zijn. En het aantal mogelijkheden dat voor kan komen is vaak niet te bevatten. Tussen al die vele mogelijkheden kan gemakkelijk een onbedoelde voorkomen, ofwel door onoplettendheid ofwel door kwaadwillendheid van de programmeur. Correctheid van programmatuur is dan ook een onderwerp dat van begin af aan veel aandacht heeft gekregen binnen het informaticaonderzoek. Het is het gebied waarvan onze vorig jaar overleden landgenoot, en mijn voormalige dorpsgenoot, Edsger Dijkstra een van de grondleggers is. Het is zo langzamerhand wel duidelijk geworden dat op dit gebied alleen iets bereikt kan worden met speciale computerprogramma's, zoals modelcheckers of stellingbewijzers, die helpen bij het systematisch controleren van alle mogelijke gevallen die in het te analyseren programma op kunnen treden. Deze formele, wiskundige methoden

werken tot nu toe eigenlijk alleen bij heel kleine programma's, van hooguit een handvol pagina's lang. Bij grotere programma's is men voor de correctheid aangewezen op minder alomvattende technieken zoals testen, codeinspecties, en systematisch ontwerp.

De begrippen 'veiligheid' en 'beveiliging' worden in het Nederlands niet altijd goed onderscheiden. In het Engels is er een duidelijker verschil: veiligheid is *safety* en beveiliging is *security*. Laat ik met het laatste beginnen. Beveiliging gaat over het reguleren van toegang; toegang tot een gebouw, een netwerk, een computer, of gegevens meer in het algemeen. In het Engels klinkt het vaak lekkerder: *security is about regulating access to assets*. Computervirussen, zoals bijvoorbeeld in email-attachments, vormen een beveiligingsprobleem omdat ze aan gegevens komen waar ze helemaal niet aan zouden mogen komen. Binnen de informatica komen beveiligingsissues voor zoals: wie mag dit programma starten? En: wie mag de resultaten ervan zien? Of: wie mag deze gegevens lezen, of veranderen? Maar ook: wie mag weten wie dit programma gestart heeft, en wie mag weten wie de gegevens veranderd heeft? Dus, een systeem heet secure of beveiligd als alleen geautoriseerde partijen toegang hebben. Iets technischer, wanneer het systeemvoldoet aan z'n *security policy*. Excuus, maar hiervoor weet ik geen goed, ongekunsteld Nederlands equivalent. Zo'n *security policy* omvat een analyse van de beveiligingsrisico's, beveiligingsdoelen, en de beveiligingsstrategie in een specifieke situatie. Het moge duidelijk zijn dat wanneer we spreken over beveiliging als regulering van toegang een juridisch kader snel in zicht komt. Datgene waartoe de toegang gereguleerd wordt is typisch de eerder genoemde juridische "zaak".

Nu we weten wat correctheid en wat beveiliging is, blijft de vraag wat veiligheid betekent. Ik maak hier voor het gemak geen onderscheid tussen correctheid en veiligheid[13]. Dus, een chemische fabriek functioneert correct of is veilig wanneer die doet wat hij moet doen en niet spontaan, om interne redenen ontploft. En die fabriek is beveiligd wanneer de toegang goed gereguleerd is en de fabriek niet om externe redenen ontploft.

Dit voorbeeld brengt ons tot de samenhang tussen correctheid (of veiligheid) enerzijds, en beveiling anderzijds. Het zal duidelijk zijn dat een goede beveiling moeilijk te realiseren is als het systeem zelf niet correct functioneert. Daarom zie ik beveiliging als een uitbreiding van correctheid. Een mooie manier om het uit te drukken is dat een systeem beveiligd is als het goed blijft functioneren ook als de omgeving en de gebruikers zich niet aan de regels houden, en moedwillig proberen de zaak onderuit te halen. Met andere woorden *security is safety under attack*. Terug in de context van software heet een computerprogramma correct of veilig wanneer het onder normale omstandigheden doet wat het moet doen, en heet het programma *secure* of beveiligd indien het goed blijft functioneren ook wanneer kwaadwilligen proberen het te verstorenen onderuit te halen. Dit is vanzelfsprekend een veel sterkere eis. Maar het is wel een zeer relevante eis in de hedendaagse context waarin allerlei computersystemen via openbare netwerken met elkaar verbonden zijn.

Kwaliteit van software

De subfaculteit informatica waarbinnen ik aangesteld ben heeft als onderzoeksthema "kwaliteit van software". Binnen dat thema zijn correctheid en beveiliging van programma's belangrijke issues. Maar, zo vraagt u zich misschien af, waarom is die kwaliteit van software eigenlijk een thema?

Laten we eerlijk zijn, informatici hebben er de afgelopen decennia vaak een potje van gemaakt. De kwaliteit van software is nogal eens beneden alle peil. Het vastlopen van computers en van programma's komt zo vaak voor dat mensen het als onvermijdelijk kwaad lijken te zijn gaan beschouwen. Computervirussen veroorzaken ieder jaar weer een ongekend verlies van productiviteit. Als ik een strijkijzer koop dat niet goed blijkt te werken, ga ik verontwaardigd terug naar de winkel en krijg ik zonder probleem een nieuwe. Heeft u dat wel eens geprobeerd bij een computerprogramma? De winkelier zal u zien aankomen! Indien er al garantie gegeven wordt, beperkt die zich bijna altijd tot de drager, dat wil zeggen, tot bijvoorbeeld de CDROM waarop het programma aangeleverd wordt. Over het programma zelf wordt niets gegarandeerd.

De eenvoudige vraag die ik mij hier in al mijn naïviteit stel is: waarom komen de softwareproducenten hiermee weg, en waarom accepteren wij dit? Waarom wordt niemand voor wanprestaties op softwaregebied voor een rechter gedaagd en verantwoordelijk gesteld? Onze wetgeving kent het begrip conformiteit bij aankoop: de afgeleverde zaak moet aan de overeenkomst beantwoorden[14]. Dat wil zeggen dat de verkoper verplicht is er voor te zorgen dat de verkochte zaak alle eigenschappen heeft die nodig zijn voor een normaal gebruik. Het zou aardig zijn als bij een com-

puterprogramma dat wel erg vaak vastloopt, of tot de welbekende lichtblauwe schermen leidt, deze verplichting afgedwongen wordt. Formeel heeft de consument ook het recht herstel te eisen, of het herstel opkosten van de winkelier elders te laten uitvoeren[15]. Eventuele *enduser agreements* die iedereen bij het installeren gewoon is weg te klikken hebben hierop geen invloed.

Deze aansprakelijkheidsvraag houdt mij al enige tijd bezig. Ik leg deze vraag vooral graag bij voordrachten in Amerika aan de zaal voor. Ik vertel daarbij dan een beetje pesterig dat wij in Europa het beeld hebben van Amerikanen als assertieve aanklagers, die elkaar met de kleinste onbenulligheden de grootste schadevergoedingen afhandig proberen te maken. Specifiek vraag ik daarbij graag waarom niemand de grote, bekende softwaregigant uit het noordwesten van de Verenigde Staten aanklaagt. Deze kwestie is interessant want Amerika kent het fenomeen Ralph Nader[16]. Deze jurist (en voormalig presidentskandidaat) heeft zich intensief beziggehouden met consumentenzaken, en heeft bijvoorbeeld in rechtszaken om verkeersongelukken veel succes en invloed gehad. Zozeer zelfs dat de Amerikaanse automobielindustrie er bij ieder ongeluk als de kippen bij is om te betogen dat er geen verband is tussen de betreffende gebeurtenis en het ontwerp. De toegekende schadevergoedingen hebben onmiskenbare invloed op de veiligheid van auto's.

Ik kom terug tot mijn vraag: waarom worden er geen aansprakelijkheidsprocessen gevoerd tegen de software-industrie? Ik heb daar geen bevredigend antwoord op, maar kan wel een aantal relevante motieven noemen. Vaak is er sprake van vele, kleine individuele ergernissen en niet zozeer van verwijtbaar lichamelijk letsel. Dit maakt het moeilijk een zaak te beginnen. Ook is het niet gemakkelijk de precieze oorzaak van falen in een aanklacht vast te leggen, waardoor er veel ruimte is voor zogenaamd *fingerpointing*: andere partijen de schuld geven. Maar voor grote bedrijven of voor overheden zijn de totale kosten als gevolg van gebrekkig functionerende en gebrekkig beveiligde software wel degelijk omvangrijk. Natuurlijk is het zo dat de softwareindustrie over zware financiële en juridische middelen kan beschikken. Maar is het dan vooral angst om de confrontatie aan te gaan?

Of moeten we wachten op een echt groot ongeluk, bijvoorbeeld in de luchtvaart, waar letseladvocaten zeer actief zijn. Op 1 juli 2002 heeft er een tragische botsing plaatsgevonden boven Zuid-Duitsland tussen een Boeing 757 vrachtvliegtuig van DHL en een Russisch Tupolev 154 verkeersvliegtuig[17]. In de daarop volgende berichtgeving kwam het beeld naar voren dat de zogenaamde TCAS-software om zulke botsingen tevermijden goed gefunctioneerd heeft, maar door een foute menselijke inschatting *overruled* werd. Stel nu eens dat het andersom was geweest,en dat het ongeluk aantoonbaar veroorzaakt zou zijn geweest door een programmeerfout. Ik denk dat de uit zo'n situatie voortvloeiende juridische aansprakelijkheidskwesties een grote invloed zouden kunnen hebben op de manier waarop software ontwikkeld wordt. En ik verwachtdat dit, net als in de automobielindustrie, een positieve invloed zal zijn,gericht op kwaliteitsverbetering.

Ik meen dat het in het algemeen belang is wanneer ook op dit gebied de computer vaker de wet gesteld wordt: wanneer softwareproducenten nadrukkelijker worden aangesproken op eventuele gebreken in hun producten en, bij aantoonbaar in gebreke blijven, gedwongen worden tot schadeloosstellingen. Gezien de voorkomende winstmarges van boven de 80%[18] lijkt er geen direct gevaar voor een resulterende ondergang van de sector. Een meer klantgerichte houding zou de sector geen kwaad doen. In plaats van klanten van zich te vervreemden door zich zo druk te maken over illegale kopieën, bijvoorbeeld via de speurders van de BSA[19], zou men er misschien beter aan doen om meer te investeren in kwaliteit en bijbehorende garantie. Als duidelijk is dat een legaal gekocht computerprogramma ook recht op garantie geeft, is er ook meer motivatie om netjes te betalen. Dit is denk ik een wezenlijk punt, waar misschien te weinig aandacht aan wordt besteed.

Helaas is er kennelijk onvoldoende druk vanuit de markt aanwezig. Vanuit commercieel perspectief is marktaandeel belangrijk, vooral op softwaregebied, waar vaak een of enkele producten dominant zijn, die alles moeten kunnen. Het gaat daarbij om de zogenaamde *mindshare* van het gebruikerspubliek, die zo groot mogelijk moet zijn. De werkwijze is dan: *we ship next monday, and we'll get it right in version 3*. Dit leidt tot een houding van *penetrate and patch*[20], waarbij de markt zo snel mogelijk veroverd moet worden en de verantwoordelijkheid voor de veiligheid van software systemen op de gebruikers afgeschoven wordt. Zij moeten immers maar bijhouden wanneer en waarvoor er weer een reparatieprogramma, een zogenaamde *patch*, beschikbaar is en geïnstalleerd moet worden. Is het niet doodgewoon vanzelfsprekender dat het de verantwoordelijkheid van de producent is om direct een goed product af te leveren? Als je het allemaal zo op een rijtje zet vraag je je werkelijk af hoe het mogelijk is dat softwareproducenten zich deze houding kun-

nen permitteren. En natuurlijk ook: waarom wij dit allemaal maar accepteren.

Deze zojuist geschetste heersende praktijk is onacceptabel voor software die *secure* moet zijn. Daarvoor zal men de functionaliteit vaak moeten beperken en rustig de tijd moeten nemen om de zaak aantoonbaar goed in elkaar te zetten. Bij gebrek aan aansprakelijkheidsstelling en commerciële motivatie gebeurt dit kennelijk niet vanzelf. Welke drijfveer is dan nodig?[21]

Certificatie

Het is niet mijn bedoeling hier een al te negatief beeld te schetsen van het softwareproductieproces. Er zijn sectoren, zoals bijvoorbeeld de luchtvaart, waar strenge regels gelden en nauwgezette procedures gevolgd dienen te worden. Inderdaad had men bij het eerder genoemde vliegtuigongeluk de beslissingen beter aan de software over kunnen laten. Zulke strenge procedures bij softwareproductie kunnen leiden tot zogenaamde certificatie van computerprogramma's. Kort gezegd komt het er daarbij op neer dat programma's een soort kwaliteitsstempel krijgen. Een ouderwets KEMA of NVVH keurmerk. In steeds meer sectoren wordt dit gezien als de toekomst. Dit is een ontwikkeling die vooral gestuurd wordt door de grote kopers van software, zoals bijvoorbeeld banken of defensie, voor toepassingen waarmee men zich geen problemen kan veroorloven. Voor mij en mijn directe vakgenoten liggen juist hier grote mogelijkheden voor het gebruik van formele methoden. Sterker nog, dit is naar mijn mening de manier om impact te hebben met wiskundige methoden en speciale computertools (zoals stellingbewijzers en modelcheckers) binnen de informatica. Hier wil ik nader op ingaan.

De afgelopen jaren heb ik veel gewerkt met chipkaarten, of *smartcards* zoals ze in het Engels heten. U kent ze wel, in de vorm van bankpasjes met goudkleurige contactpuntjes, waarachter een klein computertje verborgen zit. Ook de zogenaamde SIM-kaarten in uw mobiele telefoon zijn chipkaarten, maar dan zonder omringend plastic[22]. Dit soort chipkaarten wordt vaak gebruikt voor allerlei securitygevoelige toepassingen[23]. Een voorbeeld is authentificatie. Een chipkaart kan zich identificeren door een bepaald geheim dat het bezit. Zo'n geheim bestaat uit een groot getal, dat voor iedere chipkaart uniek is. Een chipkaartlezer, zoals bijvoorbeeld een automaat voor betaling of toegangscontrole, kan een aangeboden chipkaart natuurlijk direct om dit geheim vragen. Maar dan is het geheime getal niet langer geheim.

Een subtielere manier werkt als volgt. De chipkaartlezer geeft aan de chipkaart een sommetje dat alleen gemakkelijk en snel op te lossen is als men het geheime getal weet. Deze authentificatiemethode komt dus neer op: ik geloof dat jij die-en-die bent, als jij – of jouw chipkaart – een oplossing weet voor de volgende opdracht. Om zulke "cryptografische" sommetjes te kunnen uitvoeren bevat een chipkaart dus een ingebedde computer. Maar er kan natuurlijk ook meer met zo'n computer gedaan worden.

De moderne chipkaarten bevatten een klein besturingssysteem – een soort mini-Windows[24] – waarop verschillende programmaatjes kunnen draaien. Deze chipkaartprogramma's kunnen gebruikt worden voor allerlei toepassingen, zoals bijvoorbeeld elektronisch geld, bonuspunten, ziekenfondsgegevens, openbaar vervoersbewijzen, toegang tot gebouwen, netwerken of computers, etcetera. In principe is het geen probleem om verschillende van dit soort toepassingen te combineren op één enkele kaart, maar in de praktijk is dit een moeizame aangelegenheid, niet alleen vanwege de angst voor ongewenste onderlinge interferentie, maar bijvoorbeeld ook vanwege onenigheid over de grootte en de plaats van de verschillende logo's op het plastic.

U zult begrijpen dat aan dit soort programma's voor chipkaarten hoge kwaliteitseisen gesteld dienen te worden. Immers, het gaat om programmatuur die gebruikt wordt voor gevoelige toepassingen en in grote aantallen verspreid wordt. Wanneer er iets misgaat met chipkaarten is de schade groot en is er vaak ruime aandacht van de pers – waar de sector niet blij mee is. Chipkaarttoepassingen worden alleen door het grote publiek geaccepteerd wanneer er voldoende vertrouwen bestaat. Daar zijn alle partijen het over eens. Ook ziet men bijvoorbeeld in het eerder genoemde Nederlandse wetsvoorstel voor digitale handtekeningen de eis dat een rechtsgeldige digitale handtekening gezet moet zijn met een zogenaamd veilig middel ". . . dat voldoet aan de bij of krachtens algemene maatregel van bestuur te stellen eisen"[25]. Ik ben erg benieuwd naar de precieze omschrijving van deze eisen. Vervolgens kan de betreffende minister een instelling aanwijzen – denk aan TNO – die belast zal zijn met het beoordelen van de overeenstemming van zo'n veilig middel – denk aan een chipkaart – met de gestelde eisen. Interessant is hier de koppeling tussen technische eisen aan een computersysteem en juridische geldigheid. Zulke koppelingen scheppen nieuwe kansen en mogelijkheden voor het daadwerkelijke gebruik van formele methoden in de informatica.

Chipkaarten vormen een Europees succesverhaal, vergelijkbaar met de GSM. De producenten zijn voornamelijk Europees (vooral Frans en Duits), en toepassingen van chipkaarten vindt men in Europa veel meer dan bijvoorbeeld in Amerika en Japan. Het is dan ook om deze reden dat de Europese Unie in haar onderzoeksprojecten speciale aandacht heeft voor chipkaarten. Daar heb ik met mijn onderzoeksgroep in Nijmegen veel profijt van. Ik ben sinds januari 2001 coördinator van een Europees IST project VerifiCard[26] dat zich richt op het toepassen van formele methoden op het gebied van chipkaarten. Een deel van de aandacht richt zich daarbij op de inrichting van de kaart zelf, en een ander deel op de applicaties. Wij in Nijmegen houden ons vooral bezig met correctheidseigenschappen van de Java applicatieprogramma's die op die chipkaarten moeten draaien. Dat werk vormt een grote wetenschappelijke uitdaging. Niet alleen om de betekenis van deze Java-programma's juist te vatten, maar ook om dat op een zodanige wijze te doen dat maximale computerondersteuning mogelijk is, niet alleen bij het specificeren maar ook bij het verifiëren van de gewenste correctheidseigenschappen. Met gepaste trots meen ik te mogen stellen dat wij in Nijmegen op dat gebied tot de wereldtop behoren. We hebben de vereiste technieken onder de knie en onze aandacht richt zich nu voor het grootste deel op de verdere schaalbaarheid van deze technieken. Dit soort verificatiewerk is decennia lang gezien als academisch, onpraktisch gefröbel. Maar tot mijn genoegen begint daarin verandering te komen. Zo hebben wij binnen het zojuist genoemde Europese project een *case study* gedaan over een bestaand Java-chipkaartprogramma dat het gehele interne testtraject bij de fabrikant doorlopen heeft, alvorens het aan klanten overgedragen is. Toch hebben wij met onze formele methoden daar nog fouten kunnen detecteren.

Het is bemoedigend te merken dat door steeds meer partijen in de markt het belang van certificatie van computerprogramma's, met inzet van formele methoden, nu wordt ingezien. En natuurlijk ook dat deze partijen bereid zijn daarvoor te betalen en de onvermijdelijk resulterende vertraging in het productieproces te accepteren. Deze ontwikkeling biedt vele nieuwe mogelijkheden voor samenwerking tussen universiteiten en bedrijven die geïnteresseerd zijn in certificatie. Een noodzakelijk onderdeel van zo'n samenwerking zal een kennisuitwisseling zijn. Daarbij gaat het vanuit het bedrijfsleven richting academie om vaak confidentiële praktijkvoorbeelden en de daarvoor gewenste eigenschappen en vanuit de academie richting bedrijfsleven om technieken en gereedschappen. Deze ontwikkelingen bieden ook de mogelijkheid voor commerciële spinoff bedrijven, waarin hoogwaardig wetenschappelijk werk van direct nut kan zijn. In dit verband verheugt het mij zeer u te kunnen melden dat er sinds kort concrete plannen bestaan voor samenwerking op het gebied van certificatie van kleine Java-programma's voor chipkaarten tussen de smartcard afdeling TNO-EIB in Delft en mijn onderzoeksgroep hier aan de universiteit in Nijmegen.

Er zullen echter nog grote investeringen nodig zijn om de huidige formele technieken uit te breiden tot certificatieprojecten, waarin grote lappen code in detail doorlopen moeten worden. Het lijkt mij wel dat juist op dit gebied de Nederlandse informatica, met haar rijke theoretische traditie, zich kan profileren en internationaal impact kan hebben.

In het bovenstaande ben ik niet in gegaan op wat certificatie van computerprogramma's zou moeten behelzen. Dit is een onderwerp op zich, dat nog onvoldoende is uitgekristalliseerd. Er bestaan verschillende internationale standaards voor de beoordeling van computersystemen. Daarvan zijn de zogenaamde Common Criteria[27] wel de bekendste - zeker in de wereld van chipkaarten. Volgens deze Common Criteria dient een evaluatie uitgevoerd te worden door een geaccrediteerde organisatie en is zo'n evaluatie mogelijk op verschillende niveaus, op een schaal van 1 tot en met 7. Ter illustratie van de huidige situatie: banken vragen nu evaluaties op niveau 4, terwijl in defensiekringen vaker niveau 5 gewenst is. Dit soort evaluaties zijn niet onomstreden, omdat ze soms maar een beperkt deel of gebruik van een systeem beslaan, voor een specifieke, soms reeds verouderde versie. Bovendien laten ze ruimte voor interpretatieverschillen. Ook leiden certificatie-eisen tot een beperkte markt, waarin er weinig stimulans kan zijn om het aanbod van gecertificeerde producten te vergroten.

Zo'n Common Criteria evaluatie is een kostbare en tijdrovende aangelegenheid en naar het zich laat aanzien, een te zware procedure voor de voor ons interessante kleine applicatieprogramma's voor bijvoorbeeld chipkaarten of mobiele telefoons en organisers[28] (waarop Javaprogramma's gedownload kunnen worden). De komende jaren zal in de praktijk duidelijk moeten worden welke technieken op de meest efficiënte manier ingezet kunnen worden om te komen tot een werkbare en betrouwbare certificatiemethode voor kleine maar essentiële computerprogramma's.

Een interessante situatie zal zich voordoen wanneer een bepaald computerprogramma, ondanks certificatie, op een of andere wijze toch niet blijkt te voldoen. Dan zal moeten worden nagegaan of het ongewenste gedrag door certificatie uitgesloten had moeten worden. Ik neem aan dat de aansprakelijkheidsvraag dan snel gesteld zal zijn. Het is onduidelijk of in dat geval de producent of de certificaatverlener aansprakelijk is. Het is in dit verband relevant dat hier in Nederland TNO om dit soort redenen een zelfstandige status heeft gegeven aan haar groep[29] die zich met Common Criteria certificaties bezighoudt.

Beveiliging is multidisciplinair

Na dit op correctheid en certificatie toegespitste verhaal wil ik het in iets ruimere context over beveiliging van computersystemen hebben. Beveiliging is een spel van kat en muis. De kwalititeit van de beveiliging van een systeem wordt zoals gewoonlijk bepaald door de zwakste schakel. Maar hoe beveilig ik een computersysteem[30]? Net zoals pas van correctheid van programma's gesproken kan worden in het licht van een duidelijke specificatie, kan pas van beveiliging gesproken worden als er een *security policy* voorhanden is. Zo'n policy moet bestaan uit een analyse van de mogelijke bedreigingen, tezamen met de bijbehorende beschermingsmaatregelen. Daarbij gaat het er steeds om een juiste en flexibele mix te vinden van technische, organisatorische en juridische maatregelen. Laat ik dit aan de hand van een aantal voorbeelden illustreren.

Een ouderwetse, fysieke handtekening vormt nog steeds een veel gebruikte (biometrische) manier voor identificatie of ondertekening. De grootste bedreiging in dit voorbeeld is vervalsing. Vanuit puur technisch oogpunt is de handtekening een zwak middel. Ik denk dat ik na een uurtje oefenen van veel mensen de handtekening aardig zou kunnen imiteren. Toch functioneert dit systeem redelijk goed. We hebben met z'n allen een geheel van gebruiken en wetten opgebouwd rond de fysieke handtekening waardoor misbruik beperkt blijft. Vervalsing is strafbaar en voor bijvoorbeeld de verkoop van een huis moet min of meer gelijktijdig getekend worden in aanwezigheid van een notaris – die weer aanbepaalde beroepscodes gebonden is. Bij de nieuwe digitale handtekeningen zullen we het vooralsnog vooral van de technische aspecten van beveiliging moeten hebben, omdat een geheel van bijbehorende gebruiken en regels nog moet ontstaan. Deze technische maatregelen moeten zeer goed zijn, omdat een computer met een gestolen digitale handtekening in korte tijd veel grotere schade aan kan richten dan met een fysieke handtekening mogelijk is.

De chipknip vormt een ander aardig voorbeeld. De chipknip is een chipkaart met daarop een elektronische portemonnee met een bepaald saldo, waarmee relatief kleine bedragen gemakkelijk afgerekend kunnen worden. De belangrijkste scenario's (of protocollen) voor de chipknip zijn betalen en opladen. De grootste bedreigingen voor de banken zijn: betalen zonder dat het chipknipsaldo met het juiste bedrag verminderd wordt en opladen zonder corresponderende vermindering van het saldo op de juiste, bijbehorende bankrekening. De technische beveiligingsmaatregelen van de chipknip zitten goed in elkaar. De kaarten bevatten geheime cryptografische sleutels, waardoor de betaal- en oplaadprotocollen gebruik kunnen maken van standaard mechanismen voor authentificatie en integriteit. Zover ik weet is de (technische) beveiliging van de chipknip dan ook nog niet gebroken. Maar naast deze technische maatregelen, kent de chipknip ook organisatorische beveiligingsmaatregelen. Zo heeft iedere chipknip een maximumsaldo van € 500,- waardoor fraude beperkt kan blijven. Maar serieuzer is de schaduwboekhouding die banken van iedere chipknip bijhouden[31]. Daarin worden alle transacties opgeslagen en geanalyseerd. Mocht daaruit blijken dat er met een bepaalde chipknip meer betaald wordt dan er opgeladen is, dan wordt deze chipknip afgeschoten. Concreet betekent dit dat deze chipknip op een zwarte lijst komt te staan en niet meer gebruikt kan worden. Als het goed is wordt deze zwarte lijst dagelijks ververst, waardoor er hoogstens één dag gefraudeerd kan worden. Tenslotte vindt het gebruik van de chipknip plaats binnen een civiel rechterlijk kader dat gevormd wordt door de gebruiksvoorwaarden. De Postbank stelt daarin[32] bijvoorbeeld dat:

> In geval van opzet, grove schuld of grove nalatigheid aan de zijde van de Chipkniphouder is de Chipkniphouder onbeperkt aansprakelijk, een en ander onverminderd de verplichting van de Bank om (de mogelijkheid van) schade te beperken.

Mocht het iemand op een of andere manier dus toch lukken de technische beveiligingsmaatregelen van de chipknip te doorbreken, dan wordt dit snel geconstateerd

en kan de bank de betreffende persoon in een civiele procedure aanpakken en de schade verhalen[33].

Uiteindelijk gaat het in deze business om *risk management* en om een kosten-baten analyse. Het zal daarbij misschien een zinvolle keuze zijn om niet de sterkste technische maatregelen te kiezen, bijvoorbeeld vanwege de kosten, maar om meer te investeren in de ondersteunende organisatorische en juridische maatregelen.

Een informaticus die zich met computerbeveiliging bezighoudt zal oog moeten hebben voor al deze aspecten. Het vakgebied is dus breed en multidisciplinair: het strekt zich uit van cryptografische wiskundige technieken tot rechten. Bovendien komt men er zeer uiteenlopende types tegen, variërend van kwajongens en wetenschappers tot burgerrechtactivisten en geheimagenten. Computerbeveiliging behoort duidelijk tot de spannendste deelgebieden van de hedendaagse informatica.

Openheid en beveiliging I: wat moet geheim zijn?

Een wezenlijk kenmerk van een academische cultuur is openheid. Bronnenmateriaal en feiten moeten in principe voor iedereen toegankelijk en controleerbaar zijn en debatten moeten in alle openheid gevoerd kunnen worden, om tot een redelijke afweging van argumenten te komen. Dit kenmerk is echter niet vanzelfsprekend binnen de context van beveiliging. Daar bestaat de niet geheel onnatuurlijke neiging om aan te nemen dat beveiliging juist gebaat is bij geslotenheid: naar mate minder mensen weten hoe een bepaald beveiligingsmechanisme werkt, kan men meer op dit mechanisme vertrouwen. Deze houding wordt vaak aangeduid met *security by obscurity*. Dit lijkt een verstandige en logische benadering, maar is het uiteindelijk vaak niet, zeker niet in het huidige tijdperk waarin zoveel al of niet vertrouwelijke informatie, vaak anoniem, op internet beschikbaar komt.

Ik noem twee bekende voorbeelden. Bij het ontwerp van de huidige DVD standaard is een digitaal beveiligingsmechanisme ingebouwd dat CSS genoemd wordt, voor *Content Scrambling System*. Dit mechanisme is geheim. Het heeft niet blootgestaan aan publieke inspectie en onderzoekingen. Het moet ingebouwd worden (en geheim gehouden worden) door alle fabrikanten die een DVD logo op hun apparaten willen voeren. Deze fabrikanten omvatten niet alleen producenten van consumentenelektronica, maar ook die van computersoftware voor DVD spelers,waaronder Microsoft en Apple. Echter de ongrijpbare wereld van het *open source* besturingssysteem Linux werd hiervan uitgesloten. Binnen deze wereld zijn er veel goede programmeurs, die ook wel eens een DVD willen afspelen en die zich niet graag de wet laten voorschrijven door een platenbaas. Het heeft dus niet lang geduurd voordat men uitvond dat het DVD beveiligingsmechanisme helemaal niet sterk was. Programma's om het te doorbreken verschenen op internet en werden onderdeel van Linux besturingssystemen. De muziek en filmindustrie is hiertegen juridisch ten strijde getrokken, maar zoals eerder vermeld zonder veel succes. Een vergelijkbaar verhaal kan verteld worden overde digitale beveiligingsmechanismen die gebruikt worden in de GSM mobiele telefoon standaard. Het gevolg is dat mobiele telefoongesprekken niet goed beschermd zijn en in principe afgeluisterd kunnen worden.

Reeds in 1831 heeft de van oorsprong Nederlandse cryptograaf Auguste Kerckhoff het principe verwoord[34] dat de sterkte van een beveiligingsmechanisme niet mag afhangen van de geheimhouding van dit mechanisme, maar enkel van de sterkte van de daarbij gebruikte cryptografische sleutels. De achterliggende idee is dat het vaak onmogelijk is om het mechanisme geheim te houden (onder toen geldende krijgsomstandigheden, maar ook in het huidige internettijdperk, zie de reeds genoemde DVD). Het is dus uiteindelijk beter ervan uit te gaan dat een aanvaller bekend is met de werking van het systeem. Een bijkomend voordeel is dat wanneer het beveiligingsmechanisme publiekelijk bekend is, het door verschillende onafhankelijke partijen bekeken en beoordeeld kan worden. Dit principe van Kerckhoff is nog steeds actueelen wordt door vrijwel iedereen op het vakgebied – ten minste in de academische wereld – onderschreven, maar helaas niet altijd in de praktijk gebracht.

Ik ben mijn betoog begonnen met mogelijke geavanceerde vormen van stemmen op afstand, via mobiele telefoon of internet. In feite bestaat er in Nederland al enige jaren de mogelijkheid om elektronischte stemmen, via zogenaamde stemcomputers. Die worden gebruikt op sommige stembureaus en niet bij mensen thuis. Daardoor staan ze onder strikte controle van de overheid. In feite bestaan er drie verschillende systemen[35] die ieder goedgekeurd zijn door het ministerie van Binnenlandse Zaken, na uitvoerige testen door TNO, zoals vereist in de relevante algemene maatregel van bestuur bij de kieswet. Echter, de in deze stemcomputers gebruikte mechanismen zijn niet openbaar. Iets technischer, de broncode van de gebruikte software is niet openbaar. Wij hebben als burgers het recht om het tellen van gewoon met potlood

en papier uitgebrachte stemmen bij te wonen en te controleren, maar wij hebben geen inzage in de werking van deze stemcomputers[36]. Vinden wij dit acceptabel?[37]. Het lijkt me interessant om deze merkwaardige geslotenheid eens aan een bestuursrechter voor te leggen, met een beroep op de Wet Openbaarheid van Bestuur[38].

Een ander controversieel voorbeeld betreft het systeem dat in Nederland in zogenaamde tapkamers door politie en inlichtingendiensten gebruikt wordt om telefoongesprekken op te nemen. Dit systeem is geleverd door het Israëlische bedrijf Verint (voorheen Comverse), dat voortgekomen is uit de Israëlische geheime dienst en dat in de Verenigde Staten in opspraak is geraakt vanwege mogelijke spionage praktijken. Het probleem met deze tapkamers is dat niemand, behalve de experts van Verint-Comverse zelf, weet hoe de apparaten precies werken, omdat geen toegang tot de *source code* gegeven wordt. Medewerkers van het Israëlische bedrijf echter hebben regelmatig, voor onderhoud, toegang tot de Nederlandse tapkamers[39].

In het proces tegen de Koerd Hüseyin Baybasin, waarbij afgeluisterde telefoongesprekken een cruciale rol speelden, is de betrouwbaarheid en integriteit van deze tapkamersystemen door de verdediging in twijfel getrokken. Baybasin is namelijk geen vriend van de Turkse overheid: hij is een van de oprichters, financiers en leden van het Koerdische parlement in ballingschap in Den Haag en hij heeft een boekje open gedaan over de vermeende banden tussen belangrijke Turkse politici en de heroïnemaffia in dat land. De advocate van Baybasin, Adèle van der Plas, beweert dat Turkse en Israëlische geheime diensten hebben samengespannen om Baybasin in Nederland veroordeeld te krijgen via het manipuleren van opgenomen telefoongesprekken. Manipulaties zijn door verschillende onafhankelijke experts inderdaad bevestigd.[40] De veroordeling heeft echter plaatsgevonden en heeft afgelopen juli in hoger beroep stand gehouden[41].

Ik ben natuurlijk niet in een positie om klaarheid in deze gevoelige zaak te brengen. Daar gaat het me ook niet om. Ik hoop dat u het met me eens bent dat het onacceptabel is in onze rechtsstaat dat de gerezen twijfel aan de betrouwbaarheid van een zeer veel gebruikt bewijsmiddel niet ontzenuwd kan worden. De heer J.W.M. van de Ven, een oud lid van de Militaire Inlichtingen Dienst (MID) en autoriteit op het gebied van afluistertechnieken, heeft zich in deze zaak verdiept en spreekt van wantoestanden[42]. Hij pleit voor certificering van het afluisterproces en voor openbaarmaking van de *source code* van de tapcentrales, om een justitiële crisis te voorkomen.

Aan de hand van dit tapkamervoorbeeld wil ik nog een punt maken. Het uitblijven van investeringen in technologische kennis wordt heden ten dage soms gerechtvaardigd met het argument van de handelaar: we hoeven zelf toch geen kennis in huis te hebben als we de benodigde producten gewoon kunnen kopen. Het Israëlische bedrijf Verint-Comverse toont ons hoe gevaarlijk dit argument is in de context van computerbeveiliging.

Het lijkt mij dat we nog maar aan het begin staan. Daarom is het extra belangrijk nu goed na te denken. Kunnen we ermee leven dat velerlei procedures die een wezenlijk onderdeel uitmaken van onze democratie, van onze rechtsspraak en van ons openbaar bestuur afgehandeld worden door computers in *black boxes* met misschien een stickertje van TNO, waarbij niemand weet wat er precies gebeurt? Natuurlijk niet! Openheid en transparantie moeten ook bij vergaande automatisering gegarandeerd zijn. Een voor de hand liggende eis in deze sector is het gebruik van open standaards, open ontwerpen en van *open source* software, zodat iedere burger in principe de juiste werking zou kunnen controleren[43]. Ook kan men eisen dat software die ingrijpende beslissingen neemt, bijvoorbeeld over het wel of niet toekennen van een uitkering, zulke besluiten voorziet van een controleerbare motivatie. Daardoor worden eventuele foute beslissingen door programmeerfouten zichtbaar.

Openheid en beveiliging II: wat te onderzoeken?

Wanneer er aan deze universiteit een college over bijvoorbeeld algebra gegeven wordt, kan daarin in principe alle bestaande kennis op het gebied van de algebra aan bod komen. Wanneer ik hier echter een college over computerbeveiliging geef zijn er veel elementaire en relevante zaken die ik gewoon niet weet en ook niet zomaar te weten kom. Een simpel voorbeeld vormt de welbekende elektronische autosleutel. Die kan een of ander signaal versturen waardoor de portieren van de bijbehorende auto ontgrendeld worden. Dit is een typisch beveiligingsonderwerp, omdat het gaat over regulering van toegang. Je zou misschien willen weten of een zogenaamde *replay attack* mogelijk is. Daarbij neemt een kwaadwillende het door de autosleutel verstuurde signaal op, bijvoorbeeld via de infraroodpoort van een organiser of laptop, teneinde het opgenomen signaal op een geschikt moment nog eens rustig af te spelen – om er zodoende met de bijbehorende auto vandoor te gaan. Zo'n aanval was mogelijk bij de eerste elektronische autosleutels die beschikbaar

kwamen[44], maar de moderne sleutels zouden er tegen bestand moeten zijn. Of dit inderdaad zo is weet ik echter niet zeker. Ik zou nu een mooi onderzoeksplan op kunnen stellen om bij verschillende typen elektronische autosleutels na te gaan of deze *replay attacks* mogelijk zijn. Ik zou kunnen aanvoeren dat dit voor mij als publiek gefinancierde onderzoeker een mooie taak is, met als uiteindelijk doel de beveiliging van auto's te verbeteren. Maar u kunt zich vast wel voorstellen dat de automobielindustrie helemaal niet zo ingenomen is met dergelijke onderzoeksplannen. Immers, er zou kunnen blijken dat hun producten niet optimaal beveiligd zijn, waardoor hun imago schade oploopt, hun auto's misschien teruggehaald moeten worden ter vervanging van de sleutelsystemen en uiteindelijk hun omzet mogelijk daalt. Zou ik mij als onafhankelijk onderzoeker hier iets van aan moeten trekken?

In mijn onderzoeksgroep hier aan de universiteit is het afgelopen jaar onderzoek verricht naar chipkaarten met elektronisch geld. Daarbij hebben we gekeken naar het chippersysteem, dat inmiddels ter ziele is en naar de operationele chipknip. Na enig aandringen hebben we op vertrouwelijke basis inzage gekregen in de werking van de oude chipper. Daarvan hebben we veel geleerd. Over de chipknip voeren de banken een strikt geheimhoudingsbeleid en hebben wij geen materiaal ontvangen. Daarom zijn wij zelf begonnen, via allerlei experimenten, te achterhalen hoe het chipknipsysteem feitelijk werkt. De motivatie hierbij is een wetenschappelijke: in de open literatuur zijn weinig realistische security protocollen bekend. En in de protocollen die wel bekend zijn blijken vaak subtiele zwakheden voor te komen. Wij wilden wel eens met een onafhankelijke blik naar de chipknip kijken. De banken waren echter *not amused*. Er is ons op vriendelijke, maar niet mis te verstane wijze, duidelijk gemaakt dat dergelijk onderzoek niet gewaardeerd wordt. Moet ons dat weerhouden?

Er staat ons de komende jaren nog heel wat te wachten op ICT gebied. Daarbij zullen wij steeds afhankelijker worden van de ons omringende computers en een steeds groter deel van ons doen en laten zal digitaal geregeld en geregistreerd worden. Vinden wij als Nederlandse samenleving dat de daadwerkelijke implementatie van de daarbij gebruikte mechanismen transparant en open moet zijn en dat daarbij ruimte moet zijn voor onafhankelijk onderzoek naar de betrouwbaarheid van deze mechanismen?

Openheid en beveiliging III: wat zijn de grenzen?

De internationale ontwikkelingen van de laatste jaren versterken het belang dat gehecht wordt aan beveiliging in het algemeen en aan digitale beveiliging in het bijzonder. Opvallend daarbij is dat aan politie en inlichtingendiensten vergaande bevoegdheden tot het verrichten van onderzoek worden toegekend[45]. Tegelijkertijd worden ondermijnende activiteiten van kwaadwillende computergebruikers als zeer bedreigend ervaren. Kringen die zich met beveiliging bezighouden ontwikkelen zich gemakkelijk tot gesloten bastions en lopen het risico vervreemd te raken van de hen omringende werkelijkheid.

In de Verenigde Staten is in 1998 onder druk van de muziek en filmindustrie een speciale wet ingevoerd, de zogenaamde *Digital Millenium Copyright Act* (DMCA), die het doorbreken van digitale beschermingsmaatregelen verbiedt. Deze wet heeft geleid tot verschillende aanklachten tegen wetenschappers op het gebied van versleuteling en beveiliging[46]. Zoals reeds vermeld ligt in Nederland een wetsvoorstel ter goedkeuring bij de Tweede Kamer, dat de Auteurswet uit 1912 moet aanpassen aan de moderne tijd. Deze wet verbiedt wetenschappers niet expliciet om onderzoek te doen naar bestaande beveiligingsmechanismen, maar verbiedt wel om over eventueel gevonden zwakheden te publiceren. Dit is in strijd met de wetenschappelijke traditie, waarin reproduceerbaarheid van resultaten en openheid van debat centraal staan. De voorgestelde wet heeft dus een aantal kwalijke gevolgen.

- Wetenschappelijk onderzoek naar correctheid en beveiliging van computersystemen is er inherent op gericht om fouten te vinden. Een verbod om vervolgens zulke gebreken te rapporteren leidt tot een wezenlijke beperking van dergelijk onderzoek. Zo'n aantasting leidt vervolgens tot een vermindering van de waarde van certificaties – die op dergelijke onderzoeksmethoden berusten – en uiteindelijk dus ook tot een verslechtering van de beveiligingsmechanismen.

- Het verwijderen van kritische feedbackloops is in het algemeen een kortzichtige benadering, die op de lange termijn een zeer schadelijke werking heeft. Open onderzoek en kritiek vormen een wezenlijk onderdeel van (het succes van) onze westerse cultuur en aantasting daarvan is een ernstige zaak.

- Eerder noemde ik dat beveiliging in iedere situatie een juiste balans vraagt tussen technische, organisatorische en juridische maatregelen. Wanneer het juridisch kader met zo'n nieuwe Auteurswet sterker wordt zal dit ongetwijfeld ten koste gaan van de kwaliteit van de technische en organisatorische maatregelen. Dit maakt het dan alleen maar gemakkelijker om beveiligingsmechanismen te door breken voor individuen die zich toch niks van de wet aantrekken.

- Tenslotte leidt de voorgestelde strafbaarheidsstelling van het omzeilen van technische beveiligingsmaatregelen ook tot een aantasting van de vrijheid van meningsuiting. Dit aspect speelt een belangrijke rol in de DMCA rechtszaken in de Verenigde Staten.

Het moge duidelijk zijn dat ik niet geloof dat strafbaarheidstelling het probleem van mogelijke doorbrekingen oplost. Hier wordt het kind met het badwater weggegooid en kunnen zelfs averechtse effecten optreden. Het ware beter geweest wanneer het wetsvoorstel enkel de openbaarmaking van een auteursrechtelijk beschermd werk als onrechtmatig aanmerkt – want daar gaat het tenslotte om – en niet de omzeiling van de technische beschermingsmaatregel. Zo'n formulering raakt de kern van de zaak en laat ruimte voor (wetenschappelijke) kritiek op de beveiligingsmechanismen. Maar het is misschien nog niet te laat.

Oproepen

Mogelijk bent u mij gaandeweg mijn lezing gaan beschouwen als een tragische figuur. Immers, ik heb mij laten benoemen als onderzoeker op een vakgebied waarop de werkelijk interessante zaken geheim zijn en volgens een nieuwe wet ook nog niet eens onderzocht mogen worden. Mogelijk dacht u van tevoren: de onafhankelijke professor zal wel weten hoe het werkt hier in Nederland en zal wel zeggen dat het goed zit. De verontrustende boodschap is: ofwel ik mag het niet weten, ofwel ik mag niet zeggen wat er fout aan is. Zit hier wel toekomst in, vraagt u zich dan wellicht af? Of sterker nog: kan die man niet beter direct zijn afscheidsrede houden?

Deze schets is ongenuanceerd en kort door de bocht. Maar er zit een kern van waarheid in. Misschien tegen beter weten in, wil ik mijn pasverworven positie gebruiken om op kritische wijze te werken aan een open en betrouwbare inrichting van essentiële beveiligingsinfrastructuur. Ik kan en wil dat niet als eenling doen, en wil daarom van deze mooie gelegenheid gebruik maken een aantal oproepen te doen.

- Ik wil de Nederlandse overheid oproepen met kracht de voorzichtig ingezette weg richting open standaards en *open source* software[47] voort te zetten. Verleden jaar heeft het GroenLinks kamerlid Kees Vendrik, een oud-student en zoon van een bekend hoogleraar en bestuurder aan deze universiteit, het nobele initiatief genomen tot een kamermotie die het gebruik van open standaards en *open source* software door de Nederlandse overheid sterk aanmoedigt[48]. Het mag niet zo zijn dat een overheid haar fundamentele taken toevertrouwt aan systemen waar ze zelf geen inzicht in heeft. En ook niet dat ver weg, op commerciële basis genomen beslissingen hier leiden tot gedwongen aanschaf en implementatie van nieuwe versies en omzettingen van essentiële gegevensbestanden. Open standaards en open software kunnen bijdragen aan een veilige en transparante gang van zaken.

- Mijn collega informatici wil ik oproepen nadrukkelijker aan het maatschappelijke debat deel te nemen en een prominentere rol te spelen in de media. Dat doen wij niet goed. Ik kijk vaak vol bewondering en ook jaloezie naar sterrenkundigen. Iedere keer wanneer er weer een onbenullige komeet voorbij scheert komt er een groot stuk in de krant. Waarom legt niet één van ons bijvoorbeeld bij het verschijnen van een nieuw computervirus in een tvprogramma uit wat er aan de hand is? Er is redelijk wat aandacht in de media voor *computergadgets*, voor *toys for boys*, maar niet voor de onderliggende wetenschappelijke issues. Dat is jammer, want er is veel interessants te vertellen, dat mogelijk ook nog eens meer studenten en studentes aantrekt.

- Ook wil ik mijn geachte universitaire collegae nog eens voorhouden welke mogelijkheden voor het gebruik van formele methoden zich aandienen door de toenemende vraag om certificaties. Het is van belang voor ons vakgebied om hier gezamelijk te zorgen voor het bruikbaar maken van onze theorieën en technieken.

- De leden van de Nederlandse Staten Generaal roep ik op kritisch te kijken naar het voorliggende ontwerp voor een nieuwe Auteurswet en de mogelijkheden voor onafhankelijk kritisch onderzoek naar beveiligingsmechanismen niet onmogelijk te maken, zodat Nederlands onderzoek op dit gebied ongehinderd kan bijdragen aan een sterke economische positie.

- De nieuwe Nederlandse Regering roep ik op om werkelijk iets te doen aan het internationaal genant lage niveau van investeringen in wetenschappelijk onderzoek en onderwijs, tenminste wanneer men in Nederland werkelijk een kenniseconomie wil laten bloeien. Daarbij is de situatie van de exacte en technische vakken cruciaal, maar zeer zorgelijk. Ik begrijp dat het enigszins voorspelbaar is dat ik me hierover beklaag en dat dit misschien weinig resultaat heeft. Triester is het dat het minder voorspelbare luiden van de noodklok door Nederlandse *captains of industry* evenmin invloed lijkt te hebben. Misschien is er wil en durf nodig om onconventionele stappen te zetten, zoals bijvoorbeeld het volledig afschaffen van collegegeld voor de bedreigde beta studierichtingen, met als doel het aantal studenten in deze richtingen te vergroten. Daardoor zouden wij als docenten mogelijk niet ideaal gemotiveerde studenten in onze collegebanken krijgen. Maar het zou ons ertoe moeten aanzetten met goed en inspirerend onderwijs meer studenten te enthousiasmeren voor de waarde en schoonheid van onze vakken.

- Meer in het algemeen meen ik dat de Wetgever meer oog zou mogen hebben voor consumentenbelangen. De trend van de laatste jaren is om vooral de belangen van grote spelers (zoals de *content providers*, softwareproducenten en opsporings en inlichtingendiensten) te verdedigen. Ik doe hierbij slechts één concreet voorstel. Volgens mij zou het expliciet verboden moeten worden, ongeacht *license agreements*, dat consumentensoftware ongevraagd, dat wil zeggen zonder toestemming van de gebruiker, via een computernetwerk informatie uitwisselt met andere partijen. Dit zou het strafbaar moeten maken dat zogenaamde *Spyware* ongewenst informatie over bijvoorbeeld de inrichting van uw computer, uw gegevens, of uw surfgedrag verspreidt.

- Ik doe ook een oproep aan consumenten en burgers om assertief eisen te stellen aan de ICT infrastructuur die hen in steeds dwingender mate omringt en deze eisen zonodig via een juridisch traject af te dwingen. Ik denk hierbij aan het recht op garantie op software, of aan het recht op openbaarheid met betrekking tot bijvoorbeeld stemcomputers of andere systemen die een essentiële rol spelen in het reguleren van het maatschappelijke verkeer. Het is nog relatief zeldzaam dat aan de computer de wet wordt gesteld.

Conclusie en dankwoord

Het is een grote wetenschappelijke uitdaging op het gebied van computerbeveiliging om een *security policy* niet alleen op een heldere, niet ambigue wijze te formaliseren, maar ook op een effectieve manier te kunnen vaststellen. Dit beschouw ik als de grote uitdaging waar ik me de komende jaren mee bezig wil houden. Iets meer toegespitst zal de aandacht zich daarbij concentreren op protocollen en programma's voor chipkaarten en op certificatie. Ik wil daarbij enerzijds het vertrouwen verdienen om te kunnen weten hoe de relevante systemen werken, maar anderzijds de onafhankelijkheid hebben om publiekelijk commentaar te kunnen leveren. Het zal de komende jaren moeten blijken of ik deze twee rollen inderdaad kan combineren.

Tot slot wil ik enkele woorden van dank uitspreken. Ik ben nu bijna veertig en het ambt dat ik vandaag officieel aanvaard vormt mijn eerste aanstelling voor onbepaalde tijd. Dat wil zeggen dat ik tot niet zo lang geleden op allerlei tijdelijke posities gewerkt heb, vaak slechts voor twee of drie jaar, in soms onzekere tijden. Ik heb echter veel geleerd en nuttige ervaring opgedaan in al deze posities. Ik wil mijn vele collega's uit deze jaren danken voor de prettige samenwerking. Deze aanstellingen zijn mogelijk gemaakt door de inzet, de steunen het vertrouwen van velen, bij het beoordelen van projectvoorstellen, bij het schrijven van aanbevelingsbrieven en bij het selecteren van kandidaten. Expliciet wil ik noemen: Henk Barendregt, Ieke Moerdijk, Jaco de Bakker, Jan-Willem Klop, Frits Vaandrager en Ed Brinksma. Mijn erkentelijkheid is groot. Ook wil ik mijn dank uitspreken voor de genereuze steun van NWO die ik door de jaren heen ontvangen heb, waarbij de recente Pioniersubsidie het hoogtepunt vormt.

Hier in Nijmegen heb ik, vooral met steun uit verschillende externe bronnen, gaandeweg een grote groep kunnen opbouwen, die inmiddels uit twaalf personen be-

staat. Het initiatief tot het instellen van een leerstoel daarbij komt van het bestuur van de Faculteit der Natuurwetenschappen, Wiskunde en Informatica. Daar ben ik zeer blij mee. En ook met de ondersteuning en ruimte die de Subfaculteit Informatica geboden heeft. Maar vooral ben ik blij met de goede sfeer en het enthousiasme binnen mijn groep. Speciaal wil ik daarbij de mensen van het eerste uur noemen, met wie zo veel samen is opgebouwd: Joachim van den Berg, Erik Poll en Marieke Huisman.

Mijn woorden van dank voor mijn dierbaren in mijn directe omgeving beschouw ik als confidentieel en wil ik daarom niet in het openbaar, maar privé uitspreken.

Ik heb gezegd.

Noten

1 De zogenaamde Wet Elektronische Handtekeningen (27 743) ter uitvoering van de Europese richtlijn nr. 1999/93/EG.

2 Tweede kamer stuk 28 664.

3 Zie de website www.minbzk.nl van het Ministerie voor Binnenlandse zaken en Koninkrijksrelaties voor meer informatie.

4 Wetsvoorstel Uitvoering Richtlijn Auteursrecht, Kamerstuk 28 482, ter uitvoering van de Europese Auteursrichtlijn (2001/29/EG).

5 Namelijk op 24 dec. 2002.

6 Op 7 januari 2003, maar inmiddels in hoger beroep.

7 Zie voor de details van deze en andere uitspraken de website www.rechtspraak.nl.

8 Uitspraak op 13 maart 2002 van de rechtbank in Maastricht.

9 Uitspraak van de Arnhemse rechtbank van 27 jan. 2003; zie ook Automatiseringsgids 7, 14 feb.2003.

10 Artikel 3:2, Burgerlijk Wetboek.

11 In arresten van 13 juni 1995 en van 3 december 1996.

12 Zie bijvoorbeeld Y. Buruma, Computerfraude. In: H.J.B. Sackers en P.A.M. Mevis (red.), Fraudedelicten, Deventer 2000, (166–174).

13 Er valt wat voor te zeggen om dat wel te doen, omdat veiligheid in enge zin enkel zogenaamde *safety* properties betreft, en bijvoorbeeld geen *liveness* properties, die wel degelijk onderdeel uitmakenvan correctheid voor programma's.

14 Artikel 7:17, Burgerlijk Wetboek, eerste lid.

15 Zie Artikel 7:21 in het Burgerlijk Wetboek. Bij toepassing moet de winkelier wel eerst aangemaand worden, en heeft deze de mogelijkheid de aankoop ongedaan te maken door de koopprijs terug te geven.

16 Zie www.nader.org.

17 Zie http://aviationsafety.net/database/2002/020701o.htm voor een gedetailleerd verslag.

18 Artikel `Microsoft onthult winst op Windows' in NRC Handelsblad, 18 nov. 2002.

19 De Business Software Alliance, zie www.bsa.org/netherlands.

20 Zie J. Viega and G. McGraw, Building Secure Software, AddisonWesley, 2002

21 De bekende expert op het gebied van computerbeveiliging Bruce Schneier stelt dat aansprakelijkheid en bijbehorende verzekeringen beter zou moeten werken. Zo stelt

hij de mogelijkheid voor om bedrijfsnetwerken tegen inbraken te verzekeren. Verzekeringsmaatschappijen zullen de hoogte van hun premies dan afhankelijk maken van de aanwezige beveiligingsmechanismen, en daar een positieve invloed op hebben, zie: Bruce Schneier, Insurance and the Computer Industry, Communications of the ACM, 44(3), 2001 (p.114–115).

22 Strikt gesproken: met minder omringend plastic.

23 Vanwege de zogenaamde tamper evidence: eventuele fysieke toegang kan gedetecteerd worden.

24 Maar dan uiteraard zonder windows.

25 Uit artikel 18.17.1 uit het wetsvoorstel (Eerste Kamerstuk 27 743, nr. 265).

26 Om precies te zijn IST-200026328-VERIFICARD, zie www.verificard.org.

27 Zie www.commoncriteria.org en in Nederland www.commoncriteria.nl dat verwijst naar een afsplitsing van TNO die zich richt op Common Criteria evaluaties.

28 Binnen het MIDP raamwerk (zie http://java.sun.com/products/midp/), met verschillende security domeinen waarvoor ook bijbehorende certificatieeisen gesteld moeten worden.

29 Zie www.commoncriteria.nl.

30 Dat is de centrale vraag in R. Anderson, Security Engineering. John Wiley & Sons, 2001.

31 Het bestaan van deze schaduwboekhouding blijkt bijvoorbeeld uit de Postbank Chipknip voorwaarden, artikel 2.8, waarin duidelijk wordt dat de bank het chipknipsaldo aan de klant terug kan geven zelfs in het geval dat de kaart onklaar geworden is.

32 In artikel 8.2 d, in de Postbank Chipknip voorwaarden.

33 In de praktijk blijken banken zeer terughoudend met juridische stappen, waarschijnlijk vanwege ongewenstheid van ermee samengaande publiciteit.

34 In zijn boekwerk *La Cryptographie Militaire*, zie ook het begin van hoofdstuk 8 in: David Kahn, *The Code Breakers*, 1967 (herziene druk in 1996).

35 Een PC met aanraakscherm en software van Sdu uitgevers, een stemmachine van Nedap met software van Groenendaal en een stemmachine van Samson met software van Sdu.

36 In Amerika zijn zogenaamde *touchscreen* stemmachines in opspraak geraakt vanwege mogelijk gebrekkige certificatie en het mogelijk aanbrengen van ongecertificeerde *patches* vlak voor verkiezingen, zie bijvoorbeeld www.salon.com/tech/feature/2003/-02/20/voting machines en www.blackboxvoting.com. David Dill en vele andere bekende informatici hebben zich inmiddels in de debatten gemengd, zie http://verify.stanford.edu/evote.html.

37 In dit speciale geval van verkiezingen is het ook mogelijk de zaak zo op te zetten dat aan het resultaat van de verkiezingen gezien kan worden of een bepaalde stem inderdaad meegeteld is. Wehebben het dan over een zogenaamd Verifiable voting system, zie: B. Schoenmakers, A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting, In: Advances in CryptologyCRYPTO'99, LNCS 1666, Springer 1999 (p.148–164).

38 Een mogelijke afwijzingsgrond voor openbaarmaking zou economische confidentialiteit kunnen zijn: publieke bekendheid van de mechanismen van deze stemcomputers zou de economische situatievan de producenten nadelig kunnen beïnvloeden. Overigens dient opgemerkt te worden dat, ten tijde van de opstelling van de regelgeving voor stemcomputers, zo'n tien jaar geleden, open source geen issue was zoals vandaag de dag.

39 Veel informatie en verwijzingen over deze zaak zijn te vinden in het artikel: Paul Wouters en Patrick Smits, Nederlandse tapkamers niet kosjer, C'T Magazine voor Computer Techniek 1/2, 2003 (p.34–35), zie ook www.fnl.nl/ctnl/archief2003/ct-20030102/aftappen.htm. Dit onderwerp krijgt ook aandacht van Bits of Freedom, zie bijv. www.bof.nl/nieuwsbrief/nieuwsbrief_2003_4.html.

40 Zie de Zembla uitzending van donderdag 6 feb. 2003, te vinden in het archief op www.omroep.nl/vara/tv/zembla/.

41 Uitspraak van 30 juli 2002 van het Gerechtshof te Den Bosch.

42 Aangehaald in het artikel: René Zwaap, Aftappers in het nauw, Groene Amsterdammer, 22 juni 2002.

43 Het moet echter niet overschat worden hoeveel mensen de code ook daadwerkelijk controleren. Ook is het een interessante, aparte onderzoeksvraag of *open source* tot betere beveiliging leidt.

44 En bijvoorbeeld ook bij afstandsbedieningen voor garagedeuren.

45 Zie bijvoorbeeld de artikelen 138a, 139c en 350a van het Wetboek van Strafrecht die hacken en afluisteren verbieden, terwijl dit in artikelen 126l en 126m van het Wetboek van Strafvorderling en in artikelen 24.1 en 25.1 van de Wet op de Inlichtingen en Veiligheidsdiensten expliciet wordt toegestaan (alleen voor de betreffende diensten, natuurlijk).

46 De Russische programmeur Dmitry Sklyarov is op 17 july 2001 in Las Vegas door de FBI gearresteerd nadat hij op een congres had gesproken over de mogelijkheid om de beveiliging van Adobe ebooks te omzeilen, zie www.freesklyarov.org/. De hoogleraar Edward Felten in Princeton werd verboden een onderzoek te publiceren waarin de gebreken van de muziekencryptie standaard SDMI worden beschreven, zie http://www.eff.org/IP/DMCA/Felten_v_RIAA/faq felten.html. Kritiek op de DMCA is te vinden op http://antidmca.org.

47 Zie het ICTU programma Open Standaarden en Open Source Software (OSOSS) op www.ictu.nl/ososs.php.

48 Motie Vendrik c.s. 28600XIII Nr. 30, zie http://overheidop.sdu.nl/cgibin/showdoc/pos=20/session=anonymous@3A1901335360/query=6/action=pdf/KST64791.pdf. Besprekingen staan in: Aad Offerman, Open source als overheidsbeleid, Computable, 13 dec. 2002, en in: Patrick Smits, Nerderlands overheid open source?, C'T Magazine voor Computer Techniek 1/2, 2003 (p.22).