Institute for Computing and Information Sciences

SECURITY OF SYSTEMS

Faculteit der Natuurwetenschappen, Wiskunde en Informatica

Postadres:
Postbus 9010
6500 GL Nijmegen

Bezoekadres:
Toernooiveld 1, Kamer HG 02.076
6525 ED NIJMEGEN

Telefoon 024-3653133
Fax 024-3652298

http://www.niii.ru.nl/

Vaste commissie voor Verkeer en Waterstaat
Tweede Kamer
Postbus 20018
2500 EA DEN HAAG

Ons kenmerk	Uw kenmerk	Doorkiesnummer	Datum
08.001/BJ/MvK		+31 24 365 22 36	22 januari 2008

Betreft	E-mail
Hoorzitting 31 januari a.s.	B.Jacobs@cs.ru.nl

Geachte Leden van de Tweede- Kamercommissie Verkeer en Waterstaat,

Allereerst mijn dank voor de uitnodiging voor de hoorzitting van 31 januari 2008. Ik maak bij deze graag gebruik van de daarbij horende mogelijkheid een schriftelijke toelichting te geven.

Het is wellicht nuttig eerst iets van mijn achtergrond te schetsen. Ik ben hoogleraar (in Nijmegen en ook in Eindhoven) op het gebied computerbeveiliging. Dat is een actueel (en m.b.t. ABvM relevant) onderwerp, met een eigen invalshoek. Waar mijn collega-ICT'ers vaak sterk gericht zijn op functionaliteit ("wat kan ik voor mooie dingen doen met dit computersysteem") wordt in de computerbeveiliging juist sterk gelet op de nare, onbedoelde dingen die ermee kunnen gebeuren, via bijv. misbruik, hacken, of ondermijning, typisch door uitbuiting van kwetsbaarheden. Deze invalshoek is van meet af aan belangrijk, maar wordt vaak onderbelicht (zie bijv. stemmachines of OV-chipkaart) hetgeen kan leiden tot aanzienlijke schade, vertraging en verspilling. Ook bij ABvM bestaat het risico dat na jaren werk en na investering van honderden miljoenen euro's een student toont hoe men gratis kan reizen.

Dit beveiligingsperspectief is dus ook voor ABvM zeer relevant. Automobilisten hebben er immers mogelijk financieel voordeel bij wanneer het systeem niet functioneert zoals het zou moeten: het is daarom verstandig uit te gaan van een "vijandige" houding van tenminste een deel van de gebruikersgroep. Sommigen zullen moedwillig proberen het systeem niet naar behoren te laten functioneren. Daar dient bij het ontwerp van begin af aan rekening mee te worden gehouden.

Ik zal mij in het vervolg concentreren op twee punten: openheid en architectuur.

1. Openheid

Het wekt in eerste instantie wellicht verwondering dat openheid een belangrijk aspect is van beveiliging. Als een tegenstander bepaalde dingen niet gemakkelijk te weten kan komen, kost het meer moeite om beveiliging te doorbreken. In werkelijkheid liggen de zaken toch anders en is vooral belangrijk welke dingen onbekend zijn. De werking van een goed slot bijvoorbeeld, mag best bekend zijn. Veel belangrijker is dat een inbreker niet gemakkelijk alle sleutels uit kan proberen, of anderszins kan uitvinden welke sleutel de juiste is. Het gaat erom dat er veel verschillende sleutels zijn, van

goede kwaliteit (met veel verschillende patronen van sleufjes etc.). Sterker nog, door de werking van het slot openbaar te maken gaat het beveiligingsniveau omhoog: de fabrikant wordt gedwongen werkelijk duidelijk te maken dat zijn slot echt goed is, zonder te appelleren aan blind vertrouwen. Verder kunnen eventuele ontwerpfouten bij openbaarmaking sneller gedetecteerd en verbeterd worden. Kortom, het is een goede zaak een fabrikant te dwingen publiek duidelijk te maken dat zijn slot echt goed is, en niet te accepteren dat hij een beroep doet op (blind) vertrouwen.

Dit geldt des te sterker in de ICT. Openheid is belangrijk voor veiligheid en vertrouwen. Wanneer fabrikanten geen openheid m.b.t. de kwaliteit van de beveiliging willen geven is dat een reden tot wantrouwen. Met stemmachines en OV-chipkaarten hebben we daar de negatieve gevolgen van gezien (en met z'n allen de kosten van moeten dragen). Er werd gezegd: "het is veilig, maar we kunnen niet zeggen hoe of waarom, maar vertrouw ons maar", terwijl vervolgens bleek dat er toch beveiligings-problemen waren. Zoiets is dodelijk.

Deze lessen m.b.t. openheid beginnen langzaam door te dringen. De door de Kamer ondersteunde nota "Nederland Open in Verbinding" van staatssecretaris Heemskerk is een belangrijke stap. Bij het nadenken over een nieuwe generatie stemcomputers wordt nu ook langs deze "open" en “transparante" lijnen gewerkt. En bij het nieuwe biometrische paspoort is al eerder van begin af aan gewerkt met open standaarden, die internationaal ontwikkeld en gepubliceerd zijn door de ICAO. Het paspoort is inderdaad veel beter beveiligd dan de OV-chipkaart (natuurlijk ook omdat er een duurdere chip in zit).

Welk systeem er ook gekozen zal worden voor ABvM, deze openheid is van cruciaal belang, ten behoeve van beveiliging en (publiek) vertrouwen. Tevens kunnen door het gebruik van open ontwerp en open standaarden mogelijk andere diensten van de te ontwikkelen infrastructuur gebruik maken. Verder neemt de leveranciersafhankelijkheid af. Met betrekking tot deze openheid dient de overheid naar mijn mening een duidelijk sturende (en kaderstellende) rol te hebben, vanuit een eigen onderbouwde visie.

2. Architectuur

Informatici worden vaak gezien als architecten van de digitale wereld. Ze zijn echter steeds vaker ook architecten van de sociale wereld: door de manier waarop we onze ICT-infrastructuur inrichten ontwerpen we belangrijke (machts)structuren in onze samenleving. Het gaat dan met name om wie er toegang heeft tot welke informatiestromen. Informatie is immers macht, en bescherming van individuele belangen van burgers is (helaas) vaak afhankelijk van sturing en regulering door de overheid.

Ook bij ABvM speelt dit punt in belangrijke mate. Het spitst zich toe op de vraag of gedetailleerde locatiegegevens van individuele voertuigen centraal of decentraal (in de kastjes in de voertuigen) opgeslagen dienen te worden. In het laatste geval hoeft periodiek alleen geaggregeerde informatie doorgegeven te worden (hoeveel kilometer op welke tarief). Dat is voldoende voor de afrekening, zoals eerder beschreven in het "plan Pieper".

Een centraal systeem behelst meer centrale controle en centrale macht. Deze informatie kan ingezet worden - en dat zal ongetwijfeld op den duur gebeuren - voor opsporing, monitoring, preventie (bijv. via datamining) en autorisatie. Bij dat laatste kan gedacht worden aan de mogelijkheid dat vooraf toestemming gevraagd en gekocht moet worden voor een autorit via een bepaalde route. Al deze mogelijkheden kunnen handig zijn. Het is echter een politieke vraag of we een samenleving willen met een dergelijke vergaande mate van centrale machtsconcentratie.

Voor veel mensen is een dictatuur veiliger dan een democratie. In een democratie gedragen individuen zich autonoom en onvoorspelbaar, hetgeen risico's met zich meebrengt. Dat kan een reden zijn om zo'n dictatuur maar (gedeeltelijk) in te voeren, door steeds meer middelen en structuren daartoe gereed te zetten. Maar onvoorspelbaarheid en dynamiek zijn ook wezenlijke kenmerken die onze samenleving succesvol en de moeite waard maken.

Er zijn ook technische nadelen aan een centraal systeem. Het is kwetsbaar voor aanvallen met grote gevolgen, waardoor locatiegegevens massaal op straat kunnen komen te liggen (en bijvoorbeeld gekeken kan worden welke mensen de laatste tijd in hoerenbuurten zijn geweest). Ook is onbedoeld verlies van centraal verzamelde gegevens een reëel risico, zie bijv. de affaire met de kinderbijslag-gegevens in het Verenigd Koninkrijk. Verder zal er meer communicatie plaats moeten vinden (tussen voertuigen en het centrale opslagpunt), waardoor de kosten stijgen.

Een decentrale structuur geeft burgers de mogelijkheid om zelf de detailgegevens uit het kastje in hun auto te lezen en te controleren, bijv. op hun eigen PC (via bijv. een USB-poort of een geheugen-kaartje). Het systeem kan desgewenst zo ingericht worden dat opsporingsdiensten selectief toegang hebben tot de gegevens, bijv. op basis van goedkeuring van hogerhand. Dat kan zonder dat de automobilist het (gemakkelijk) merkt. Op een dergelijke wijze kan een redelijke balans worden verkregen tussen gerechtvaardigde opsporingsbelangen en de privacy van burgers.

Dit tweede punt laat zich samenvatten als "architectuur is politiek". Ook op dit punt is heldere aansturing en kaderstelling door politiek en overheid gewenst, zodat dergelijke ingrijpende architectuurbesluiten niet overgelaten worden aan (commerciële) partijen met hun eigen agenda. Zoals we bij de OV-chipkaart zien komen de (privacy)belangen van burgers dan snel in het geding.

Ik kijk uit naar de hoorzitting op 31 januari, waar ik bovenstaande (en andere) punten desgevraagd graag nader met u bespreek. Voor de goede orde meld ik dat ik deze brief als openbaar beschouw.

Met gevoelens van hoogachting,

Prof. dr. B.P.F. Jacobs