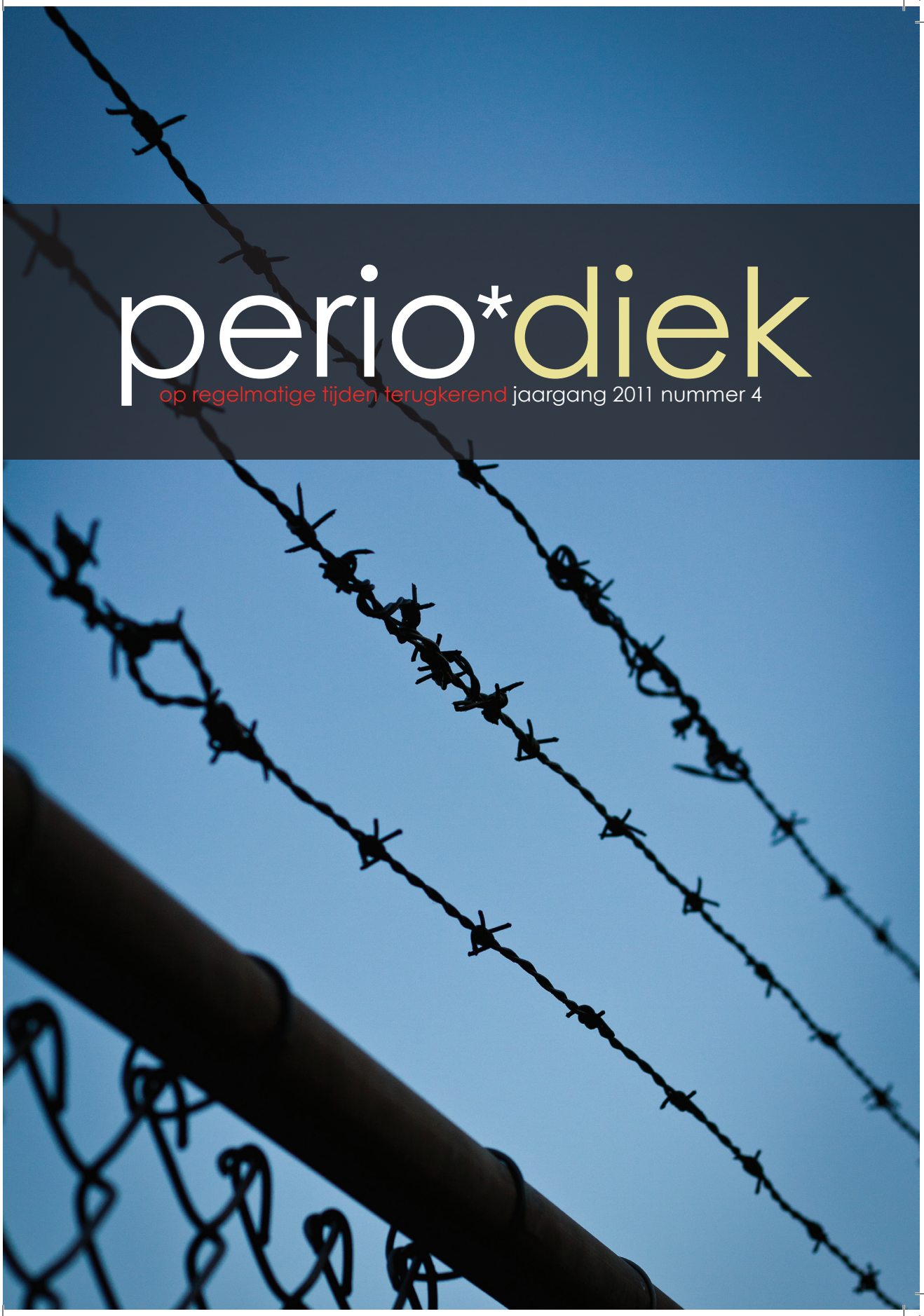
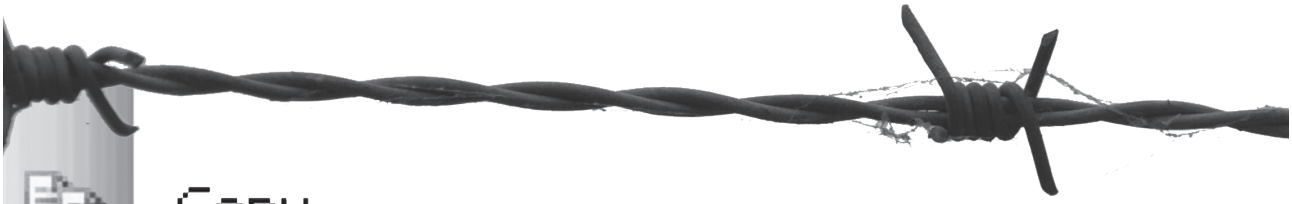
perio*diek

op regelmatige tijden terugkerend jaargang 2011 nummer 4



Inhoud



Copy

Paste

12 Een verslag in één nacht

We gebruiken allemaal het internet om informatie op te zoeken. maar denken we er wel altijd goed aan om alle bronnen te vermelden?

8 Secure communication

Hoe kunnen we communicatie in tijden van steeds snellere computers nog beveiligen?

En verder

4 In het nieuws

7 Van de secretaris

14 Ghost in the Wires

16 Te amo México

21 Toegepaste computersecurity

24 NAVO en C++

34 Criminele burger

20 Perio schrijfwedstrijd

Doe mee aan de schrijfwedstrijd en win een van de drie Kindle e-readers!

29 Tax me if you can

Waarschijnlijk betaal jij altijd netjes je belasting, maar doet iedereen dat? In dit artikel leer je hoe sommige mensen voorkomen dat ze belasting moeten betalen.

Van de redactie

Het thema van deze Periodiek is criminaliteit. Omdat het belangrijk is om te weten waar je over schrijft moest de redactie zich verdiepen in het onderwerp. Dus mengden we ons in het criminele circuit van Groningen. We stapten laag in, 's nachts op de grote markt waar fietsen illegaal verhandeld worden. Maar al snel klommen we hogerop en bevonden we ons diep in de onderwereld van Groningen. Omringd door de grootste criminele bazen van Noord-Nederland, konden we alle fijne details van het criminele circuit ontdekken. Waar we ook achterkwamen was dat het geen lieve wereld is. Toen het eenmaal uitlekte dat wij voor de perio werkten en binnenkort alle details uit het criminele circuit wilden uitlekken, werden we opgepakt. Geblinddoekt en terwijl we onder shot werden gehouden, werden we in een zwart busje gegooid en naar het Zernike gereden. Ze gijzelden ons een weekend lang in de FMF-kamer. Hier werden wij gedwongen de hele perio over de kop te gooien, al het materiaal dat we verzameld hadden te vernietigen en een nieuwe perio te maken. Behalve dit stukje van de redactie, die we er nog wel in hebben weten te smokkelen, zoals het een echte crimineel betaamt.

— Armin

Redactie Bart Visser, Herbert Kruitbosch, Paulus Meessen, Armin Palavra.

Scribenten Frank Brokken, Esther van der Pol, Caspar van der Wal.

Adverteerder TMC (p. 6), Thales (p. 28), Philips (p. 32), Technolution (p. 36).

Ook adverteren? Neem contact op met bestuur@fmf.nl.

Oplage 1200 stuks

Druk Scholma

ISSN 1875-4546

De Periodiek is een uitgave van de Fysisch-Mathematische Faculteitsvereniging en verschijnt vijf keer per jaar. Eerder uitgebrachte Periodieken zijn na te lezen op perio.fmf.nl. De redactie is te bereiken via perio@fmf.nl.

In het nieuws

Licht uit vacuum

Wetenschappers hebben aangetoond dat fotonen uit vacuüm gemaakt kunnen worden. Hiermee wordt een oude kwantumtheorie bewezen waarin wordt beweerd dat in vacuüm virtuele deeltjes kunnen bestaan. Tijdens het onderzoek werd een magnetisch veld gebruikt dat miljarden keer per seconde van richting werd veranderd. Hiermee wordt een apparaat aangedreven dat gevoelig is voor magnetisme. Het geheel werkt volgens de onderzoekers als een vibrerende spiegel waar virtuele deeltjes tegenaan botsen. Virtuele deeltjes zijn de beschrijving van een fenomeen waarbij deeltjes in een vacuüm spontaan ontstaan en weer verdwijnen. Door de spiegel krijgen de deeltjes voldoende energie om te materialiseren, waarna ze gedetecteerd kunnen worden.

chalmers.se

Waarom je vergeet wat je zocht als je een nieuwe kamer inloopt

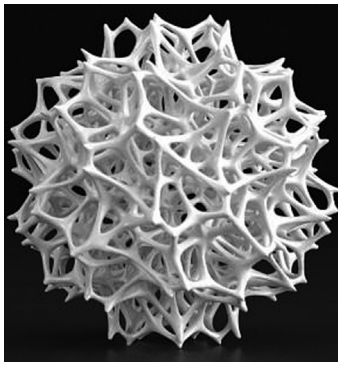
Iedereen kent het wel, je loopt een kamer binnen om iets te doen of te pakken, maar zodra je in de kamer staat ben je al weer vergeten waarom je er heen ging. Dit fenomeen wordt grotendeels veroorzaakt door de deur. Een deur is een soort van grens waar je hersenen een signaal krijgen dat er een herinneringsepisode is gestopt en een nieuwe is begonnen. Je hersenen beginnen dus 'overnieuw'. Deze conclusie werd getrokken door wetenschappers uit Indiana, door proefpersonen door virtule kamers te laten lopen en objecten mee te nemen of te laten liggen. Later werd dan gevraagd de objecten weer te noemen. Het bleek dat personen die dezelfde afstand aflegden, maar niet door een deur heen moesten, veel beter presteerden.

volkskrant.nl

Nieuwe generatie printers

De volgende industriële revolutie kan wel eens dichtbij zijn aangezien machines die objecten in beton en plastic maken steeds goedkoper worden. 3D-printers zouden veel dingen wel eens kunnen veranderen. Met 3-D printers wordt een object laag voor laag opgebouwd. Een groot voordeel hiervan is dat je erg complexe objecten kunt bedenken en maken zonder dat er veel materiaal wordt verspild. Misschien printen we in de toekomst onze eigen objecten wel.

telegraph.co.uk



Spam op het laagste niveau sinds 2008

Het wereldwijde aantal spammail dat wordt verzonden is gedaald tot het laagste niveau in drie jaar. Op dit moment is 70,5 procent van alle mail die verzonden wordt spam, een getal wat heel wat lager is dan in 2010 toen spam nog 90 procent van alle mail voor zijn rekening nam. Deze afname kan worden verklaard door het ontmantelen van twee grote botnets door de FBI eerder dit jaar.

scientificamerican.com

SETI zoekt weer verder

In april dit jaar werd de Allen Telescope Array, zo'n 500 km ten noorden van San Francisco, tijdelijk gesloten wegens budgettaire problemen. Het SETI instituut heeft inmiddels de financiën weer op orde zodat de zoektocht naar buitenaards leven kan worden hervat. Dit nieuws komt extra gelegen gezien het feit dat er recent door de Kepler ruimtetelescoop veel nieuwe kandidaten voor exoplaneten zijn gevonden.

mashable.com

Snelle neutrino´s

Na het recente OPERA experiment werd de wetenschappelijke wereld even op zijn kop gezet. Neutrino's die sneller dan het licht reizen, dat kan toch niet? Wat blijkt, 50 jaar geleden werd

het afwijkende gedrag van neutrino's al gesuggereerd door Jayant Narlikar. In zijn artikel wordt een experiment gesuggereerd met een neutrino emmitor en een ontvanger, ondenkbaar in die tijd. Het artikel analyseert hoe neutrino's zich gedragen in zowel uitdijende als onveranderde *steady state* universums. Narlikar vond dat in een uitdijend universum na de oerknal, neutrino's eerder bij een detector aan kunnen komen dan dat ze uitgezonden werden. Als het artikel wordt ontdaan van de wiskundige formules dan leest het als een goed science-fiction boek. Experimentele fysici hebben er 50 jaar over gedaan, maar misschien wordt door het recente onderzoek weer nieuw licht geschenen op iets wat 50 jaar geleden al geopperd werd.

newscientist.com

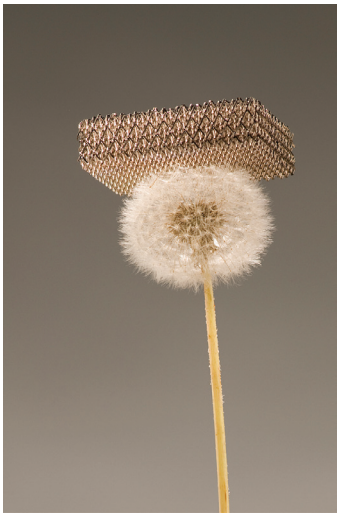
´s Werelds lichtste materiaal

Drie groepen onderzoekers uit de Verenigde staten hebben het lichtste materiaal ter wereld ontwikkeld. Met 0.9 microgram per kubieke centimeter is het twintig keer zo licht als piepschuim, maar wel sterker. Dit is gerealiseerd door het materiaal op te bouwen uit holle nikkel-nanotubes met een wanddikte van 100 nanometer, 1000 maal dunner dan een mensenhaar. Naast de lage dichtheid heeft het materiaal ook de mogelijkheid om ver in te deuken en terug te veren.

tweakers.net

Nano-auto

Ben Feringa en zijn onderzoeksgroep hebben een molecuul ontwikkeld dat zich kan voortbewegen door te roteren. Het voertuig wordt aangedreven door de elektrische energie van een scanning tunneling microscope. De beweging wordt veroorzaakt door vier peddels die zijn bevestigd aan een langwerpig middenstuk. De elektronen veranderen de vorm van de peddels waardoor deze gaan roteren. In tien stappen zou het voertuig zes nanometer moeten kunnen afleggen op een koperen laag in een vacuüm gecontroleerde omgeving. Deze demonstratie wordt als een belangrijke stap gezien in de ontwikkeling van nanomachines. Dit onderzoek stond op de cover van het prestigieuze tijdschrift Nature.



rug.nl

Europa's Extreme Large Telescope is onderweg

Er is begonnen met de bouw van wat de grootste optische-infrarood telescoop ter wereld moet worden. Met een spiegeldiameter van 39,2 meter valt de huidige grootste telescoop in het niet, deze heeft slechts een spiegeldiameter van 11,9 meter. De E-ELT zal gebouwd worden in de Atacama woestijn in Chili.

sciencemag.org

IEDEREEN ONDERNEMEND

WERKONDERNEMERSCHAP

- Langdurige arbeidsrelatie
- Individuele winstdeling
- 1-op-1 carrière coaching
- Werkzaam in een gespecialiseerde, ondernemende businesscel
- Entrepreneurial Lab

TMC Group, technology & ICT-dienstverlener, is specialist in hoogwaardige ondersteuning in de vorm van kennis en advies. Onze vakspecialisten zetten we op projectbasis in bij hoogwaardige opdrachtgevers binnen de profit en non-profit sector.

Met drie member companies bewerken wij de markt: TMC Technology, TMC ICT en Bouwkunde & Civiele Techniek. Specialistische kennis en goede 'soft skills' zijn voor onze mensen vanzelfsprekend. Maar we gaan een stapje verder. Een langdurige relatie, individuele winstdeling, 1-op-1 carrière coaching en gespecialiseerde businesscellen: dat is werkondernemen. Het bewezen werkondernemerschapsmodel biedt continuïteit en flexibiliteit aan onze opdrachtgevers. **Iedereen ondernemend!**

TMC Group
Postbus 700
5600 AS Eindhoven
+31 (0)40 239 2260
info@tmc.nl
www.tmc.nl

TMC GROUP

Van de secretaris

DOOR **RICARDO DE RUITER**

Nadat in de vorige Periodiek de voorzitter een verhaaltje heeft geschreven, is het nu de beurt aan de secretaris. Deze rubriek zal de tweede zijn in een reeks, waarbij elk bestuurslid een keer een pagina vol typt voor ons verenigingsblad.

Allereerst, voor de mensen die mijn gezicht niet eerder hebben gezien: mijn naam is Ricardo de Ruiter, vijfdejaars student theoretische natuurkunde. Sinds eind september heb ik de eer deel uit te mogen maken van het 53e bestuur van de FMF, samen met vier gezellige studiegenoten. Inmiddels zijn we met zijn vijven ruim tweeënhalve maand aan het werk. Elke dag is het nog steeds leuk om met het besturen bezig te zijn. De goede sfeer binnen het bestuur is zeer bevorderlijk voor onze samenwerking.

Terwijl het einde van het kalenderjaar in zicht komt, zijn we druk bezig met allerlei dingen. Zo staat het opruimen van de kamers van de FMF (de NSFW, KNOB en Vectorruimte) op het programma. We hopen de kamers de komende tijd een beetje te herinrichten, om er zo nog prettigere (werk)ruimtes van te maken.

Uiteraard zijn er ook genoeg dagelijkse dingen die moeten gebeuren. Iedere dag zijn wij bestuursleden bezig met onze dagelijkse werkzaamheden. Tussendoor is er natuurlijk ook tijd om gezellig koffie of thee te drinken met de leden. Dit is iets wat ik zelf ook altijd erg leuk vind, om dan gezellig tijdens de pauzes van de colleges even met leden bij te praten.

De ervaring die ik tot nu toe heb met het bestuurswerk zijn door dit soort dingen dan ook ronduit positief. Soms is het wat lastiger werken in de drukte van de NSFW, maar het is toch fijn om de leden om je heen te hebben. Door ook zoveel mogelijk activiteiten af te lopen leer je meer mensen beter kennen en kom je er achter wat er leeft onder de leden.

Een voorbeeld hiervan is het napraten over de activiteiten die door de (commissies van) de FMF georganiseerd worden. Recentelijk waren er het jaarlijks FMF-symposium, het Consulting Event en een excursie naar ASML. Alle drie de evenementen waren goed bezocht en een groot succes.

Begin december hebben we als bestuur ook onze eerste, volledig zelfs georganiseerde, ALV gehad. Hier is de begroting van de KBE-commissie goedgekeurd. Dit geeft deze commissie de mogelijkheid om nu echt aan het werk te gaan om eind april een succesvolle en vooral leuke reis naar München en Milaan te organiseren!

Daarnaast is het bestuur dit jaar ook druk bezig om de nieuwe media (Facebook en Twitter) die door onze voorgangers zijn geïntroduceerd verder te benutten. Zo kunnen we allerlei activiteiten en kleine nieuwtjes onder de aandacht van de leden brengen.

Ook wordt er gekeken naar de mogelijkheid om een nieuwe website te laten maken. Het kost veel tijd om daarvoor een plan te maken, maar we hopen nog steeds dat voor het einde van dit collegejaar er een nieuwe site zal zijn.

Ondanks de drukte van het besturen probeer ik toch ook nog mijn studie mee te laten draaien, al is het op een laag pitje. Ik hoop dan ook dat ik aan het eind van het jaar kan terugkijken op een leuk en leerzaam jaar, waarbij ik misschien ook nog wat punten heb gehaald. Tot die tijd hoop ik jullie snel een keer te zien op een FMF-activiteit of in de NSFW •

Securing communication

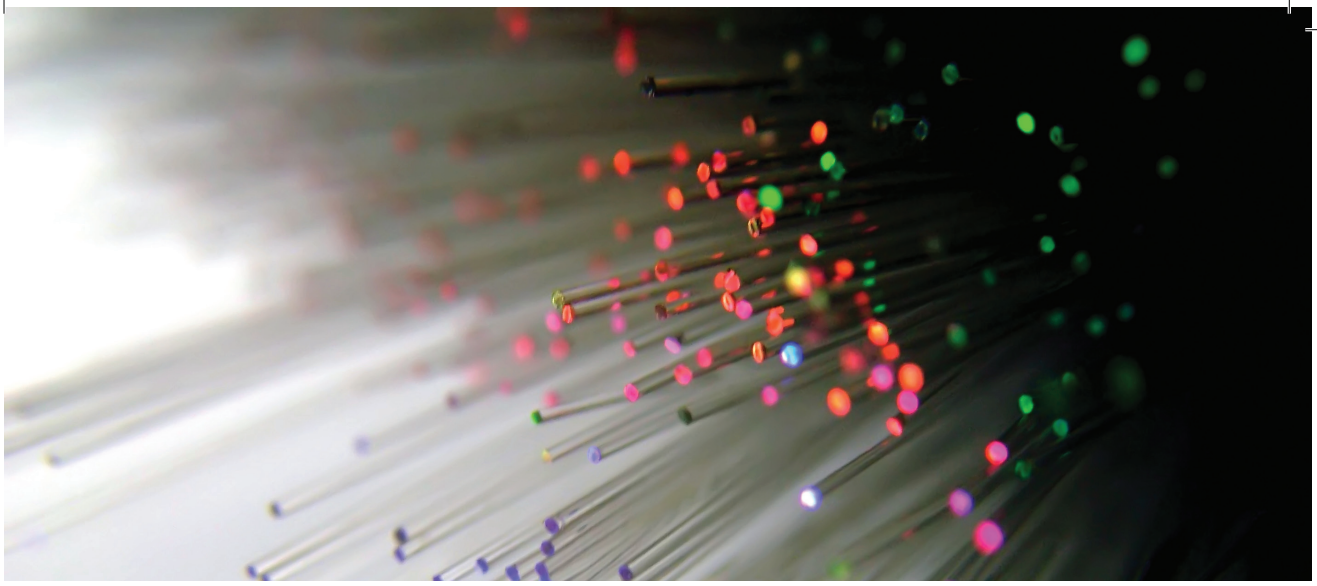
DOOR **CASPAR VAN DER WAL**

In most urban areas, people lock the door when they leave their home. It is simply a reality that this is needed for protecting your privacy and valuable items at a reasonable level against theft. But in our modern lives, much of what is of value can be stolen from us via the internet. We almost constantly use the internet for exchanging personal information, controlling bank and business transactions, and maintaining medical and insurance records. This comes along with possibilities for crime. The need to protect information during such communication against eavesdropping is therefore now just as important as locking the door of your home.

There is, therefore, almost always a form of encryption (also known as cryptography) applied when you use the internet for exchanging information that should remain secret to outsiders. A well-known example is that the connection uses an *https* protocol in instead of a plain *http* protocol. Encryption is making communication incomprehensible to an eavesdropper by applying a mathematical operation to the information (which you can think of as a long row of 1's and 0's in digital representation) before sending it off, and the receiving party knows how to turn this back in the original row of 1's and 0's.

Let's make encryption a bit more vivid with a simple example. Say, it is needed for some reason that you send the PIN code for your bank card to a party you trust. Assume your pin number is 2360. If you and the receiving party both have the same random number in mind that nobody else knows about (say 3567), you can add the random number to your PIN code, and communicate the number 5927. The receiving party then simply subtracts 3567 for getting back the PIN code. Information theorists can prove that if this number is truly random, and if you use it only once, that it is impossible to eavesdrop on this communication. The random number is in this case called the cryptography key, and all secure commutation protocols boil down to setting up a situation where the sender and receiver have a suitable key. It is good to remember this for later on when we discuss the quantum version of encryption: All the sender and receiver need to do is to generate a large random number that they both know, while nobody else knows it.

Nowadays on the internet, most encryption is based on the RSA algorithm for public-key cryptography. The key is generated by exchanging a few numbers in a smart order [1]. These are special numbers, chosen in relation to the mathematics of factorizing a number into its prime factors. The security of the algorithm is based on the fact that 9749 x 7753 (multiplication of two prime numbers) is an easy mathematical problem, while it is much more difficult to find these two prime numbers if you are only given the product (in this case 75583997, go ahead and try it). In practice they use much larger prime numbers. However, there is no mathematical proof that finding the two prime factors of 75583997 is much harder than doing the multiplication 9749 x 7753. So, there is no mathematical evidence that the current encryption system for the internet is secure. And there is even some slow but steady and worrisome progress under mathematicians that aim to understand how one can efficiently factorize a big number in its prime factors. For example, the science pages of NRC Handelsblad of 11 & 12 Feb. 2006 report about a brilliant mathematician from China. She found a way to crack the codes that were then used on the internet in 2^{39} computational steps (one day of work on your laptop) instead of the 2^{64} steps of the fastest protocol till that discovery (about 2^{25} days of waiting time if you only have one laptop). For the time being this is simply solved by using larger



prime numbers, but there is clearly a need for a protocol that is more fundamentally secure.

Quantum cryptography

Here quantum mechanics can help. And while many ideas in quantum information science did not yet leave the laboratory (with experimentalists that are on track to *maybe* get a breakthrough some ten years from now), quantum cryptography over distances up to about 100 km really works. There are a few small companies that sell the instruments for it, and it is applied at a few places for communication between banks in financial districts. One of the most famous companies in the field is ID Quantique in Geneva, Switzerland, they have an interesting website on their products and the physics behind it [2,3].

Quantum cryptography uses several of the most fundamental aspects of quantum physics. For example, the fact that it is impossible to measure an unknown quantum state without disturbing it. Or that we can only predict the probabilities of measurement outcomes, while it is impossible to predict one particular measurement outcome. And this latter aspect can only be applied if we already have a lot of information about the quantum state, which an eavesdropper typically does not have. Derived from this, it can be shown that it is impossible to make a copy of an unknown quantum state (no-cloning theorem). In addition to this, some proposed protocols use quantum entanglement (the aspect quantum physics that became famous through the Einstein-Podolsky-Rosen paradox).

Let's illustrate this with a simple physical system in mind. Let's communicate through an optical fiber. We will send individual photons, one at the time. We will only use photons with linear polarization, but that still leaves a lot of playground for interesting quantum physics. The quantum state that describes the polarization is now always in the form $|\Psi\rangle = \alpha|H\rangle + \beta|V\rangle$. The probability amplitudes α and β are in this case real and obey $|\alpha| \leq 1$, $|\beta| \leq 1$ and $\alpha^2 + \beta^2 = 1$. The states $|H\rangle$ and $|V\rangle$ are two basis states (and a complete set), which represent states with linear polarization along the horizontal and vertical axis in the labs of the sender and the receiver. They can for example agree that $|H\rangle$ represents a 1 in digital information, and that $|V\rangle$ represents a 0. However, they can also switch to using two other orthogonal states: for 1 the state $|\Psi_{1-45}\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$, and for 0 the state $|\Psi_{0-45}\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$ (in the lab this means they simply need to rotate all the polarization optics for the sending station and detection station by 45 degrees). This simple physical system underlies the so-called BB84 protocol (proposed by Charles Bennett and Gilles Brassard in 1984), and also lies at the heart of the quantum cryptography systems that you can now buy commercially.

Let's shortly discuss the main aspects of the BB84 protocol for illustrating the fact that quantum physics can make communication fundamentally secure. How does it work? The sender and receiver (from now on named Alice and Bob, respectively, according to a widely accepted convention in quantum information science) do the following. Alice just starts sending out a random string of 1's and 0's, while also randomly

rotating her polarization optics back and forth all the time over 45 degrees. She writes up what she sent out (1 or 0) for each photon. Bob is detecting all the incoming photons, and tries to measure whether it is a 1 or a 0. He also randomly rotates his polarization optics back and forth all the time. They exchange in this manner a very large set of photons, but that can happen in a few seconds in practice. In this series, it's only half the time that Alice and Bob are sending and detecting 1's and 0's in the same basis (indeed, just by accident). For the other half of the events they were not working in the same basis (one had the basis rotated over 45 degrees with respect to the other). They keep track of their polarization settings as a function of time, and after sending all the photons, they make a phone call and discuss what basis they had in use for each photon (or they use computers to do this automated). They do so *without mentioning the associated value 0 or 1*, so it is no problem if an eavesdropper listens in on this phone call. Then, they just throw away all events for which they were not working in the same basis. What they are left with is an identical string of 1's and 0's at each location that is also a long random number. From this string, they will only use half of the 1's and 0's for the cryptography key. But

before doing so, they first use the other half of the bits for a security check. For this check, Alice picks half the bits from the string. She does this at random locations in the string, and tells Bob both the location and bit value for each case. Bob compares this to his string. If all results are identical, they can trust the key with very high probability. If there are differences, they know that something went wrong, and it could mean that an eavesdropper has been trying to listen in (while the eavesdropper made sure that Bob still got the right amount of photons at the right times, but he cannot always give the photons the right polarization).

Why is it impossible to eavesdrop on this communication? The eavesdropper cannot for all pulses measure the polarization state of a single photon without disturbing it, or in a way that he gets the right answer (1 or 0) with certainty. The reason is that he does not know in what basis he should measure (normal, or 45 degrees rotated). Say Alice sends a 1 in the rotated basis (she sends the state $|\Psi_{1-45}\rangle = (|H\rangle + |V\rangle)/\sqrt{2}$), and the eavesdropper happens to measure in the non-rotated basis. The laws of quantum mechanics then say that he can then get the answer H with 50% probability, or V with 50% probability. He can only get these distinct answers, and he can never get certainty what the polarization state was before his measurement. Let's assume he measured V. The best he then can do to hide his actions is to still send a photon to Bob very rapidly with polarization state $|V\rangle$. However, Bob (if he happens to measure in the same basis as Alice) will then detect a 0 instead of a 1 with 50% probability. So, when this is applied to a long string of bits, Alice and Bob will later find out that they have different bit values for many bits, even when they measured in the same basis.

Current research in the Quantum Devices Team and elsewhere

So, BB84 works in practice. Does this mean that research into quantum communication is finished? No, it is rather the opposite. One problem, for example, is that there are no cheap, stable and tunable

optical emitters that can deliver a single photon on demand. In practice, one now works with very weak laser pulses. But these then often contain (as it turns out after measurement) zero photons. And, a small fraction of the pulses then has two photons, or even three. This makes the implemented BB84 protocol less secure than the ideal one.

Another problem is that one cannot amplify the optical signals on the way without disturbing the quantum state. In practice, this means that BB84 cannot be applied for distances over 100 km (both for optical fibers and propagation through air), simply because the probability that a photon gets lost on the way gets very high after 100 km. The research in my group carries out experiments that aim to tackle this problem by trying to build a so-called quantum repeater with electron spins in semiconductors.

The quantum repeater helps to realize quantum communication over distances larger than 100 km in an efficient way [4,5], efficient means that the required resources and time do not grow exponentially with distance. The communication channel is now divided in segments of 100 km, and at each node there is a quantum memory element for photons. We try to implement this with tiny semiconductor devices. The idea is that the spin of an electron can be in a quantum superposition of spin-up and spin-down. We try to implement that during the absorption of one photon by a semiconductor device, the photonic quantum state is transferred to the quantum state of the electron spin. This does not violate the no-cloning theorem, since the optical pulse is gone after the absorption process. Also note that the electron spin can now carry the quantum state, while operating this process does not reveal the quantum state (that is, it is not a measurement process). In a second step, we aim to operate the inverse process: operate the semiconductor as a light emitter, where the quantum state of the spin is transferred back to the quantum state of an optical pulse. These are exciting experiments, and you are welcome to drop by our labs for further questions, an update and a cup of coffee. •

Caspar van der Wal (Netherlands, 1971) obtained his PhD degree in 2001, in the group of Prof. Hans Mooij at Delft University of Technology for research on quantum coherent dynamics of superconducting circuits. This was followed by a postdoc position of two years in the labs of Prof. Misha Lukin and Dr. Ron Walsworth at Harvard University (USA), where he did research on quantum optics with atomic vapors. At the end of 2003, he started working as an assistant professor at the University of Groningen in the Physics of Nanodevices Group. In 2009, he obtained here a permanent position as associate professor in Physics of Quantum Devices. The research of his team focuses on exploring spintronic and quantum information functionalities with electron spins and nuclear spins in semiconductor devices, using both quantum optical methods and electron transport methods. For his current research he obtained the NWO-Vidi Grant (2005) and the ERC Starting Grant (2011).

Referenties

[1] http://en.wikipedia.org/wiki/RSA_(algorithm)
[2] http://www.idquantique.com/
[3] http://swissquantum.idquantique.com/?Key-Sifting
[4] Long-distance quantum communication with atomic ensembles and linear optics, L.-M. Duan, M. D. Lukin, J. I. Cirac, P. Zoller, Nature 414, 413 (2001).
[5] Towards quantum optics and entanglement with electron spin ensembles in semiconductors, Caspar H. van der Wal, Maksym Sladkov, Solid State Sciences 11, 935 (2009).

Een verslag in één nacht?

DOOR **BART VISSER**

Zoals iedereen wel zal ervaren is het leven van een student druk. Er moet namelijk niet alleen gestudeerd worden maar ook nevenactiviteiten nemen veel tijd in beslag. Sporten bij de sportvereniging met daarnaast nog vele activiteiten of toch nog een goed feest meepakken van je studentenvereniging. Als er dan 's avonds laat nog een verslag gemaakt moet worden dan is letterlijk stukken tekst van het internet overnemen tegenwoordig niet meer zo verstandig. De meeste onderwijsinstellingen beschikken sinds een aantal jaren over een plagiaatscanner die valsspelers moeten ontmaskeren. Maar hoe werkt zo'n plagiaatscanner nou eigenlijk?

Volgens de van Dale is plagiaat het zich toeeigenen van het geestelijk werk van anderen en het als eigen werk openbaar maken. Er mogen best stukken tekst van een andere auteur worden overgenomen, echter moet hier dan wel een correcte bronvermelding bij geplaatst worden. Met name in de academische wereld wordt plagiaat als een doodzonde beschouwd. Het is echter erg moeilijk om de grenzen van plagiaat te trekken. Wetenschappelijke publicaties bouwen bijna altijd voort op ideeën in andere publicaties. Het is dan ook niet voor niets dat bij wetenschappelijke publicaties het aantal referenties gigantisch is. Sommige ideeën zijn inmiddels zo ingeburgerd dat het plaatsen van een referentie niet nodig is.

Het grote gevaar van het maken van verslagen in dit digitale tijdperk is de ongelofelijk grote berg aan informatie die internet heet. Waar vroeger iedereen misschien nog naar de bibliotheek ging om informatie op te zoeken over een bepaald onderwerp, wordt nu bijna altijd het internet geraadpleegd. Google en Wikipedia worden gebruikt om bepaalde kernideeën te begrijpen en goed te kunnen verwoorden. Als er iets dieper in de materie dient te worden gegaan dan wordt er meestal verder gezocht op het internet. Hier schuilt het grote gevaar van plagiaat. Het komt namelijk best wel vaak voor dat iemand anders ook al een keer een verslag heeft moeten schrijven over hetzelfde onderwerp. Veel studenten weten niet precies of teksten en afbeeldingen in een verslag opgenomen mogen worden en hoe zij dat correct kunnen doen.

"De grote berg aan informatie die internet heet"

De meeste onderwijsinstellingen zijn hier nu op voorbereid met de hulp van plagiaatscanners. Plagiaatscanners komen in verschillende vormen voor, meestal wordt er gebruik gemaakt van de digitale leeromgeving waar studenten hun verslagen kunnen inleveren. Het verslag wordt vervolgens automatisch doorgestuurd naar de plagiaatscanner voor onderzoek. De meeste plagiaatscanners kijken naar twee verschillende dingen. Ten eerste wordt er gekeken naar documenten op het internet, vervolgens wordt er ook nog gekeken naar documenten in de eigen database.

De techniek van het vergelijken van documenten is vergelijkbaar met die van zoekmachines op het internet. De tekst van een ingezonden verslag wordt eerst vergeleken met de teksten op het internet die in de database zijn opgeslagen. Net als bij een zoekmachine wordt er niet alleen gekeken naar internetpagina's maar ook naar PDF- en Worddocumenten. De database van een plagiaatscanner wordt continu aangepast. Er komen steeds nieuwe documenten bij en daarnaast worden links naar opgeheven pagina's verwijderd. Het is niet mogelijk alle pagina's

van het internet in een database te zetten, er dienen dus keuzes te worden gemaakt.

De uitslag van het onderzoek naar plagiaat wordt verstuurd naar de docent. Als de plagiaatscanner overeenkomsten heeft gevonden tussen teksten uit het verslag en bestanden op het internet of in de database, dan wordt deze verdachte tekst gemarkeerd. Als een student bepaalde tekst heeft overgenomen, maar enkele woorden heeft aangepast, dan zal de scanner dit alsnog als plagiaat aanmerken. Echter als er maar voldoende werkwoorden en zelfstandige naamwoorden in een stuk gekopieerde tekst veel worden aangepast, dan zal het de scanner het onterecht niet als plagiaat aanmerken. Ook bestanden die wiskundige formules bevatten zijn lastig te herkennen als plagiaat. Aan de andere kant is de scanner niet in staat om te kijken naar de context van een stuk tekst, het komt dan ook vaak voor dat correct geciteerde passages als plagiaat aangemerkt worden.

Op dit moment is het beoordelen van de uitkomst nog steeds mensenwerk, de docent zal zelf moeten beoordelen of er inderdaad sprake is van plagiaat. Als er inderdaad sprake is van buitensporig veel gekopieerde stukken tekst dan zal er een rapportage moeten worden gestuurd naar de examencommissie. De examencommissie van de desbetreffende onderwijsinstelling zal vervolgens de strafmaat bepalen.

De controle op plagiaat wordt door plagiaatscanners sterk vereenvoudigd, aangezien verslagen niet meer handmatig op plagiaat hoeven te worden gecontroleerd. Doordat de kans op het constateren van plagiaat toeneemt, zullen studenten zich wel twee keer bedenken voordat ze stukken tekst letterlijk gaan overnemen. Bij sommige onderwijsinstellingen wordt de plagiaatscannersoftware beschikbaar gesteld voor studenten. Op deze manier kunnen studenten onbedoelde plagiaat voorkomen.

Plagiaat valt moeilijk exact te definiëren, daardoor zal elk geval individueel beoordeeld moeten worden. Een plagiaatscanner is een hulpmiddel om eventuele plagiaat te constateren, het resultaat van de scanner moet altijd nog wel inhoudelijk worden gecontroleerd. De uiteindelijke beoordeling ligt bij de docent, deze is misschien iets lastiger om de tuin te leiden. •

Referenties

[1] www.ephorus.nl

Ghost in the Wires

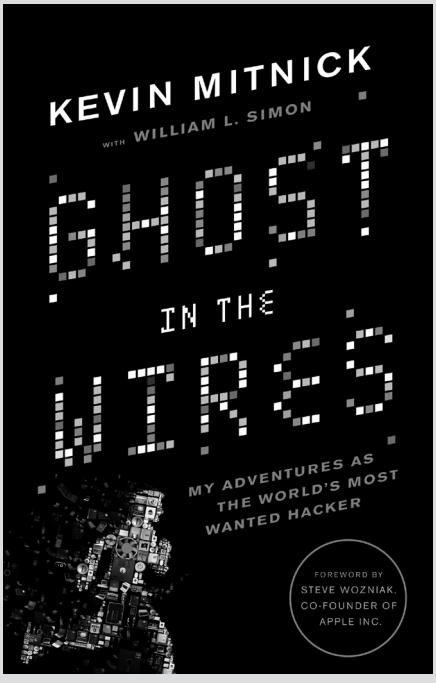
DOOR **PAULUS MEESSEN**

Voor deze perio leek het me leuk om de biografie van een crimineel te reviewen. Nu had ik gewoon het meest recente boek dat ik heb gelezen kunnen bespreken hier: de biografie van Stephen Fry, notoir vanwege zijn gevangenisstraf voor diefstal en creditcardfraude. Iets recenter is natuurlijk het verhaal van Steve Jobs. Zijn eerste stap in de zakenwereld was, om samen met Steve Wozniak de *blue box* te verkopen waarmee men gratis telefoongesprekken kon voeren. Later zou dit tweetal binnen de marges van de wet het bedrijf Apple oprichten.

De bovengenoemde personages hebben een inspirerend levensverhaal, maar ze hebben echter niets betekend voor de criminaliteit. Als we de criminele ambities van Jobs en Wozniak een beetje verder volgen, dat wil zeggen, phone phreaking opzoeken op wikipedia, dan komen we Kevin Mitnick tegen. En laat hij nou toevallig enkele maanden geleden het relaas van zijn criminele verleden te hebben gepubliceerd. Hierin legt hij uit hoe hij 's werelds meest meest gezochte cybercrimineel werd. Tevens schreef hij hèt boek over social-engineering. Dit zijn technieken die hackers gebruiken om niet de computersystemen maar de gebruikers ervan te compromitteren. Iedereen is bekend met deze technieken, denk bijvoorbeeld aan hoe kleine kinderen bij hun ouders snoep weten los te peuteren terwijl beide partijen eigenlijk weten dat dit niet de bedoeling is [1].

Mitnick publiceerde in augustus dit jaar zijn memoires in het boek *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. Het verhaal van Kevin begint heel onschuldig. Als kind raakt hij gefacineerd door het misleiden van mensen wanneer hij de vader van een van zijn jeugdvriendinnetjes goocheltrucs ziet uitvoeren. Hij verliest al snel zijn onschuld wanneer hij uitvogelt hoe hij zelf buskaartjes kan stempelen om op die manier gratis zijn hele zomervakantie met de bus door Los Angeles te reizen. Wanneer zijn ouders en de buschaufeurs erachter kwamen, dan vonden ze het eigenlijk alleen maar leuk van iemand die zo jong is. Dit is het eerste voorbeeld van de positieve feedback die hij in zijn jeugd van zijn omgeving krijgt omtrend zijn hacken. In zijn tienerjaren begint hij met *phonephreaking*, middels de telefoon het netwerk van de telecomaanbieder hacken. Hij leert ook om computers te hacken en bij gebrek aan echte negatieve feedback gaat hij daarin steeds verder.

Het boek is een verzameling van leuke anekdotes en spannende verhalen over hoe Mitnick jarenlang uit handen wist te blijven van de FBI. Verder is er een



wijze les te leren over het impliciete vertrouwen dat er is tussen mensen uit de voorbeelden van social engineering aanvallen waarbij Mitnick bij de grootste technologiebedrijven uit die tijd geheime informatie lost wist te krijgen door er eenvoudigweg naar te vragen. Uiteraard zien we wel dat Mitnick een talent heeft om precies de juiste vraag te stellen.

Uiteindelijk wist de FBI Mitnick in 1995 te arresteren nadat hij de security expert Tsutomu Shimomura had geprovoceerd, waarna deze de FBI assisteerde om Mitnick te pakken. Hoewel hij al op de voorkant van de New York Times had gestaan en daardoor 's werelds meest gezochte cybercrimineel werd, dankt Mitnick zijn bekendheid vooral aan de Free Kevin beweging die daarna werd opgezet. Hoewel hij natuurlijk wetten had overtreden en daarvoor een straf moest uitzitten, werd hij door de publieke bekendheid zeer zwaar gestraft en poogde de rechter tevens om een voorbeeld van hem te maken om andere hackers af te schrikken.

Een voorbeeld hiervan zijn de maanden die hij tijdens zijn voorarrest in eenzame opsluiting zat omdat de openbaar aanklager de rechter er van had overtuigd dat Mitnick door in de telefoon te fluiten een atoombom zou kunnen afvuren. Eenzame opsluiting was vervolgens de enige mogelijkheid om hem weg te houden van telefoons.

Dit toont aan hoe beperkt de perceptie van mensen was rondom hacking. Daarnaast werden er enkele boeken over hem gepubliceerd en zou er een film worden uitgebracht, Takedown, waarin zijn rol zou worden vertolkt door Skeet Ulrich, die bekendheid genoot door hoofdrollen in horrorfilms.

De Amerikaanse phonephreaking-gemeenschap 2600 kreeg lucht van deze oneerlijke behandeling waardoor eerlijke juryrechtspraak niet meer mogelijk zou zijn en wist over de hele wereld mensen te mobiliseren voor de Free Kevin beweging. Hierover is de documentaire Freedom Downtime gemaakt die je gratis kunt downloaden [2].

Sinds 2000 is Mitnick weer op vrije voeten, maar hij mocht onder de voorwaarden van zijn vrijlating pas in 2003 weer een telefoon of computer aanraken of een adviserende rol hebben in computerbeveiliging. Tegenwoordig heeft Mitnick een eigen beveiligingsadviesbureau waarmee hij op verzoek computernetwerken van bedrijven aanvalt om zo de beveiligingsgaten bloot te leggen [3].

Hoewel Mitnick zijn tijd ver vooruit was en door zijn obsessie met puzzelen waarschijnlijk toch aan de verkeerde kant van de wet terecht was gekomen, schrijft hij dat uiteindelijk het enige verschil tussen wat hem nu in staat stelt om te kunnen hacken en wat hem een aanzienlijk deel van zijn leven in de gevangenis gebracht één woord is: toestemming.

"Dit toont aan hoe beperkt de perceptie van mensen was rondom hacking"

Of de nuance zo simpel is, daar kan de lezer zijn eigen oordeel over vellen. Mitnick maakt in ieder geval het argument dat hij slechts gedreven werd door een kinderlijke nieuwsgierigheid en onbegrensde ambitie in combinatie met een verslaving aan puzzelen. Dit is zonder twijfel ook wat ons bétawetenschappers drijft waardoor je dit in ieder geval een amusant boek zult vinden •

Referenties

[1] www.socialengineering.com
[2] en.wikipedia.org/wiki/Freedom_Downtime
[3] mitnicksecurity.com

Te amo México

DOOR **ESTHER VAN DER POL**

Het is het land van de drugsoorlogen en de afrekeningen, het is het land van de Maya's en het einde van de wereld, het is het land van een van de grootste en gevaarlijkste steden ter wereld, het is het land van prachtige natuur, cultuur en mensen, het is het land van de taco's, quesadilla's en tortas, en het is het land waar ik een half jaar heb mogen studeren, wonen en leven.

Het land waar ik het over heb is uiteraard Mexico. Het beeld dat de meeste mensen in Nederland hebben is een erg dubbel. Aan de ene kant heeft iedereen wel eens de plaatjes gezien van stralend witte stranden en een helblauwe zee, maar de nieuwsberichten over de vele schietpartijen en afrekeningen kan niemand negeren. Als je dan ook nog vertelt dat je naar een van de grootste steden ter wereld wilt, is de reactie vaak niet echt positief. Gelukkig heb ik mijn tijd in Mexico als erg positief ervaren. Eigenlijk waren het gewoon zeven van de beste maanden uit mijn leven. De verhalen die je meekrijgt over het geweld in het land is verschrikkelijk, maar Mexico heeft zo veel meer te bieden dan alleen geweld. Het land is prachtig, de steden divers en de mensen ongelooflijk vriendelijk, om over het overheerlijke eten nog maar te zwijgen.

Lo siento, no hablo español

In januari 2011, inmiddels dus een jaar geleden, vloog ik naar Mexico-stad om daar een aantal vakken voor mijn master technische wiskunde te volgen. De voorbereidingen in mijn hoofd waren al meerdere maanden bezig, maar toen ik daar eenmaal aankwam bleek dat ik er eigenlijk niets van gebakken had. De grootste fout die ik gemaakt heb is dat ik eigenlijk maar een paar woorden Spaans kon. Ondanks dat Mexico zo dicht bij de Verenigde Staten ligt en de Mexicanen bijna alles kopen van Amerikaanse makelij spreken de meeste Mexicanen geen Engels. Gelukkig had ik voor de eerste twee weken een taalschool geboekt om mijn Spaans wat op te krikken en meteen de stad een beetje te leren kennen. De taalschool staat redelijk dicht bij het centrum, wat betekent dat je nog steeds twintig minuten met de metro bezig bent om er te komen. Gelukkig is die metro er, want het verkeer is daar de hele dag door een file. Vroeger stond Mexico dan ook bekend om het grote smog-probleem. Inmiddels is dit een stuk minder en dat komt mede door de goede promotie voor het openbaar vervoer. Meestal pakte ik in de stad het openbaar vervoer, maar soms ontkom je niet aan een taxi tripje. Ondanks dat je meestal langer stil staat in de file dan dat je aan het rijden bent, is een taxiritje meestal we een leuk tripje, zeker als de taxichauffeur Nederland kent als het land waar ze zoveel koeien hebben.

Tijdens mijn tijd op de taalschool heb ik de basis geleerd van het Spaans en proberen de stad te bekijken. Mexico-stad of eigenlijk Distrito Federal wordt in de volksmond vaak gewoon Mexico of D.F. genoemd. De stad heeft een zeer rijke geschiedenis. Ze werd gesticht door de Azteken in 1325 bij een aantal grote meren in de vallei van Mexico. In de komende 200 jaar groeide de stad enorm tot het werd veroverd door de Spanjaarden in 1521. De Spaanse verovering heeft grote invloed gehad in het land, ze spreken daar niet voor niets Spaans, maar ook het uiterlijk van de stad heeft veel Spaanse invloeden. Op het hoofdplein van Mexico-stad, genaamd het Zócalo, staat een kathedraal . Deze werd gebouwd door de Spanjaarden op een plek waar eerst een belangrijke tempel voor de Azteken stond. Nadat de Spanjaarden jaren aan de macht waren was er een strijd om onafhankelijkheid aan het begin van de 19^{e} eeuw. Er kwam ook nog een Amerikaans-Mexicaanse oorlog en in 1910 een revolutie. Niet een makkelijke periode voor de Mexicanen dus. Gelukkig ging het daarna een stuk beter met de stad en groeide het aantal inwoners enorm. Hedendaags heeft de metropool Mexico-stad zo'n 22 miljoen inwoners.

UNAM

Na een paar weken sfeer proeven was het dan toch echt tijd om te beginnen met waarvoor ik gekomen was: studeren. De universiteit waar ik een drietal vakken zou gaan volgen was de Universidad National Autónoma de México, of kort gezegd de UNAM. De UNAM staat bekend als een van de grootste universiteiten van Latijns-Amerika en met goed recht. In 2011 had de UNAM meer dan 300.000 studenten. Dat is anderhalf keer zoveel dan de hele stad Groningen bij elkaar. De campus waar les wordt gegeven, de ciudad universitaria, in het zuiden van de stad is dan ook een stad op zich. Om daar van het ene gebouw naar het andere te komen maken ze gebruik van een aantal gratis buslijnen, pumabussen genaamd. Hier kun je op en af stappen om bijvoorbeeld naar de universiteitsbibliotheek te gaan of naar het cultureel centrum. Naast het feit dat de universiteit zo enorm groot is, is hij ook nog eens erg mooi. De universiteitsbibliotheek en het rectorgebouw dat daarnaast ligt zijn beide beschilderd door een van de bekendste schilders van Mexico, namelijk Diego Rivera, de man van Frida Kahlo. Vlakbij de twee gebouwen heb je het Olympisch stadion dat nu wordt gebruikt door de voetbalclub van de UNAM, de Pumas. Ondanks dat de UNAM erg groot, en ook zeer goedkoop is, kunnen de jong volwassenen van Mexico er niet zomaar gaan studeren. Een medestudent vertelde mij dat er jaarlijks honderdduizenden mensen zich aanmelden en dat er maar plek is voor zo'n 50.000 per jaar. Door middel van een test wordt dan ook bepaald wie er mag gaan studeren en wie het een jaartje later nog maar eens moet proberen.

Ik hoefde gelukkig geen test te doen om binnen te komen. De universiteit van Groningen en de UNAM hebben sinds twee jaar een uitwisselingsovereenkomst. Jaarlijks komen er hier Mexicanen en gaan er dus een aantal Groningers die kant op. Samen met nog drie andere meiden waren wij de afvaardiging uit Groningen voor het eerste semester van 2011. Van de vier was ik de enige die mastervakken zou gaan volgen en ook de enige die dit aan de wetenschapsfaculteit zou gaan doen. Aan de wetenschapsfaculteit, maar ook aan de rest van de universiteit, studeren voornamelijk bachelorstudenten. Aan de UNAM is het vrij uitzonderlijk om een master te gaan doen na je vijfjarige bachelor. Ik volgde mijn vakken dan ook met gemiddeld zo'n acht andere studenten. Dat gaf wel een vertrouwd gevoel en zo leerde ik mijn medestudenten snel kennen. Tegen de tijd dat ik begon met mijn vakken was mijn Spaans nog steeds niet zo goed. Bij het eerste college huiverde ik dan ook een beetje, want alle vakken zouden in het Spaans zijn. Ik ben na dat eerste college nog nooit zo blij geweest dat ik wiskunde studeer, het is echt een universele taal. De meeste termen die wij gebruiken in het Engels worden in het Spaans wat zwoeler en exotischer uitgesproken, maar de betekenis is er goed uit te halen. In de achttien weken die volgden begon ik de grapjes van de docent steeds beter te begrijpen en kostte het mij ook steeds minder moeite om 2,5 uur achter elkaar, zonder pauze, in een Spaanstalig college te zitten en ook nog op te letten. Naast mijn drietal wiskunde vakken die ik volgde had ik iedere dag ook nog Spaanse les. Dit volgde ik aan het centrum voor buitenlanders van de universiteit. Drie uur aan het einde van elke dag was het tijd voor een intensief stukje Spaans leren.

Na mijn tijd aan de universiteit heb ik nog zes weken de tijd genomen om het land beter te leren kennen. Zo heb ik uitgevonden waar je het lekkerste eten kan krijgen, namelijk door heel het land. Maar de beste tortas vind je bij restaurant el Jardin in Mexico-stad, voor het adres mag je mij aantikken. Zo heb ik ook ontdekt wat de beste stranden zijn, dat zijn overduidelijk de stranden van Tulum en Isla Mujeres. Hier kun je de beste handgemaakte spullen van Mexico kopen. Hiervoor moet je naar de staat Chiapas, dit is ook een plek waar nog Maya's wonen en waar de natuur floreert. Kortom Mexico is een land dat een slechte reputatie heeft, maar dit maakt het des te leuker om het te onderzoeken. Zo ook Mexico-stad, de stad die meer inwoners heeft dan ons koeien-landje en misschien nog wel diverser is. Als dit je nog niet overtuigd heeft dan zal het eten daar je zeker overtuigen. •

In Colombia werden in 2010 per 100.000 mensen er 38 vermoord
In 1972 veroordeelc
rechtbank een postboc
gevangenisstraf voor
gen van post, er was 3
In 2010 werden in Nederland per 100.000 mensen
In Nederland zitten per 100.000 mensen ongeveer 100 in de gevangenis, in de Verenigde Staten 700
Een halfje wit kost ong
Volgens de BBC zou in 2004 70% van de mensen hun computerwachtwoord met een reep chocolade ruilen, 34% zou hem ook geven zonder chocolade te krijgen
De f
brac
Bij banken werden in Nederland in 2006 172.873 ongebruikelijke en 34.531 verdachte transacties gedaan
Nederland registreerde
de eerste 9 maanden
2011 77 fraudege
len bij internetbankie
Tussen 1997 en 2002 zijn in N
diplomaten onbetaald gebleven

de een Spaanse
de tot 7.109 jaar
het niet bezor-
84.912 jaar geeist

In 2005 werd in Afrika 2.523 keer cocaine in beslag genomen, in 2007 meer dan 5.691 keer

er 0,87 vermoord

Een gevangene in Nederland kost tussen de 145 en 180 euro per dag

In 2009 is in Nederland 2 keer iemand veroordeeld tot levenslang, in 2010 1 keer

geveer 25 euro

Vaticaanstad heeft geen gevangenis

ilm Hackers uit 1995

nt 7.564.000 USD op

in
van
val-
eren

In 2006 werden in Congo ongeveer 1.100 vrouwen en meisjes per dag verkracht, in de Verenigde Staten waren dat er toen ongeveer 15.000 per jaar

In 2011 werd in Europa 1 natuurwet overtreden

New York geen parkeerboetes aan Nederlandse
, Koeweit liet 1.231 van die boetes onbetaald

In 2010 is in Nederland 20 miljoen euro schade aan skimming geleden, in 2009 36 miljoen euro

perio*diek

schrijf een stuk win een Kindle e-reader

Stel een onderwerp voor

Je mag zelf een onderwerp uitkiezen, om vervolgens aan de redactie voor te stellen. Je stuk en het onderwerp moeten namelijk voldoen aan een aantal eisen.

Schrijf een stuk

Als je onderwerp is goedgekeurd, dan kun je natuurlijk gaan schrijven. Er zijn nog wel een paar dingen waar je aan moet denken.

Win een e-reader

Als we je stuk gaan plaatsen, dan krijg je sowieso een Periovulpen. Maar als je tot de beste drie stukken behoort, dan win je daarnaast een gloednieuwe Kindle e-reader.

Kijk voor voor meer informatie en de voorwaarden op schrijfwedstrijd.fmf.nl

Toegepaste computersecurity

Ben je licht-paranoïde of misschien buitensporig sadistisch? Hier zijn enkele richtlijnen.

DOOR **PAULUS MEESSEN**

Wanneer je een nieuw geïnstalleerde Windows computer aan het internet koppelt bestaat er een redelijke kans dat deze binnen een minuut wordt aangevallen en, omdat je nog geen veiligheidsmaatregelen hebt genomen, geïnfecteerd wordt met malware door een geautomatiseerd systeem. Zelfs zonder dat de gebruiker de computer ook maar aanraakt.

Dit is een voorbeeld van de gevaren die je als moderne computergebruiker met een dorst naar youtube-filmpjes en een honger naar facebook-vrienden tegen kunt komen in je dagelijkse gang van zaken. Er zijn gelukkig ook maatregelen die je kunt nemen om je te beschermen tegen een groot deel van de gevaren van het internet. In dit artikel zullen we een aantal beveiligingsmaatregelen aan bod laten komen variërend in een aantal gradaties van paranoia.

- [o_o] - De persoonsinformatie-exhibitionist

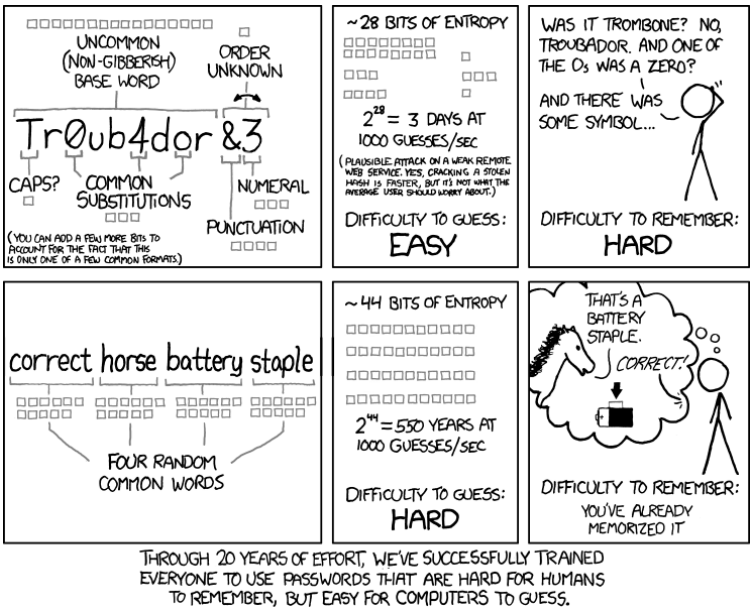
Voor de exhibitionist is het belangrijk dat zijn hele leven op straat ligt. Alle privacy gaat overboord en beveiligingsmaatregelen verdwijnen. Zo pak je dit aan: schakel je firewall uit, deïnstalleer je virusscanner, sluit je computer rechtstreeks aan op het internet en adverteer dit op Google. Indien je een wachtwoord moet gebruiken, kies er dan een uit deze lijst: [*123456, 12345, 123456789, Password, iloveyou, princess, rockyou, 1234567, 12345678, abc123*] [1]. Zorg dat er zoveel mogelijk persoonsgevevens op je computer staan opgeslagen en eventueel andere dingen waarvan je het gevoel hebt dat andere mensen zoiets als 'privé' classificeren. Twitter is bij uitstek een platform om informatie op kwijt te kunnen maar vergeet dan ook niet om elke stoelgang binnen de 140 tekens zo nauwkeurig mogelijk over te brengen. Vergeet vooral ook niet andere sociale media te gebruiken.

Intermezzo, wat er mis zou kunnen gaan

Wie zou er zich nou toegang willen verschaffen tot jouw bankrekening? Wie heeft er baat bij een mooie lijst met daarop alle muziek en films die jij ooit illegaal hebt gedownload? Wie wil jou computer gebruiken in een botnet om spam te versturen of onderdeel maken van een netwerk om kinderporno te verspreiden? Wie gaat er de hele dag door jou webcam meekijken naar alles wat je doet? Wie gaat er in jouw naam dreigbrieven sturen en wie haalt in jouw naam venijnige grappen met je vrienden uit? Tenslotte vragen we onszelf af wie die foto van jou, toen je zo enorm dronken was op dat ene hele foute feest koppelt aan je linked-in pagina? Juist: De gemene cybercrimineel die we proberen uit te sluiten.

- [-_-] - De Gewone gebruiker

De meeste lezers zullen onder deze categorie vallen. Het grootste gevaar hier is gemak en luiheid. Maak regelmatig backups. Zorg dat je besturingssysteem en software, in het bijzonder je beveiligingspakket, up to date is. Let bij internetbankieren op het slotje in je browser dat een veilige ssl verbinding aangeeft en open geen bestanden en websites die je niet vertrouwt. Kies elke zes maanden een nieuw wachtwoord met evenveel entropie als jij je gegevens waard vind. Maak regelmatig backups en/of bewaar informatie in een cloudservice zoals Dropbox. Het gebruik van een sleutelhangerprogramma voor je wachtwoorden, is iets wat je zelf kunt afwegen. Enerzijds staan al je



wachtwoorden bij elkaar in een makkelijk te vinden bestand. Anderzijds bied het eenvoudige bescherming tegen keyloggers die je wachtwoorden proberen te stelen [2].

- [*_*] - De gevorderde computergebruiker

Versleutel al je data. Dit kan met programma's als truecrypt en veel besturingssystemen zoals OS X en Ubuntu bieden je tijdens de instalatie aan je partities te versleutelen. Scan je netwerkverkeer. Als je een beetje begrijpt hoe je computer communiceert met de buitenwereld kun je zelf af en toe je netwerkverkeer monitoren. Als je firewall gemist heeft dat mspaint.exe over poort 1337 ongeveer je hele bandbreedte opsnoept, dan is er iets aan de hand. Tevens zou je er ook achter kunnen komen dat je verkeer niet meer direct naar de router gaat, maar naar een andere computer in je netwerk. Dan heb je last van een *man-in-the-middle* aanval. Tegenwoordig kan iedereen met firesheep of Anti op je android telefoon netwerkverkeer afluisteren als ze eenmaal binnen zijn op je netwerk. Dit is een goede reden om je router altijd te beveiligen met WPA beveiliging of beter. Monitor je geheugen, hoewel goede malware zich altijd probeert te verstoppen kom je hier soms processen tegen waarvan je niet weet wat ze doen of hoe ze op je computer zijn gekomen.

- [>_<] - De systeembeheerder/ WebsiteAdmin

Als systeembeheerder behoor je natuurlijk te weten wat er in dit artikel zou moeten staan. Ik zal hier echter wat passief agressieve technieken aankaarten die ook leuk kunnen zijn voor de andere lezers die het tot hier hebben gered. Recursieve bestandsstructuren zijn altijd leuk. Spiders die je website doorzoeken kun je vangen in een web van virtuele directories. Een van de meest favoriete backdoors van de moderne hacker: meterpreter (metasploit toolkit) loopt vast wanneer deze in windows een recursieve directory tegenkomt. Pas wel op dat je geen gewone gebruikers en vooral geen digibeten in deze vallen laat trappen. *Honeypots* zijn fictieve servers met aantrekkelijke namen en beloften voor hackers. Noem je honeypot 'systeembeheerder-server' en sla tijdig alarm of verzamel sporen van van de overtreders. Een amusant voorbeeld hiervan is de noorse website http://skattelister.no/ waar de belastingen van dit land publiek zijn in te zien. In de robots.txt file, die zoekmachines zoals Google moet helpen, lezen we: Disallow: /admin. We kijken vervolgens in de /admin directory en zien een login scherm. Wanneer we daar proberen in te loggen met willekeurige logingegevens komen we op een volgende pagina waar we lezen: *Trodde du virkelig det skulle være så enkelt?* - Dacht je echt dat het zo makkelijk zou zijn?

en wordt je ge-*Rick-Rolled* [4]. Verder kun je in je netwerk vallen zetten op plekken waar mensen normaal niet horen te kijken. Je kunt een blacklist maken van alle mensen die proberen te connecten op poort 1337 in je netwerk. Dit is zeer irritant voor aanvallers, maar een ander netwerkadres aannemen is een eenvoudige oplossing (eenvoudig als je denkt geblacklist te zijn, niet als je denkt dat je net het hele netwerk hebt laten crashen). Een iets sadistischer optie is om een paar interessante, maar door normale gebruikers niet gebruikte: poorten zeer traag te maken. De zogeheten *tar-pits*, teerputten, waarin programma's en gebruikers altijd de maximale tijd nemen om een antwoord te geven op jou connectieverzoek waardoor je het netwerk als tergend traag ervaart en hopelijk op zoek gaat naar een ander slachtoffer.

- Q['O_O']~D - Paranoide sadisten

Encrypt alles, heb je een terabyte hardeschijf en maar 300mb aan files? Genereer een hooiberg. Verstop je echte bestandssysteem achter een windows bestandsysteem en boot je computer vanaf een usb stick met daarop ook de ontsleuteling van je partities. Is het stuk van je harde schijf waarmee je je computer normaal opstart, de *master boot record*, nu toch vrij? Schrijf daar een heel simpel script in zodat je, wanneer je niet vanaf usb maar vanaf de harde schijf probeert te booten, je data in ieder geval nooit in handen kan komen van anderen, maar overschreven wordt wanneer ze je computer proberen op te starten. Heb je je computer al opgestart? Zorg dan dat er een goede access policy is over usb-devices: indien ze niet van jou zijn: WISSEN DIE HAP. Leuk voor al je forensics tools. Natuurlijk moet je in al je angst niet elk half uur al je gegevens wissen. Ook hier zijn er mogelijkheden om backups bij te houden. Gelukkig is er voor deze doelgroep een commercieel pakket te verkrijgen om veilig backups te maken genaamd TarSnap (backups for paranoid) [5].

Concluderende opmerkingen

Tenslotte zijn er nog een aantal dingen waar je gewoon helemaal niets tegen kunt doen. Er zijn namelijk een aantal dingen waar een impliciete vertrouwensrelatie geldt waar je je maar moelijk tegen kunt verdedigen:

a. Je familie en 'vrienden'

Uiteraard zal dit niet je grootste beveiligingsrisico zijn maar wees er wel bewust van dat je deze mensen toegang geeft tot je computer en privégegevens. Niemand kan uitsluiten dat je kleine broertje die je een spelletje laat spelen op je computer 'per ongeluk' je thesis wist of je privéfotos online plaatst.

b. Je toetsenbord

Je toetsenbord kan best een andere computer zijn die binnen 10 minuten een heel malware programma uittypt en runt op je computer terwijl jij koffie loopt te halen. Oké, je kunt je computer fysiek afschermen van de wereld maar dan kom je ook echt totaal paranoia over Daarnaast kun je ge-ei-ed worden in tien seconden als je even niet aan het opletten bent.

c. Bekende netwerken

'Vertrouwde netwerken' herkennen jou niet. Een device 'schreeuwt' gewoon heel hard: "Is mijn thuisnetwerk hier ergens in de buurt?" en een kwaadaardig iemand kan dan gewoon roepen: "JA! dat ben ik!" om vervolgens al je verkeer af te luisteren. Smartphones in je broekzak en tablets in je rugzak proberen automatisch je thuisnetwerk te vinden. Dit zou je met gps-gegevens of andere trucs uit kunnen zetten. Altijd via een vpn of ssh-tunnnel werken; je netwerkverkeer encrypten is ook een beetje overkill. En je gaat ook niet altijd en overal iedere keer dat je een nieuwe verbinding met wifi wil aangaan (laptop sluimert, je loopt iets te ver weg bij je router) je password opnieuw intoetsen. •

Referenties

[1] http://www.huffingtonpost.com/2010/01/21/worst-internet-passwords_n_431055.html

[2] Defcon z0zhttp://www.youtube.com/watch?v=U4oB28ksilo

[3] www.xkcd.com

[4] www.dafk.net/what

[3] www.tarsnap.com

NAVO en C++

Je C++-programma onder water

DOOR **FRANK BROKKEN**

Vorige week was ik in LaSpezia bij de NAVO, Noord-Atlantische Verdragsorganisatie. De NAVO heeft daar op het terrein van de Italiaanse marine, een onderzoeksinstituut gevestigd. Het NAVO Undersea Research Center (NURC). Zij zijn een interessante club, die allerlei spannende dingen met 'submersible vehicles' doet. Het research center, hoewel onderdeel van de NAVO, wordt primair bevolkt door onderzoekers met een niet-militaire aanstelling. Men houdt zich onder meer bezig met het in kaart brengen van stukken van de zeebodem doormiddel van sonar-technologie. Natuurlijk zit er ook een militaire component aan dit soort onderzoek. Wanneer je dit karteren eenmaal kunt is het slechts een kleine stap verder om je `submersibles' te gebruiken om onderzeeboten of mijnen te detecteren, en daar is het onderzoek dan eveneens op gericht.

Nou werk ik niet bij de NAVO, maar bij de RUG, dus wat moest ik daar nou doen? Vlak voor de afgelopen zomervakantie werd ik benaderd door een medewerker van het NURC die mij vroeg of ik bereid was om een C++ cursus voor hun programmeurs en andere geïnteresseerden te verzorgen. Daartoe ben ik **altijd** bereid :-).

Over C++ zometeen nog wat meer, maar in het geval NURC blijkt dat de NAVO software nodig heeft die de besturing van de 'submersibles' regelt. Deze software bestaat deels uit 'black boxes' die de NAVO 'krijgt' een commercieel software bedrijf dat begint met het sturen van rekeningen van 30.000 euro voor 'voorrijkosten'. Ik kan er iets naastzitten, maar dit soort idiote situaties blijken te bestaan. Als je dan tenminste nog goede software zou krijgen, dan heb je in ieder geval nog wat, maar dan blijkt weer dat er een bug in de software zit. Nadat het ding 8 tracks parallel heeft gevaren gaat het daardoor verder met track 1 in plaats van track 9. Oeps... nouja, een kleine bug, maar wel één waarvan de rekening voor reparatie wat hoger uitvalt dan je had verwacht. 'The joy and fun of closed source software', zullen we maar zeggen.

Het NURC heeft zelf een groep enthousiaste en competente software engineers. Deels afkomstig uit Nederland, zelfs deels afkomstig van ons aller RUG, waar de nodige kennis bijvoorbeeld aanwezig is bij de afdeling KI. De onderzoekers bij KI doen iets met robots, en dat is weer 'gefundenes Fressen' voor de NURCers. Maar hoewel veel in de wereld van de robotica is gebaseerd op de programmeertaal C++, kunnen we ook constateren dat er veel vlees aan de C++-kluif zit.

Ten gevolge van de Java-hype besloot KI begin 2000 om Java als programmeertaal aan te bieden, in plaats van Pascal. In de context van het tot eind jaren 90 bestaande ICCE, het Interdisciplinair Centrum voor de ontwikkeling van Computer-coaches en Expertsystemen, had ik rond die tijd al jaren Java cursussen binnen de RUG aangeboden. Ik werd dan ook gevraagd om de overgang van Pascal naar Java te helpen realizeren. Ik vond toen al, en nog steeds, dat de

keuze voor Java een minder gelukkige beslissing was, die ik tot op de dag van vandaag alleen kan verklaren uit de Java-hype van destijds. Ik begrijp nog steeds niet waarom je de intelligentie van de 'creme de la creme' der Nederlandse intelligentia, universitaire studenten dus, moet beledigen met pure magie. Om een computerprogramma te maken moet je eerst een 'class' definieren. Géén idee wat dat is of waarom dat zou moeten. Vervolgens moet je daarin iets vreemds schrijven als 'public static void main'. Pure magie, want je kunt als docent maar moeilijk uitleggen waarom dat dan moet. "Ja, later als je groot bent, ...", maar ja, "later" klinkt als "in the long run", nietwaar? En zoals Ivo Molenaar, mijn docent statistiek weleens opmerkte: "In the long run we're all dead".

Kortom, wetenschap en magie zijn als water en vuur. Tegen een taal als Pascal steekt Java maar schril af. Pascal is dan geen C, maar is ten minste gebaseerd op een aantal 'safe and sound' mathematische begrippen, die vervolgens in een programmeertaal zijn geoperationaliseerd.

Maar nee, Pascal gaat eruit, Java komt er in. Maar de arme KI-ers moeten vervolgens in C++ hun robots besturen en Java is toch ècht geen C++. De NURCers moeten ook gebruik maken van C++, maar zij gebruiken al geen Java, dat is toch opmerkelijk. De NURCers programmeren wel in C, maar merken ook dat hun C++ kennis wat beperkt is. De KI-ers programmeren in Java en moeten dan hun robots in C++ gaan programmeren. Wat nu? Net zoals in de film, waarin Superman te hulp schiet: verschijnt hier *Yours Truly* ten tonele.

C en Pascal zijn neefjes. Beide zijn begin jaren 70 van de vorige eeuw ontwikkeld. C bij Bell Labs door Kernighan en Ritchie. Dennis Ritchie stierf op 12 oktober 2011. Steve Jobs ging hem net voor, hij stierf op 5 oktober. Ik vind het nog steeds opmerkelijk dat onze nieuwsmedia eigenlijk alleen maar aandacht hebben gehad voor iemand met een goede handelsgeest,

Frank Brokken ken je misschien als docent aan de Universiteit van Groningen. Hij heeft inmiddels aan veel studenten, en docenten, de C++-cursus gegeven. Enthousiast en met veel anekdotes vertelt hij zijn cursisten wat je aan je C++-vertaler mag voeren en wat *not done* is.

Hij geeft ook colleges, speciaal voor informaticastudenten, voor Computerarchitecturen en Netwerken *en* Information Security.

Toch is hij niet alleen voor het doceren van onderwijs in dienst bij universiteit. Sterker nog, hij werkt voor het Donald Smits Centrum voor Informatie Technologie als Security Manager. Daarmee is hij verantwoordelijk voor de beveiliging van alle computers van de universiteit, waaronder natuurlijk ook het rekencentrum.

Maar computers zijn niet de enige machines waarmee hij overweg kan. Frank Brokken is namelijk bevoegd om vlieglessen te geven. Dat doet hij bij Avia Noord.

en nauwelijks voor een pioneer op informaticagebied als Dennis Ritchie. Het zij zo.

Niettemin waren het Kernighan en Ritchie die voor een werkelijke stap voorwaards in de informatica hebben gezorgd door het ontwikkelen van een hogere programmeertaal. Daarmee kon je voor het eerst een heel besturingssysteem schrijven, iets wat voorheen eigenlijk alleen maar in assembleertaal kon worden gedaan. Vrijwel alle programmatuur die iets voorstelt is momenteel gebaseerd op C of op zijn `grote broer' C++.

Een aardige anekdote

In de hoogtijdagen van het ICCE waren er ook collega's die zich bezig hielden met Prolog. Met name de Japanners deden toen hun best om de wereld te overtuigen dat we er goed aan zouden doen met deze nieuwe, 'vijfde generatie' computertalen onze software te ontwikkelen. Het gaat er immers niet om, toen een populaire slogan, **hoe** je iets doet maar **wat** je wilt doen. Ik heb dat nooit goed begrepen. Al komt het zelden voor, als ik een lekke band heb met mijn auto dan helpt het me niet echt dat ik weet **dat** ik mijn wiel wil verwisselen. Ik moet toch echt ook weten **hoe** ik dat moet doen, of ik blijf afhankelijk van de vriendelijke wegenwachter die het klusje voor mij klaart. Beschamend, dat wel. Wij, de C-jongens, hadden zo onze twijfels over Prolog. Enorm traag, in onze optiek, want alles is geïnterpreteerd.

Tot de dag dat een van onze Prolog collega's ons triomfantelijk kwam vertellen: "Nou, je kunt Prolog programma's ook vertalen hoor, dus jullie argument gaat niet meer op". Hoe kan dat überhaubt? Maar

```
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 53]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 47]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 43]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 41]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 37]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 31]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 29]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 23]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 19]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 17]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 13]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 11]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 7]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 5]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 3]':
unruh.cc: In member function 'void Prime_print<current_prime>::f() [with int current_prime = 2]':
```

FIGUUR 1 Als de vertalen het c++-programma unruh.cc probeert te vertalen, blijkt unruh.cc een fout te bevatten. De foutmelding drukt vervolgens de eerste 53 priemgetallen af.

'sure enough', hij komt met een .exe file. We leven nog in het MS-DOS tijdperk en het is een Prolog-programma dat op kunstmatig intelligente wijze de tekst "hello world" op het scherm tovert. Maar het programma is wèl groot. Namelijk zo'n 300k terwijl de maximum grootte voor een DOS-executable zo'n 512k was. En dat alles alleen maar voor "hello world"? Daar zit een luchtje aan. Wat blijkt? Het programma waarmee je een Prolog-executable maakte verpakte het Prolog script en de volledige Prolog-interpreter, die nota bene in C was geschreven, in een programma dat vervolgens de Prolog interpreter als 'child-process' startte. Vanaf dat moment waren we niet meer zo onder de indruk van executable Prolog-programma's.

Terug naar het onderwerp: C en Pascal. Hoewel beide neefjes zijn, zijn toch echt van andere families. C is een echte productietaal. Je kunt er iets mee maken waar je feitelijk iets aan hebt, zoals een Unix-besturingssysteem. Wat later komt de C++ extensie en begin jaren 90 hebben we C++ aan onze C cursus toegevoegd. Dat is dus al weer een jaar of twintig geleden. De C++ Annotaties uit 1993 bestaan op dat moment uit zo'n 100 A5 pagina's. We hebben niet stilgezeten. Inmiddels zijn het zo'n 800 A4 pagina's en de Annotaties worden intensief over de hele wereld gebruikt. Ondanks dat het ICCE niet meer bestaat, leeft de geest van het ICCE nog steeds voort, en hetzelfde geldt voor de C/C++ cursus die ooit, rond 1985, als C cursus is begonnen.

En zo werd ik via, via, door het NURC benaderd voor een C++ cursus. In twee weken, eigenlijk twee keer drie dagen, werd ongeveer alles behandeld waar ik in mijn reguliere cursus bijna vier maanden de tijd voor neem. Maar goed, het zijn geen kinderen daar bij het NURC. Verre van zelfs, week 1 ging dan ook redelijk goed. Hoewel... de constructie van objecten in raw geheugen en 'tricky questions' zoals: "waarom mag je een `Data **` niet toekennen aan een `Data const **`?" waren voor de meeste NURCers toch nieuw of verrassend. Het kwam dan ook niet helemaal als een verrassing dat week 2, met C++-onderwerpen zoals operator-overloading en abstracte containers, maar ook met onderwerpen als polymorfisme en excepties, dat wordt in C++ toch echt anders gebruikt dan in Java, als moeilijk werd ervaren.

Ondanks de grote hoeveelheid C++ die over ze werd uitgestort bleven de cursisten enthousiast, wat, denk ik, tekenend is voor de sfeer bij het NURC. De klapper was natuurlijk de demonstratie van Erwin Unruh's C++ programma: het programma vertaalt niet, maar de uitvoer laat zien dat de C++ vertaler zodanig kan worden gestuurd dat hij in zijn foutmeldingen priemgetallen gaat genereren. Je wint er geen prijzen mee, maar het is een prachtige illustratie van de kracht van het stuk gereedschap dat wij kennen als de C++-vertaler. Hij gebruikt templates, ook zo'n bijzondere mogelijkheid die de taal C++ aan haar gebruikers biedt. In figuur 1 zie je de eerste 53 priemgetallen, daaruit blijkt dat de vertaler priemgetallen wkan genereren.

Overigens is men bij het NURC vaak op zoek naar competente C++ software-engineers. Wie geïnteresseerd is of meer wil weten: kom gerust eens langs om over de details te praten.

Volgens mij raak ik door de aan mij toegekende ruimte heen... Eigenlijk wou ik oorspronkelijk iets schrijven over mijn vlucht met een 1-motorige Piper Arrow over de Atlantische Oceaan. Maar 'I got carried away' terwijl ik over C++ begon te schrijven. Zo gaat dat. Wellicht komt het verhaal over de transatlantische vlucht dan later nog wel eens. •

Become part of a learning adventure

THALES

THALES NEDERLAND
Toonaangevend in de sectoren Defence en Security. Met ca. 2.000 gedreven medewerkers de topaanbieder van hightech-banen. Onze primaire focus is het innoveren van onze producten en het ontwikkelen van nieuwe technologieën. Spraakmakende voorbeelden hiervan zijn radar-, communicatie- en command & controlsystemen voor marineschepen en communicatie-, beveiligings- en betaalsystemen voor het bedrijfsleven. Naast onze betrokkenheid in het OV-chipkaartprogramma zijn wij bekend door onze uiterst betrouwbare dataswitches. Qua omvang van onze R&D investeringen staan wij in Nederland op de negende plaats. Thales Nederland, met vestigingen in Hengelo, Huizen, Houten, Eindhoven, Delft en Enschede, is onderdeel van de internationale Thales Group

OUR CAREER FEATURES

HIGHTECH
Je werkt aan unieke en zeer complexe producten.

MULTIDISCIPLINAIR
Je werkt als specialist in gevarieerde, multidisciplinaire teams.

INTERNATIONAAL
Je werkt voor opdrachtgevers over de hele wereld door systemen te ontwikkelen, te verkopen, te installeren, te testen en te onderhouden.

DYNAMISCH
Je werkt in de dynamiek van de multinational Thales. Onze vestigingen vind je overal ter wereld. Je internationale doorgroeikansen dus ook.

UITDAGEND
Je werkt aan je persoonlijke ontwikkeling in een omgeving die je constant uitdaagt.

EMBARK ON A THALES ADVENTURE IN THE NETHERLANDS
Ben jij in het bezit van een afgeronde opleiding Informatica, Elektrotechniek, Technische Natuurkunde of vergelijkbaar dan kan jouw loopbaan zich in verschillende richtingen ontwikkelen. Bijvoorbeeld van Engineer naar uiteindelijk Architect, Project Manager of Lijn Management.

By courtesy of Royal Schelde Group

Worldwide: with 68.000 employees, a presence in 50 countries, Thales is a global leader in aerospace, defence and security.

Apply straight away
Thales komt graag in contact met jou om samen jouw mogelijkheden te bekijken en je carrièrepad uit te stippelen. Ook bieden wij studenten met een technische achtergrond meer dan 100 uitdagende stage- en afstudeeropdrachten. Vraag onze gids aan of bezoek onze website. Je kunt daar ook solliciteren.

www.thalesgroup.com/netherlands

START YOUR THALES ADVENTURE

Tax me if you can

DOOR **HERBERT KRUITBOSCH**

In 2008 betaalde de Duitse overheid vijf miljoen euro voor een CD met daarop bankgegevens die eigenlijk geheim waren. De bankgegevens zouden een hoop belastingfraudeurs aan het licht brengen. Tijdens de aanloop naar het kopen van de CD besloten 600 fraudeurs zichzelf aan te geven, uit angst dat de consequenties groter zouden zijn wanneer ze opgepakt zouden worden. Met de CD werden echter maar 210 gevallen ontdekt, het geheel bracht uiteindelijk zo'n 180 miljoen euro op aan alsnog geïncasseerde belastingen en boetes.

Valsspelers namen een enorm risico op gerechtelijke vervolging door zichzelf niet aan te geven. Belastingfraude kan *dan* ook niet alleen tot boetes leiden, maar bijvoorbeeld ook tot een gevangenisstraf. Welke gegevens moest de regering kopen en waarom had ze deze niet gewoon al beschikbaar? De belastingdienst heeft immers toegang tot alle rekeningen, salarisspecificaties en dergelijke van iedereen. Nouja, dat is dus niet helemaal waar. Soms staat wetgeving banken niet toe om rekeninggegevens van klanten aan overheden te verstrekken. In Nederland moeten alle banken dat doen zodra de overheid er maar om vraagt. Maar bijvoorbeeld in Zwitserland mag een bank zoiets alleen verstrekken zodra er een gedegen aanleiding is de eigenaar van belastingfraude te verdenken. De eerder genoemde CD zou bijvoorbeeld zo'n aanleiding kunnen zijn.

Zo'n land als Zwitserland noemt men een belastinghaven. Wanneer bijvoorbeeld een Europese autoriteit aanklopt bij een bank in zo'n land, om bankgegevens van een verdachte te krijgen, dan worden die waarschijnlijk niet verstrekt. Toen Duitsland in 2010 met de aankoop van eenzelfde CD kwam, nu met gegevens van 1500 potentiele fraudeurs, liepen de spanningen tussen Duitsland en Zwitserland op. De CD bevatte gegevens van klanten van een Zwitserse bank. Maar Duitsland is, net als veel andere landen, erg afhankelijk van samenwerking met Zwitserland als ze belastingfraudeurs willen opsporen. Immers moet zij met Zwiterseland overleggen over het beleid waarmee bankgegevens van verdachten vrijgegeven worden.

Zwitserland dreigde dat als Duitsland de CD zou kopen, ze geen informatie van verdachten naar aanleiding van de CD zou vrijgeven. De CD bevat immers gestolen informatie en het zou daarom niet een rechtmatige aanleiding zijn iemand te verdenken. Ook dient een regering niet om te gaan met criminelen. Echter gaven ook nu veel fraudeurs zich al aan voordat de CD gekocht was. Maar niet alleen Duitsland had problemen met de belastinghavens, ook de Verenigde Staten ergerden zich groen en geel. Zij dreigden een zwarte lijst te publiceren van alle landen die weigerden samen te werken met belastinginspecties. Uiteindelijk heeft Zwitserland, samen met andere belastinghavens zoals Monaco, de Bahamas en Hong Kong, haar bankgeheimwetgeving aangepast, zodat makkelijker op belastingfraude gecontroleerd kan worden.

Natuurlijk hebben niet alleen Duitsland en de Verenigde Staten zich geërgerd aan de bankgeheimen. Dat komt natuurlijk omdat belastingfraude overheden enorm veel geld kost. Maar vaak worden enorme bedragen via belastinghavens belastingvrij gehouden, wat oneerlijke concurrentie ten gevolge heeft. Een bedrijf dat dividend uitkeert op Zwitserse bankrekeningen kan bijvoorbeeld populairder zijn bij investeerders. Daarnaast kan een vereniging meer eigen vermogen hebben dan controleerbaar is voor de balastingdienst. Omdat oneerlijke concurrentie veel negatieve effecten voor de economie heeft, immers gaan eerlijke bedrijven sneller falliet wanneer sommigen vals spelen. Aan de andere kant was het tot voor kort zelfs mogelijk dat je (bijna) 100%

belasting moest betalen over je inkomsten. Nadat er eerst inkomsten- en daarna vermogensbelasting was geincaseerd, bleef er simpelweg niets over. Hierdoor is het voor de overheid niet alleen maar een kwestie van belastinginkomsten.

Sinds de vernieuwde regelgeving omtrent bankgeheim is niet alleen belastingontduiking, maar ook het witwassen van geld veel lastiger geworden. Europa is ten opzichte van de Verenigde Staten echter nog steeds heel geschikt voor het witwassen van geld. Wanneer iemand geld witwast, dan zorgt diegene ervoor dat illegaal geld legaal gaat lijken. Illegaal kan hier van alles betekenen, bijvoorbeeld geld waarover geen belasting is betaald of winst van een cocaïneproducent. Een Amerikaan moet dan ook aantonen dat hij zijn geld netjes heeft verdiend als die wordt aangeklaagd. In Europa ligt dat precies andersom dankzij het Europees Verdrag van de Rechten van de Mens. Hierin staat dat een aangeklaagde van een proces niet hoeft mee te werken aan zijn eigen zaak.

Voor een crimineel is het natuurlijk altijd de vraag hoe goed iets is witgewassen. Misschien dat de standaarddetectie van fraude niets opmerkt, maar wanneer iemand er beter naar gaat kijken kan alles wel ontrafelen. Daarom probeert de overheid deze doerakken op te pakken door het spoor van geld te traceren. Vroeger gebeurde witwassen daadwerkelijk in wasserettes. Wanneer een client bij een bank veel contant geld komt storten, dan kan die veel vragen verwachten. Voor een wasserette was het echter gebruikelijk om met veel muntgeld te maken te hebben. De inkomsten van zo'n zaak kon je dan tegelijk met je drugsgeld storten. Daar komt de term witwassen ook vandaan. Het zal je dan ook niets verbazen dat Al Capone veel wasserettes had.

Het is niet altijd illegaal om geen belasting te betalen, maar in bepaalde gevallen gaat het buiten de doelstellingen van onze overheid of andere overheden. Voor deze gevallen is Nederland een goede belastinghaven, dat komt omdat de Nederlandse politiek is gericht op relaties en handel met andere landen. Een buitenlands bedrijf hoeft bijvoorbeeld geen belasting te betalen over dividend dat ze via een dochteronderneming in Nederland aan zichzelf verstrekken. Op die manier kan het bedrijf dan inkomen genereren dat niet of weinig belast wordt. Daarnaast heeft Nederland een heel uitgebreid netwerk van verdragen met andere landen om te voorkomen dat bedrijven aan meerdere landen belasting moeten betalen over hetzelfde geld. Daarnaast heeft Nederland veel dienstverlening voor de financiële markt.

Bedrijven die op deze manier belasting ontwijken zijn zogenaamde bijzondere financiële instellingen of brievenbusbedrijven. Nederland kent er ongeveer 20.000, echter telt De Nederlandse Bank ze niet allemaal mee in hun officiële telling, zij stelt dat er ongeveer 10.000 zijn. Jaarlijks vinden er voor ongeveer drie tot vijf biljard euro (twaalf nullen) aan transacties plaats die door deze bijzondere instellingen heenvloeien, dat is acht tot negen keer het bruto nationaal product (BNP) van Nederland. In figuur 1 zie je de precieze getallen tot 2006. In figuur 2 zie je de aandelen van de tegenpartijen wat deze handel betreft .

Een bedrijf uit Zweden, dat we ook hier wel kennen, heeft een complexe structuur van BV's en stichtingen in Nederland, met helemaal bovenaan een stichting [2]. Die stichting werd in 2006 op een waarde van ongeveer 28 miljard euro geschat. Daarmee is de stichting groter dan de tweede grootste stichting ter wereld, *The Bill & Melinda Gates Foundation* [2]. De stichting haalde in 2004 een winst van ongeveer 2 miljard euro, zo'n 15% van hun omzet. Daarover betaalden ze ongeveer 555 miljoen aan belastingen, dat is een effectief belastingspercentage van ongeveer 28% [2, KvK 2006]. Dat is iets meer dan de winstbelasting in Zweden typisch is.

Echter is er een tweede bedrijf, dat het intellectuele eigendom heeft op het logo en concept van het bedrijf in kwestie. Volgens een overeenkomst krijgt dit tweede bedrijf ongeveer 3% van de omzet van de stichting om zo gebruik te maken van het concept en het logo. Dit tweede bedrijf is gevestigd in Nederland, samen met

de eigenaar van dit tweede bedrijf. Op zijn beurt is de eigenaar van deze eigenaar gevestigd in Luxemburg, nog een stapje hoger komen we op de Nederlandse Antillen. Uiteindelijk betaalde de stichting zo'n 638 miljoen euro aan het tweede bedrijf. Die maakte uiteindelijk een winst van 553 miljoen euro, en betaalde daar in Luxemburg ongeveer 19 miljoen euro belasting over. De gecombineerde winst, 2,55 miljard euro, en de totaal betaalde belasting, 574 miljoen euro, komt dan uit op een effectieve belasting van 22,5%. [2, KvK 2006]

Dit soort situaties leveren Nederland zo'n anderhalf miljard euro per jaar op, ongeveer 0,3 procent van het BNP. Daarnaast zorgt het voor werkgelegenheid, 2500 vaak goede banen, bijvoorbeeld accountants en notarissen. Deze zijn het directe gevolg van zulke bijzondere financiële instellingen. Er zijn ook negatieve gevolgen; Nederland wordt via bijvoorbeeld de Europese Unie door omliggende landen, maar ook de Verenigde Staten gezien als een onwenselijke belastinghaven. Zij lopen immers belastingen mis over enorm grote bedragen.

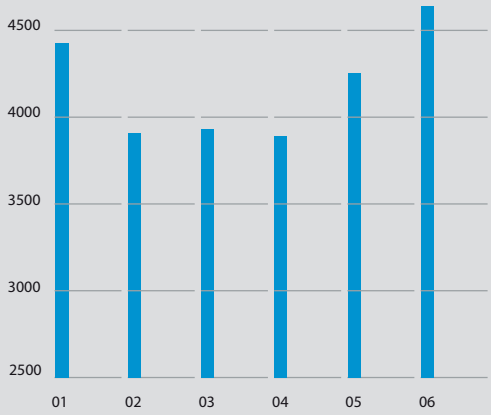
In [2] wordt beargumenteerd dat ook ontwikkelingslanden worden geschaad door dit beleid. De rijke bevolking in Latijns-Amerika heeft bijvoorbeeld 50% van hun geld op geheime bankrekeningen staan Zo lopen feitelijk ook landen die het heel hard nodig hebben belastingen mis. Of Nederland daadwerkelijk een grote bijdrage hieraan levert kan ik niet bevestigen en niet uitsluiten. De argumenten die in artikel [2] worden geleverd zeggen namelijk alleen iets over het gecombineerde effect van illegale belastingfraude en legale maar onwenselijke belastingontwijking. Daarin zou Nederland dan alleen gedeelde verantwoordelijk hebben voor het laatste.

Feit blijft natuurlijk dat zulke belastingontduiking veelal voor een elitaire groep oneerlijke concurrentie mogelijk maakt. Of de oorzaak nu illegaal of legaal is en of kleine bedrijven in ontwikkelingslanden of in het Verenigd Koninkrijk er last van hebben doet er dan niet zoveel meer toe •

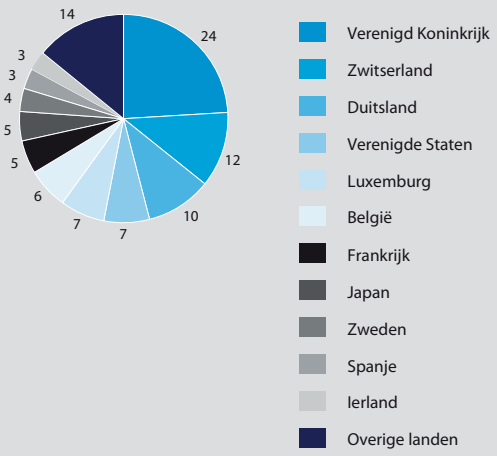
Referenties

[1] De Nederlandsche Bank, "Bijzondere financiële instellingen – integriteitrisico bij grote geldstromen" www.dnb.nl

[2] Michiel van Dijk, Francis Weyzig & Richard Murphy, "The Netherlands: A Tax Haven?", Stichting Onderzoek Multinational Ondernemingen www.somo.nl



FIGUUR 1 Bruto bfi-transacties van Nederland in miljarden euros [1].



FIGUUR 2 Bruto bfi-transacties verdeeld over tegenpartijen van Nederland (2006) [1].

Techniek die het leven eenvoudiger en aangenamer maakt

Bij Philips in Drachten zijn we ervan overtuigd dat technologie tegelijk zinvol en eenvoudig moet zijn. Wij brengen dat dagelijks in de praktijk met de ontwikkeling en productie van producten als de shaver, stofzuiger, Senseo, Wake-up Light en Airfryer. Producten die het leven van mensen vereenvoudigen en veraangenamen.

Groei mee met Philips. Kom werken bij een innovatief bedrijf dat een verschil maakt in de gezondheid en het welzijn van mensen. Je gaat deel uitmaken van één van de grootste ontwikkel- en productiecentra van Philips. Op deze site werken 2000 medewerkers, waaronder 600 ontwikkelaars van meer dan 35 verschillende nationaliteiten. De samenwerking in multidisciplinaire teams binnen de onderdelen High Impact Innovation Center, Innovation Personal Care, Innovation Domestic Appliances en Shaver Production Center biedt interessante loopbaanmogelijkheden.

Meer weten over een mogelijke start van je carrière? Bezoek dan **www.philips.com/careers** of **www.philips.com/engineers** voor traineeships, stages of een vaste baan, er is altijd wel een start die bij je past.

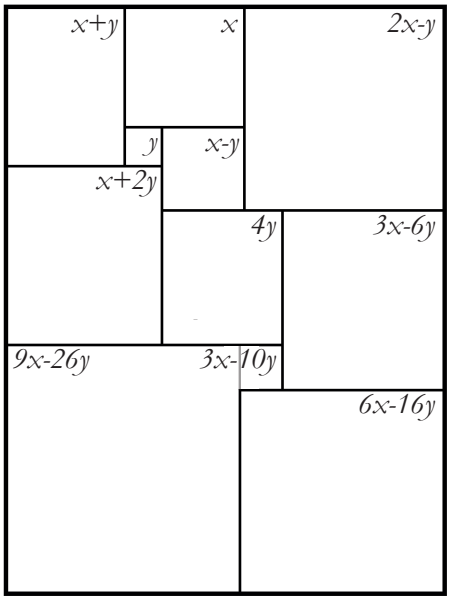
PHILIPS
sense and simplicity

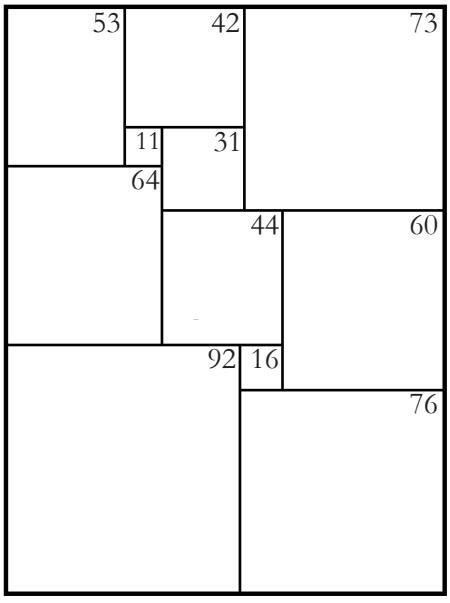
Vorig Breinwerk

DOOR **DE REDACTIE**

Voor de oplossing van de vorige breinwerk moest je twee van de vierkanten respectievelijk het formaat x en y geven. Aan de hand daarvan kon je de overige vierkanten ook als lineaire combinatie van x en y omschrijven. Wanneer je dan voor een van beide vierkanten degene van lengte 11 had gekozen, dan kon je bijvoorbeeld stellen dat y=11. Uiteindelijk kon je op die manier het formaat van alle vierkanten berekenen.

Uit de juiste inzendingen is Jorrit Hagen als prijswinnaar uit de bus gekomen. Hij wint een wetenschapscheurkalendar en kan deze komen ophalen in de NSFW •





Nieuw Breinwerk

DOOR **HERBERT KRUITBOSCH** EN **PAULUS MEESSEN**

assoucd tmd zctmdzcdkiicd kd tmukbmmdiumv vkc dmmiu mggcfmmg mmovmaacgicpyskmi iummd qkjd ncgmiu fcu nyzi. nyzi kd lcu aoszomffm tmd vc assoucd tcossoqmmhcd vmu sazcigsucd fkivmvkzcoi qsd assou hyddcd lmbhcd mmd vc lmdv tmd bsvci. lcu zcumg fscu vcd zctmdzcd fkivmvkzco hyddcd iblokjtcd mgi e usu vcd fmblu w fmmo fscu ssh cembu w dyffcoi gmdz qkjd. kggyiuomukci tmd qyghc zcumggcd qkjd 32768 vmu iblokjxnmmo ki mgi mblu usu vc fmblu tkjx fmmo ssh 416777216 vmu iblokjxnmmo ki mgi mblu usu vc fmblu mblu cbluco hmd ccd qsd e igcblui ccd fmmg zcnoykhu rsovcd vc ncrmmovcoi tmd vc zctmdzcdkiicd tomzcd qkbl mx sx lyd zctmdzcdki tckgkz ncrmmhu rsovu qsvmu ykunommhokikbsi vommznmmo ngkjtcd.

rcgh mmdumg assoucd fscucd kd qsd zctmdzcdki uyiicd mggc fkivmvkzcoi cd vc tokjlckv qkuucd qsvmu vc fkivmvkzcoi dssku hyddcd sduidmaacd.

Stuur de oplossing voor 1 februari naar perio@fmf.nl en win het boek Forbidden Knowledge. De tekst kun je downloaden vanaf perio.fmf.nl/breinwerk201104 •

Criminele burger

DOOR **PAULUS MEESSEN**

Een van de meest verschrikkelijke soorten voedsel is de hamburger: symbool voor buitensporig eetgedrag en onmogelijk om te consumeren zonder je handen vuil te maken. Daarnaast zijn ze soms zo heerlijk dat je onmogelijk maat kunt houden en zo nu en dan zou je er bijna een moord voor doen. Het bovenstaande is net zoals het een goede crimineel betaamt, zonder moraal, maar het doet ons wel een aanbod wat we niet kunnen weigeren: een recept voor een criminele hamburger.

Essentieel voor een hamburger zijn vlees en brood. Voor de 'hamburger' kneed je gehakt, eieren, zout, peper en (andere kruiden naar smaak) door elkaar. Een criminele burger vraagt natuurlijk ook om wat knoflooktereur. Maak vervolgens centimeter-dikke schijven van je vleeschmengsel en bak deze op een heet vuur goed gaar.

Het vlees voor hamburgers komt niet, zoals veel mensen denken, van de in Noord-Duitsland wonende Hamburgers, noch van Amerikaanse presidenten die claimen: "Ich bin ein Hamburger". Rundvlees, dat moet je gebruiken, capice? Hamburgerbroodjes haal je eenvoudig weg uit de supermarkt. Vaak zijn ze per vier verpakt.

Wanneer je deze twee elementen hebt gecombineerd, dan kun je het een hamburger noemen. Om een criminele hamburger te construeren moet je echter nog wat meer moeite doen. Als je hamburger nog redelijk stabiel staat, dan heb je te weinig producten gebruikt.

Een saus maak je door mayonaise, ketchup en een beetje mosterd te mengen. Deze receptuur is gestolen van, naar veler mening, 's werelds beste hamburgertent uit New York [1].

Iedereen weet dat criminelen als kind nooit hun groente en fruit hebben gegeten. Om onze doelgroep te tergen, fruiten we we enkele versnipperde uien en leggen we wat gewassen en knisperende ijsbergsla op onze burger.

Hoewel we de vegetariërs al lang en breed achter ons hebben gelaten zullen we nu ook de lactose intolerante mensen uitsluiten: we plaatsen een plakje cheddar op de hamburger.

Criminelen hebben ook geen compassie met mensen die geen varkens eten: Bak een plak bacon en voeg deze toe aan je hamburger. Snijd ook een plak tomaat op je hamburger. Iedereen weet dat criminelen van rood houden. Rode auto's worden daarom ook vaker gestolen dan andere kleuren.

Ingrediënten:

- hamburgerbroodjes of witte bolletjes
- 1 kleine ui
- 2 theelepels mosterd
- 500 gram rundergehakt
- cheddar
- bacon
- krop ijsbergsla
- 2 tomaten
- augurken
- mayonaise
- ketchup
- sambal of chilisaus

Materiaal:

- Koekenpan

Moeilijkheid:
Bereidingstijd: **+/- 25 min**

Laffe mensen zullen wij uitsluiten middels een dot sambal of een kwak chilisaus over de burger. Herhaal nu naar smaak de bovenstaande stappen tot je product nauwelijks meer op eigen benen kan staan. Voeg tot slot enkele plakjes augurk toe. Geen enkele hamburger is namelijk compleet zonder augurk.

Disclaimer

Geen enkele van de motieven ingrediënten te kiezen voor de hamburger moet serieus worden genomen anders dan eventuele meerwaarde in het genieten van de smaak van je hamburger. De redactie stelt zich dan ook niet verantwoordelijk voor conflicten die ontstaan door het lezen en/of uitvoeren van dit recept. Smullen is op eigen risico. Eventueel commentaar kunt u kwijt in /dev/null.

Indien iemand een truc kent om een hamburger te eten zonder dat je hele handen, je gezicht en alles in een straal van anderhalve meter onder de troep komt te zitten, dan ben ik daar zeer in geïnteresseerd. Bestek is valsspelen. •

Referenties

[1] http://aht.seriouseats.com/archives/2009/10/the-burger-lab-the-fake-shack-how-to-make-shake-shack-burger.html

Technolution

>Tim's passie voor techniek

"Mijn drijfveer is puzzelen: het oplossen van een probleem op een technisch mooie manier."

Software Designer

Lees meer over Tim's passie voor techniek op

www.technolution.eu/collega

Technolution is een project-bureau, specialist in het gecombineerd ontwikkelen van elektronica, programmeerbare logica en software voor embedded en technische informatiesystemen.
In opdracht van onze klanten werken wij op ons kantoor in teams aan multidisciplinaire, technisch complexe en innovatieve (deel)systemen.

>the right development