Artikel Automatisering Gids 23 mei 2003

Kop:

Informatici moeten meer
optreden in de media

Intro:

Zijn computers te vertrouwen? Als het er echt op aankomt niet, zegt Bart Jacobs. In zijn oratie van 16 mei noemt hij drie belangrijke aandachtsgebieden: aansprakelijkheid, certificatie en openheid. En in het verlengde daarvan doet hij een aantal oproepen. Een kort overzicht.

Platte tekst:

Computers zijn de laatste jaren in hoge mate ingeburgerd. Wij zijn er aan gewend geraakt dat computerprogramma's regelmatig ongewenst gedrag vertonen. Zulk gedrag wordt meestal veroorzaakt door onopzettelijke fouten van de programmeur, maar het kan ook het gevolg zijn van moedwillig aangebrachte kwaadaardige programmafragmenten, of van aanvallen van buiten (computervirussen). Het is daarom een terechte vraag of wij computers kunnen vertrouwen. Natuurlijk doen wij dat al in belangrijke mate, bijvoorbeeld wanneer we in een vliegtuig stappen, of onze chipknip opladen. Maar vertrouwen we onze computers ook in voldoende mate om bijvoorbeeld verkiezingen elektronisch te laten plaatsvinden, via internet of via de mobiele telefoon? Een geslaagde poging van een kwaadwillende om de gang van zaken te beïnvloeden is daarbij een nachtmerriescenario.
Kunnen wij computers echt vertrouwen? In veel gevallen niet, bijvoorbeeld omdat er geen enkele controle is op het installeren van nieuwe, mogelijk besmette programma's. Ik zie drie belangrijke elementen die het vertrouwen in cruciale computersystemen kunnen vergroten: aansprakelijkheid, certificatie en openheid.

Lichamelijk letsel
Gaat iemand wel eens met een computerspelletje of een besturingssysteem dat vastloopt terug naar de winkel? De winkelier zal ervan opkijken. Indien er al garantie wordt gegeven, beperkt die zich bijna altijd tot de drager, dat wil zeggen, tot bijvoorbeeld de cd-rom waarop het programma wordt aangeleverd. Waarom worden er zelden of nooit 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.

Het zal de kwaliteit van computerprogramma's ongetwijfeld ten goede komen wanneer softwareproducenten nadrukkelijker worden aangesproken op eventuele gebreken in hun producten en, bij aantoonbaar in gebreke blijven, worden gedwongen tot schadeloosstellingen. 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, zou men er misschien beter aan doen meer te investeren in kwaliteit en de bijbehorende garantie. Als duidelijk is dat een legaal gekocht computerprogramma ook recht op garantie geeft, is er ook meer motivatie om netjes te betalen.

Kwaliteitsstempel

Er zijn sectoren, zoals bijvoorbeeld de luchtvaart, waar strenge regels gelden en nauwgezette procedures gevolgd dienen te worden. Zulke 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, liefst van een onafhankelijke partij, binnen een internationaal erkend kader (zoals de Common Criteria). In steeds meer sectoren wordt dit gezien als de toekomst. Dit is een ontwikkeling die vooral wordt gestuurd door de grote kopers van software, bijvoorbeeld de banken of defensie, voor toepassingen waarmee men zich geen problemen kan veroorloven. Maar ook bij de nieuwe wet Elektronische Handtekeningen die nu bij de Eerste Kamer ligt, wordt vereist 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".

In dit kader is het relevant dat er concrete plannen voor samenwerking zijn tussen de smartcardafdeling van TNO in Delft en de computersecurity-onderzoeksgroep aan de Universiteit van Nijmegen. Daar worden certificatietechnieken ontwikkeld voor de nieuwste generatie chipkaarten, die kleine Java-programmaatjes kan uitvoeren voor verschillende security-gevoelige toepassingen.

Wanneer verkiezingen met potlood en papier plaatsvinden heeft iedere burger het recht de telling van de stemmen bij te wonen. Wat blijft er over van dit recht bij elektronische verkiezingen? Transparantie moet ook gewaarborgd zijn bij vergaande automatisering. Het mag niet zo zijn dat veel 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. Open standaards, open ontwerpen en open-sourcesoftware kunnen hieraan bijdragen. 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.

In het licht van deze problematiek moet men de oproepen (kaders) lezen die verder op deze pagina staan.

Bart Jacobs

Prof.dr. Bart Jacobs is als hoogleraar beveiliging en correctheid van programmatuur verbonden aan de Universiteit van Nijmegen. Dit artikel is een bewerking van zijn oratie, gehouden op 16 mei: 'De computer de wet gesteld' (www.cs.kun.nl/~bart).

—— Zeven losse kaders ——

Open source
De Nederlandse overheid dient met kracht de voorzichtig ingezette weg richting open standaards en open-sourcesoftware voort te zetten. Verleden jaar heeft het GroenLinks kamerlid Kees Vendrik het nobele initiatief genomen tot een kamermotie die het gebruik van open standaards en open-sourcesoftware door de Nederlandse overheid sterk aanmoedigt. Het kan 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.

In de media
Informatici zouden nadrukkelijker aan het maatschappelijke debat deel moeten nemen en een prominentere rol moeten 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 voorbijscheert komt er een groot stuk in de krant. Waarom legt niet één van ons bijvoorbeeld bij het verschijnen van een nieuw computervirus in een tv-programma 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.

Formele methoden
De mogelijkheden voor het gebruik van formele methoden die zich aandienen door de toenemende vraag om certificaties mogen niet gemist worden door de academische informaticagemeenschap. Bij de genoemde digitale handtekeningen zien we een expliciet verband tussen juridische geldigheid en technische eisen. Dit soort zaken zijn de manier om impact te hebben met wiskundige methoden en speciale computertools op de correctheid van software. Het is van belang voor het vakgebied informatica om hier gezamelijk te zorgen voor het bruikbaar maken van de beschikbare theorieën en technieken.

Auteurswet
De leden van de Nederlandse Staten Generaal zouden zeer kritisch moeten kijken naar het voorliggende ontwerp voor een nieuwe auteurswet. Deze wet maakt het omzeilen van digitale beveiligingsmechanismen strafbaar, en lijkt daarmee sterk op de controversiële Amerikaanse Digital Millenium Copyright Act (DMCA), die onder sterke druk van de muziek- en filmindustrie tot stand is gekomen. Publicatie van eventuele zwakheden van dergelijke beveiligingsmechanismen valt ook onder de strafbaarheidsstelling in deze nieuwe auteurswet. Wetenschappelijk onderzoek naar computerbeveiliging is echter sterk gericht op het vinden van fouten. Het onmogelijk maken van een open discussie over eventuele zwakheden vormt een aantasting van kritische feedback loops, en zal uiteindelijk een negatief effect hebben op de kwaliteit van beveiligingsmechanismen.

Tevens zal het bemoeilijken dat Nederlands onderzoek op dit gebied bijdraagt aan een sterke economische positie. De wet zou zich moeten concentreren op de handeling van het openbaar maken van auteursrechtelijk beschermde werken (de kern van de zaak), en niet op het omzeilen van de digitale bescherming.

Onderwijsinvesteringen

De nieuwe Nederlandse regering zou werkelijk iets moeten doen aan het internationaal gênant 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. Het is enigszins voorspelbaar dat een hoogleraar zich hierover beklaagt. Dat heeft misschien ook weinig resultaat. 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 bèta-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 de exacte vakken.

Consumentenbelangen

De wetgever zou meer oog 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. Hier is slechts één concreet voorstel. Het zou expliciet verboden moeten worden, ongeacht license agreements, dat (consumenten)software ongevraagd, dat wil zeggen zonder toestemming van de gebruiker, via een computernetwerk informatie uitwisselt met andere partijen. Het zou strafbaar moeten zijn dat zogenaamde Spyware ongewenst informatie over bijvoorbeeld de inrichting van iemands computer, gegevens of surfgedrag verspreidt.

Assertiviteit

Tevens zouden consumenten en burgers assertiever eisen mogen stellen aan de ICT-infrastructuur die hen in steeds dwingender mate omringt. Zij zouden deze eisen zonodig via een juridisch traject moeten afdwingen. Men kan hierbij denken 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.