I/O VIVAT

JAARGANG 28
NUMMER 4

De bits en bytes van Bitcoin
Het cryptogeld uitgelegd

Muziekpiraterij en de muziekindustrie
Feiten over de strijd tussen piraterij en de muziekindustrie

Online tracking & analytics
Bedrijven willen weten wie je bent!

Virtueel Utopia
De sleutel voor een successvolle Virtual Economy

Anonymous E-Commerce
Handel op de online zwarte markt

Dit is privé
Waarom het verplicht ontsleutelen van data averechts werkt

En verder...
COMMIT/TimeTrails
Gamification
Op bezoek bij KPMG, Thales en Quinity
Van de voorzitter en kandidaat-voorzitter
Van het ENIAC-bestuur

Inter-Actief

Advertentie

vi_imago_adv_a4_staand.pdf

//Colofon

Jaargang 28, nummer 4,
September 2013
ISSN: 1389-0468

I/O Vivat is het populair-wetenschappelijke tijdschrift van I.C.T.S.V. Inter-Actief, de studievereniging voor Technische Informatica, Bedrijfsinformatietechnologie en Telematica van de Universiteit Twente. I/O Vivat verschijnt vier maal per jaar en heeft een oplage van 1700 exemplaren.

// Hoofdredactie
Stijn van Winsen

// Redactie
Michel Brinkhuis, Martijn Bruning, Rick van Galen, Caspar Schutijser, Herman Slatman, Jip Spel

// Vormgeving
Niels Witte

// Gastschrijvers
Fleur Aalbersberg, Hugo Anbeek, Rolf de By, Sebastiaan la Fleur, Jan Flokstra, Victor de Graaff, Tom Griffioen, David Huistra, Martijn Hoogesteger, Pim Jager, Maurice van Keulen, Rick Leunissen, Mark Steunenberg, Andreas Wombacher, Zhemin Zhu

Voor vragen, suggesties en tips is I/O Vivat bereikbaar via e-mail op vivat@inter-actief.net, twitter op @iovivat, telefonisch op 053-489 3756 of per post:
Studievereniging Inter-Actief
Postbus 217
7500AE Enschede

De studievereniging wil de adverterende bedrijven bedanken voor de samenwerking.

// Drukwerk
Drukkerij van den Bosch & Fikkert

I/O VIVAT

//Redactioneel

Toen Michael Aldrich in 1979 de basis legde voor het online winkelen, zou hij nooit gedacht hebben dat hij een revolutie op het internet zou starten. Meer dan 30 jaar later zijn we van een simpele business-2-business betaling gegaan naar een wereld waar crowdfunding en bitcoins steeds belangrijker worden. E-commerce is niet alleen een bit-buzzword, maar begint een manier van leven te worden. Tijd dus, om E-commerce eens goed onder de loep te nemen.

Net zoals in de goede oude tijd, gaat de I/O Vivat-redactie zich weer focussen op themanummers. Een nummer waar we één onderwerp vanuit meerdere perspectieven zullen bekijken, waarbij we aftrappen met een themanummer over E-commerce, dát is ons vakgebied, met onderwerpen als: de werking van Bitcoins, team Greenlight, het nieuwe initiatief van Steam, de zwarte e-commerce markt en de strijd van de muziekindustrie om illegaal downloaden tegen te gaan. Genoeg te lezen dus als je op het strand ligt op Gran Canaria met je op het internet gekochte vliegticket en op het internet geboekte hotelkamer.

Zoals je misschien al gezien zult hebben onderaan deze pagina is Herman niet langer de hoofdredacteur van de I/O Vivat. Na meer dan een jaar zich ingezet te hebben om elke Vivat weer bij jouw op de deurmat te leggen heeft hij besloten dat het tijd werd om het stokje over te geven. Uiteraard bedanken we hem als redactie graag voor de inzet die hij getoond heeft in dat jaar en moeten we ons meteen verontschuldigen voor alle niet-gehaalde deadlines en frustaties waar we voor gezorgd hebben. Gelukkig zal Herman onze redactie nog wel blijven versterken als redacteur en kan hij zijn tijd nu steken in het nog beter maken van zijn artikelen.

Dit keer is het dus voor mij de eerste kans om jou niet teleur te stellen en ook deze Vivat vol inhoud aan jullie te presenteren. Dus voor het eerst namens mijzelf en de rest van de redactie veel plezier gewenst bij dit eerste themanummer over E-commerce!

Stijn van Winsen

Hoofdredacteur

//Inhoud 28.4

//Nieuws

AdLeaks: 'advertentiesysteem' voor het lekken van informatie

Onderzoekers van de Freie Universität Berlin hebben een systeem ontwikkeld dat door klokkenluiders gebruikt zou kunnen worden om op confidentiële wijze informatie door te spelen aan de pers, zonder dat zij daarbij gemonitord kunnen worden door bijvoorbeeld bedrijven of overheden.

Vaak is het voor klokkenluiders niet veilig om zaken openbaar aan te kaarten, zelfs niet als er regelgeving bestaat omtrent het beveiligen van klokkenluiders. Daarom zoeken zij in veel gevallen naar andere kanalen om hun informatie anoniem te kunnen verspreiden. Huidige oplossingen zijn onder andere het gebruik van versleutelde verbindingen, maar tegen tegenstanders die een globaal overzicht van het netwerk hebben, hebben die oplossingen maar een beperkte mate van privacy.

Het nieuwe systeem is ontwikkeld als een soort advertentiesysteem voor geheime berichten. Websitebeheerders kunnen de service van AdLeaks integreren op hun website, waarna iedereen die de website gebruikt, berichten versleuteld verstuurt naar een AdLeaks server. Een klokkenluider kan zijn eigen berichten versturen; andere gebruikers zorgen er door de website te bezoeken voor dat het bericht van een klokkenluider niet opvalt. Als het systeem zeer wijdverspreid raakt, zal het voor een aanvaller niet mogelijk zijn om berichten van een klokkenluider op te vangen tussen alle onzinnige berichten van normale gebruikers.

Het systeem is op dit moment nog niet volledig en er wordt nog aan de backend ontwikkeld. Meer informatie is beschikbaar op http://www.adleaks.org/.

Bron: http://arxiv.org/abs/1301.6263, A Secure Submission System for Online Whistleblowing Platforms, Roth, V., e.a.

Nieuw algoritme voor homomorfische encryptie gevonden

Het volledige afschermen van data in de cloud is weer een stuk dichterbij gekomen nu onderzoekers van het Massachusetts Institute of Technology's Computer Science and Artificial Intelligence Laboratory een nieuw algoritme hebben ontwikkeld voor homomorfische encryptie.

Het was al lange tijd mogelijk om data versleuteld op te slaan in de cloud door de data te versleutelen voordat het naar de cloudopslag verstuurd wordt. Het nadeel hiervan is dat er niet makkelijke operaties op uitgevoerd kunnen worden: hiervoor zou de data eerst ontsleuteld moeten worden, waarna operaties op de data wel mogelijk zijn.

Homomorfische encryptie is een techniek waarbij er wèl operaties op versleutelde data mogelijk is. Er worden versleutelde operaties naar de cloud gestuurd, waarna de server de versleutelde operatie op de versleutelde data uitvoert. Het resultaat hiervan, dat ook versleuteld is, wordt daarna teruggestuurd. De gebruiker kan het versleutelde resultaat ontsleutelen, en met het resultaat werken. Op deze manier is op geen enkel moment bij de server bekend welke data er verwerkt wordt.

Het nieuwe algoritme, dat een functioneel versleutelings schema genoemd wordt, bestaat uit meerdere bestaande onderdelen. Homomorfische encryptie is daar één van. De andere onderdelen zijn een zogenaamd garbled circuit en attribute-based encryption. De verschillende onderdelen vullen elkaar op de zwakke punten aan, waardoor een robuust algoritme ontstaat voor homomorfische encryptie.

Het probleem met bestaande homomorfische encryptie is dat berekeningen in veel gevallen nog te zwaar zijn om praktisch te zijn. Berekeningen op versleutelde data duren simpelweg te lang om er echt iets mee te kunnen doen. Zeldovich, één van de onderzoekers, stipt aan dat het nieuwe algoritme ook nog steeds dit nadeel bevat, maar dat het algoritme zó nieuw is dat er nog veel aan te onderzoeken valt. Sinds de eerste algoritmes voor homomorfische encryptie gevonden zijn, zijn deze ook op veel punten verbeterd, en zijn er grote snelheidsverbeteringen behaald.

Van de kandidaat-voorzitter

BAM.

Door: Martijn Hoogesteger
Kandidaat-voorzitter Inter-Actief

De I/O Vivat. Een tijdschrift dat ik al bijna 4 jaar met interesse lees, maar nooit had gedacht er in te schrijven. Dit komt (helaas) niet door een miraculeuze stijging in mijn schrijf- en spellingskunsten, maar door het geweldige feit dat ik me samen met 5 helden het kandidaat-bestuur voor het jaar '13/'14 mag noemen.

Een tijd lang heb ik de beslissing om bestuur te gaan doen niet kunnen maken. In mijn eerste jaren zat ik altijd wel bij de bestuursinteresseborrels en was ik vaak bij Inter-*Actief* te vinden, maar er waren destijds nog wat bergen om tegen op te kijken. Zo was er de P-in-2 regeling, de mogelijke langstudeerboete, de daadwerkelijke langstudeerboete, de harde knip, etcetera.

Toen was het moment daar, met mijn bachelor bijna klaar dacht ik: "BAM! Gewoon doen." Deze gedachtegang heeft in mijn eerste jaar ook geholpen bij het oprichten van een LAN-Commissie, en dit jaar weer bij de Rially. De beslissing om ergens vol voor te gaan en enthousiast te blijven zorgt niet alleen dat het gemakkelijk is om ergens hard aan te werken, maar ook dat het erg leuk blijft om te doen.

Nu ben ik bijna twee weken kandidaat-voorzitter, en ik kan er al geen spijt meer van hebben. Zoals ik ze eerder benoemde, de helden waarmee ik kandidaat-bestuur ben, maken het helemaal waard. Het nieuwe kandidaat-bestuur bestaat nu weer uit 6 mensen. Samen gaan we er in ieder geval een gaaf jaar van maken.

Natuurlijk wordt het niet alleen een jaar van gave dingen doen, er staan ook een aantal uitdagingen voor de boeg. Zo zal vanaf volgend jaar het TOM ingevoerd worden, waarbij we goed op de eerstejaars zullen gaan letten. We zullen ons ook hard moeten blijven maken voor realistische overgangsregelingen. De studiereiscommissie zal ook zijn beginsprint maken om hopelijk Noodle weer te evenaren of zelfs te overtreffen.

Daarnaast zal het komende jaar hoogst waarschijnlijk nog allemaal uitdagingen voor onze neus zetten, en met deze groep mensen kunnen we zeker weten aan. Als deze uitdagingen er niet zijn? Dan zijn er ideeën genoeg binnen het kandidaat-bestuur!

Als deze I/O Vivat je deurmat heeft bereikt zijn we alweer een tijdje kandidaat-bestuur. Hopelijk heb je ons al veel gezien tijdens alle borrels en activiteiten van Inter-*Actief*, en zie je aankomend jaar nog meer van ons en alle leden die ons helpen Inter-*Actief* zo gaaf te maken!

Martijn Hoogesteger,

Kandidaat-voorzitter Inter-*Actief*

Martijn Hoogesteger is geboren op 3 september 1991 in het westerse Leiden. Na 12 jaar bij het strand gewoond te hebben in het prachtige Noordwijkverhuisde hij naar het weinig bekende Zelhem, in de achterhoek. Hier volgde hij VWO gymnasium aan het Ludger College. Na een succesvolle afronding van het N&T profiel volgde de gemakkelijke keuze voor Technische Informatica op de UT.

Hier werd hij onmiddellijk actief in de LanCie, gevolgd door de aXi, WWW, LusCie, KasCo, Soccie, TostCie, BHV, Beheer en de Rially. De volgende stap heeft hij dan eindelijk genomen en kan hij zich sinds 9 mei kandidaat-voorzitter voor het jaar '13/'14 noemen.

Inter-*Actief*

Online tracking & analytics

Bedrijven willen weten wie je bent!

Door: Michel Brinkhuis
Redacteur I/O Vivat

Sinds de invoering van de nieuwe cookiewetgeving, nog niet zo heel lang geleden, vragen veel websites bezoekers om eerst akkoord te gaan met het plaatsen van cookies, alvorens de site verder kan worden bezocht. Bijna iedereen accepteert die cookies wel, immers: je kunt anders de site niet bezoeken. Maar waar worden deze cookies voor gebruikt? In dit artikel proberen we daar een antwoord op te vinden. De focus ligt daarbij op cookies die worden gebruikt voor tracking (het volgen van bezoekers) en analytics (het vergaren van bezoekersinformatie).

Grote websites doen er alles aan om de conversie op hun website zo hoog mogelijk te laten zijn. Dat wil zeggen: ze willen zoveel mogelijk bezoekers omzetten in klanten. Amazom.com zal er bijvoorbeeld alles aan doen om een bezoeker te verleiden tot een aankoop. En wanneer de bezoeker zo'n aankoop doet, dan probeert men er het maximale uit te halen. Let er maar eens op wanneer je bezig bent met het afrekenen in een webwinkel. Ineens verdwijnt een deel van de menubalken, en men doet suggesties voor nog een kleine extra aankoop. Om die suggesties te doen houdt men vaak bij welke producten je zelf al eerder hebt bekeken.

Een andere optie is dat je een lijstje met producten ziet dat zegt 'Andere mensen die dit product bekeken zagen ook..'. Om zo'n lijst te kunnen tonen moet er dus per bezoeker worden bijgehouden welke producten er allemaal worden bekeken. En om je als bezoeker te kunnen volgen gedurende een bezoek aan een website wordt er vaak een cookie geplaatst. Wat ook steeds meer gebeurt is het tonen van advertenties gebaseerd op bekeken producten. Stel, je koelkast gaat stuk, en je besluit even te Googlen om te kijken hoeveel een nieuwe gaat kosten. Zodra je een paar webwinkels hebt bezocht, zul je zien dat advertenties op andere websites ineens allemaal koelkasten laten zien. Dat is niet omdat het je ineens opvalt, maar dat is omdat de advertenties puur op je persoonlijke profiel kunnen worden afgestemd.

Prijsdiscriminatie

Doordat met name grote bedrijven in staat zijn om veel informatie van hun bezoekers te verkrijgen, kunnen ze de informatie gebruiken om bezoekers precies voor te schotelen wat het bedrijf wil. Op deze manier kan er ook prijsdiscriminatie worden toegepast. Prijsdiscriminatie houdt in dat je bezoekers dezelfde producten aanbiedt, maar dan voor verschillende prijzen. Onderzoek genaamd 'Detecting price and search discrimination on the Internet' door Mikians et al. leert dat prijsdiscriminatie zeker door sommige bedrijven wordt toegepast. De Amerikaanse online retailer Shoplet, leverancier van verkoopproducten, toont je bijvoorbeeld een hogere prijs als je het product opent door een bezoekje aan de website van Shoplet zelf. Kom je op een productpagina terecht via een prijsvergelijkingswebsite, dan zie je ineens een lagere prijs voor exact hetzelfde product. Wat gebeurt er namelijk? Zodra je vanuit de prijsvergelijkingswebsite doorklikt naar Shoplet kom je eerst op een tussenpagina. Daar wordt een cookie geplaatst, met gegevens van de referral (in dit geval de vergelijkingswebsite). Het is namelijk vaak zo dat dat soort websites een commissie krijgen per verkocht product, waarvan de verkoop terug te traceren is naar die partij (op deze manier geld verdienen wordt ook wel affiliate marketing genoemd).

De Wall Street Journal deed recent ook een onderzoek naar het fenomeen online prijsdiscriminatie. Een opzienbarende toepassing van 'kennis over de bezoeker' die zij ontdekten wordt toegepast door Staples, ook een grote handelaar in kantoorartikelen. Zij stellen hun prijzen af op basis van de locatie van de bezoeker. Daar zou nog wat voor te zeggen kunnen zijn, als dat gebeurt omdat de transportkosten naar iedere locatie binnen de VS wel eens wat verschillend kunnen zijn. De Wall Street Journal ontdekte echter dat de prijzen afhankelijk waren van de afstand tot concurrenten van Staples. Zit er veel concurrentie van Staples bij jou in je fysieke omgeving? Dan zul je een lagere prijs te zien krijgen. Vermoedelijk is dat niet de enige factor die meespeelt in de dynamische prijsbepaling. Het bleek namelijk ook dat prijzen hoger lagen in gebieden waar het gemiddelde inkomen lager ligt.

Enerzijds lijkt dit vreemd, de bedrijven die dit soort technologie toepassen zien dat anders. Volgens hen is het slechts een reflectie van de werkelijkheid: echte winkels passen ook hun prijzen aan op basis van hoeveel concurrentie er is, en doen ook lokale aanbiedingen. Klanten worden er echter minder blij van. 76% Van de Amerikanen gaf aan dat het hen zou raken als ze erachter kwamen dat andere mensen voor hetzelfde product minder geld hoeven te betalen, zo ontdekte men op de University of Pennsylvania.

Optimalisatie

Gegevens van bezoekers kunnen worden gebruikt om websites te optimaliseren. Daarvoor kan een split-test worden uitgevoerd. De ene helft van de bezoekers krijgt bijvoorbeeld een landingspagina te zien met een gele knop, en de andere helft dezelfde pagina met een oranje knop. Door de conversie van die twee pagina's te meten en naast elkaar te leggen kun je bepalen welke pagina het best presteert. Met software als bijvoorbeeld MouseFlow is het mogelijk om het gedrag van een bezoeker op een website als het ware 'te filmen'. Dit soort software kan alle muisbewegingen, kliks, scroll- en typacties registreren en zodoende kun je als websiteeigenaar meekijken met mensen die je website gebruiken. Door dit soort dingen bij veel mensen te meten kun je heatmaps genereren. Heatmaps geven met kleuren aan welke delen van de pagina veel worden bekeken (of bezocht door de muis) en welke juist niet. Zo kun je precies achterhalen waar op een pagina precies de focus van bezoekers ligt.

Bezoekersidentificatie

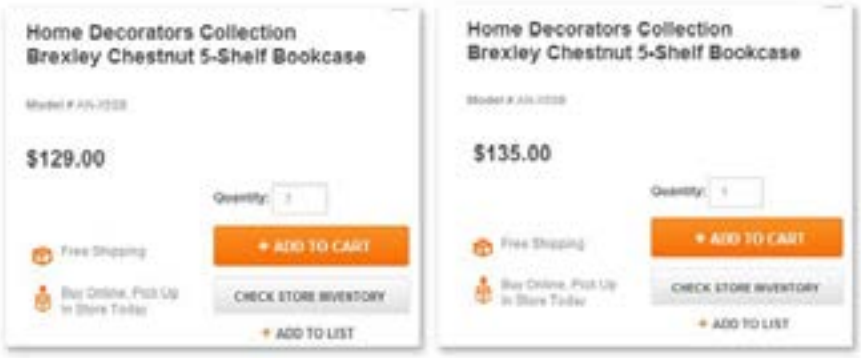
Sommige grote websites zetten derde partijen in om bezoekers te kunnen identificeren. Dat is iets dat bijvoorbeeld wordt aangeboden door een bedrijf als LeadLander. Zij bieden een paar javascriptjes aan die eenvoudig in iedere website kunnen worden geïntegreerd, en die monitoren wat er allemaal gebeurt. Vul je bijvoorbeeld een contactformulier in, dan worden de gegevens die je in het formulier invult ook door hun Formalyzer-tool opgenomen Die gegevens worden dan weer geanalyseerd en gedeeld met andere klanten van de dienst. Op die manier kunnen IP-adressen (of wellicht een combinatie van IP-adressen, cookies en browser—identificatiemethoden) worden omgezet naar een bedrijfsnaam. Als je als bedrijf weet welke bedrijven kijken op je website, dan kun je daar gerichte actie op ondernemen. Het grote voordeel voor bedrijven is dat ze weten wie hun website bezoeken, zonder dat die bezoekers ook maar íets hoeven in te vullen. Dat kunnen ze namelijk al op een andere site gedaan hebben. Via zo'n identificatiebedrijf kun je dan toch aan e-mailadressen van je bezoekers komen, en ze een persoonlijke mail sturen. Iets dat de mensen van de website 42Floors.com overkwam. Op hun blog (http://42floors.com/blog/youre-not-anonymous-i-know-your-name-email-and-company/) schrijven ze meer over de werking van het systeem.

> "Zij stellen hun prijzen af op basis van je locatie."

Er is geen ontkomen aan!?

Met de cookiewetgeving poogde de overheid dit soort dingen lastiger te maken. Waarschijnlijk zal er echter niet veel gaan veranderen. Websites hoeven binnenkort namelijk niet meer expliciet om toestemming te vragen. Enkel een melding tonen is voldoende; zodra de bezoeker verder gaat met het bezoeken van de site geeft deze impliciet toestemming voor het plaatsen van cookies.

Wil je voorkomen dat bedrijven veel over jou en je browsegedrag te weten komen? Met een browserplugin als Ghostery is het mogelijk om te zien met welke tracking-javascripts, pixels en noem maar op, je in aanraking komt, en kun je ze blokkeren.



Figuur 2: Prijsdiscriminatie (Bron: eConsultancy.com)

Referenties

Websites Vary Prices, Deals Based on Users' Information
http://online.wsj.com/article/SB10001424127887323777204578189391813881534.html

Detecting price and search discrimination on the Internet
http://conferences.sigcomm.org/hotnets/2012/papers/hotnets12-final94.pdf

Online price discrimination: a surprising reality in ecommerce
http://econsultancy.com/nl/blog/62699-online-price-discrimination-a-surprising-reality-in-ecommerce

LeadLander.com

News.yCombinator.com
https://news.ycombinator.com/item?id=4891764

Ghostery.com

You're not anonymous. I know your name, email, and company.
http://42floors.com/blog/youre-not-anonymous-i-know-your-name-email-and-company/

Gamification

Het concept en het toepassen hiervan

Door: David Huistra
Gastschrijver

Gamification, het toevoegen van spelelementen in software, is een buzzword dat CEO's graag in de mond nemen. Zo heeft 40% van de top 1000 Globale organisaties aangeven tegen 2015 Gamification te willen gaan toepassen in het bedrijfsproces. Gamification nadert echter ook de piek van zijn 'nieuwheid hype' en het wordt voorspeld dat binnen twee jaar 80% van de huidige Gamification applicaties niet hun doel hebben kunnen bereiken en als gefaald zal worden gezien. Desondanks zijn er inmiddels ook talloze succesverhalen en word er over het algemeen verwacht dat er ook op de lange termijn veel kansen zijn voor Gamification. Het succesvol toepassen vergt echter de juiste aanpak.

Beeldvorming

Mischien wel het bekendste voorbeeld van Gamification is het 'Fleet consultancy' project van Scania. Via dit project worden chauffeurs gecoached om zuiniger en anticiperender hun vrachtwagen te besturen. Dit doen ze door het rijgedrag van chauffeurs via zeven parameters te beoordelen. Na een rit krijgt een chauffeur zijn score te zien en geeft het systeem verbeterpunten aan. De chauffeur kan op alle punten steeds beter scoren en met collega's concurreren. Naast een behoorlijke brandstof besparing heeft dit project ook geleid tot enthousiaste chauffeurs die zo met plezier 'beter' zijn gaan rijden. Vergelijkbare projecten zijn er om bijvoorbeeld mensen te helpen met gezonder te leven en af te vallen, denk bijvoorbeeld aan de Wii Fit Plus.

Een geheel andere vorm van is het spel Ribbon Hero van Micorsoft. Als je niet beter weet denk je een spel te spelen samen met je trouwe vriend Clippy, maar 'stiekem' leer je via dit spel de basis om met de ribon interface van producten zoals Microsoft office te werken.

Weer een andere vorm word toegepast door Khan Academy. Khan Academy is gratis site met meer dan 2000 video tutorials voor vakgebieden als wiskunde, natuurkunde, geschiedenis, sterrenkunde etc. Deze site heeft echter ook verschillende vormen van Gamification toegepast. Bijvoorbeeld door alle filmpjes aan elkaar te knopen en een soort 'RPG skill tree' te maken kun je duidelijk zien hoe een vak gebied in elkaar zit en in welke manieren je de stof kan doorlopen en wat je kan oversaan. Hierdoor word het saaie 'boek doorlopen' ineens veranderd in een stappenserie waarbij je levelt en ervaring in de stof opbouwt. Hiernaast krijg je ook nog feedback op basis van welke filmpjes jij gekeken hebt en hoe je verder kan gaan. Een andere vorm hebben ze bijvoorbeeld met opgaves waarvoor je ook punten en ervaring krijgt en een onderwerp kan afronden door 10 willekeurige opgaves over dat onderwerp af te ronden. Je krijgt bonus punten voor een reeks goede antwoorden en mocht je niet zeker van het antwoord zijn, dan linked de vraag altijd naar een max 10 min filmpje waarin de theorie word uitgelegd.

Het kan bijvoorbeeld ook gebruikt worden om repititive taken plezieriger te maken of gebruikers de applicatie te laten verkennen. Gamification kun je dus op verschillende manieren toepassen en gebruiken om uiteenliggende doelen te bereiken, maar het algemene doel is de betrokkenheid van gebruikers met de software te verhogen.

De theorie

"Gamification is, per definitie, het toepassen van game-design denken op niet-game applicaties om de gebruikers participatie te verhogen. Het maakt gebruik van de mens zijn natuurlijke verlangen om te spelen en te concurreren en dit resulteert in hoger niveau van participatie." - Adam Swann

In 1996 werd de theorie ontwikkeld dat er verschillende type spelers zijn die verschillende doelen hebben in een spel. Via veel verschillende mensen te vragen wat ze wouden zien in games verdeelde hij de resultaten in vier groepen:

> Achievers: Spelers met het goal om binnen het spel zoveel mogelijk te verzamelen/bereiken, bijvoorbeeld alle coins verzamelen of moeilijke bazen verslaan.

> Explorers: Spelers die zoveelmogelijk van het spel/spelwereld willen zien. Vaak begint dit met de spelwereld geheel verkennen en gaat verder in het

uitzoeken van de spel mechanics.

> Socializers: Spelers die het spel voornamelijk gebruiken om contact te hebben met andere spelers, bijvoorbeeld voor role play of samenwerken in groepsopdrachten.

> Killers: Spelers met het doel om andere spelers in het spel te verslaan of op een andere manier proberen lastig te zitten.

"Gamification toepassen is een plan hebben."

Veel vergelijkbaar onderzoek heeft deze theorie als basis genomen. Hieruit blijkt bijvoorbeeld dat mannen vaak beter scoren op het gebied van achievers en vrouwen beter scoren op het Socializers gedeelte.

Bij het ontwikkelen van een applicatie kun je dus rekening houden met de (verwachte) gebruikersgroep en kijken welke type(s) gamer hier bij passen met als simpelste voorbeeld het verschil tussen mannen en vrouwen. Microsoft heeft bijvoorbeeld in Microsoft Visual Studio Achievements ingebouwd en heeft zich hiermee wellicht specifiek gericht op de gebruikers groep van het software pakket (voornamelijk mannen).

Gamification toepassen is een plan hebben.

Er zijn vele vormen van Gamification en voor elke manier zullen er specifieke Do's en Dont's zijn. Maar er zijn een aantal algemene punten waar je voor moet oppassen. Het is belangrijk een goed plan te hebben en afwegingen te maken.

> Geen aspecten uit spellen overnemen - Met Gamification leggen mensen logischerwijs direct een verband met games. Hierdoor zie je vaak dat aspecten uit games direct worden gekopieerd, met als meest gebruikte voorbeeld achievements. Dit is niet per definitie slecht, maar het is belangrijk om te kijken of dit wel past bij de gebruikersgroep die je voor ogen hebt en voornamelijk of het de juiste manier is om je doel te bereiken. Games zijn een goede inspiratie bron, maar het is belangrijk om na te gaan waarom games bepaalde dingen doen en welke doelen ze hiermee willen bereiken.

> Leer geen verkeerd gedrag aan – Met het toekennen van belonging zie je helaas vaak dat er ongewenst gedrag optreed doordat men zich gaat richten op het verkrijgen van deze beloningen. Een simpel voorbeeld hiervan is dat mensen slordiger gaan werken als ze worden beloond op de quantiteit van hun werk. Bij het bedenken van beloningen is het belangrijk om te bedenken hoe dit het gedrag van mensen zal kunnen beinvloeden en welke negatieve aspecten dit zou kunnen veroorzaken. Probeer beloningen te verzinnen die goed of geheel werk belonen.

> Gebruik betekenisvolle beloningen – Veel van de huidige Gamification projecten lijken in de veronderstelling te zijn dat je met het weggeven van nietszeggende achievements, punten of scores het gedrag van gebruikers kunt aanpassen. Nietszeggende belogingen hebben vaak echter geen enkel effect. Gebruikers moeten getrokken worden door betekenisvolle belonging.

> Geen beoordelingsplatform – Probeer te voorkomen dat met het bijhouden van statestieken en scoreborden de Gamification implementatie een beoordelingen platform word in plaats van een manier om gebruikers participatie te verhogen. Als gebruikers het idee hebben constant beoordeeld te worden kan dit juist negatieve gevolgen hebben waarbij ze gestressed of met tegenzin aan het werk gaan. Gamification moet de gebruiker op een positieve manier proberen te beinvloeden, dus zorg ervoor dat de beloningen/scores/statestieken zich niet volledig focusen op productiviteit, accuratie etc.

> Een doel voor ogen hebben – Met de huidige hype van Gamification kijken veel bedrijven naar de vraag "Hoe kunnen we Gamification gebruiken in ons project/bedrijf?". Het is natuurlijk geen slecht idee om te kijken waar je in een process Gamification kan toepassen, maar het moet niet omwille van Gamification zelf gebruikt worden. Als er een gelegenheid is voor het toepassen van Gamification, is het belangrijk om een duidelijk doel voor ogen te hebben met wat je hiermee wil bereiken en een analyse uitvoeren of Gamification de geschikte methode is om dit doel te bereiken.

> Ontwerp Gamification vanuit een gebruikers perspectief – Een veel voorkomende fout is dat bedrijven Gamification ontwerpen vanuit een perspectief om hun eigen doelen te bereiken en niet kijken naar het perspectief van de gebruiker. Veel succesvolle projecten als bijvoorbeeld Khan Academy zijn juist vanuit de gebruiker zijn perspectief ontwikkeld om ervoor te zorgen dat de gebruiker word gemotiveerd om beloningen te krijgen. Een succesvol project ontwikkeld de Gamification vanuit het perspectief van de gebruiker om te zorgen dat deze gemotiveerd word om er mee aan de slag te gaan.

Conclusie

Met Gamification kunnen diverse doelen bereikt worden en het bied vele mogelijkheden om dit doel te bereiken, maar met een verkeerde aanpak kan het ook netatieve resultaten opleveren. Om Gamification toe te passen is een goed plan en een goede uitvoering nodig, maar dan kan het ook zeker vruchten afleveren.

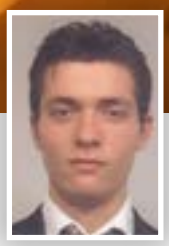
Referenties

Targeting Gamification Applications to Increase User Participation - Marc Hulsebosch
http://referaat.cs.utwente.nl/conference/18/paper/7368/targeting-gamification-applications-to-increase-user-participation.pdf

The Gamification of Business
http://www.forbes.com/sites/gartnergroup/2013/01/21/the-gamification-of-business/

Virtueel Utopia

De sleutel voor een successvolle Virtual Economy



Door: Martijn Bruning
Redacteur I/O Vivat

Virtual economies kom je het meeste tegen in MMORPGs en real life simulation games: een voorbeeld hiervan is Second Life. Toen in 2004 de MMORPG World of Warcraft (WoW) uitgebracht werd, had dat grote gevolgen en werden zowel MMORPGs en de virtual economies die daarbij horen, onder de aandacht gebracht van het mainstream publiek. Maar hoe maak je een virtual economy die succesvol is? En misschien wel belangrijker; hoe zorg je ervoor dat een virtual economy ook succesvol blijft?

Virtuele crisis?

Als je tegenwoordig de term 'WoW Gold' intypt bij Google, krijg je meer dan 90 gesponsorde resultaten voor websites die je de ingame currency van WoW verkopen voor real currency (wettige betaalmiddelen). Overal ter wereld, maar met name in Hong Kong, zijn bedrijven ontstaan die gespecialiseerd zijn in het verzamelen van ingame commodities en currency, die ze vervolgens te koop aanbieden aan andere spelers. Zodoende is hier een hele industrie omheen ontstaan.

Toen de economische crisis Europa trof, waren de gevolgen duidelijk terug te zien in de economie. Toch bleek dat virtual economies hier minder last van ondervonden. Iemand zou natuurlijk kunnen opmerken dat dit niet verbazingwekkend is, aangezien het in virtual economies niet om echt geld draait en dat mensen daardoor minder geneigd zijn om zich iets aan te trekken van hun financiële situatie in de werkelijkheid.

Niets blijkt minder waar te zijn: hoewel er in virtual economies sprake is van virtual currency en assets, is het toch vaak het geval dat mensen deze kopen en verkopen voor en met real currency. Hierdoor zou je dus sterk kunnen vermoeden dat er wel degelijk een verband bestaat tussen virtuele en non-virtuele economieën.

Maar naar wat voor een verband kijken we dan? Die vraag blijkt alleen te beantwoorden wanneer virtual economies goed bestudeerd en begrepen worden. Zo kan men zich afvragen wat de drijfkrachten achter een virtual economy zijn, met andere woorden; waar ligt het initiatief voor deelname? Waar haalt een speler genoegdoening uit?

Wat is het waard?

Als een speler een MMORPG aan het spelen is, dan is bij de meeste spelers het doel zich te vermaken. Hoe dit bereikt wordt kan verschillen van persoon tot persoon, maar meestal zijn er kosten verbonden aan vooruitgang. Als je een voorbeeld neemt aan WoW; als een speler level 40 bereikt komt hij voor een belangrijk dilemma te staan: de nieuwe gebieden waar hij terecht gaat komen zijn groter, meer uitgestrekt en kosten de speler dus ook meer tijd om doorheen te komen. Op level 40 is het dan ook mogelijk om een mount(vervoersmiddel) te kopen, hiermee kan een speler zich sneller voortbewegen en hoewel het niet een vereiste is wordt er wel sterk op aan-

Figuur 1: De online auctionhouse

gedrongen dat een speler deze mount koopt. Hiernaast komen dan ook een aantal andere zaken kijken waar de speler mee geconfronteerd word en al snel kom je op een kosten plaatje van 1000 goud. Maar hoe komt de speler hier aan?

Geld verdienen kan op veel verschillende manieren in een MMORPG: een speler kan quests ondernemen waar hij een uiteindelijke beloning voor krijgt en daarnaast heeft hij ook nog eens kans om geld te verdienen door het verslaan van monsters die hij onderweg tegenkomt. Een andere manier zou kunnen zijn dat de speler een crafting profesion neemt en op zoek gaat naar materialen, bijvoorbeeld ijzer, en daar vervolgens wapens mee maakt die hij verkoopt om zo zijn geld te verdienen.

Er zijn dus vele manieren voor een speler om geld te verdienen maar de vraag is en blijft, wat is het waard? Als een speler namelijk 10 minuten bezig is met het verzamelen van ijzer en dan onderweg ook monsters tegenkomt waar hij geld van verdient en dan evenveel geld verdient als iemand die 20 minuten bezig is met een quest op te lossen, kan een speler al snel de afweging maken dat het verzamelen van materialen meer geld oplevert. Maar als alle spelers op deze manier gaan redeneren, kan het zo zijn dat er een overvloed aan aanbod van een bepaald type materiaal ontstaat, waardoor de waarde drastisch kan zakken.

Geld in geld uit principe

Het grootste probleem waar de meeste virtual economies mee kampen, is niet het reguleren van de hoeveelheid geld dat verdient kan worden door spelers, maar om dit te balanceren met de uitgave ervan, om er zo voor te zorgen dat de waarde van goederen stabiel blijft.

Weer verwijs ik naar WoW die een cruciale fout maakte bij het uitbrengen van Sunwell Island bij de uitbreiding: The Burning Crusade. spelers moesten een reeks van daily quests (dagelijks herhaalbare quests) uitvoeren om zodoende de reputatie op te bouwen bij een factie, zodat de speler toegang zou krijgen tot een nieuw gebied. Maar spelers die bezig waren met het verzamelen van deze reputatie kregen ook een heleboel geld als beloning voor het voltooien van deze quests.

Hierdoor kregen spelers die niet bezig waren met het verzamelen van geld dit alsnog voor een activiteit die dit niet als hoofddoel had. Het gevolg hiervan, inflatie doordat spelers een methode hadden om meer geld te verdienen in minder tijd, werd verder versterkt door het inflatie-effect van spelers die deze quests niet voor het geld uitvoerden, maar voor de reputatie. Heel veel geld dat binnenkomt, maar geen geld dat uitgegeven wordt.

De Conclusie voor een stabiele economie

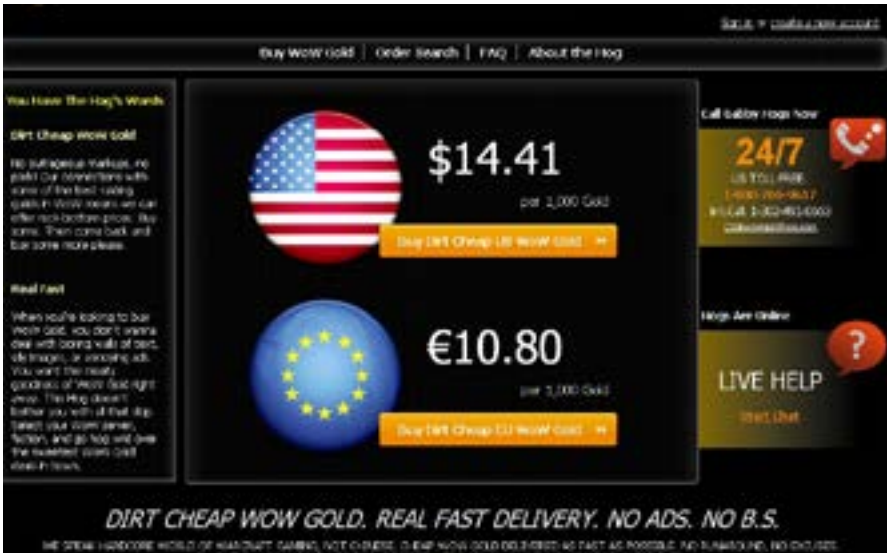
Wat is dus een goede manier om een stabiele virtual economy te maken?

Een gezonde en sterke virtual economy wordt gemaakt door voldoende mogelijkheid tot kopen en verkopen; waar alle spelers kunnen inzien wat de prijzen zijn voor producten.

Zorg ervoor dat er een goede balans is tussen risico en winst als het aankomt op het uitvoeren van activiteiten zoals quests en materiaal verzamelen.

Daarnaast is het belangrijk dat het geld dat de wereld in komt, er ook weer uitgaat met de zelfde hoeveelheid. Als laatste maar niet het onbelangrijkste; moedig alle vormen van spelers aan om te participeren in de economie: geef elke speler de droom dat ook hij of zij een virtueel economisch succes kan zijn.

> "Heel veel geld dat binnenkomt, maar geen geld dat uitgegeven wordt"



Figuur 2: Koers WoW Gold

Referenties

Auctionhouse images from www.pcgamesn.com

en.wikipedia.org/wiki/Virtual_economy

http://www.psmag.com/business-economics/the-real-value-of-virtual-economies-eve-world-of-warcraft-64593/

//Artikel

Anonymous E-Commerce

Handel op de online zwarte markt

Door: Herman Slatman
Redacteur I/O Vivat

E-commerce heeft zich de afgelopen jaren bewezen als een wezenlijke toevoeging op de traditionele 'stenen' winkel. Uiteraard zijn er de grote, gespecialiseerde webwinkels, maar ook een groot aantal winkeleigenaren heeft inmiddels een webwinkel opgezet. Naar verwachting zal dit aantal in de nabije toekomst blijven groeien.

Ook voor partijen die handelen in minder alledaagse goederen blijkt de verkoop via een online kanaal een waardevolle aanvulling op de omzet. In schimmige achterhoeken op het web en op verborgen webservers draaien fora en IRC servers op volle toeren om handel op de online zwarte markt te faciliteren. Dit artikel zal ingaan op het ontstaan van deze markten en de invloed die zij (kunnen) hebben op de samenleving.

De online zwarte markt

Ongure handeltjes hebben eigenlijk altijd al plaatsgevonden: goedkope deals van particuliere aanbieders die eigenlijk te mooi zijn om waar te zijn, of de verkoop van drugs door lugubere personen op de hoek van de straat. Dat deze zwarte handel niet enkel meer een offline probleem is, is onder andere een gevolg van het makkelijker worden om een online marktplaats op te zetten. Veel criminelen zijn op deze trend ingesprongen, en hebben zo'n marktplaats opgezet, soms met een compleet netwerk van individuen en georganiseerde criminaliteit als aanbieders.

In eerdere artikelen is er al eens geschreven over de grote hoeveelheden persoonlijke gegevens die verhandeld worden op het web. Daarbij gaat het om accountgegevens voor bijvoorbeeld Twitter of Facebook, maar ook creditcardgegevens vallen hieronder. Dit gebeurde rond het jaar 2002 veelal op speciaal hiervoor ingerichte fora zoals ShadowCrew.com en CardersPlanet.com. Op de fora kwamen aanbieders en kopers voornamelijk met elkaar in contact om creditcardgegevens uit te wisselen, die de koper daarna kon gebruiken om andere zaken mee aan te schaffen tot de limiet van de creditcard bereikt wordt. De fora kregen echter behoorlijk wat weerstand te verduren van de geldende wetten, en werden vaak binnen niet al te lange tijd opgerold. Criminelen gingen op zoek naar betere manieren van online zaken doen, en gingen vaak ondergronds.

Zo ontstond in februari van 2011 de online markplaats 'Silk Road'. Op deze marktplaats waren in maart van dit jaar meer dan 10000 producten te koop, waarvan het in 70% van de gevallen om drugs gaat. Naast illegale goederen zijn er echter ook legale goederen te vinden op Silk Road, zoals kunst en boeken. De marktplaats is vrij simpel opgezet: verkopers hebben een account en kunnen daarmee producten aanbieden. Kopers kunnen feedback geven over een bepaalde verkoper, waardoor de betere aanbieders een hogere rating krijgen en meer bestellingen kunnen verwachten.

Om een marktplaats als Silk Road mogelijk te maken, en open te houden zonder te kunnen worden opgeheven door een overheid, wordt Silk Road gehost als een TOR-service. Het TOR (The Onion Routing) netwerk is een netwerk van virtuele tunnels waardoor requests van gebruikers gestuurd worden. Het pad van deze requests zal over de tijd verschillen, waardoor je acties online niet aan elkaar gerelateerd kunnen worden, en je relatief anoniem kunt surfen. Door Silk Road als een TOR-service te draaien, is het niet makkelijk om de mensen achter de website te vinden en de website te sluiten, wat tot gevolg heeft dat de site tot nog toe met succes heeft kunnen voortbestaan.

Een andere technische ontwikkeling die nodig was om de Silk Road te doen laten ontstaan, is de ontwikkeling van Bitcoin geweest. Kopers en verkopers moesten op de Silk Road anoniem kunnen handelen en normaal betalingsverkeer dat via de bank verloopt is dat natuurlijk niet. Het gebruik van Bitcoin als betaalmiddel heeft ervoor gezorgd dat er anoniem gehandeld kan worden op de Silk Road.

Silk Road is niet de enige marktplaats die gebruikmaakt van het TOR netwerk. Zo zijn er op de Hidden Wiki tientallen links te vinden naar andere marktplaatsen waar wapens, gadgets, elektronica en illegale diensten verhandeld worden.

Ook buiten het TOR netwerk om zijn er markten te vinden waarvan het bestaan op zijn minst de wenkbrauwen doet fronsen. Een prominent voorbeeld hiervan is bijvoorbeeld het verhandelen van zogenaamde zero-day vulnerabilities op internet fora. Crackers bieden hier de lekken aan die ze in software hebben gevonden. Deze lekken worden door cybercriminelen misbruikt om bedrijven of personen aan te vallen en hen in de meeste gevallen geld afhandig te maken. De bedragen voor verschillende soorten exploits kunnen oplopen tot enkele tienduizenden dollars per exploit.

Deze exploits worden ook verkocht aan overheden die deze exploits kunnen gebruiken in hun strijd tegen cybercriminaliteit. Een bedrijf dat zeer actief is in deze handel is het Franse VUPEN. Het interne team van onderzoekers zoekt naar zwakheden aan software, om deze door te verkopen aan geselecteerde overheden. De vraag blijft echter of VUPEN enkel aan overheden verkoopt; er liggen natuurlijk veel cybercriminelen op de loer die hun kans afwachten om binnen te lopen met een aangeschafte exploit.

Consequenties van de online zwarte markt

Allereerst is het natuurlijk duidelijk dat er door het bestaan van een online zwarte markt allerlei handel plaatsvindt in het illegale en informele circuit. Mensen kunnen in veel gevallen anoniem aan bijvoorbeeld drugs of wapens komen. Nu verschilt dat niet heel veel van de offline zwarte markt, want ook daar kun je relatief anoniem opereren, maar toch blijkt dat het online handelen een extra gevoel van veiligheid met zich meebrengt. Daardoor zullen ook mensen die zich normaliter niet met lugubere zaakjes bezig zouden houden een aankoop kunnen wagen. Een groot voordeel aan het online kopen is natuurlijk dat je makkelijk in contact kan komen met een verkoper zonder dat je allerlei gegevens over jezelf moet prijsgeven.

> “Enkele tienduizenden dollars per exploit”

De vraag is of men meer risico loopt als men online drugs koopt. Het grote succes van Silk Road toont aan dat een systeem waar kopers een verkoper een rating kunnen geven goed werkt. Zo komen vanzelf de betere verkopers aan de top, waarvan je kan verwachten dat ze goede kwaliteit leveren, en dat er relatief weinig gevaar is voor de drugsgebruiker. Wat dat betreft is er dus wel iets te zeggen voor een zo’n online marktplaats. Feit blijft dat het om illegale goederen gaat, en dat het voor de lokale autoriteiten eigenlijk niet te doen is om elke brief of pakket te checken op inhoud.

Waarschijnlijk loopt de gemiddelde consument meer gevaar door de online fora waarop zero-days verkocht worden aan cybercriminelen. Omdat het hier gaat om nieuwe exploits voor software die veel gebruikt wordt, kunnen veel consumenten vatbaar zijn voor de nieuw aangeboden exploits, om nog maar niet te spreken van exploits die binnen enkele uren al in zogenaamde exploitkits te vinden zijn. Er ligt hier een taak voor overheden en software ontwikkelaars om consumenten hier tegen te beschermen.

Conclusie

Online marktplaatsen bieden aan zowel de klant als de verkoper enkele voordelen. Zo kan de koper uit zijn luie stoel bestellen, en krijgt de verkoper er een extra verkoopkanaal bij. Op het web zijn diverse marktplaatsen te vinden waar zaken worden aangeboden die in een normale winkel niet thuishoren. Deze marktplaatsen worden in veel gevallen gerund door criminelen, of hebben op de achtergrond een netwerk van criminelen waarmee samengewerkt wordt om de zaak draaiende te houden. Het bestaan van deze online zwarte markten brengt reële risico’s met zich mee voor consumenten.

Referenties

The Underground Credentials Market, Shulman, A. http://dx.doi.org/10.1016%2fS1361-3723(10)70022-1

Cyber crime black market almost as big as illegal drugs industry now http://venturebeat.com/2012/07/12/cyber-crime-rasmussen/

Cybercrime Inc.: The Business Of The Digital Black Market http://www.darkreading.com/attacks-breaches/cybercrime-inc-the-business-of-the-digit/240145072

Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees) http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/

COMMIT/TimeTrails

Wie, Wat, Waar, Wanneer

eurocottage UNIVERSITEIT TWENTE. ARCADIS

Door: Maurice van Keulen(*), Victor de Graaff(*), Zhemin Zhu(*), Rolf de By($), Andreas Wombacher(*), Jan Flokstra(*) (*)DB-groep [1], Faculteit EWI; ($)GIP-groep [2], Faculteit ITC

Het project en onze partners

Het TimeTrails-project[3] gaat over data mining in grote hoeveelheden gegevens over gebeurtenissen in ruimte en tijd, d.w.z. met coördinaten en time-stamps. Dergelijke gegevens worden doorgaans vergaard door mensen, sensoren en wetenschappelijke observaties. Gegevensanalyse richt zich vaak op de vier W's: Wie, Wat, Waar en Wanneer. Een belangrijke kwestie is het kunnen behappen van de grote hoeveelheden gegevens, d.w.z. "big data". Vanuit de UT werken we, d.w.z. de groepen EWI/DB en ITC/GIP, aan twee applicaties:

- Het in kaart brengen van de mening van het publiek bij grote infrastructuurproject zoals de aanleg van een nieuw stuk snelweg. Dit doen we met Twitteranalyse en data-visualisatie.

- Het vinden van goede vakantiebestemmingen. Hierbij spelen Social media, web harvesting en analyse van GPS-traces een rol.

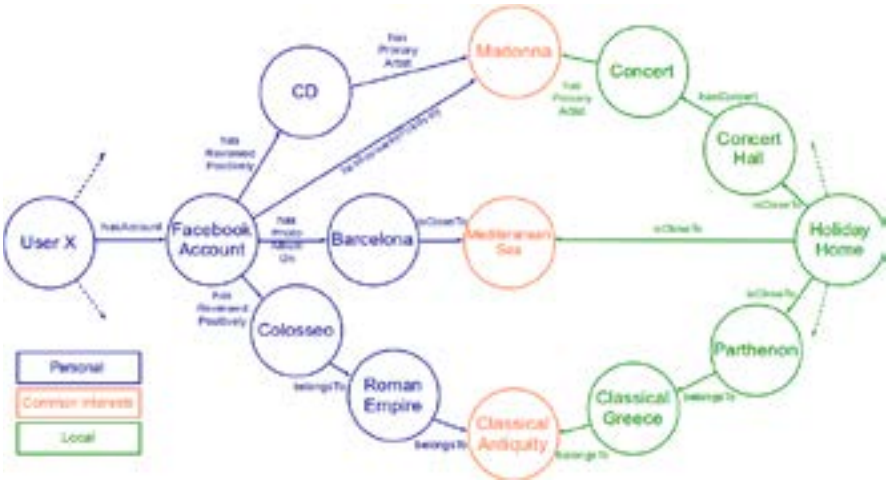
De COMMIT/-manier van onderzoek doen

TimeTrails is één van 16 projecten in het COMMIT/-programma. Een van de principes van COMMIT/ is het werktafel-model: elke universiteit of onderzoeksinstelling werkt nauw samen met één of enkele bedrijven. Zo werken wij in de eerste applicatie samen met Arcadis[4] en in de tweede met EuroCottage[5]. Een ander principe van COMMIT/ is use-inspired: de bedrijven bepalen niet wat er onderzocht moet worden, maar zijn inspiratie voor onderzoek dat uiteindelijk de maatschappij en de economie van Nederland echt kan verbeteren. Er wordt in COMMIT/ veel aandacht besteed aan onderzoeksresultaten uitwerken tot bruikbare software en communiceren naar een breed publiek.

> "Geografische data kan ons helpen bij het maken van beslissingen. De vraag is nu: hoe?"

De mening van het publiek bij grote infrastructuurprojecten

Arcadis is een internationaal bedrijf dat onder meer diensten levert rondom grote infrastructuurprojecten. Arcadis wil graag meer grip krijgen op wat het publiek vindt over zo'n project, bijvoorbeeld wat omwonenden vinden van een bepaald snelwegtraject of de locatie van een afrit. Twitter zou hen die informatie kunnen geven. Hoewel tweets over van alles kunnen gaan, worden ze voornamelijk gebruikt om meningen en gevoelens te uiten over wat er om ons heen



Figuur 1: Een goede match tussen gebruiker en vakantiehuisje.

gebeurt. We werken zowel aan het kunnen visualiseren van discussies op een kaart en tijdslijn als ook aan taalanalysetechnologie. Met het laatste hebben we recentelijk een Twitter-analyse challenge gewonnen [3]. Uiteindelijk hopen we de redenen voor bepaalde meningen te kunnen achterhalen.

Het vinden van goede vakantiebestemmingen

EuroCottage is een bedrijf dat vakantiehuizen door heel Europa aanbiedt. Vakantiegangers hebben over het algemeen een helder beeld van hoe de vakantie eruit moet zien: een wintersport-vakantie, een strandvakantie, een fietstocht, etc. In welk land dit plaats zal gaan vinden is meestal van ondergeschikt belang. Toch is juist dit laatste de vraag die als eerst gesteld wordt op vakantie-websites (zie Figuur 2). Door middel van "geo-social recommender systems" proberen wij de match tussen vakantieganger en vakantiehuisje op een hele andere manier te benaderen.

We zoeken voor ieder vakantiehuisje naar interessante objecten in de buurt. Deze informatie stamt uit vele verschillende online bronnen, zoals Wikipedia, de Gouden Gids, restaurant-websites, etc. De vakantieganger kan dan d.m.v. andere bronnen (bijv. een Facebook-profiel, GPS traces, of d.m.v. een wizard) een gebruikersprofiel vullen. Het systeem zoekt dan hiermee naar goede matches met vakantiehuisjes. Als een gebruiker bijvoorbeeld graag op vakantie gaat rondom de Middellandse zee, en een fan is van Madonna en de klassieke oudheid, dan kan deze gebruiker een aanbeveling krijgen voor een Grieks vakantiehuisje in de buurt van een Madonna-concert (zie Figuur 1).

Figuur 2: op zoek naar een strandvakantie.

Tot slot

Ben je geïnteresseerd in data mining, natuurlijke taal-analyse, data-visualisatie, big data, web harvesting of het omgaan met beperkte gegevenskwaliteit [2]? Of zoek je naar een afstudeeropdracht, mogelijk deels bij het ITC? Wil je op de hoogte gehouden worden? Neem gerust contact op met Maurice van Keulen (m.vankeulen@utwente.nl).

Referenties

[1] de Graaff, V. and van Keulen, M. and de By, R.A. "Towards Geosocial Recommender Systems". In: 4th International Workshop on Web Intelligence & Communities (WI&C 2012), 16 Apr 2012, Lyon, France. pp.8:1-8:4.http://eprints.eemcs.utwente.nl/21619/

[2] Keulen, M. (2010) "Onzekere databases". DB/M: database magazine, 21 (4). pp. 22-27. ISSN 0925-6911.http://eprints.eemcs.utwente.nl/18030/

[3]Habib,M.B.andvanKeulen,M.and Zhu, Zhemin , "Concept Extraction Challenge: University of Twente at #MSM2013". In: Proceedings of the 3rd workshop on 'Making Sense of Microposts' (#MSM2013), 13 May 2013, Rio de Janeiro, Brazil. Best IE challenge submission. http://eprints.eemcs.utwente.nl/23249/

KPMG

Business Intelligence afdeling

Door: Mark Steunenberg
Junior Adviseur, KPMG Management Consulting

Mark Steunenberg is bij veel Inter-*Actief* leden nog wel bekend als oud-bestuurder en functionaris onderwijs in 2008-2009. Na het afronden van de master Business Information Technology werkt hij nu fulltime bij KPMG op de afdeling Business Intelligence. Hij woont in Leiden en vertelt over zijn ervaringen bij KPMG.

Aangekomen in het café van KPMG valt direct op dat er een grote zeepkist staat. Mark vertelt dat het doel van de zeepkist niet is om "out of the box", maar juist "in the box" te denken. In de zeepkist staat een camera opgesteld waarbij medewerkers van KPMG iets kunnen vertellen over iets wat op het moment dagelijks gebruik is binnen hun afdeling, maar waar de rest van KPMG nog veel van kan leren. Mark vertelt dat zijn afdeling bezig is om een eigen hoekje te creëren waarin verschillende dashboards en best practices van de afdeling komen te hangen. Dit gaan zij als zeepkistidee indienen.

Van start bij KPMG; hoe ben je begonnen bij KPMG?

Vanaf december 2011 ben ik zeven maanden bij KPMG bezig geweest met afstuderen. Tijdens die periode heb ik de mogelijkheid gehad om de KPMG-organisatie te leren kennen. Het leuke tijdens zo'n periode is dat je dan ook alle trainingen mag volgen, zoals de KPMG summer school, maar ook de meer inhoudelijke, technische trainingen.

In september ben ik fulltime aan de slag gegaan bij KPMG, en ik werd toen direct op een groot project gezet. Dit was een zwaar project waarbij we een dashboard voor een financieel systeem ontwikkelden. Bij dit project werkten we op een agile manier, in sprints van zes weken. Na elke zes weken was er een meeting om het resultaat te beoordelen. Omdat de opdrachtgever niet direct een grote investering wilde doen zonder zeker te zijn van resultaat, gaf deze manier van werken de opdrachtgever de mogelijkheid om iedere keer de investering te rechtvaardigen. We boekten veel vooruitgang, waardoor we steeds weer door konden. Uiteindelijk heb ik hier tot en met afgelopen februari aan gewerkt.

Wat doet de Business Intelligence afdeling?

De Business Intelligence afdeling is onderdeel van IT Management Consulting binnen de Advisory-tak van KPMG. Er werken ongeveer 24 mensen. De afdeling helpt bedrijven op verschillende niveaus binnen Business Intelligence. Vaak heeft een bedrijf veel data over wat er binnen het bedrijf gebeurt, maar weten ze niet goed wat die data betekent, of wat ze ermee moeten. Het begint dan met kijken welke data er beschikbaar is. Soms kom je er dan achter dat er hele domme fouten in de data zitten. Zoals bij data over baby's geboren in de afgelopen vijf jaar. Hier bleken geboortedata tussen te zitten uit de jaren '80. Iets wat dus helemaal niet mogelijk zou mogen zijn. Uiteindelijk bleek dit de geboortedatum van de moeder te zijn. Als je eenmaal weet welke data je hebt, kan je daar analyses op uitvoeren. Zo kan je een analyse uitvoeren op hoe eenzelfde behandeling in verschillende ziekenhuizen wordt uitgevoerd. Hieruit kan blijken dat een aanpassing in de behandeling voordelen kan opleveren voor de genezing. Soms is de analyse eenmalig (one-time analytics), maar vaak genoeg moet er een dashboard komen dat gekoppeld wordt met systemen binnen het bedrijf. Het leuke hieraan is dat je soms heel operationeel bezig bent (welke systemen levert de data aan) en soms heel strategisch (met welke KPI's stuur je een bedrijf).

Wat is jouw rol binnen de afdeling?

Ik ben nu vooral bezig op het gebied van Analytics en Dashboarding . Ik vind het erg leuk en ik had niet verwacht dat ik na mijn studie Business & IT in staat zou zijn om dit soort applicaties te ontwikkelen. We werken vaak met QlikView, wat het ontwikkelen van een dashboard makkelijk maakt. QlikView is een softwarepakket waarmee je eenvoudig mooie grafische weergaven van data kan maken; dat scheelt in ontwikkelingskosten.

Wat doe je nu?

Sinds het afronden van het project ben ik bezig met een aantal kleinere projecten. Daarnaast ben ik bezig om samen met een aantal collega's een 3D printing event op te zetten. Leuk om even in een heel ander kennisgebied te duiken. Het is erg leuk om dit soort dingen er naast te kunnen doen en dat geeft mij erg veel energie. Daarna begin ik weer met een nieuwe grote opdracht. Dan met een heel internationaal team met mensen uit Rusland, Italië, Egypte, etc. Ik kijk er nu al naar uit!

Bedankt voor het interview!

Quinity

E-Business voor verzekeraars

Door: Fleur Aalbersberg
Werknemer Quinity

Bij deze 'op bezoek bij' zijn we bij Quinity, een bedrijf dat e-business oplossingen maakt voor verzekeraars. Ik spreek daar met Fleur Aalbersberg. Geen onbekende voor Inter-Actief: zij was namelijk de voorzitter van het 22e bestuur van onze vereniging!

Wat doe je nu bij Quinity?

Ruim zes jaar geleden ben ik bij Quinity aan de slag gegaan als consultant. Quinity is een bedrijf dat verzekeraars een geïntegreerd webbased polis- en schadeadministratie systeem biedt: de Quinity Insurance Solution (QIS). Als consultant adviseer ik verzekeringsmaatschappijen hoe wij hun polisadministratie het beste kunnen automatiseren met behulp van QIS.

Waarom heb je voor Quinity gekozen?

Eigenlijk om dezelfde reden waarom ik voor de UT heb gekozen: er werken veel slimme koppen en toch is de sfeer informeel. Ik voel me hier absoluut geen nummer en ken iedereen uit het bedrijf. Daarnaast zijn de ontwikkelingsmogelijkheden erg goed. Doordat de lijnen erg kort zijn, en we 'maar' met 120 man zijn, kan je veel wendingen aan je carrière geven. Zo werk ik sinds een half jaar ook als recruiter, en zit ik ineens met studieverenigingen als Inter-Actief te praten over sponsorcontracten. Hartstikke leuk! Dat had ik voordat ik bij Quinity begon niet kunnen bedenken.

Hoe ziet een gemiddelde werkdag eruit?

Het klinkt cliché, maar elke werkdag is anders. Het ene moment werk je een functioneel of technisch ontwerp uit, het andere moment rij je richting de klant om een ontwerpvergadering te leiden. In mijn rol als consultant voer ik daarnaast verschillende rollen uit. Zo ben ik bijvoorbeeld ook vaktechnisch begeleider en peoplemanager. Hieronder een voorbeeld van een dag uit mijn agenda:

Wat is de indruk van Bas?

Bij het langsgaan van verschillende afdelingen van Quinity, kreeg ik snel een goed idee van de sfeer binnen Quinity: open en gezellig. Als je komt te werken bij Quinity volg je een opleidingstraject waar je direct een people manager aangewezen krijgt, die je begeleidt in je carrière binnen Quinity. Zo kan je met veel ambitie snel doorgroeien binnen Quinity, zoals Fleur heeft gedaan.

08:30-09:30	mails van klanten/collega's doorlezen en beantwoorden
09:30-12:00	Ontwerpsessie voorbereiden (o.a. prototype bijwerken n.a.v. vorige sessie/agenda/actielijst opstellen)
12:00-12:30	Werkoverleg
12:30-13:00	Lunch
13:00-16:00	Cursus 'Schade verzekeringsbedrijf' volgen
16:00-17:00	Technisch ontwerp van project X reviewen

Figuur 1: Een dag uit de agenda van Fleur

Gedurende de rondleiding kwam ook een belangrijk aspect naar voren dat speelt bij het werken met verzekeraars: de impact die je hebt als bedrijf. Omdat Quinity bedrijfskritische processen automatiseert moet het resultaat altijd veilig, betrouwbaar en van hoog niveau zijn. Zo is de programmatuur, maar ook het bedrijfspand is goed beveiligd. Dit is een onderdeel waarop niet veel nadruk gelegd wordt in je studie.

Ik wil Fleur bedanken voor een mooi bezoek!

Muziekpiraterij en de muziekindustrie

Feiten over de strijd tussen piraterij en de muziekindustrie

Door: Sebastiaan la Fleur
Gastschrijver

Iedereen is gek op muziek en de muziekindustrie heeft hier weet van. Waar we vroeger nog verhalen hoorde van opa waar een singletje maar 25 cent kost, is de muziek van tegenwoordig vrij prijzig. €20,- voor een nieuw album van 10 nummers is de regel en uiteraard proberen mensen hier onderuit te komen. Dit is waar het begin van de muziekpiraterij om de hoek komt kijken. Het is tegenwoordig vrij eenvoudig om, met het internet als medium, even snel illegaal een nummertje te downloaden.. Uiteraard was de muziekindustrie het hier niet mee eens en zie daar het begin van wat een aardige strijd zou worden. Er is veel gebeurd in de tussentijd maar waar is het nou mee begonnen, welke acties heeft de muziek industrie nou werkelijk genomen, is het downloaden nou echt zo schadelijk als beweerd wordt en wat voor alternatieven zijn er ondertussen op de markt gebracht om legaal van de eenvoudigheid van downloaden te kunnen genieten?

Komst van muziekpiraterij in 1999

Sinds de komst van het internet zijn er altijd mensen geweest die opkomen voor het vrije internet. Zo is IRC opgericht als vrij communicatiemiddel maar ook Napster.com was in 1999 opgericht als vrije downloaddienst om bestanden te verspreiden. Napster.com bleek al snel een makkelijke manier te zijn om muziek gratis te verspreiden en zelf albums samen te stellen. Na de komst en ondergang van Napster.com zijn er nog een aantal spirituele opvolgers geweest zoals Kazaa, LimeWire en het nog altijd populaire Torrent netwerk.

> "Even snel een nummertje downloaden"

De RIAA verdedigt

Het keerpunt in de strijd begon met de rechtszaak tegen Napster.com eind 2000. De RIAA (Recording Industry Association of America) had Napster.com aangeklaagd op een aantal punten: directe aantasting van het copyright, verdediging van eerlijk gebruik, medeplichtigheid aan aantasting van het copyright en indirecte aantasting van het copyright. Ze zijn door de rechtbank schuldig bevonden op alle gronden en verloren ook het hoger beroep. Door de gevraagde schadevergoeding van 26 miljoen dollar, ging Napster.com al snel failliet en sloot het mei 2002 zijn deuren. Al snel kwamen er alternatieve programma's zoals Kazaa maar ook deze werden voor de rechtbank gesleept. Ook LimeWire moest het onderspit delven door de RIAA.

Tegenwoordig heeft de RIAA zijn kanonnen gericht op het Torrent netwerk. Zo waren ze een grote speler in het SOPA/PIPA voorstel dat dergelijke partijen zoals de RIAA meer mogelijkheden moest geven tot het vervolgen van auteursrecht schendende websites. Ook is de RIAA in december 2012 tot een overeenkomst gekomen met vijf van de grootste internetproviders van de US en de MPAA (Motion Picture Assocation). In deze overeenkomst zullen gebruikers die de copyright schenden m.b.v. bijvoorbeeld het Torrent netwerk te maken krijgen met een "six-strikes" programma. Dit programma houdt in dat bijgehouden wordt hoe vaak een gebruiker illegaal download en vervolgens stappen onderneemt zoals de download snelheid verlagen of documentatie opstuurt over het illegale downloaden en de gevolgen. Na zes overtredingen mag de MPAA of de RIAA een strafrechtelijke zaak tegen

Figuur 1: RIAA Logo

de gebruiker beginnen met data verkregen van de provider.

Is het nou echt zo schadelijk?

De muziekindustrie heeft altijd beweerd dat het downloaden schadelijk is voor de inkomsten en dat klinkt logisch aangezien elk illegaal gedownload nummer niet de vraagprijs in het laatje van de uitgever brengt. Maar is dat nou echt waar? Kortgezegd, nee. In opdracht van de Europese Unie heeft er in 2013 een onderzoek plaatsgevonden naar de effecten die illegaal downloaden heeft voor de muziekindustrie. De bevindingen worden beschreven in de paper "Digital Music Consumption on the Internet: Evidence from Clickstream Data" van Luis Aguiar en Bertin Martens. Het onderzoek maakt gebruik van de clickstream data van 16,000 Europese consumenten. Uit het onderzoek volgt dat de gebruikers 0,2% meer kliks genereren op legale muzieksites wanneer de gebruikers de vrijheid krijgen om 10% meer kliks te genereren op illegale websites. Ook werd gevonden dat gebruikers 0,7% meer kliks op legale muziekwebsites doorbrachten als de hoeveelheid kliks op legale muziekstreaming websites met 10% omhoog ging. Er werden wel grote verschillen gevonden in de data tussen verscheidene landen. De reden voor dit laatste is onbekend maar ze speculeren dat het door het verschil in cultuur komt. Kortom, het lijkt erop alsof de mogelijkheid tot illegaal downloaden juist tot positieve resultaten leidt voor de muziekindustrie.

Digitale alternatieven

In de tussentijd zijn er ook een aantal bedrijven die de gulden tussenweg proberen te vinden door muziek aan te bieden dat online naar je apparaat gestreamd kan worden. Populaire en bekende voorbeelden hiervan zijn Spotify, Grooveshark en Rhapsody. Voor vaak €5,- tot €10,- per maand heeft men toegang tot een grote bibliotheek van verschillende nummers, artiesten en albums. Over de gelicenseerde muziek worden royalties betaald aan de rechthebbenden. In totaal werd in 2012 34% van de wereldwijde omzet verdient aan deze vorm van distributie. Dit zorgde voor de eerste stijging in totale waarde van de muziekindustrie sinds 1998 met een hoogte van 0,3%. Dit meldt het IFPI Digital Music Report 2013. Het lijkt dus een effectieve en voor consumenten een aantrekkelijke oplossing om het piraterij probleem tegen te gaan.

De muziekindustrie, onder leiding van de RIAA, probeert de rechten van de rechthebbenden al sinds 2000 te beschermen tegen piraterij. Ze hebben er voor gezorgd dat Napster.com, dat begon in 1999, failliet ging en zijn tegenwoordig nog volop in de strijd bezig tegen het Torrent netwerk met bijvoorbeeld het "six-strikes" programma. Deze strijd lijkt nutteloos aangezien onderzoek aantoont dat het illegaal downloaden zelfs leidt tot meer verkeer bij de legale muziek sites. Als reactie op deze strijd zijn er bedrijven gestart die muziek online aanbiedt. Dit laatste lijkt een oplossing te vormen voor het piraterij probleem.

"Piraterij leidt tot positieve resultaten"

Figuur 2 [Bron: Digital Trends]

Referenties

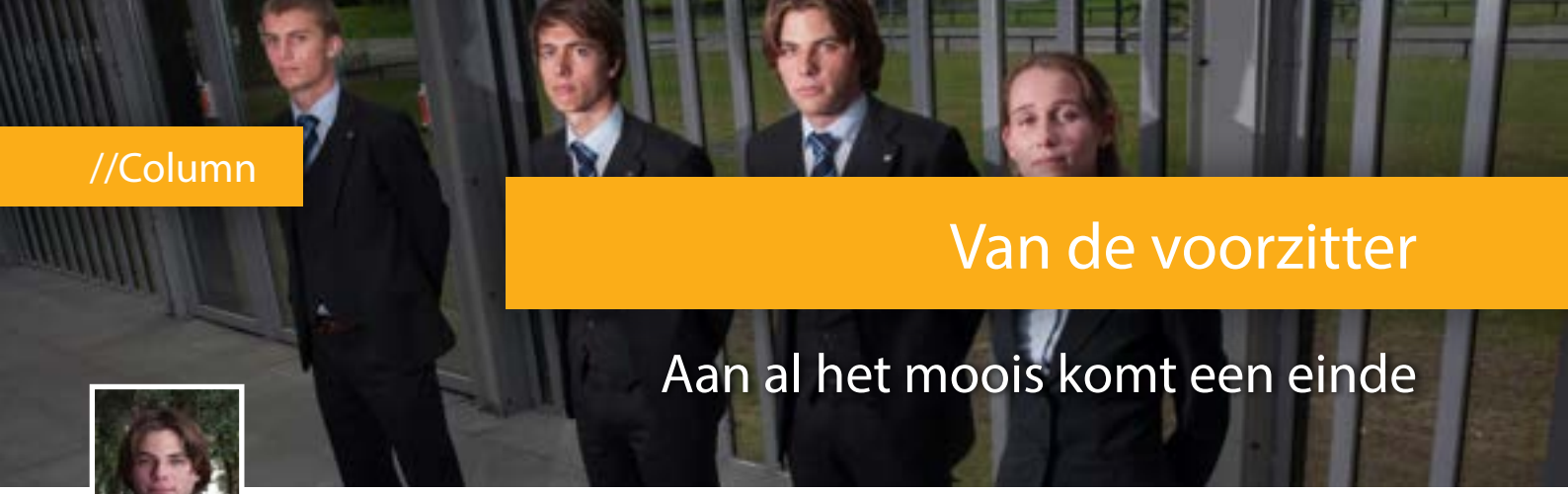
A&M Records, Inc. v. Napster, Inc. - Wikipedia
http://en.wikipedia.org/wiki/A%26M_Records,_Inc._v._Napster,_Inc.

Digital Music Consumption on the Internet: Evidence from Clickstream Data
http://ftp.jrc.es/EURdoc/JRC79605.pdf

Recording Industry Association of America - Wikipedia
http://en.wikipedia.org/wiki/Recording_Industry_Association_of_America

Napster - Wikipedia
http://en.wikipedia.org/wiki/Napster

IFPI Digital Music Report 2013 - Engine of a digital world
http://www.ifpi.org/content/library/DMR2013.pdf



//Column

Van de voorzitter

Aan al het moois komt een einde

Door: Pim Jager
Voorzitter Inter-Actief

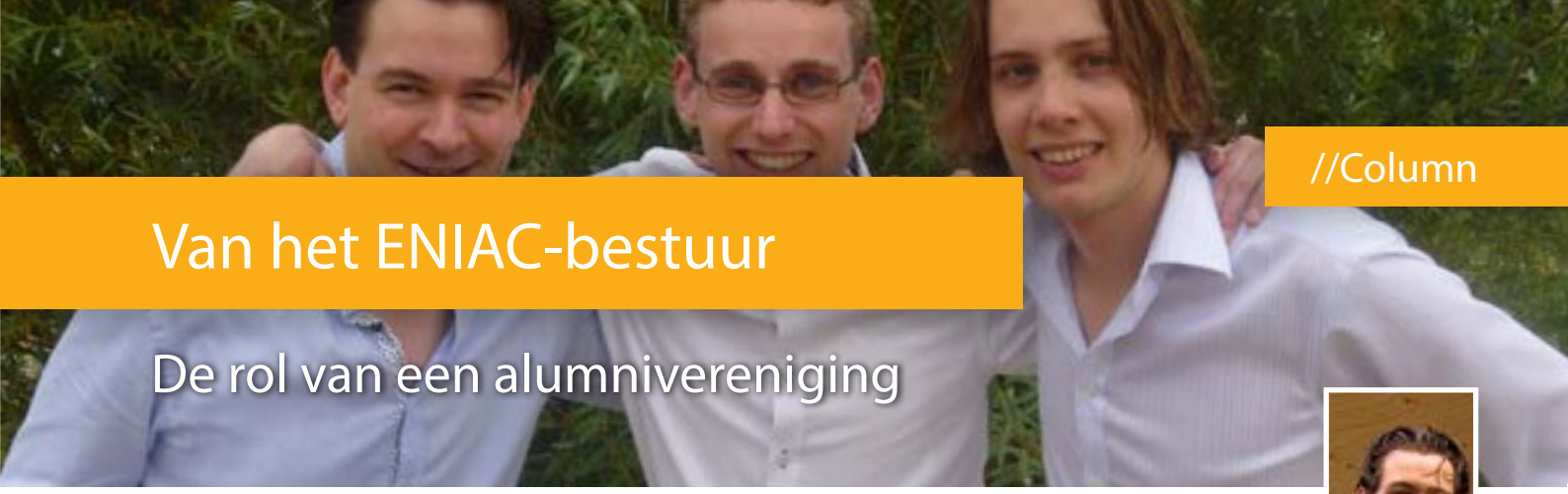
Pim Jager opende voor de eerste maal zijn ogen op 29 augustus 1990 in het altijd bruisende Utrecht. Na een glansrijke carrière op basisschool de Zonheuvel in het immer gezellige Driebergen (incidenteel ook de plaats waar Pim tot zijn studie in Twente woonachtig is geweest) was het tijd voor de volgende logische stap en begon Pim aan zijn VWO-opleiding aan het Revius Lyceum in het pittoreske Doorn. Na zes jaar was duidelijk dat het VWO-onderwijshemweiniguitdagingmeer kon bieden en het tijd was voor een nieuwe uitdaging. Deze nieuwe uitdaging vond Pim aan de Universiteit Twente, na een wat moeilijk begin, waarin de verkeerde keuzes zijn gemaakt (de nasleep van deze keuzes zijn nog terug te vinden in zijn primair lidmaatschap bij E.T.S.V. Scintilla) zag hij na twee weken studeren alsnog het licht en schreef hij zich in bij I.C.T.S.V. Inter-Actief. Na onder andere actief te zijn geweest in de ECie, Kick-IT, FlitCie, Cinema, TostCie en EWI-trip is hij tegenwoordig voorzitter van het 34e bestuur der I.C.T.S.V. Inter-Actief.

10 maanden, 44 weken, 307 dagen, 7368 uur, 442.008 minuten, 26.524.800 seconden. Aan al het moois komt een eind. Het lijkt wel vorige week dat we, als vier toen nog relatief onwetende individuen, gechargeerd werden als bestuur van Inter-*Actief*. Daar sta je dan, je krijgt een mooi speldje op, de sleutels van de kamer in je hand gedrukt en dan is het opeens jouw vereniging. Nu, ruim 10 maanden later, kunnen wij niet meer dan terugkijken op een fantastisch collegejaar.

Een jaar waarin wij als bestuur enorm gegroeid zijn, verschrikkelijk veel geleerd hebben en bovenal enorm veel plezier hebben gehad! Een jaar dat begon met een fantastische studiereis naar China en Zuid-Korea, een geslaagde LAN-party en een lezing van kolonel Hans Fölmer. De CIO van de Olympische Spelen in Londen heeft een lezing gegeven over de ICT-problemen en –oplossingen daarbij, we zijn weer op skireis geweest, is er voor de Dies een rially georganiseerd en hebben op 20 maart een groots, interessant en bovenal fantastisch landelijk symposium georganiseerd. Bij de Bata heeft het Inter-*Actief*-team harder gelopen dan ooit, tijdens Pandora hebben maarliefst 15 teams geholpen het mysterie op te lossen en tijdens de Business Course zijn Topicus, Capgemini en ING eens van dichterbij bekeken. Daarnaast hebben we tussendoor natuurlijk elke week geborreld, een lunchlezing gehad en nog veel meer prachtige, leerzame en gezellige activiteiten gehad.

Voor aankomend collegejaar zal er weer minstens zoveel moois georganiseerd worden. We zijn zeer tevreden dat het weer gelukt is een zes-koppig kandidaat-bestuur te vinden. Een kandidaat-bestuur dat te maken zal krijgen met uitdagingen door het Twents Onderwijsmodel en bezuinigingen binnen de UT en de faculteit EWI in het bijzonder. Maar vooral een kandidaat-bestuur waarin wij het vertrouwen hebben dat ze deze uitdagingen aankunnen en Inter-*Actief* tot nog grotere hoogtes kunnen stuwen. Een kandidaat-bestuur dat weer de ruimte heeft om projecten op te pakken en te innoveren. Kortom een kandidaat-bestuur dat, als ze eenmaal bestuur zijn, 10 maanden lang keihard zal werken aan een zo mogelijk nog mooiere vereniging.

Wij hebben in ieder geval van het afgelopen jaar genoten. Hierbij ook alle commissies, actieve leden en betrokken leden bedankt voor alle mooie dingen die we dit jaar hebben meegemaakt. Wij hebben ervan genoten en hopen, en verwachten, dat dat voor iedereen zo geldt. Geniet van de zomervakantie en tot september!



//Column

Van het ENIAC-bestuur

De rol van een alumnivereniging

Door: Rick Leunissen
Secretaris ENIAC

Onlangs kregen we als ENIAC bestuur vanuit het alumnibureau van de Universiteit Twente de vraag om samen met Inter-*Actief* het alumnibeleid voor INF/BIT/TEL op te stellen. Hierbij kregen we ook een aantal handvaten geboden om na te denken over onze doelgroep, maar ook over de rol van de studievereniging en welke activiteiten je hierbij wil ontplooien. De vraag van het alumnibureau was de trigger om weer eens terug te blikken naar wat we op dit moment als ENIAC allemaal doen. Daarnaast willen we in deze column vast vooruitkijken naar de mogelijkheden van een alumnivereniging, maar zijn we vooral benieuwd naar de input van de alumnus zelf.

Het doel van ENIAC is in het verleden als volgt opgesteld; "*Het doel van de vereniging is het onderhouden van contacten tussen alumni onderling en met de Faculteit Elektrotechniek, Wiskunde en Informatica (EWI) aan de Universiteit Twente*". De afgelopen jaren is dit doel voornamelijk ingevuld door het organiseren van informele activiteiten voor leden en de scriptieprijs voor net afgestudeerden. Daarnaast ontvangen leden van ENIAC al jaren de I/O Vivat met hierin de ENIAC column. Als bestuur hebben we de afgelopen 2 jaar de invulling van ons doel uitgebreid met het afstudeerdersevent voor bachelor alumni en is er dit jaar voor het eerst het ENIAC Scholarship uitgereikt voor masterstudenten met een buitenlandambitie. Hiermee willen we als bestuur studenten alvast bewust maken van ENIAC en ze op deze manier binden aan de alumnivereniging. Ook willen we dit jaar op het inhoudelijke vlak leden bij elkaar brengen door middel van een training of lezing.

Met deze activiteiten denken wij als bestuur een aardige invulling te geven aan het doel van ENIAC. Om in de toekomst invulling aan dit doel te geven zullen we echter wel rekening moeten houden met ontwikkelingen in de maatschappij. Een voorbeeld hiervan is de impact van internationalisering op de rol van de alumnivereniging. Op dit moment zien we al dat een aantal leden in het buitenland wonen en werken. Deze groep zal de komende jaren alleen nog maar toenemen. Om deze groep in de toekomst aan te blijven spreken zal er dus gezocht moeten worden naar een alternatief voor activiteiten in Nederland. Een ander voorbeeld is de impact van social media op de rol van de alumnivereniging. Het onderhouden van contacten tussen alumni onderling zal meer en meer via social media gaan lopen. Zo bevat LinkedIn op dit moment vergelijkbare informatie als het ENIAC jaarboek.

We kunnen natuurlijk nog meer voorbeelden bedenken van de veranderingen rol van de studievereniging. Waar we echter veel meer aan hebben is om te weten welke rol onze alumni graag zien van ENIAC. Daarom zullen we met het uitbrengen van deze I/O Vivat een discussie starten op LinkedIn om jullie visie op de alumnivereniging te horen. Graag zien we hier jouw input ook terug.

Rick Leunissen is secretaris van ENIAC: de ENschedese Informatica Alumni Club. ENIAC is de alumnivereniging voor oud-studenten Informatica, bedrijfsinformatietechnologie en Telematica aan de Universiteit Twente.

Voor slechts € 5,- per jaar kan je al lid worden van deze club. Je krijgt dan in ieder geval de Vivats die jaarlijks verschijnen (meestal zo'n 4 stuks, maar niet helemaal per kwartaal) en uitnodigingen voor de activiteiten die we organiseren (meestal per mail). Daar mag je dan vervolgens (veelal gratis!) aan deelnemen. En al doe je maar eens in de paar jaar ergens aan mee, die € 5,- kan toch bijna iedere informatica-alumnus wel missen? Zo houd je toch nog wat binding met je wetenschappe- lijke roots en af en toe contact met vrienden uit je studietijd.

Rick Leunissen
secretaris@eniac.utwente.nl

Dit is privé

Waarom het verplicht ontsleutelen van data averechts werkt

Door: Caspar Schutijser
Redacteur I/O Vivat

Minister van Veiligheid en Justitie Ivo Opstelten stuurde op 27 november 2012 een brief naar de Tweede Kamer met daarin de resultaten van het onderzoek dat hij heeft laten uitvoeren naar de mogelijkheden voor een wettelijk decryptiebevel. Dit houdt in dat er een bevel kan worden gegeven om versleutelde gegevens door een verdachte zelf te laten ontsleutelen. Opstelten zou graag zien dat een dergelijke wet wordt ingevoerd. Aan zo'n wettelijk decryptiebevel zitten echter wel wat haken en ogen.

De aanleiding

Als argument voor het invoeren van een wettelijk decryptiebevel draagt Opstelten onder andere de Amsterdamse zedenzaak met Robert M. (de hoofdverdachte in deze zaak) aan. Het ging in deze zaak om een grote hoeveelheid kinderporno, welke Robert M. zorgvuldig versleuteld had op zijn computer. Hij is hiervoor opgepakt door de politie en na een paar weken van verhoor werkte hij mee aan het onderzoek door de bestanden te ontsleutelen. Wettelijk was hij hiertoe niet verplicht. Opstelten ziet graag dat er een bevel kan worden gegeven om bestanden te ontsleutelen, ondanks het feit dat Robert M. heeft meegewerkt aan het ontsleutelen van zijn bestanden. Dit zou goed zijn voor "een effectieve bestrijding van de vervaardiging, de verspreiding en het bezit van kinderpornografie".

Mogelijkheden wetgeving

Opstelten noemt drie mogelijke implementaties van een wettelijk decryptiebevel. De eerste mogelijkheid houdt in dat aan de verdachte een bevel tot ontsleuteling kan worden gegeven. De verdachte kan zich bij deze mogelijkheid echter beroepen op zijn zwijgrecht, waardoor hij dus niet verplicht is om zijn wachtwoord af te geven. Als de verdachte zich beroept op zijn zwijgrecht, kan dat wel gevolgen hebben; zo kan de verdachte langer "voorwerp van onderzoek" zijn.

De tweede mogelijkheid houdt in dat er een verzoek of bevel kan worden gegeven. Bij een verzoek kan de officier van justitie toezeggen dat de ontsleutelde bestanden niet als bewijs tegen de verdachte gebruikt zullen worden. De wet wordt dan wel zodanig aangepast dat het niet nakomen van het bevel strafbaar kan worden gesteld.

De derde mogelijkheid houdt in dat er een bevel tot ontsleuteling kan worden gegeven, waarbij aan weigering consequenties kunnen worden verbonden. Hierbij kan gedacht worden aan strafbaarstelling van weigering of "een expliciete strafverhogingsgrond voor het betreffende gronddelict in het Wetboek van Strafrecht".

Kritiek

Vanuit meerdere hoeken wordt er kritiek geuit op het voorstel van Opstelten en op bijvoorbeeld het idee van het CDA om de strafmaat te verhogen voor verdachten die hun wachtwoorden niet afgeven. Het bedrijf Fox-IT reageerde op het voorstel van het CDA. Om meerdere redenen vindt Fox-IT dit een slecht idee. Zo beschrijft de blogger van Fox-IT het concept "Deniable Encryption". Dit houdt in dat een versleuteld bestand met verschillende wachtwoorden ontsleuteld kan worden. Dit betekent bijvoorbeeld dat je met het ene wachtwoord de "geheime" gegevens ontsleutelt (bijvoorbeeld kinderporno) en met het andere wachtwoord de "niet-geheime" gegevens (bijvoorbeeld plaatjes van de achtertuin). Op deze manier is het dus mogelijk voor een verdachte om een wachtwoord te geven voor de niet-geheime gegevens, de gegevens waar de opsporende instantie helemaal niet naar op zoek is. Bewijs dat de geheime gegevens te benaderen zijn met een ander wachtwoord is er niet. Wanneer een verdachte Deniable Encryption gebruikt, heeft een wettelijk decryptiebevel dus helemaal geen zin; de verdachte heeft dan wel zijn wachtwoord gegeven maar de bestanden waarnaar wordt gezocht, worden niet gevonden.

Bits of Freedom, een Nederlandse organisatie die opkomt voor vrijheid en privacy van de burger op het internet, heeft ook kritiek op het voorstel van Opstelten. Opstelten schrijft dat er in het door hem aangevraagde onderzoek staat dat het gebruik van versleuteling door computergebruikers toeneemt. In hoeverre dit een probleem is, is echter

niet duidelijk. Bits of Freedom heeft contact gehad met het Openbaar Ministerie (OM) en uit de correspondentie blijkt dat het OM geen data bijhoudt over moeilijkheden bij het openen van versleutelde bestanden. Er zijn dus geen harde cijfers waaruit de conclusie kan worden getrokken dat versleuteling een (groot) probleem is voor de politie bij de bestrijding van bijvoorbeeld kinderporno.

Verder vraagt Bits of Freedom zich af wat er gebeurt als iemand zijn wachtwoord is vergeten. Als een verdachte zijn wachtwoord vergeten is en dat als reden aandraagt om het wachtwoord niet te geven, dan kan een rechter ervoor kiezen hem niet te geloven en hem te straffen voor het feit dat hij zijn wachtwoord niet afgeeft. Een gevolg hiervan zou kunnen zijn dat mensen om deze reden hun gegevens niet meer willen versleutelen en dat zou Nederland alleen maar onveiliger maken, aldus Bits of Freedom.

> “Wat gebeurt er als iemand zijn wachtwoord is vergeten?”

Alternatieven voor het voorstel

Wetgeving zoals voorgesteld door Opstelten zou het werk van de politie kunnen verlichten, is de gedachte. Als voornaamste reden van het mogelijkerwijs invoeren van deze wetgeving noemt Opstelten de Amsterdamse zedenzaak en de bestrijding van kinderporno in het algemeen. Fox-IT schrijft dat ze liever ziet dat de politie infiltreert in kinderporno-groepen, of dat de politie deze groepen hackt. Ook Bits of Freedom ziet een decryptiebevel niet als oplossing voor seksueel misbruik van kinderen. In plaats daarvan ziet ze liever dat de opsporing effectiever en efficiënter wordt gemaakt.

Fouten bij zaak Robert M.

In het geval van Robert M. kan worden gesteld dat de politie fouten gemaakt heeft. Op het moment dat de politie binnenviel bij Robert M. stond zijn computer namelijk aan. Dit kan betekenen dat de bestanden van Robert M. ontsleuteld waren, waardoor het bewijs dus voor het oprapen lag. De politie heeft de computer van Robert M. echter uitgezet. Dit houdt in dat eventuele ontsleutelde bestanden weer ”gesloten” worden, dus dat de politie niet meer bij de data kan komen. Volgens experts had de politie dit dus beter kunnen aanpakken. De computer van Robert M. had niet uitgeschakeld mogen worden, maar moeten worden onderzocht door experts terwijl hij nog aanstond. Het feit dat de computer werd uitgezet door de politie lijkt erop te duiden dat er te weinig kennis over versleuteling bij de politie is. Als de politie door deze kennis wel bij de kinderporno had kunnen komen, betekent dit dat een decryptiebevel helemaal niet nodig is. In plaats daarvan moet de politie haar kennis snel op peil brengen, zo lijkt het. Daarna kan gekeken worden naar aanpassing van de wetgeving.

Verder is het opvallend dat Robert M. gewoon aan het werk kon in Nederland. In het jaar 2003 is Robert M. namelijk al veroordeeld voor het in bezit hebben van kinderporno. Dit gebeurde in Duitsland. Volgens staatssecretaris Teeven van Veiligheid en Justitie kon Robert M. toch gewoon in Nederland aan het werk omdat de veroordelingen in Duitsland hier niet bekend zijn. Hierdoor kon Robert M. ongestoord aan het werk bij een crèche.

Conclusie

Naast het feit dat een decryptiebevel geen directe oplossing biedt tegen kindermisbruik, is er geen hard bewijs voor het feit dat versleuteling de opsporing en vervolging van deze groepen bemoeilijkt. Hieruit kan geconcludeerd worden dat minister Opstelten graag een decryptiebevel wil invoeren, maar dat er over de noodzaak en uitvoerbaarheid nog goed moet worden nagedacht. Als Opstelten daarnaast de zedenzaak van Robert M. blijft aandragen als argument voor een decryptiebevel, dan gaat hij voorbij aan het feit dat het rechtssysteem van Nederland in dit geval beter had kunnen presteren, door een al veroordeelde pedofiel niet ongestoord zijn gang te laten gaan.

Referenties

http://blog.fox-it.com/2011/06/02/over-het-cda-en-het-bestraffen-van-gebruik-van-crypto/

http://blog.iusmentis.com/2012/11/29/kan-een-ontsleutelplicht-voor-verdachten-worden-ingevoerd/

https://www.bof.nl/2012/11/28/decryptiebevel-werkt-niet-en-maakt-nederland-onveiliger/

https://www.bof.nl/over-ons/

Brief aan de Tweede Kamer van minister Opstelten, 27 november 2012. http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2012/11/28/brief-over-onderzoek-naar-wettelijk-decryptiebevel.html

https://en.wikipedia.org/wiki/Deniable_Encryption

https://www.bof.nl/2012/02/16/encryptie-geen-groot-probleem-voor-politie/

http://rickey-g.blogspot.nl/2011/01/blunder-van-politie-thtc-bij-arrestatie.html

http://nos.nl/artikel/205721-robert-m-al-in-duitsland-betrapt-op-kinderporno.html

Op bezoek bij Thales Nederland

een interview met Tom Griffioen (links) en Hugo Anbeek (rechts)

Door: Tom Griffioen en Hugo Anbeek

Beiden werken bij Thales Nederland te Hengelo. Tom heeft Elektrotechniek gestudeerd aan de Universiteit Twente en Hugo heeft technische natuurkunde aan de Universiteit Twente gestudeerd. Ze werken nu allebei ongeveer 4 jaar bij Thales en vertellen over hun dagelijkse werkzaamheden en andere ervaringen als Young Professional binnen Thales.

Wat doe je nu bij Thales?

Hugo: "In mijn dagelijkse werk houd ik mij bezig met het bepalen en analyseren van operationele radar performance. Met behulp van complexe modellen simuleren we wat de detectie-afstand van onze radarsystemen is tegen verschillende doelen (dreigingen)- onder verschillende atmosferische omstandigheden. Bij het ontwikkelen van modellen, het simuleren en analyseren van simulatieresultaten maak ik elke dag opnieuw gebruik van de kennis die ik tijdens mijn studie heb opgedaan."

Tom: "Als system engineer is het belangrijk systeem performance en subsysteem performance op elkaar af te stemmen. Neem bijvoorbeeld een verzonden signaal. Een radar zendt, net als sonar, een signaal uit dat reflecteert op het doel en weer terug valt op de radar. Zonder verder diep op de details in te gaan heeft de kwaliteit van dit signaal (gegenereerd door de signaal generator op subsysteem niveau) invloed op de performance van de radar (systeem niveau)."

Wat gebruik je nog van je studie?

Hugo: "Netwerktheorie tot en met signaaltheorie en veel wiskunde. Dit kan je allemaal toepassen op de techniek. Bij Thales kan je terecht met veel verschillende disciplines, van werktuigbouwkunde tot elektrotechniek tot IT."

Tom: "Het leuke is dat ik zeker nog 50% gebruik van wat ik heb geleerd tijdens mijn studie. Je werkt hier aan complexe systemen en de optimalisatie gaat heel ver. Elke beslissing die je neemt kan verregaande gevolgen hebben voor het systeem."

Hugo: "Het is echt High Tech, je moet op de hoogte blijven van de laatste stand van zaken omtrent de nieuwste technologische ontwikkelingen en de wetenschap."

Tom: "Als voorbeeld heb je een radar die je nu ontwikkelt en pas over 7 jaar aflevert; in die 7 jaar gebeurt er heel veel in de techniek. Ook al maak je de radar daarna opnieuw, dan heb je te maken met nieuwe technieken en nieuwe mogelijkheden."

Hugo: "We werken nauw samen met de TU's, maar we ontwikkelen hier zelf veel nieuwe technologieën, verder doen we research waardoor de TU ook weer van onze kennis gebruik kan maken."

Waarom heb je voor Thales gekozen?

Tom: "Mijn vader werkte bij Defensie als bouwkundig architect. Ik ging een keer mee naar de Marinedagen en het enige wat ik zag was een ronddraaiende radar. Jammer dat de Phased-Array radars (Red: op alle vier de zijden zitten radarantennes, zodat het systeem niet meer rond hoeft te draaien) niet meer draaien. Nu werk ik aan de SMART-L EWC (Red: lange afstand radar tegen ballistische raketten, zie foto Tom en Hugo), die draait weer wel."

Hugo: "Mijn vader werkte vroeger bij Thales dus ik kende het bedrijf en de verhalen. Hiervoor heb ik bij de NAVO gewerkt. Ik was dus al bekend met de Defensiewereld en die wereld vond ik heel interessant."

Wat is dan interessant?

Hugo: "De diversiteit in projecten. Je doet bij Thales geen alledaagse dingen, je werkt aan High Tech systemen. Dat geeft een enorme kick."

Tom: "Je opereert echt op wereldniveau en het is 'grote jongens speelgoed'."

Hoe ziet een gemiddelde werkdag eruit?

Tom: "Heel verschillend. De ene dag werk je aan een project en moet je heel veel overleggen om te kijken

wat we willen en kunnen, terwijl ik de

andere dag de hele dag aan het simuleren en modelleren ben."

Hugo: "Nee je werkt nooit aan één project tegelijk. Soms werk je aan iets intern terwijl je de volgende keer met de klant zit en vragen moet stellen als; wat heb je nodig? Wat past bij jullie? Met welke dreiging hebben jullie te maken? Hier moet je dan weer analyses op loslaten en engineers opzetten."

Aan wat voor projecten werken jullie nu?

Hugo: "Nu werk ik aan een paper voor een conferentie, dit doen we in nauwe samenwerking met TNO en daarnaast ook aan de gatekeeper en de goalkeeper."

Tom: "SMART-L en het STARS project http://starsproject.nl/."

Hoe zou je de cultuur bij Thales omschrijven?

Hugo: "Je hebt heel veel verschillende mensen die hier werken en het verschilt per afdeling. Daarnaast is het gemiddelde werk niveau heel hoog. Bijna alleen HBO en WO en dit is een leuke mix."

Tom: "Er is een hoge gemiddelde leeftijd, maar van deze oudere mensen kan je als jong persoon heel veel leren. Dit bedrijf is juist dankzij de jarenlange ervaring en kennis wereldleider geworden op het gebied van marine radarsystemen. Over het algemeen is er ruimte genoeg om je eigen ideeën in te brengen."

Hugo: "In het begin moest ik even schakelen. Ik was jong en ambitieus en nam een sprint. Ik werd wel even afgeremd, maar dat kan niet anders. Bij Thales heb je één á twee jaar nodig om de wereld en de techniek erachter te begrijpen. Je hebt bepaalde ervaring en kennis nodig voordat ze je naar de klant laten gaan. Het is niet een alledaags product dat als je het niet aan de één kan verkopen, je naar de buurman kan gaan. Deze wereld is delicaat en potentiële klanten kan en mag je niet kwijtraken."

Tom: "Wat verder leuk is dat als je hier werkt, je langzaamaan ook doorkrijgt dat je projecten/opdrachten naar je toe kunt trekken. Zo kan je je door de organisatie heen manoeuvreren. Je moet hier proactief zijn, anders wordt het niets."

Waar ben je trots op?

Tom: "Ons hele productportfolio. Als je bijvoorbeeld naar een land in Zuid-Amerika gaat hebben ze onze sensoren op hun schepen staan. Onze aanwezigheid in de wereld is gigantisch."

Hugo: "Daarnaast moeten we altijd opnieuw op technisch vlak blijven innoveren ten opzichte van de concurrent. Dat houd je scherp."

Tom: "De complexiteit van de systemen en het proces. Je werkt met gemak met 100 mensen aan één project. Dat moet ook gecoördineerd worden. Zelfs universiteiten vragen ons wat we nodig hebben qua techniek en vragen ons om nieuwe technieken. Dat zie ik als een goede referentie en als uitdaging."

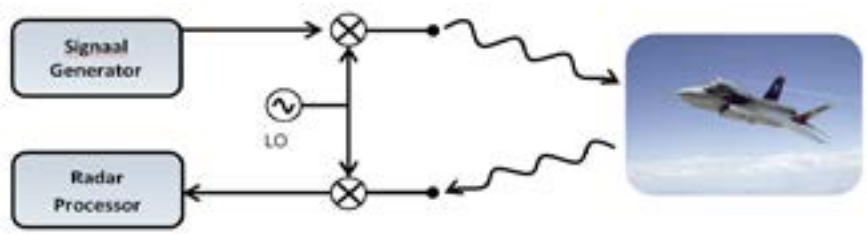
Heb je nog laatste toevoegingen?

Tom: "Ja, je kan hier je hele leven blijven werken. Mijn vrouw denkt dan; 'saai zeg', maar er is hier zoveel te doen. Het is niet saai, het is gewoon echt interessant en divers werk. Wil je meer met mensen werken? Wil je meer alleen werken? Bespreek het en het behoort tot de mogelijkheden. Ik vind het wel jammer dat de man/ vrouwverhouding binnen Thales scheef is. Het lijkt me leuk als er meer vrouwen zouden werken."

Hugo: "In het begin is het wel lastig en moet je even wennen, je moet jezelf de tijd gunnen om alles te leren en je de systemen eigen te maken maar na twee jaar ben je echt op stoom."

Tom: "Ja, dat merk je en je ziet ook dat de mensen die hier werken echt gepassioneerd zijn voor het vak. Dat kan ook niet anders, maar iedereen gaat er voor de volle 100% voor. Ik hoorde van de 34 WO-ers die hier de afgelopen drie jaar zijn aangenomen, er in totaal maar drie zijn weg gegaan."

"Altijd opnieuw op technisch vlak blijven innoveren"



Figuur 1: Radar principe

Thales Nederland

Actief in de sectoren Aerospace, Defense en Security is Thales Nederland met 1.800 medewerkers de topaanbieder van hightechbanen. Productinnovatie en snel inspelen op de nieuwste technologische mogelijkheden zijn onze drijfveren. Spraakmakende voorbeelden daarvan zijn radar-, communicatie- en command & controlsystemen voor marineschepen en communicatie-, beveiligings- en betaalsystemen voor het bedrijfsleven. Thales Nederland is onderdeel van de Thales Group met 70.000 medewerkers in ruim 50 landen, waarvan 22.000 werkzaam in R&D en daarmee is Thales een van Europa's grootste elektronicabedrijven en heeft wereldwijd een uitermate sterke positie.

www.thalesgroup.com/nl

www.facebook.com/thalesnederland

wytske.oijevaar@nl.thalesgroup.com

De bits en bytes van Bitcoin

Het cryptogeld uitgelegd

Door: Rick van Galen
Redacteur I/O Vivat

Bitcoin is verworden tot een mysterieus geldalternatief op het internet. De digitale cryptovaluta is het meest populaire 100% digitale alternatief aan het worden. In dit artikel bekijken we de ins en outs van Bitcoin – wat zijn de eigenschappen van dit cryptografische geld, en hoe werkt het nu precies?

Wat is geld eigenlijk? Als je dagelijks muntjes in frisdrankautomaten stopt en je boodschappen met je pinpas afrekent, sta je niet altijd stil bij wat die metalen klompjes of digitale certificaten die je verstuurt nu eigenlijk betekenen. Geld is uitgevonden als een uniforme manier om economische waarde te representeren en in te kunnen wisselen. Het klinkt onzinnig om te vragen hoeveel kilo graan een koe waard is of hoeveel liter melk een tuinman per uur zou moeten verdienen. Dit komt omdat het heel moeilijk is om het een in termen van het andere uit te drukken – geld is een handige manier om economische waarde te definiëren. Daarnaast functioneert het als een ruilmiddel in die context. Geld kan worden gebruikt om die economische waarde te representeren aan elkaar.

Om als ruilmiddel te kunnen gelden, moet geld moeilijk zijn om te maken. Als dit niet het geval is kan een ruilmiddel worden gemaakt zonder dat er economische waarde achter zit, en dan verliest geld de eigenschap om als uitwisselingseenheid te dienen. In de praktijk van 'gewone' valuta werd dit in eerste instantie gereguleerd door geld van materialen als goud en zilver te maken, zodanig dat geld de letterlijke waarde van het materiaal waarvan de munten gemaakt werden had. Tegenwoordig wordt zeldzaamheid gegarandeerd door een monopolie van overheden op het maken van geld. Het is moeilijk om geld te 'vervalsen' en het is bovendien niet lucratief om het te doen omdat het strafbaar is. De euro's in onze portemonnee en op onze bankrekening zijn een fiduciair geld – de enige waarde van het geld is gebaseerd op het vertrouwen dat economische actoren hebben dat er met euro's goederen gekocht kunnen worden.

Bitcoins maken

De afhankelijkheid van een staat om waarde te kunnen geven aan een munteenheid wordt als zwakte gezien door sommige mensen. Overheden zouden vluchtige en oude instanties zijn, die bovendien niet altijd met de beste vaardigheden en intenties de waarde van valuta willen manipuleren. De belangrijkste eigenschap van bitcoins is dan ook dat het een gedecentraliseerde munteenheid is. Er is geen centrale autoriteit die bitcoins kan beïnvloeden: de waarde en zeldzaamheid van bitcoins wordt gegarandeerd door cryptografische principes.

We hebben al gezien dat het een belangrijke eigenschap van geld is om moeilijk te maken te zijn. De zeldzaamheid van bitcoins wordt gegarandeerd door een cryptografische constructie. Een bitcoin wordt gemaakt door gebruik

Figuur 1: Het minen van Bitcoins wordt meestal gedaan door hobbyisten

te maken van de SHA-256 hashfunctie. Deze SHA-256 wordt, zoals andere hashfuncties, gebruikt om een invoer om te zetten naar een willekeurige uitvoer, zonder dat het mogelijk is om dit terug te draaien – de hashfunctie werkt maar één kant op. Invoer die op elkaar lijkt geeft door SHA-256 gehaald compleet andere uitvoer.

Een bitcoin maken wordt gedaan door een collision te vinden in deze hashfunctie: er wordt gezocht naar twee verschillende stukjes invoer die dezelfde soort uitvoer creëren.

> "Wat maakt geld nou geld eigenlijk?"

In het geval van Bitcoin wordt gekeken naar welke stukjes invoer na twee keer hashen met SHA-256 met een bepaald aantal nullen beginnen. Elke bitcoin bevat deze twee invoeren, en een bepaald aantal nullen. Omdat het aantal mogelijke nieuwe collisions steeds afneemt naarmate er meer gevonden worden, en omdat het protocol maar een beperkt aantal beginnullen van de hashuitvoer toestaat, wordt het steeds moeilijker om nieuwe paren te genereren. Bovendien zijn op een bepaald moment in de toekomst alle invoertekstparen gevonden. De verwachting is dat er door introductie van nieuwe bitcoins een 'natuurlijke inflatie' plaatsvindt van de waarde van Bitcoins totdat rond 2017 alle invoerparen zijn gevonden. Dan zijn alle 21 miljoen Bitcoins gegenereerd – daar moeten we het mee doen.

Het vinden van deze hashes wordt bitcoin mining genoemd. Mining is een erg intensieve taak: de beste manier om de invoerparen te vinden is namelijk via niets anders dan het brute forcen. Daarom zijn er veel hobbyisten die zware grafische kaarten inzetten om met de brute rekenkracht van de chips bitcoins te genereren. Het feit dat bitcoins genereren een niet-triviale taak is en dat de voorraad bitcoins eindig is, zorgt voor de zeldzaamheid die het nodig heeft om als geld te functioneren.

Bitcoins uiwisselen

Het vinden van goede hashes is een moeilijke taak, en het is daarom moeilijk om nieuwe bitcoins te maken. Maar waarom zou je nieuwe bitcoins maken als je bestaande bitcoins gewoon kunt blijven kopiëren en uitgeven aan andere mensen? Hoe zorg je er voor dat iemand zijn geld niet meerdere keren kan uitgeven?

Allereerst moeten we daarom het begrip transactie definiëren. Een transactie is een datastructuur die definieert dat er geld is overgemaakt tussen twee partijen. Transacties worden ondertekend door de uitgevende partij met een digitale handtekening. De digitale handtekening wordt gezet met de privésleutel uit een publiek/privésleutelpaar dat is gegenereerd op basis van elliptische krommes. De handtekening wordt gezet onder een transactiebericht dat bestaat uit een hash van de publieke sleutels van beide betrokken partijen en informatie over de hoeveelheid over te brengen bitcoins.

Er zijn cryptovaluta die dit oplossen door een derde partij alle transacties te laten controleren. Deze trusted third party treedt als middelman op in de transactie: de betaler stuurt zijn geld naar de middelman en deze controleert of de hashblokken echt nog eigendom

Figuur 2: Specialistische hardware gaat het minen van Bitcoin veel gemakkelijker maken

Andere cryptovaluta

Hoewel bitcoin de eerste cryptovaluta was, en inmiddels veruit de populairste, zijn er meerdere alternatieven in omloop. In de sidebars bij dit artikel behandelen we er twee. Beide gebruiken het zelfde concept transacties uit te voeren en een vergelijkbaar systeem om coins te minen: door aan te tonen dat er een hash collision is gevonden wordt er een 'werkbewijs', of proof-of-work, gegeven.

Litecoin

Het populairste alternatief voor bitcoin. Litecoin werkt vergelijkbaar aan bitcoin, maar gebruikt als hashingfunctie om de coins te genereren niet het SHA-256 hashingalgoritme maar het cryptografisch geavanceerdere scrypt. scrypt is een algoritme met een heel ander karakter dan SHA, en is veel minder geschikt om op GPU's te laten minen. Hierdoor is het moeilijker om een mining-voordeel te bemachtigen door simpelweg veel grafische chips of andere specialistische parallelle hardware in te zetten om te minen. Ook specialistische hardware om bitcoins te minen zou minder voordelen hebben bij Litecoin.

Een ander voordeel dat de Litecoin-auteurs claimen is dat de verwerkingstijd van transacties minder is: waar Bitcoin 10 minuten nodig heeft om een transactie door het netwerk te verspreiden, is dat bij Litecoin slechts 2,5 minuut.

zijn van de betaler. Als dat echt zo is, registreert de middelman de transactie en geeft deze het geld door aan de ontvanger. Het nadeel dat deze trusted third party heeft is dat die erg veel invloed uitoefent op de transactie. Als deze middelman niet meer werkt of niet meer te vertrouwen is, stort de valuta in.

In plaats van het bekendmaken van een transactie aan de middelman neemt Bitcoin de route om de transactie bekend te maken aan iedereen. Ja – bitcoin-transacties worden publiekelijk verspreid zodat het voor iedereen mogelijk is om de transacties te verifiëren. Er wordt hierdoor een wereldwijd peer-to-peer netwerk gecreëerd waarin iedereen dienst kan doen als verificatiepartij.

Maar hoe kun je zo maar wildvreemde servers op het internet vertrouwen dat zij de goede data hebben om zo'n transactie te verifiëren. Immers, als jij geld ontvangt van een kwaadwillende partij kan deze onder één hoedje spelen met de server waar jij je transacties controleert, en je zo geld sturen dat de betaler allang had uitgegeven.

Een server moet daarom kunnen bewijzen dat de gegevens waarover deze beschikt ook daadwerkelijk kloppen. Elke keer als er een transactie wordt gedaan moet deze daarom aan het wereldwijde netwerk van bitcoins worden toegevoegd. Daarom wordt bij elke transactie een timestamp gegenereerd van de status van de alle bitcoin-transacties die er op dat moment bekend zijn. Deze wordt gepubliceerd op het bitcoin-netwerk. Als deze timestamp wordt overgenomen door andere bitcoin-servers, is de transactie compleet. Omdat wordt aangenomen dat de gebruikte hashes niet omkeerbaar zijn, is de acceptatie van deze timestamp een vastlegging van het feit dat de transactie gedaan is, en dat het geld niet meer in het bezit is van de betalende partij.

Het is belangrijk om op te merken dat de rol van trusted third party, de plek waar onafhankelijk de correctie van een transactie kan worden gecontroleerd, wordt overgenomen door het netwerk. De aanname moet dus zijn dat het netwerk te vertrouwen is. Aangezien elke node in het netwerk de integriteit van de transactiedata garandeert, is het alleen mogelijk om dit netwerk aan te vallen door over meer rekenkracht te bezitten dan het netwerk zelf. De veiligheid van Bitcoin berust dus over het aanwezig zijn van genoeg rekenkracht in het netwerk. In maart 2013 was het Bitcoin-netwerk acht keer krachtiger dan gehele top 500 krachtigste supercomputers ter wereld bij elkaar opgeteld - dat is dus behoorlijk veilig!

Kritiek van technische aard

De gedecentraliseerde natuur van het protocol wordt niet alleen positief bevonden. Omdat de geschiedenis van alle transacties bekend is voor iedereen die het wil, is het niet heel moeilijk om een persoon te koppelen aan gemaakt bitcoin-transacties. Weliswaar zie je aan de transactie alleen maar een hash van de publieke key van iemand, maar zodra je weet welke public key iemand heeft (bijvoorbeeld als je een transactie met iemand aangaat) is het relatief eenvoudig om een compleet overzicht van zijn of haar eerdere betalingen te krijgen.

Daarnaast is het zo dat implementaties van het Bitcoin-protocol soms wat compatibiliteitsproblemen opleveren. In maart 2013 werd versie 0.80 van de miningsoftware uitgebracht. In deze software accepteerde het protocol hashes van een iets andere vorm als een valide bitcoin ten opzichte van eerdere versies. Meteen werden er bitcoins gegenereerd die niet compatible waren met eerdere versies, en werd er een splitsing in de community gevormd. Na een dag werd, na het downgraden van de software, pas weer concensus bereikt en kon het betalingsverkeer weer hervat worden.

Een verschil dat bitcoins hebben met 'gewoon' geld is de beperkte vrijheid in het creëren of vernietigen van geld. Mits je een overheid bent, is het betrekkelijk eenvoudig om geld dat verloren gaat te vervangen door nieuw geld. Als er in bitcoin geld verloren gaat (door verwijdering van de bitcoinhashes van een computer) kunnen deze hashes niet opnieuw worden ingevoerd, omdat ze al als eerdere transacties uitgewisseld zijn. Daarom heeft Bitcoin een zogenaamde negatieve entropie – nadat alle Bitcoins zijn gemaakt zijn, kunnen ze alleen maar verdwijnen. Dit heeft deflatie tot gevolg, en een natuurlijke ingebakken deflatie is een slechte eigenschap van een valuta. Aanvallers zouden door het

> "De waarde van bitcoins kan nogal fluctueren"

Andere cryptovaluta

PPCoin

PPCoin is gebaseerd op Bitcoin, maar probeert het deflatieprobleem van Bitcoin op te lossen. Dit wordt gedaan door het proof-of-work-concept van Bitcoin uit te breiden met een proof-of-stake.

Een mogelijke zwakte van Bitcoin is de 51%-aanval: als iemand over 51% van de miningcapaciteit bezit, is het mogelijk om coins twee keer uit te geven aangezien diegene bepaald wat het netwerk als geldige transactie ziet door zijn meerderheid in de rekenkracht. Hoewel dat niet goed mogelijk is in de huidige situatie, verandert dit in de toekomst wellicht. Door de werking van Bitcoins proof-of-work wordt steeds moeilijker om bitcoins te genereren: daarom zou het aantal miners in de toekomst wellicht drastisch kunnen afnemen en iemand in staat kunnen stellen 51% van de rekenkracht van het netwerk te bezitten.

Proof-of-stake is een manier ervoor te zorgen dat de macht om transacties goed te keuren niet komt te liggen bij de houders van de meeste rekenkracht, maar de houders van de meeste coins. Een gevolg is dat de motivatie om het netwerk te ontregelen verdwijnt: als je zelf veel coins hebt heb je er geen belang bij om het netwerk dat de waarde van jouw coins in stand houdt te ontregelen.

Figuur 3: De waarde van Bitcoins heeft het afgelopen jaar sterk gefluctueerd

massaal verwijderen van bitcoins de economie zelfs kunnen destabiliseren.

Kritiek op het concept

Het voordeel van een valuta die wordt gesteund door een sterke centrale entiteit als een land heeft als voordeel dat het relatief waardevast is. Een staat is vaak in staat de waarde van een munt redelijk vast te houden omdat de staat de grootste bezitter van een bepaalde valuta is. economische gemotiveerde veranderingen te doen aan de valuta.

Een natuurlijke bijkomstigheid van een cryptovaluta is criminaliteit. Omdat bitcoin de eerste cryptovaluta is die breed geaccepteerd wordt, is het dus mogelijk om direct economische waarde te creëren uit rekenkracht. Het is daarom een krachtige motivatie om met botnets bitcoins te minen. Er is zelfs een incident geweest dat een verborgen bitcoinminer

“Gedecentraliseerd is niet altijd positief”

Dit is niet het geval voor Bitcoin – er is intrinsiek geen dominante speler in de markt. Het gevolg is dat de waarde van Bitcoins nogal kan fluctueren. De waarde van een bitcoin in dollars fluctueerde in het afgelopen jaar tussen 10 dollar en 220 dollar. Ter vergelijking: de euro fluctueerde in het afgelopen jaar tussen $1.19 en $1.35 – een verschil van niet meer dan een paar procent. Als de economie afhankelijk zou zijn van een dergelijke fluctuerende munt als Bitcoin zou dit rampzalige gevolgen hebben. De grootste bitcoin-exchange Mt. Gox, een bedrijf dat als een soort wisselkantoor Bitcoins opkoopt en verkoopt, moest een aantal keren het wisselen sluiten omdat de fluctuaties de markt dreigden te destabiliseren.

Een tekort aan investeringen betekent economische achteruitgang. Als door andere economische omstandigheden inflatie te laag wordt gedreven kunnen overheden dit ten dele compenseren door extra geld te introduceren. Naast het feit dat Bitcoin zoals hierboven vermeld inherent deflationair is, is het ook niet mogelijk om kunstmatig de inflatie te verbeteren: het is niet mogelijk om werd verwerkt in een gamingtool, die gebruik maakte van krachtige GPU in de geïnstalleerde systemen om bitcoins te minen als persoonlijk gewin voor een ontwikkelaar bij dat bedrijf.

Het pseudonieme karakter van de bitcoin maakt het ook een aantrekkelijke valuta om in te handelen in het criminele circuit. Een aantal websites die aangemerkt zijn als ‘zwarte markt’, waar voornamelijk drugs worden verkocht, draaien hun transacties al volledig op bitcoin. Bitcoins kunnen worden gebruikt om geld wit te wassen.

Het geld van de toekomst?

Bitcoin wordt vaak ontvangen als “het geld van de toekomst”. Het volledig digitale, cryptografische karakter is echter waarschijnlijk niet genoeg om bitcoin ook echt een valuta van formaat te kunnen laten worden in de wereldeconomie. Als toekomstige cryptovaluta dit wél willen zijn, hebben ze aardig wat problemen op te lossen. Het is überhaupt de vraag of decentrale valuta de concurrentie aankunnen met valuta die ondersteund worden door een overheid op het gebied van stabiliteit. Het lijkt er in ieder geval nog op dat de euro’s op je bankrekening voorlopig niet weggeconcurreerd gaan worden.

Bronnen

BitCoin Wiki
https://en.bitcoin.it/Main_Page

“BitCon: Don’t” - Karl Denninger
http://market-ticker.org/akcs-www?post=219284

The Pros and Cons of Bitcoin Martin Bryant
http://www.youtube.com/watch?v=gNXZKwR6Lio

Advertentie

TECHNO-ADV-A4-INFORM-INTERACTI-EF-CONT-hi.pdf