



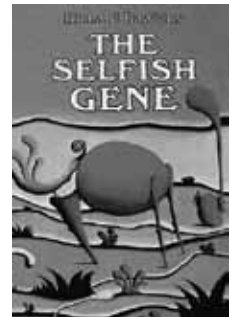
# 'I'

Frank Brokken is security manager bij het CIT. Met het instellen van deze functie probeert de RUG het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column houdt Frank ons op de hoogte van de stand van zaken met betrekking tot zijn missie.



**I**edereen weet natuurlijk dat 'I' de Engelse vertaling is van 'ik'. Schept dat nou een ander licht op 'iPhone' en 'iPad'? De popgroep Alan Parsons Project bracht in 1977 de elpee 'I Robot' uit. Er is een Wikipedia-pagina aan gewijd aan dit album: [http://en.wikipedia.org/wiki/I\\_Robot\\_\(album\)](http://en.wikipedia.org/wiki/I_Robot_(album)).

De popgroep was voor het onderwerp van het album geïnspireerd door de Amerikaanse schrijver en geleerde Isaac Asimov, u vast wel bekend. Zo niet, dan kunt u wederom voor meer informatie terecht op Wikipedia: [http://en.wikipedia.org/wiki/Isaac\\_Asimov](http://en.wikipedia.org/wiki/Isaac_Asimov).



*I robot...the story of the rise of the machine and the decline of man, which paradoxically coincided with his discovery of the wheel...and a warning that his brief dominance of this planet will probably end, because man tried to create robot in his own image.*



## Prachtige infrastructuur

Nou ben ik niet zo'n cultuurpessimist, hoewel Richard Dawkins in 1976 in zijn boek 'The Selfish Gene' ook al verkondigde dat de essentie van het bestaan niet zozeer de propagatie van onze genen maar van onze 'memen' zou zijn, kort samengevat: van 'ideeën, concepten en filosofieën'.

Informatieverwerkende systemen zijn misschien nog niet zo goed in het genereren van nieuwe ideeën en filosofieën, maar we hebben natuurlijk inmiddels wel een prachtige infrastructuur gecreëerd die voor een waanzinnig snelle en efficiënte verspreiding van ideeën kan zorgen.

De voorloper van ons aller internet, het ARPANet (<http://en.wikipedia.org/wiki/ARPANET>), was in de Verenigde Staten primair bedoeld om militaire Command & Control informatie te kunnen transporteren wanneer de VS zou worden geconfronteerd met een massieve aanval vanuit het toenmalige Oostblok.

Hoera! De infrastructuur is er dus al. Als wat Richard Dawkins stelde waar is, dan kunnen die computers en hun netwerken dus al heel goed snel informatie verspreiden. En als dat is waar het eigenlijk om gaat, waarom heb je dan eigenlijk nog mensen nodig?

## Dominante plaats

Inmiddels hoor je niet meer zoveel over de gedachte dat de robots het zullen overnemen. Maar misschien is dat ook wel zo omdat dat al is gebeurd, en een nieuwe generatie zich helemaal niet meer kan voorstellen dat het ook anders kan.

Zo kregen wij onlangs bezoek van vrienden. Voorzien van attributen om het barre



bestaan op de Oostumer wierde (<http://nl.wikipedia.org/wiki/Oostum>) het hoofd te kunnen bieden, installeerden ze zich ter plekke voor een weekendje Oostum. Uiteraard ook voorzien van iPhones, want wie momenteel niet in het bezit is van een I\*-apparaat loopt toch echt wel hopeloos achter.

Toch heeft het mij verbaasd hoe dominant de plaats is die de iPhone in het leven heeft ingenomen. Letterlijk onophoudelijk moet de iPhone worden geraadpleegd. Icoontje hier, icoontje daar, de iPhone staat altijd voor u klaar. En dat merk je. Is er mail? Heeft iemand gereageerd op mijn getwitter? Is er nog iets leuks te doen in deze omgeving? Waar ben ik eigenlijk (geografische coördinaten en een plattegrond is wel het minste wat je voor je moet hebben).

Een fenomenologische studie rond de jaren zeventig stelde dat een automobilist z'n eigen dimensies onbewust uitbreidt tot de grenzen van z'n auto; zou hetzelfde gelden voor de I\*-gebruikers? Alleen dan worden de dimensies wel heel groot. Zoiets als 'de wereld'.

## Viagra-mail

Helaas zitten er in die wereld ook mensen met minder goede bedoelingen. Ik was onlangs op de SURFcert/SURF IBO-conferentie, waar tijdens een presentatie het fenomeen 'botnet', contractie van 'robot net', werd belicht: computers die in feite zijn overgenomen door een 'botmaster' die de computers kan laten doen wat-ie wil.

Hoe wordt je computer nou een 'botje'? Meestal doordat de gebruiker weer eens op een attachment of link heeft geklikt en zo zelf de malware die je computer tot bot maakt, binnenhaalt. Want zo gaat dat. Als voorbeeld werd een kort spam-mailtje getoond waarin Viagra (u wel bekend, en zo niet: <http://en.wikipedia.org/wiki/Sildenafil> voor meer informatie) werd aangeboden. Dat wordt dan zo'n beetje verspreid, en mensen klikken op de link. Nou niet direct verder lezen, maar even raden hoeveel mensen per dag op zo'n link klikken.

Niet alle besturingssystemen zijn even gevoelig voor dit soort malware, maar ook al zou 50% van alle computers dat wel zijn, dan heb je met een kleine veertigduizend reacties per dag op je uitgestuurde spam toch zo'n twintigduizend botjes per dag geogost. Dat is de moeite waard.



## Fatsoenlijk beschermd

En hoe zit dat met de iPhones en iPads? Hoe veilig zijn die eigenlijk? Tja. De veiligheid daar heeft niet alleen te maken met software, hoewel ook voor 'iPhones and friends' geldt dat software daar verouderd, en dat oude software oude (en dus bekende) bugs heeft die door de 'bad guys' worden misbruikt.

Dwivedi, Clark en Thiel noemen in hun boek 'Mobile Application Security' (McGraw-Hill, 2010) een hele serie risico's waar de gebruiker mee wordt geconfronteerd.

Het vervelende is dat die risico's snel uitzaaien naar de persoonlijke en beroepsmatige domeinen. iPhones worden uiteraard, en nog eenvoudiger dan laptops, gestolen of ze raken verloren. De doorsnee iPhone bevat een schat

aan persoonlijke informatie en mogelijkheden om binnen te dringen in een elektronische werkomgeving. Tenzij deze informatie fatsoenlijk is beschermd (lees: versleuteld) is de informatie ook bruikbaar voor iedereen die de iPhone in handen krijgt. Doorgaans is een PIN de enige toegangseis, en die kan zonder al te veel moeite worden gekraakt. Opgeslagen wachtwoorden doen de rest.

## Het Wilde Internet

Oude software is al genoemd, maar minstens zo belangrijk is verstandig gebruik door de eindgebruiker. Verwacht mag worden dat deze binnen zeer afzienbare tijd het doelwit wordt voor de bad guys, aangezien de doorsnee gebruiker nou eenmaal uitgaat van de filosofie 'hij moet het gewoon doen'. Updates zijn niet altijd even eenvoudig uit te voeren; certificaten vaak moeilijk te vervangen of te installeren (als dat al gebeurt; de meeste gebruikers klikken een waarschuwing over een ongeldig, onbekend, of afwezig certificaat immers gewoon weg en vervolgen hun tocht in het 'Wilde Internet' daarna onbeschermd).

Meer nog dan voor desk- en laptops geldt voor mobiele apparatuur 'be prepared' ([http://en.wikipedia.org/wiki/Scout\\_Motto](http://en.wikipedia.org/wiki/Scout_Motto)). 'Al is de hacker nog zo snel, een goede beveiligingsmentaliteit stopt hem wel'. Uiteindelijk is het toch weer de gebruiker waar de veiligheid begint en eindigt. 'I' als alfa en omega van een veilig I\*-gebruik. De keuze is aan ons, gebruikers.



Frank B. Brokken  
(well prepared)

