Matthijs Coster
Militaire Inlichtingen- en Veiligheidsdienst (MIVD)
Postbus 20701
2500 ES Den Haag
matthijs@coster.demon.nl

Bart Jacobs
Institute for Computing and Information Sciences (ICIS)
Radboud Universiteit Nijmegen
Heyendaalseweg 135
6525 AJ Nijmegen
b.jacobs@cs.ru.nl

Klaas Landsman
Institute for Mathematics, Astrophysics and Particle Physics (IMAPP)
Radboud Universiteit Nijmegen
Heyendaalseweg 135
6525 AJ Nijmegen
landsman@math.ru.nl

De overval: Fox-IT

Bescherming van staatsgeheimen, digitaal rechercheonderzoek, beveiligingsexpertise: Fox-IT levert wereldwijd wiskundig onderbouwde security- en intelligence oplossingen aan overheden en maatschappelijk belangrijke organisaties. Matthijs Coster, wetenschappelijk onderzoeker crypto-analyse bij de Militaire Inlichtingen- en Veiligheidsdienst, hoogleraar Digital Security Bart Jacobs en NAW-medewerker Klaas Landsman overvielen het bedrijf op 6 maart 2009.

Ronald Prins (40) is net terug uit Dubai en vliegt morgen naar Aruba. Hij is één van de drie directeuren van Fox-IT, dat naast het hoofdkantoor in Delft ook nevenvestigingen in Aruba en Engeland heeft. Als we samen met hem de bedrijfskantine inlopen schakelt hij een rode lamp in, die de lunchende medewerkers erop attendeert dat er bezoekers zijn. Gesprekken over staatsgeheimen worden onmiddellijk gestaakt en maken plaats voor de vriendelijke vraag wie wij zijn. Wiskundigen? Ja, mompelt men, daar hebben we er wel een paar van in huis. Maar de meerderheid van de bijna honderd medewerkers (onder wie twintig vrouwen) komt uit gebieden als informatica, natuurkunde en elektrotechniek. Prins zelf heeft wel degelijk wiskunde gestudeerd. Hij was als scholier al geïnteresseerd in cryptografie en raakte via het lezen van het legendarische blad *Hack-tic* van Rop Gongrijp en anderen betrokken bij de hackers-scene. Hij studeerde na een stage bij Digicash af aan de TU Delft op *applied addition chains*, een slimme manier om met behulp van zo min mogelijk vermenigvuldigingen te machtsverheffen — relevant bijvoorbeeld voor Smartcards. Vervolgens begon hij met promotieonderzoek aan de TU Eindhoven onder leiding van Henk van Tilborg en werkte tegelijk als crypto-analyst bij het Nederlands Forensisch Instituut (NFI, voorheen het Gerechtelijk Laboratorium). Ook bij zijn volgende werkgever, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), vond hij dat het allemaal niet snel genoeg ging. Om zelf achter de knoppen te kunnen zitten richtte hij samen met technisch natuurkundige en voormalig NFI-collega Menno van der Marel in maart 1999 het bedrijf Fox-IT op. Promoveren zou er niet meer van komen, de potentiële doctorstitel werd verruild voor "het waarmaken van een jongensdroom" — inclusief Maserati.

Foto: Klaas Landsman

Ronald Prins

Het bedrijf loopt namelijk bepaald niet slecht. De oprichters brachten een flink netwerk mee van hun tijd bij het NFI en konden meteen aan de slag met het verzorgen van trainingen en het uitvoeren van opdrachten voor de overheid (zie kader). Tien jaar later blijft de Nederlandse staat verreweg de belangrijkste opdrachtgever, maar heeft Fox-IT ook meer dan honderd bedrijven als klant om de missie van het bedrijf uit te voeren: het bijdragen aan een veiligere samenleving (*"Making technical and innovative contributions for a more secure society"*). Hierbij moeten we eerder denken aan de wereld van James Bond dan aan die van Pieter van Vollenhoven: het gaat bij Fox-IT om zaken als de bescherming van staatsgeheimen, digitaal rechercheonderzoek voor grote fraude- en hackingonderzoeken, *security audits* binnen complexe en vertrouwelijke omgevingen, *security monitoring* voor de bewaking van informatie binnen organisaties, en tenslotte de ontwikkeling van software voor

Samenwerking met NBV

De meeste opdrachten van Fox-IT komen uit het veiligheidsdomein van de Nederlandse overheid, geen ministerie uitgezonderd. Daarbij heeft Fox-IT intensief contact met het Nationaal Bureau voor Verbindingsbeveiliging (NBV). Dit is een aparte club binnen de Algemene Inlichtingen- en Veiligheidsdienst (AIVD, de voormalige BVD) die een belangrijke vinger in de pap heeft bij de technische middelen die de Rijksoverheid gebruikt om haar geheimen te beschermen. Er werken veel wiskundigen (vooral cryptologen) en informatici. Belangrijke NBV-taken zijn het beheer van cryptografische sleutels (bijvoorbeeld voor Defensie of Buitenlandse Zaken) en de beoordeling van beveiligingsproducten (waaronder de verderop genoemde Tiger telefoons). Fox-IT werkt nauw samen met het NBV, bijvoorbeeld bij de ontwikkeling van de nieuwe 'RedFox' cryptochip voor de overheid. Dit is de beoogde opvolger van de huidige generatie cryptochips die in gebruik zijn voor de bescherming van staatsgeheimen.

het analyseren van getapt internetverkeer.

Tot voor kort maakte de ministerraad gebruik van BlackBerry, een Personal Data Assistant (PDA) die kan worden gebruikt voor mobiele telefonie, mobiel internet en e-mail. Al het dataverkeer wordt versleuteld over de lijn, maar op de BlackBerry server wordt het dataverkeer weer ontcijferd. De BlackBerry kwam in opspraak na speculaties over de Amerikaanse regering die de BlackBerry stelselmatig zou afluisteren. Inmiddels maken de Nederlandse bewindslieden gebruik van het door Fox-IT ondersteunde systeem van Tiger telefoons. Hoe deze Tigers precies werken moet helaas geheim blijven, maar een veel gebruikte technologie voor sleuteluitwisseling in dit soort systemen is de zogenaamde Diffie-Hellman key exchange (zie kader).

Het gesprek komt op het vertrouwen tussen landen. In hoeverre kunnen we als Nederlandse staat vertrouwen dat we niet worden afgeluisterd door een andere staat of misschien zelfs een bondgenoot? De hierboven genoemde speculaties over het mogelijk afluisteren door de Amerikaanse regering voorspellen niet veel goeds. Fox-IT streeft ernaar om de Nederlandse overheid veilig te laten communiceren. Het irriteert Ronald Prins dan ook mateloos als een Nederlandse ambtenaar een paar tientjeswil besparen door Nederlandse beveiligingstechnologie te vermengen met goedkopere componenten van onbekend fabricaat.

De business unit van Fox-IT die zich richt op het maken van producten voor de bescherming van staatsgeheimen, zoals de Tiger telefoons, heet *Crypto* en zit in de directieportefeuille van Prins. De hele Crypto-group blijkt zich te bevinden in een zogenaamde Verboden Ruimte, waar we overigens zonder al te veel aandringen een kijkje mogen nemen. Al wordt ons bezoek in het logboek geregistreerd, de sfeer lijkt uitgesproken relaxed en de situatie verschilt slechts in één opzicht van een normaal ICT-bedrijf: er bestaat geen internetverkeer tussen deze Verboden Ruimte en de buitenwereld (met uitzondering van twee PC's in een hoekje, die echter niet met de andere computers in de ruimte verbonden zijn). De medewerkers van de Crypto-group kunnen dus niet van huis inloggen op hun computer op het bedrijf. Navraag leert dat dit niet leidt tot extreem lange werkdagen; medewerkers die tot diep in de nacht doorwerken zouden wantrouwen opwekken. *Nadenken* over geheime apparatuur en versleuteling mag wel buiten de werkplek; het gebeurt dan ook vaak dat men juist op de fiets of onder de douche dé oplossing vindt.

Het is opmerkelijk dat de algehele sfeer van geheimhouding waarin de Crypto-group werkt die van de opdrachtgevers weerspiegelt. Het lijkt onvoorstelbaar voor de standaard internetgebruiker, maar in een high-security omgeving is het (zoals dus ook bij bepaalde onderdelen van Fox-IT zelf) meestal verboden om een fysieke verbinding (hard of wireless) te hebben tussen onderdelen van een netwerk die verschillende rubriceringen hebben (zie kader staatsgeheim). In zo'n situatie dient gebruik te worden gemaakt van een floppydisk, USB-stick, cd of dvd, met als gevolg dat dergelijke media na gebruik wellicht vernietigd dienen te worden. De gebruiker van een machine met gerubriceerde informatie kan geen contact maken met de buitenwereld, laat staan zijn e-mail lezen. Het probleem is daarbij niet zo zeer de datastroom naar de gebruiker toe, maar de potentiële lekkage van hem vandaan. Dit probleem heeft de Crypto-group opgelost met de *Fort Fox Data Diode*. Het is zelfs mogelijk dat iemand op een gerubriceerd netwerk met deze vinding zijn e-mail van internet kan lezen, maar het is niet mogelijk op deze e-mail te reageren, omdat er in dat geval informatie van het gerubriceerde netwerk zou weglekken naar het (ongerubriceerde) internet.

Prins heeft ook een tweede business unit in zijn portefeuille, genaamd *FoxReplay*. Deze houdt zich bezig met de interceptie van dataverkeer in opdracht van politie en intelligence organisaties wereldwijd; de directeur meldt met enige trots dat Fox-IT wereldleider is op het gebied van technologie voor het aftappen van het internet.

Maar hoe zit het nu toch met de wiskunde bij Fox-IT? Prins geeft ruiterlijk toe dat hij er in zijn werk zelden tot nooit gebruik van

Diffie-Hellman key exchange.
Zij G een eindige cyclische groep met generator g; in de oorspronkelijke versie van het protocol is $G = \mathbf{Z}_p$ (de multiplicatieve groep van gehele getallen modulo p voor een priemgetal p) en is g een primitieve wortel modulo p. Als de orde van G voldoende groot is (in dit voorbeeld is dat zo als p in binaire notatie uit minstens honderd cijfers bestaat), dan blijkt het praktisch onmogelijk te zijn om x terug te vinden uit g^x (mits ook x voldoende groot is); dit is het 'discrete logaritme probleem'. Deze x is de geheime sleutel die de telefoon van van beller A bij ieder gesprek opnieuw aanmaakt. Als eerste stap van de versleuteling stuurt A zijn gesprekspartner B openlijk g^x. De telefoon van B maakt nu zijn geheime sleutel y aan, en stuurt A — wederom openlijk — g^y. Zonder y te hoeven kennen berekent A's telefoon nu $(g^y)^x = g^{xy}$. Omgekeerd berekent B $(g^x)^y$, hetgeen ook gelijk is aan g^{xy}! Beiden hebben nu dezelfde geheime sleutel g^{xy} in handen en kunnen versleuteld gaan bellen. Het fascinerende is dat een gedeeld geheim wordt verkregen door uitsluitend publieke boodschappen uit te wisselen. Dit idee, een keerpunt in de cryptografie, is in 1976 gepubliceerd door de cryptologen Whitfield Diffie en Martin Hellman.

Foto: Klaas Landsman

Bart Jacobs en Matthijs Coster voor het Fox-IT gebouw in Delft

Soorten van staatsgeheim

Zeer Geheim
De hoogste classificatie van geheim. Als dergelijk materiaal publiek raakt, dan zou daardoor zeer grote schade kunnen ontstaan t.a.v. de (inter)nationale veiligheid. (Denk aan een offensief tegen de Talibaan)

Geheim
Als dergelijk materiaal publiek raakt, dan zou daardoor grote schade kunnen ontstaan t.a.v. de (inter)nationale veiligheid.

Vertrouwelijk
Als dergelijk materiaal publiek raakt, dan zou daardoor schade kunnen ontstaan t.a.v. de (inter)nationale veiligheid.

Ongerubriceerd
Materiaal dat onder geen van bovengenoemde rubriceringen valt.

Computers (en netwerken) waarop wordt gewerkt met een zekere rubricering dienen gescheiden te zijn van andere rubriceringen.

maakt; zijn typische dag bestaat uit de omgang met klanten ("we babbelen en er komt wel wat uit") en het bedenken van nieuwe investeringen. Hij doet naar eigen zeggen niets technisch meer, maar ziet als voordeel dat hij de techniek eventueel wel aan de klant kan uitleggen.

Om verder te komen met onze vraag voegt de eveneens in Delft afgestudeerde wiskundige Eelse-Jan Stutvoet zich na de lunch bij ons, geflankeerd door (de alweer Delftse) elektrotechnicus Bartek Gedrojc. Ondanks zijn jeugdige verschijning — allerminst een uitzondering in het bedrijf — behoort Stutvoet qua dienstjaren tot de oudste medewerkers van Fox-IT, waar hij al tijdens zijn studie een deeltijdbaantje had. Gedrojc werkt daarentegen pas een paar maanden bij het bedrijf: hij is bijna klaar met zijn proefschrift in de cryptologie (begeleiding: Jan van der Lubbe, promotor Inald Lagendijk). Met vooruitziende blik werkte Gedrojc al in 2005 aan de beveiliging van het Elektronisch Patiëntendossier, maar hij hield zich ook bezig met de beveiliging van e-commerce en aanverwante problematiek. Ondanks deze voor de Crypto-groep perfecte achtergrond, en ofschoon zijn coauteur Martin van Hensbergen zelfs bij Fox-IT werkt, kwam Gedrojc er min of meer toevallig terecht.

Maar ja, ook Gedrojc en Stutvoet erkennen dat ze nauwelijks wiskunde gebruiken, al is de cryptologie daar grotendeels op gebaseerd. Het gaat veel meer om slim programmeerwerk rond bestaande cryptografische protocollen, al merkt de laatste op dat het (soms!) handig is om te weten hoe zo'n protocol precies werkt. "Handig maar niet noodzakelijk", dat is het oordeel over zijn wiskundige achtergrond. Zoals we van talloze werkgevers horen, worden wiskundigen niet aangenomen om hun kennis van algebra en meetkunde, maar omdat men verwacht dat ze analytisch kunnen denken (en dan niet in de zin van ε en δ) en, laten we het ruiterlijk toegeven, slim zijn.

Hoe gaan deze slimmeriken om met het thema geheimhouding? Typerend voor Fox-IT is namelijk dat als het product al niet geheim is, de klant dat wel is. Alle medewerkers worden dan ook door de AIVD gescreend. Is het niet vervelend dat je zelfs met je partner niet over sommige zaken mag praten? Het blijkt geen issue, al helemaal niet buiten de Cryptogroep. Maar zelfs binnen die afdeling zit de geheimhouding hem vaak in technische details waar je sowieso niemand mee lastig zou willen vallen. In ieder geval is er nog nooit iets gelekt en is nog nooit iemand ontslagen.

Dit leidt wel tot de vervolgvraag naar de cultuur binnen Fox-IT: zijn het hackers in het diepst van hun gedachten, of eerder JOVD-ers die onze rechtsstaat willen beschermen? Het zit tegen het eerste aan. Om recht te doen aan de kernwaarde van Fox-IT, 'leading edge innovation', moeten de medewerkers op een speelse manier de grenzen van de technologie op willen zoeken, en om de tegenstander te doorgronden en te simuleren moeten ze ook niet vies zijn van de grenzen van de moraal. Sterker nog: "Je mag de grens opzoeken in het grijze gebied tussen wat precies wel en niet mag." Morele dilemma's zijn er niettemin op een ander vlak: wil je meewerken aan aftapsoftware voor het internet waarmee de geheime dienst van Saudi-Arabië homo's gaat vervolgen om hun hand af te hakken — of, zoals in Iran, ze aan een hijskraan op te hangen? Het is het typische probleem van alle *dual use goods*: met dezelfde technologie waarmee een zelfmoordaanslag op een markt kan worden voorkomen, gaat ook de repressie of de georganiseerde misdaad aan de haal. Aan Tiger telefoons zullen criminelen overigens niet snel komen, maar bijvoorbeeld de door Gongrijp geproduceerde cryptofoon (waarin het Diffie-Hellman protocol wordt gebruikt) kunnen ze gewoon kopen.

Al is de wiskundige spoeling dan dun, het Overvalteam ging enthousiast naar huis en kan Fox-IT van harte aanraden aan al dan niet gepromoveerde wiskundigen op zoek naar een leuke baan. Heeft het ook daadwerkelijk zin om te solliciteren? Jawel! Prins verzucht dat het moeilijk is om goede medewerkers te vinden en dat hij daar permanent naar op zoek is. "Ik zie vaak het verschil tussen de manier waarop een academicus iets oppakt en een hbo-er." Hij zoekt de combinatie van de slimheid van een academisch opgeleid wiskundige of fysicus met de "handigheid achter het toetsenbord". Een informaticus die alles al in huis heeft is natuurlijk helemaal mooi. Tegen alle managementfilosofieën in vult Prins geen vacatures op, maar bouwt hij een functie om zo iemand heen. Wie het leuk vindt mag na drie tot vijf jaar het management in, zoals bij vele andere technologiebedrijven, maar zo niet, dan niet. "Mensen worden beoordeeld op hun creativiteit."

Data diode

Een succesvol product van Fox-IT is de zogenaamde data diode. Dit systeem laat gegevens slechts in één richting door. Het eenrichtingsverkeer wordt uiteindelijk op een fysiek niveau met hardware gerealiseerd door alle overdracht via een LED (light emitting diode) en een lichtsensor te laten verlopen.

Het grote voordeel van de data diode, namelijk het garanderen van eenrichtingsverkeer, behelst tevens een nadeel: bij veel communicatieprotocollen worden korte controleberichten teruggestuurd die aankomst bevestigen of juist vragen om herzending. Sommige diensten kunnen dus slechts in beperkte mate via de data diode lopen. Je kunt er je mail bijvoorbeeld wel mee lezen, maar niet versturen.

Wie wil zoiets? De klanten van Fox-IT hebben vaak verschillende netwerken, met verschillende niveaus van vertrouwelijkheid. Het laagste niveau heeft een verbinding met het internet, maar de andere niveaus zijn daar fysiek van gescheiden. Overdracht van gegevens tussen zulke netwerken kan in de praktijk alleen plaatsvinden via een fysieke drager, zoals een USB stick of een dvd. Deze omslachtige 'air gap' methode draagt allerlei risico's in zich; de USB sticks en dvd's moeten bijvoorbeeld na de overdracht zorgvuldig gewist of vernietigd worden. Met een data diode daarentegen kun je wel degelijk zorgeloos informatie van laag (zwart) naar hoog (rood) laten lopen. Zodoende kan de generaal op zijn zeer vertrouwelijke netwerk zien wat er gaande is in de onbetrouwbare buitenwereld.