



INFORMATIEBEVEILIGING

Verleden, heden, toekomst



Sentinels, een nationaal onderzoeksprogramma over informatiebeveiliging

Auteur: Rik D.T. Janssen, Technologiestichting STW, (e-mail: rik@stw.nl).



Jarenlang heeft Nederland een nationaal onderzoeksprogramma op het gebied van informatiebeveiliging moeten ontberen. Dit programma is er nu en heet Sentinels (www.sentinels.nl). Begin december 2004 zijn de eerste projectvoorstellen gehonoreerd. Projectleiders en onderzoekers staan dus nu in de startblokken om met hun onderzoek te beginnen. Dit artikel verhaalt over het totstandkomen van dit onderzoeksprogramma, haar doelen en de plannen voor de toekomst.

De behoefte

Al gedurende lange tijd verschijnen allerlei rapporten, artikelen en boeken die het belang van informatiebeveiliging benadrukken. Om een paar willekeurige citaten te noemen:

"The nation's security and economy rely on infrastructures for communication, finance, energy distribution, and transportation - all increasingly dependent on networked information systems. When these networked information systems perform badly or do not work at all, they put life, liberty, and property at risk." [F. B. Schneider (ed.). Trust in Cyberspace. National Academy Press, Washington, 1999].

of

"Computer security lapses cost firms billions of dollars. Billions of dollars can be saved if companies spend more money on implementing preventive measures against computer security breaches rather than repair them after they have been exploited." [Mary Pat McCarthy, in Investor's Business Daily, Aug. 8, 2001]

President Bush heeft naar aanleiding van de aanvallen van 11 september 2001 op onder meer het World Trade Center in New York het U.S. Department of Homeland Security opgericht:

"With strong bipartisan support President Bush created the Department of Homeland Security - the most comprehensive reorganization of the Federal government in a half-century. The Department of Homeland Security consolidates 22 agencies and 180,000 employees, unifying once-fragmented Federal functions in a single agency dedicated to protecting America from terrorism. [...] More than \$18 billion has been awarded to state and local governments to protect the homeland. [...] The Administration developed national strategies to help secure cyberspace and the infrastructures and assets vital to our public health, safety, political institutions, and economy." [Homeland Security website, www.whitehouse.gov/homeland]

Ook in Nederland bleek een behoefte te bestaan aan een nationaal onderzoeksprogramma voor informatiebeveiliging. Technologiestichting STW heeft samen met een aantal belangrijke key players het voortouw genomen tot het oprichten van zo'n programma. Het werd al snel 'Sentinels' genoemd, naar het Engelse woord voor schildwachten die belangrijke informatie beschermen.

Introductie

Allerlei belangrijke denktanken van de Nederlandse regering hebben de laatste jaren rapporten geproduceerd over

de kwetsbaarheid van de elektronische samenleving en de veiligheid daarvan. Twee belangrijke daarvan zijn het rapport 'Samen, strategischer en sterker' van de Task Force ICT en Kennis onder leiding van C. le Pair uit 2001 en het Stratix and TNO-FEL rapport 'Samen werken voor veilig Internet verkeer: Een eDeltaplan', het eindrapport van het onderzoekproject 'kwetsbaarheid van het Internet', ook uit 2001.

Informatiebeveiliging is een aspect van informatiesystemen dat overal op alle niveaus in een systeem terug te vinden is. Een belangrijk aspect, omdat nog altijd geldt dat een systeem zo veilig is als de zwakste schakel. Hierbij hoeven die schakels niet noodzakelijkerwijs technisch te zijn. We kunnen ook denken aan organisatorische, bestuurlijke of juridische maatregelen om informatie te beschermen, denk aan regels 'waar informatie opgeborgen wordt?', 'wie de sleutels van die kast heeft?', en 'welke wetten ongeoorloofde toegang beschermen?'. Onderzoek in informatiebeveiliging is dus multidisciplinair en daarvoor is een integrale benadering nodig.

Omdat dit een heel breed gebied is, zal het Sentinels programma zich in eerste instantie concentreren op technische aspecten. Hiervoor wordt nauw samengewerkt met de academische wereld en de industrie. De organisato-

rische, bestuurlijke en juridische aspecten worden (informeel) beschouwd, en zullen een belangrijke plaats krijgen in een vervolg van Sentinels.

In het vervolg van dit artikel wordt het woord 'security' gebruikt voor het geheel van informatiebeveiliging, veiligheid van ICT, netwerken en informatiesystemen.

De problemen

Bij het ontwerpen, bouwen en aanpassen van informatiesystemen kunnen we een zekere mate van tegenstrijdigheid zien in de eisen waaraan ze moeten voldoen: aan de ene kant de openheid, connectiviteit en eenvoudige toegang voor geautoriseerden, en aan de andere kant de veiligheid en betrouwbaarheid van dat soort systemen.

Mainframes, desktop computers, laptops, palmtops, mobiele telefoons, et cetera, zijn steeds vaker met elkaar verbonden en toegankelijk via allerlei netwerken, zowel vast als draadloos (zoals Bluetooth of WiFi). We raken daaraan gewend en kunnen (lees: willen) in feite niet meer zonder. Een andere tendens is dat software steeds meer de toegang tot zaken (bankrekeningen, gebouwen, et cetera) gaat regelen, terwijl dat vroeger door mensen of dedicated hardware gedaan werd. Software biedt meer flexibiliteit, maar is wel kwetsbaarder en complexer. Communicatie tussen systemen is hierbij een noodzaak: dit moet natuurlijk wel betrouwbaar en veilig gebeuren.

Security is ook een belangrijke sociale en economische drijfveer. Neem bijvoorbeeld e-voting. Dat kan pas echt mogelijk worden wanneer mensen (en uitschrijvende instanties) erop kunnen vertrouwen dat het goed werkt en dat het betrouwbaar is, dus dat elke burger precies één stem kan uitbrengen en dat stemmen correct verwerkt worden. Iets dergelijks geldt ook voor e-commerce diensten zoals webwinkels: echt grote omzet kan pas gehaald worden wanneer de betaling van producten of diensten goed geregeld is én wanneer de koper er van op aan kan dat het afgenomen product ook maar één keer betaald wordt én dat het product ook echt afgeleverd wordt.

Door het gebruikmaken van fouten in software kunnen aanvallers de mogelijkheid krijgen tot het grondig verstoren van genoemde zaken. Hierdoor kunnen ze grote schade toebrengen aan cruciale informatiesystemen en belangrijke netwerkverbindingpunten bedreigen. Ook bestaan er voorbeelden van elektronische oorlogsvoering. Goede security kan dit voorkomen.

De doelstellingen

Het doel van het Sentinels onderzoeksprogramma is om alle soorten informatiesystemen en netwerken veiliger te maken. Hieronder vallen zowel de standaard systemen zoals pc's en netwerken, alsook hand held devices, embedded systemen en draadloze en on-chip netwerken. Sentinels wil ook bijdragen aan een alomvattend framework voor secure systems engineering. Zo'n framework helpt security-engineers in het ontwerpen en bouwen van veilige systemen.

Er bestaat al behoorlijk wat security-onderzoek in Nederland, zowel bij universiteiten als bij het bedrijfsleven. Allerlei stichtingen, instellingen en ministeries zijn hierbij betrokken. Een belangrijk doel is dan ook het coördineren hiervan en het verbeteren en stipleren van de samenhang.

Uiteraard zal Sentinels zich bezighouden met de internationale gemeenschap. Kennisuitwisseling vinden we ook heel belangrijk, zie hiervoor de paragraaf 'Kennisuitwisseling' hieronder.

Wie profiteert ervan?

De belangrijkste groepen die van het Sentinelsonderzoek profiteren zijn mensen en bedrijven die er vanuit kunnen gaan dat hun veiligheid en privacygevoelige gegevens goed beschermd zijn en dat communicatie over dat soort gegevens veilig verloopt. Praktisch betekent dat bijvoorbeeld dat er vertrouwen is in digitale handtekeningen, in e-cash en e-commerce, enzovoort. Aan dat vertrouwen ontbreekt het nu vaak door allerlei veiligheidsgaten. In sommige gevallen worden deze breed uitgemeten in de pers, maar niet altijd, omdat bedrijven die het slachtoffer zijn geworden van security-aanvallen dat liever niet aan de buitenwereld willen laten weten om imagoschade te voorkomen.

Uiteindelijk zal security-onderzoek resulteren in een verbetering van de economie en de handelspositie van Nederland door bijvoorbeeld verbeterde efficiency, hogere (omzet)volumes en/of meer klanten. Virusaanvallen leiden vaak tot enorme kostenposten:

"Virusaanvallen hebben in 2003 gezorgd voor een kostenpost van 55 miljard dollar wereldwijd. Volgens Trend Micro, een bedrijf dat anti-virus-software maakt, zal de schade dit jaar nog hoger uitvallen. [...] Het bedrijfsleven verloor in 2002 ongeveer 20 tot 30 miljard als gevolg van online virusaanvallen. In 2001 was dat nog 'slechts' 13 miljard, zo blijkt uit diverse schattingen." ['Virussen kosten 55 miljard', De Telegraaf digitaal archief, 16 jan. 2004]

Visie en focus

De Sentinelsvisie is dat de schade veroorzaakt door security-incidenten moet verminderen bij toenemend gebruik van computers, informatiesystemen en netwerken. Omdat security een heel breed onderzoeksgebied is, hebben Nederlandse security-experts uit de financiële en politieke wereld, uit het bedrijfsleven, van onderzoeksinstellingen en universiteiten de volgende twee applicatiegebieden voor het Sentinelsprogramma vastgesteld.

Gebied 1: security en privacy voor ambient intelligence. De belangrijkste focus is op de gebruiker, die omringd wordt door allerlei met elkaar verbonden apparaten.

Security en privacy in ambient intelligence zal een geheel nieuw concept van security nodig hebben, omdat de mate van beveiliging kan veranderen door verandering in tijd of locatie van de gebruiker. Dit is niet alleen een uitdaging omdat het een nieuw concept betreft, maar ook omdat het om heel veel verschillende apparaten kan gaan.

Gebied 2: security en privacy voor e-government en e-business, inclusief de vitale ICT infrastructuur.

De belangrijkste focus is op de provider van services, content en apparatuur.

Een voorbeeld is e-government, nu meestal éénrichtingsverkeer naar de burger. Omgekeerd gebeurt vaak niet, omdat het erg moeilijk is om burgers

en overheid goed en betrouwbaar te authenticeren. Een initiatief zoals de PKI infrastructuur probeert hier een oplossing voor te vinden. Hierdoor kan de serviceverlening naar burgers verbeterd worden.

Op dit moment heeft Nederland een goede internationale positie op een aantal security en privacy onderzoeksgebieden, zoals digitale watermerken, cryptografie, elektronisch stemmen, analyse van security-protocollen, smart cards en security verdeeld over verschillende systemen. Het is van cruciaal belang voor de Nederlandse economie dat Nederland haar positie op deze en andere gebieden behoudt en versterkt. Het mag niet gebeuren dat Nederland op deze belangrijke gebieden afhankelijk wordt van andere landen.

Kennisuitwisseling

Sentinels en Sentinelsonderzoekers zullen zich uitgebreid en actief bezighouden met zorgen dat de opgedane kennis ook echt gebruikt gaat worden in de Nederlandse maatschappij. Iedereen in de Nederlandse samenleving, burgers, maar natuurlijk ook industrie, bedrijfsleven, politieke wereld, ziekenhuizen, opleidingsinstellingen, scholen en universiteiten moet wat hebben aan de kennis die ontwikkeld is binnen Sentinels.

Ook wordt er een nationale ICT security-community opgezet en mogelijk ook een nationaal ICT Security Research and Competence Center. Andere activiteiten zijn bijvoorbeeld de jaarlijkse multidisciplinaire workshops, waarin experts uit het gehele security-gebied (ook uit de organisatorische, bestuurlijke en juridische wereld) uitgenodigd worden om hun visie met de aanwezigen te delen. Tevens zullen deze bijeenkomsten een platform zijn voor het genereren en bediscussiëren van gezamenlijke (en nieuwe) projecten.

Hierdoor wordt uitgebreide kennisuitwisseling verzekerd. De spin-off die hierbij ontstaat is een belangrijke bijdrage van het Sentinels programma aan de Nederlandse economie. Twee personen gaan nog uitgebreidere kennisuitwisseling garanderen: de Sentinels hoogleraar en de Sentinels security ambassadeur.



Rik D.T. Janssen

De Sentinels hoogleraar wordt hét wetenschappelijke aanspreekpunt voor security in Nederland. Hij/zij zal zich onder meer bezighouden met het stimuleren van samenwerking en van multidisciplinair onderzoek en het maken en beheren van een nationale onderzoeksagenda op het gebied van security.

De Sentinels security ambassadeur is hét aanspreekpunt voor de niet-wetenschappelijke wereld. Eén van zijn/haar taken is om zich goed en actief op de hoogte te houden van de behoefte van de Nederlandse samenleving en industrie.

Door de Sentinels hoogleraar en de Sentinels security ambassadeur kan iedereen in Nederland met security-vraagstukken terecht bij een vast aanspreekpunt.

Uiteraard is er ook een website (www.sentinels.nl) die het security-onderzoek in Nederland en de resultaten van Sentinels zichtbaar zal maken, niet alleen gedurende de looptijd van het programma, maar ook daarna. Deze website zal ook als discussieplatform kunnen gaan functioneren.

Sentinels zal ook zorgen voor de internationale inbedding. Het zal ook trainingen en lesprogramma's op het gebied van ICT security initiëren en ondersteunen.

Het budget

Het totale Sentinels budget is 10 miljoen euro. Hiervan wordt 2,5 miljoen euro gefinancierd door het Ministerie van Economische Zaken, 2,5 miljoen euro door Technologiestichting STW, 2,5 miljoen euro door de Nederlandse organisatie voor Wetenschappelijk Onderzoek (NWO) en 2,5 miljoen euro door het Nederlandse bedrijfsleven en universiteiten. Van het totale budget wordt 80 procent (8 miljoen euro) uitgegeven aan onderzoek, 10 procent (1 miljoen euro) aan kennisuitwisselingactiviteiten en 10 procent (1 miljoen euro) aan administratieve kosten en diversen. Het programma loopt 8 jaar met twee rondes waarin onderzoeksvoorstellen kunnen worden ingediend. Er is één ronde met voorstellen voor de Sentinels hoogleraar. Kennisuitwisselingactiviteiten lopen uiteraard gedurende de hele looptijd van het programma.

Het proces rond het indienen van onderzoeksvoorstellen

Het proces waarbij universiteiten financiering voor security-onderzoek kunnen aanvragen verloopt als volgt.

Eerst moet een onderzoeker een 'pre-proposal' indienen. Dat is een kort voorstel van maximaal 2 A4-tjes waarin hij/zij beschrijft wat voor onderzoek gedaan wordt, welke financiële en/of materiële steun verkregen is van deelnemende bedrijven, hoe het in het

Sentinels programma past en wat de Nederlandse samenleving aan het onderzoek heeft. De programmacommissie van Sentinels besluit vervolgens of het voorstel toegelaten kan worden tot het programma.

Wanneer dat het geval is, kan de onderzoeker een (volledig) projectvoorstel indienen. Hierin dient uitgebreid beschreven te worden wat de wetenschappelijke en maatschappelijke uitdaging is en hoe die aangepakt wordt. Ook is een argumentering van het aangevraagde budget nodig en zijn toezeggingen van de financiële en/of materiële steun van deelnemende bedrijven vereist.

Elk projectvoorstel wordt aan een aantal referenten gestuurd, mensen die expert zijn op het gebied van het voorstel. Deze referenten komen voornamelijk uit het buitenland en werken bij universiteiten, bedrijfsleven, stichtingen en onderzoeksinstituten. Zij vullen een standaardvragenlijst in. Deze lijst bestaat uit 19 vragen van het soort 'wat vindt u van het onderzoeksplan?', 'wat zijn de originele aspecten van het onderzoeksvoorstel?', 'wat zijn de sterke en zwakke punten van het plan waarin beschreven wordt wat de Nederlandse samenleving met het onderzoek kan?' en 'wat voor andere toepassingen van het onderzoek kunt u zich voorstellen?'.

De reacties van de referenten worden anoniem aan de aanvrager voorgelegd die op elk punt een reactie moet geven. Vervolgens worden alle projectvoorstellen met bijbehorend referentencommentaar en reactie van de aanvrager aan de programmacommissie van Sentinels voorgelegd. Deze programmacommissie stelt een prioriteeringsvolgorde voor, waarna de Sentinels stuurgroep (vertegenwoordigers van de financiers van het programma en belangrijke stakeholders uit bedrijfsleven) bepaalt welke voorstellen gehonoreerd worden.

De uitkomst van de eerste ronde is begin december 2004 bekend geworden en wordt in de volgende paragraaf verder besproken. Eind 2005 of begin 2006 zal een tweede ronde starten waarin onderzoeksvoorstellen ingediend kunnen worden. Precieze details

kunnen tegen die tijd op de Sentinels website www.sentinels.nl gevonden worden.

Uitkomst eerste ronde Sentinelsvoorstellen

In de eerste ronde zijn zes voorstellen gehonoreerd voor een totaalbedrag van 3 miljoen euro. De onderzoekers gaan zich de komende vier jaar buigen over onder meer de volgende onderwerpen.

ProBiTe, Protection of Biometric Templates

De onderzoekers willen biometrische identificatie, zoals vingerafdrukherkenning en irisscans, integreren in security systemen. Bijvoorbeeld om met je vingerafdruk toegang te krijgen tot een huisnetwerk waar DVD-spelers, computers en televisies met elkaar verbonden zijn. De templates die voor de herkenning gebruikt worden, moeten ook beschermd worden. Hoe zorg je ervoor dat niemand in kan breken in het herkenningssysteem? En hoe maak je de herkenning zo betrouwbaar mogelijk?

DeWorm, Worm monitoring on Internet backbones

De onderzoekers willen een methode ontwerpen om computers te beschermen tegen wormen, zichzelf vermenigvuldigende programma's die zich razendsnel over de hele wereld kunnen verspreiden en allerlei onheil kunnen aanrichten. De onderzoekers richten zich zowel op de detectie van de wormen als op de vernietiging ervan.

PINPAS JC, Program INferred Power-Analysis in Software for Java Card

JavaCard lijkt een de-facto standaard te worden voor smartcards. De onderzoekers willen een methode ontwikkelen die bescherming biedt tegen aanvallen op dit soort kaarten. In het bijzonder zullen de zogenaamde side-channel attacks onderzocht worden.

JASON, Generic and Secure Remote Management Infrastructure

De onderzoekers willen een secure systeem architectuur ontwerpen met een bijbehorend programmeerparadigma. Doel zijn juist die ambient applicaties waarbij een grote hoeveelheid

smartcards en embedded systemen betrokken zijn.

IPID, Integrated Policy-based Intrusion Detection

De onderzoekers ontwikkelen een methode om indringers zoals wormen en hackers in netwerken te detecteren. Ze werken aan een soort firewall om hele bedrijfsinfrastructuren, zoals bijvoorbeeld het netwerk van ministeries, of de databank van de sociale dienst, te beschermen tegen nieuwsgierige blikken van buitenaf.

Practical Approaches to Secure Cooperation

De onderzoekers willen een brug slaan tussen het cryptografische onderzoek en de 'echte' wereld zodat fundamentele security tools ook gebruikt gaan worden. Cryptografische methoden en technieken die nog niet tot de standaard gereedschapskist van de security engineer behoren zijn een belangrijk onderdeel van dit onderzoek.

Samenvatting

In dit artikel is beschreven wat de aanleiding was tot het oprichten van een nationaal onderzoeksprogramma op het gebied van informatiebeveiliging. De problemen rond het bouwen van grote informatiesystemen zijn beschreven, de doelstellingen van het Sentinels programma, wie van het onderzoek profiteert, de visie en focus en dat deze bepaald zijn in overleg met alle betrokkenen in Nederland. Ook is het belang van kennisuitwisseling beschreven, het budget voor het programma en tenslotte hoe een beoordelingsronde er bij Sentinels uit ziet en wat de resultaten van de eerste ronde zijn.

Meer informatie over Sentinels is te allen tijde te vinden op de Sentinels website, www.sentinels.nl, of bij de auteur van dit artikel, Rik D.T. Janssen, rik@stw.nl. Hier kunt u zich ook opgeven als u geïnteresseerd bent in het bijwonen van de multidisciplinaire workshops die in de paragraaf 'kennisuitwisseling' besproken zijn. Op de website is ook een korte Engelstalige beschrijving van dit programma te vinden: www.sentinels.nl/sentinelsnut-shell.pdf. Deze beschrijving bevat ook links naar andere relevante documenten.