I/O VIVAT

JAARGANG 29
NUMMER 1

In de wolken
Data in de cloud, een goed idee?

Alternatieve wachtwoorden
Zijn wachtwoorden dood?

Beveiliging op je telefoon
Zijn er dreigingen dan?

Blijf 'onder de radar'
Beveilig bestanden en internetverkeer

Telt mijn stem wel mee?
Een historische verkenning van de veiligheid van stem-methoden

En verder...

Inter-Actief

Advertentie

ASML.pdf

//Colofon

Jaargang 29, nummer 1,
november 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, Bedrijfsinformatie-technologie en Telematica van de Universiteit Twente. I/O Vivat verschijnt vier maal per jaar en heeft een oplage van 1800 exemplaren.

// Hoofdredactie
Stijn van Winsen

// Redactie
Danny Bergsma, Michel Brinkhuis, Martijn Bruning, Herman Slatman, Jip Spel, Stijn van Winsen

// Vormgeving
Jip Spel, Niels Witte

// Gastschrijvers
Willem de Boer, Martijn Hoogesteger, Arjan Jeckmans, Jeroen Monteban, Johan Noltes, Luís Ferreira Pirez, Stas Verberkt, Bram de Vries, Jacco Wesselius

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

Backdoors in encryptie-algoritmes, websites en databanken van enkele grote multinationals zijn maar een paar dingen waar wij als gebruikers voor gewaarschuwd zijn in de afgelopen maanden. De kans dat dit stuk, dat in Dropbox is opgeslagen op een server ergens in de Verenigde Staten, gelezen gaat worden door de NSA is natuurlijk miniem, maar niets weerhoud mij ervan toch te spelen met die gedachte. Michel Brinkhuis die op de zwarte lijst komt te staan wegens het helpen van criminelen om onder de radar van de NSA te blijven, of Herman Slatman die aangenomen wordt als beveiligingsexpert. Het zou mij niets verbazen als USB 14.0 geweigerd zal worden om Amerika binnen te komen.

Of het zover gaat komen is natuurlijk nog maar de vraag, laten we daar in ieder geval nog maar niet van uit gaan en kijken naar het heden.

Deze I/O Vivat is wat kleiner dan je normaal gesproken van ons gewend bent. De redactie wordt kleiner en daarmee ook de I/O Vivat zelf, ondanks de hoeveelheid externe content die we binnen krijgen. Dit mag uiteraard de kwaliteit niet drukken en daarom staan er weer een paar goede artikelen klaar. Zo geeft Jip alternatieven voor wachtwoorden zoals we die nu gebruiken, vertelt Arjan Jeckmans in het 'Rondje Zilverling' over privacy in aanbevelingssystemen en neemt Stas Verberkt namens ENIAC ons mee in de geschiedenis van de veiligheid van stemmethoden.

Ondanks de kleine redactie dus een interessante Vivat en hopelijk niet de laatste. Mocht je dus interesse hebben in het schrijven van artikelen over interessante ICT-onderwerpen, neem dan vooral contact op met de redactie, met Michel die aangehouden gaat worden door de NSA en Herman die aangenomen gaat worden blijft er niet veel van de redactie meer over.

Veel leesplezier,

Stijn van Winsen

Hoofdredacteur I/O Vivat

//Inhoud 29.1

//Nieuws

Facebook en Google maken advertenties persoonlijker

Gepersonaliseerde advertenties duiken steeds meer op. Ook giganten als Google en Facebook zijn continu bezig om advertenties nog meer 'op maat' te maken voor de gebruiker én voor de adverteerder. Facebook heeft bijvoorbeeld aangekondigd dat de 'Custom Audiences' functie nog verder uitgebreid gaat worden. Met deze functie is het voor bedrijven mogelijk om hun klanten specifiek te 'targetten' in advertentiecampagnes op het sociale netwerk. Met de aanstaande aanpassingen gaat Facebook nog een stap verder: bedrijven kunnen op hun website of in hun app een stukje code van Facebook implementeren dat bezoekers bijhoudt. Op deze manier kunnen bedrijven via Facebook adverteren in de Timeline van mensen die hun website hebben bezocht. In een aantal voorbeelden op hun developers-website vertelt Facebook dat het dan bijvoorbeeld voor een bedrijf ook mogelijk wordt om gebruikers van hun app, die de app al een tijdje niet hebben gebruikt, aan te sporen om via de app weer in contact te komen met het bedrijf.

Ook Google kondigde recent opvallende marketingmogelijkheden aan in hun advertentieplatform: 'shared endorsements'. Dat houdt in dat wanneer iemand in Google Play waardeert of een pagina een '+1' geeft middels Google+, dat dan mensen uit de kring van die persoon bij dat product de aanbeveling van die persoon te zien krijgen. Voor mensen die het niet zo fijn vinden om onaangekondigd ambassadeur van een product te worden biedt Google een opt-out mogelijkheid.

Bronnen:

http://blogs.wsj.com/digits/2013/10/11/google-to-sell-user-profiles-and-photos-in-ads/

http://www.volkskrant.nl/vk/nl/2694/Tech-Media/article/detail/3528197/2013/10/16/Facebook-gaat-nog-verder-met-gerichte-advertenties.dhtml

Qualcomm kondigt 'brain-inspired' computing chips aan

Qualcomm heeft in een recente blogpost van Samir Kumar, directeur business development, aangekondigd in 2014 met nieuwe chips gebaseerd op neurale netwerken te komen. Het platform, Zeroth genaamd, naar Asimov's wet, zou op zeer efficiënte wijze de wijze waarop mensen denken kunnen nabootsen.

De afgelopen jaren zijn er al veel ontwikkelingen geweest rondom neurale netwerken en brain-computer interfaces. Voor veel mensen is het verschil tussen mensen en computers iets moois, maar er zijn onderzoekers die dit gat graag kleiner zouden zien. Zo ook de onderzoekers in Research & Development bij Qualcomm. De afgelopen jaren hebben zij ontwikkeld aan een nieuw soort computerchip die het menselijk brein en zenuwstelsel imiteert. De nieuwe chips zouden daarmee een ingebouwd cognitievermogen hebben zonder dat dit expliciet in het te draaien programma geprogrammeerd hoeft te worden, zoals dat tegenwoordig bij veel programma's die machine learning implementeren wel het geval is.

Door de opzet van de chip is deze bij voorbaat al efficiënt. Ten grondslag hieraan ligt het feit dat het menselijk brein ook zeer efficiënt met energie omspringt en tevens een zeer groot rekenvermogen heeft. Qualcomm heeft voor testdoeleinden al een framework beschikbaar waarmee geprogrammeerd kan worden voor de nieuwe chip. Tijdens een demonstratie werd een robotwagentje dat opgebouwd was rond het Zeroth platform getoond. Het wagentje leerde door aanwijzingen van mensen wat 'correct gedrag' was, en kon daarop zijn gedrag zelf aanpassen. Het wagentje werd als het ware geprogrammeerd door het te laten leren; eigenlijk gelijk aan de wijze zoals je een kind opvoedt.

Nedap

Pep: digitale urenregistratie

Bram de Vries
Software Developer bij Nedap Pep

Al tijdens zijn studie Business & IT aan de Universiteit Twente werkte Bram de Vries als softwareontwikkelaar bij Nedap Pep. Daarnaast was hij actief bij Inter-Actief in de systeembeheercommissie. Sinds november 2012 werkt hij fulltime bij Nedap.

Kan je iets over Nedap Pep vertellen?

Nedap Pep is een van de marktgroepen van Nedap. Nedap is een technologiefabrikant, we maken producten voor relevante thema's. Onze ideeën over markt en technologie vertalen we in producten waar we markten mee in beweging brengen en die over de hele wereld worden verkocht. Zo ook Pep. Wij maken een urenregistratiesysteem voor de flexbranche. De rompslomp die papieren urenbriefjes met zich meebrengt is daarmee verleden tijd. Een flexkracht kan zelf zijn uren invoeren via onze website of klokken met een persoonlijke pas op onze Pep-readers.

Hoe is Nedap Pep ontstaan?

Het ontstaan van Nedap Pep is typerend voor Nedap. Onze 'grote broer' Nedap Healthcare is begonnen met het uitrusten van thuiszorgmedewerkers met kleine, persoonlijke nfc-readers. Al hun cliënten hebben pasjes hij hun voordeur hangen, waarbij de medewerkers in- en uit kunnen klokken. De thuiszorgorganisatie weet zo precies wanneer de medewerker er is geweest, maar ook dat de klant alleen betaalt voor de zorg die hij ontvangt. Een van de collega's die bij Healthcare werkte bedacht dat dit zogenaamde tijdsregistratiesysteem ook goed toegepast zou kunnen worden in de flexbranche. Door deze vorm van 'kruisbestuiving' tussen product en markt zijn al meerdere Nedap marktgroepen ontstaan.

> "Iedereen is bij Nedap verantwoordelijk voor zijn eigen werk"

Hoe is het om softwareontwikkelaar te zijn bij Nedap?

Zelf ben ik vooral bezig met het ontwerpen en implementeren van nieuwe functionaliteiten van Pep. Dit betekent bij Nedap niet dat je een opdracht krijgt voorgekauwd om een bepaalde functionaliteit te ontwikkelen. Er wordt van je verwacht dat je zelf naar klanten gaat om te onderzoeken welke functionaliteiten gewenst zijn of om de problematiek rondom bepaalde processen scherp te krijgen. Vervolgens is het jouw verantwoordelijkheid om een goede oplossing te bedenken en te ontwikkelen; uiteraard doe je dit allemaal in overleg en samen met je team.

Op dit moment werk ik aan een nieuw project. We hebben iets bedacht waar we in geloven en wat we van toegevoegde waarde voor Pep vinden. Samen met twee collega's ben ik daarom hard aan de slag gegaan om dit te ontwikkelen. We zijn van mening dat dit ons een belangrijke voorsprong in de markt gaat geven, en hebben dus lopende zaken tijdelijk op een lager pitje gezet. Dit geeft maar aan dat ik als software ontwikkelaar niet alleen bezig ben met letterlijk software ontwikkelen.

Bij Nedap werken is voor mij een unieke ervaring en niet zomaar voor iedereen weggelegd. Je moet namelijk zelf je werkveld verkennen en ontdekken. Bovendien zal niemand je vertellen wat je moet gaan doen. Dat besluit je zelf en samen met je team. Die manier van werken moet je wel liggen. Daarnaast wordt je bij Nedap al snel 'bewust onbekwaam'. Dat betekent dat je hier snel bewust wordt waar je te weinig van weet of wat je nog niet kan. Dit moet je dan zien als een kans om je daarin te verbeteren, en daar sta je natuurlijk niet alleen voor. Iedereen is bij Nedap verantwoordelijk voor zijn eigen werk. Als je die verantwoordelijkheid laat zien, dan staat niets je in de weg om binnen Nedap helemaal je eigen werk in te richten.

Bedankt voor het interview!

In de wolken

Data in de cloud; een goed idee?

Door: Herman Slatman
Redacteur I/O Vivat

Het concept van de cloud gaat al een behoorlijke tijd mee. In de jaren '60 van de vorige eeuw beschreef J. C. R. Licklider al een computernetwerk waarin gebruikers overal ter wereld toegang zouden hebben tot data en programma's die zich overal konden bevinden. In de vroege jaren was cloud computing en -storage enkel weggelegd voor de grootste bedrijven, maar de afgelopen jaren zijn er steeds meer mogelijkheden gekomen voor de normale consument. Die kan tegenwoordig met alle gemak al zijn of haar documenten makkelijk synchroniseren en beschikbaar maken op tal van apparaten en deze ook vaak makkelijk delen met collega's of vrienden.

Het grote gemak dat aanbieders van cloud storage bieden, is het overal beschikbaar maken van bestanden die de eigenaar upload. In 2012 werd er naar schatting met een gemiddelde bandbreedte van 54Gbps naar hartenlust geupload naar de populaire dienst Dropbox. Het is haast onvoorstelbaar hoeveel bestanden er inmiddels in Amerika staan, waar de opslagservers van Dropbox zich bevinden. Maar hoe veilig is dat nu eigenlijk? Kan zo'n aanbieder, of wellicht een derde partij, jouw bestanden inzien, en hoe worden deze opgeslagen op de servers?

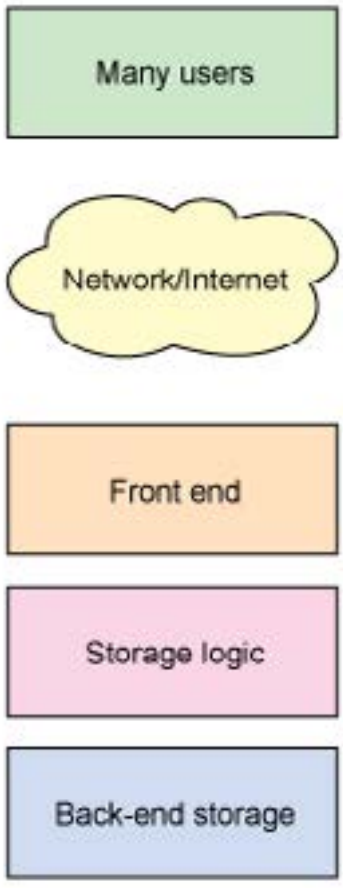
De opslagarchitectuur

Cloud storage (ook wel: gegevensopslag-als-een-service) is een technologie die een abstracte interface voor gegevensopslag biedt. Via die interface kan de opslag op ieder moment geadministreerd worden, zodat men toegang kan krijgen tot diens bestanden. Die interface is meteen ook een abstractie voor de locatie van de opgeslagen bestanden: die kunnen op een server ergens op de wereld staan, of in sommige gevallen, zelfs opgedeeld in verschillende stukken op verschillende locaties.

Zoals bij veel IT-systemen, wordt er ook bij cloud storage vaak gebruik gemaakt van een gelaagd model. De eerste laag is de front-end van het opslagsysteem. Gebruikers kunnen zich via het netwerk op de front-end authentiseren en krijgen daarmee toegang tot de bestanden waarvoor ze geautoriseerd zijn. Zo'n front-end bestaat meestal uit een API waarop verschillende applicaties aangesloten kunnen worden. Dit stelt een gebruiker in staat om op verschillende manieren, bijvoorbeeld via een website, desktop of mobiele applicatie, zijn bestanden te beheren en bekijken.

De laag daaronder omvat de logica voor de gegevensopslag. Deze zorgt ervoor dat het mogelijk wordt om bestanden geografisch te verspreiden. Ook kan er programmatuur aanwezig zijn die ervoor zorgt dat er backup-replica's van bestanden gemaakt worden en dat data gededupliceerd wordt. Dit laatste houdt in dat er in het geval van verschillende gebruikers die hetzelfde bestand op de cloud storage willen opslaan, er niet voor iedere gebruiker een aparte kopie bijgehouden hoeft te worden. Dit scheelt in de hoeveelheid opslagruimte, en in sommige gevallen ook in uploadbandbreedte.

Waar de storage logic laag ervoor zorgt dat data correct opgeslagen wordt en weer teruggehaald kan worden, zorgt de



Figuur 1: Laagmodel voor Cloud Storage

back-end storage voor het daadwerkelijk opslaan van de bestanden op harde schijven of een equivalent daarvan. Hoe de architectuur van een willekeurige aanbieder van cloud storage eruit ziet kan men meestal niet direct opmaken. Toch is deze een belangrijk aspect om de veiligheid van een service te kunnen bepalen.

Aanbieders van cloudopslag

Aanbieders van cloud storage zijn de afgelopen jaren als paddestoelen uit de grond geschoten. Onder de meest populaire bevinden zich onder andere Dropbox, SkyDrive en Google Drive. Zij bieden klanten, vooral consumenten, gratis een beperkte hoeveelheid opslag aan. Deze hoeveelheid kan vergroot worden door een betaald abonnement af te sluiten.

Bedrijven die zelf graag meer controle willen hebben over hun data kunnen beter terecht bij andere aanbieders. Het gaat hierbij bijvoorbeeld om de Amazon Simple Storage Service (Amazon S3), onderdeel van de Amazon AWS. Amazon biedt met S3 een platform voor klanten om grote hoeveelheden data op te slaan. Zo maakt Dropbox bijvoorbeeld gebruik van Amazon S3 om haar eigen service goedkoop aan consumenten te kunnen aanbieden.

Aspecten van security in de cloud

Er is een groot aantal verschillende beveiligingsaspecten aanwezig bij het opslaan van gegevens in de cloud. Deze hangen samen met de architectuur en de opzet van het systeem. Daarnaast heeft ook de 'soort' (consumenten of bedrijven) opslag hier invloed op. Hieronder volgen enkele van deze aspecten.

> "steeds vaker multi-factor authenticatie toegepast"

Beveiliging van de toegang

Ten eerste dient de interface of de API die de cloudopslag biedt veilig te zijn. Het moet voor een buitenstaander niet mogelijk zijn om toegang te krijgen tot de data van rechtmatige gebruikers van het systeem. De interface moet ingericht zijn met een geschikte vorm van authenticatie. Een rechtmatige gebruiker zal bijvoorbeeld met een gebruikersnaam en wachtwoord kunnen inloggen om bij zijn bestanden te komen. Daarnaast wordt tegenwoordig steeds vaker multi-factor authenticatie toegepast, waarbij een gebruiker zich op meerdere manieren moet authentiseren, bijvoorbeeld door een wachtwoord én een gegenereerd token. De authenticatie is dan gebaseerd op iets wat de gebruiker weet en op iets dat de gebruiker in bezit heeft.

Naast authenticatie is een ander onderdeel van de beveiliging van de interface de manier waarop er met deze interface verbinding gemaakt wordt. In het geval van cloudopslag zal dit veelal via het Internet plaatsvinden. Het is daarom zaak om ervoor te zorgen dat een buitenstaander niet kan meeluisteren op het moment dat bestanden worden verzonden. Het is bijvoorbeeld mogelijk om bestanden te versleutelen alvorens deze te verzenden, maar er kan ook gebruik gemaakt worden van een beveiligde verbinding waarover de data verzonden wordt. Dit laatste kan gerealiseerd worden door SSL/TLS te gebruiken bij het opzetten van de verbinding.

Figuur 2: Verschillende aanbieders van persoonlijke Cloud Storage

Bescherming tegen pottenkijkers

Achter een cloudopslagservice bevindt zich eigenlijk altijd een team van beheerders. Deze dienen ervoor te zorgen dat de service blijft draaien. Deze beheerders hebben in veel gevallen toegang tot de systemen nodig om hun werk te kunnen doen, en zouden daarbij mogelijk ook toegang kunnen hebben tot de gegevens van een gebruiker of metadata betreffende de opgeslagen bestanden op de opslagservers.

Zo'n voorvertoning van bestanden is voor gebruikers handig, en wordt ook wel door meerdere aanbieders aangeboden, maar de opzet brengt mogelijk ook risico's met zich mee. Zo zou het mogelijk kunnen zijn dat een aanvaller een bug in LibreOffice weet te exploiten. Dropbox opent deze bestanden immers automatisch, en het gevolg zou kunnen zijn dat Dropbox gecompromitteerd raakt waarna de aanvaller toegang zou kunnen krijgen tot alle opgeslagen bestanden. Daarnaast wor-

"diverse inlichtingendiensten hebben toegang..."

De technische beheerders zijn echter niet de enige personen die toegang tot de opgeslagen bestanden kunnen hebben. Vrij recent is bekend geworden dat diverse inlichtingendiensten toegang hebben tot gegevens die opgeslagen worden bij verschillende grote bedrijven en diensten. Ze zouden dus in principe toegang kunnen hebben tot de bestanden die in de cloud liggen opgeslagen.

Dat het zeker mogelijk is dat bestanden achter de schermen geopend worden door een cloudopslagservice, werd onlangs vastgesteld door een beveiligingsonderzoeker . Hij had een speciaal soort bestand bij Dropbox geplaatst, waarna hij een melding kreeg dat het bestand enkele minuten na het opslaan geopend was door LibreOffice. De uitleg van Dropbox was dat men previews genereert voor gebruik in de web-interface.

den de gegevens die bij zo'n preview worden aangemaakt waarschijnlijk in een database opgeslagen, tezamen met bestanden van andere gebruikers. Het idee dat de bestanden van een gebruiker dus altijd afgeschermd zijn van andere gebruikers zou dus mogelijk niet helemaal hoeven te kloppen. Ook hierbij geldt dat een aanvaller toegang zou kunnen krijgen tot (delen van) de bestanden van andere gebruikers.

Versleuteling van data is de meest logische oplossing om bovenstaande situaties tegen te gaan. Er moet dan wel sprake zijn van 'end-to-end'-versleuteling: al op het systeem van de gebruiker dient de data versleuteld te worden. De data zal versleuteld verzonden en opgeslagen worden, en niemand anders dan de rechtmatige eigenaar heeft toegang tot de sleutels. Het enige wat bekend is, is dat een gebruiker bestanden op de opslag heeft staan, maar de inhoud zal nooit beschikbaar zijn op de cloudopslag, enkel op de systemen van de gebruiker zelf.

Beschikbaarheid

De veiligheid van data houdt niet enkel in dat deze alleen toegankelijk en leesbaar dient te zijn voor de rechtmatige gebruiker, maar ook dat deze altijd en overal beschikbaar is. Als bedrijfsgegevens in de cloud worden opgeslagen, kan het voor een bedrijf desastreus zijn als deze niet bij zijn gegevens kan. In het geval van cloudopslag houdt dit uiteraard in dat er verbinding gemaakt moet kunnen worden met de opslagservers. De gebruiker is dus afhankelijk van zijn of haar internetverbinding en zal in sommige (tegenwoordig wel steeds minder) gevallen niet bij zijn of haar gegevens kunnen. Daarnaast dienen de gegevens ook bij uitval van een server of corruptie van een bestand op een bepaalde server nog te benaderen zijn. Het is dus zaak dat een cloudopslag regelmatig back-ups bijhoudt van bestanden of deze zelfs in meervoud opslaat. Het geografisch verspreiden van deze meervouden geniet daarbij uiteraard de voorkeur.

Secure sharing

Een groot voordeel van cloudopslag is dus dat data overal en altijd bereikbaar is, en als het even kan ook op een veilige manier. Tegenwoordig is het echter zeer belangrijk dat data gedeeld kan worden. Bedrijven profiteren van het feit dat het delen van data makkelijker wordt, door het via de cloud beschikbaar te maken, wat ervoor zorgt dat de productiviteit omhoog gaat. Zo kan er in de zorg makkelijk informatie over de zorgtoestand van een persoon gedeeld worden om effectiever te kunnen handelen in het geval van ziekte. Tegelijkertijd geldt wel dat deze informatie strikt vertrouwelijk moet blijven. Daarnaast geldt voor consumenten dat deze makkelijk foto's en documenten kunnen delen met familie en vrienden.

Voor de eigenaar van bestanden moet het dus mogelijk zijn om bepaalde bestanden te delen met een bepaalde groep personen. Die andere personen moeten in principe altijd bij de bestanden kunnen komen, net als de eigenaar, zonder dat de eigenaar hier na het geven van de toestemming naar om hoeft te kijken.

Een naïeve oplossing zou zijn om de eigenaar al zijn data te laten versleutelen, en de mensen met wie hij zijn bestanden wil delen de sleutel te geven. Er is hier echter een behoorlijke hoeveelheid administratief werk te verrichten, bijvoorbeeld in het geval dat de eigenaar de toegang van een bepaalde persoon wil intrekken. Hij zal zijn gedeelde data moeten ontsleutelen, opnieuw versleutelen met een nieuwe sleutel, en deze sleutel opnieuw aan de andere personen moeten geven. Deze oplossing is dus niet erg praktisch om aan te bieden.

Één van de eerste mechanismen die gebruikt werd om delen in de cloud mogelijk te maken, waren de zogenaamde Access Control Lists (ACL). Een ACL is in feite een lijst van permissies die toegekend kan worden aan een bestand. De lijst specificeert welke gebruikers toegang tot het bestand hebben en bijvoorbeeld wie er wijzigingen kunnen aanbrengen. ACLs bleken echter niet schaalbaar te zijn in de cloud, waar in sommige gevallen data gedeeld wordt met honderden, zo niet, duizenden gebruikers. Encryptie gebaseerd op attributen (Attribute-Based Encryption, ABE) kan uitkomst bieden bij het veilig delen van data in de cloud. ABE is een mechanisme voor toegangscontrole waarbij er bepaalde attributen aan een gebruiker of aan gegevens worden toegekend. Er wordt daarnaast een beleid gedefinieerd voor de toegang gebaseerd op de toegekende attributen: wanneer een gebruiker aan bepaalde attributen voldoet, krijgt deze toegang tot de bestanden.

Toegang tot de bestanden is soms niet genoeg; deze kan immers versleuteld zijn. Men zou ABE ook kunnen toepassen op het distribueren van sleutels. Wanneer men de rol van een gebruiker als attribuut toekent, bijvoorbeeld 'collega', 'vriend' of 'familielid', kan iemand met de juiste rol een sleutel toegewezen krijgen door de eigenaar, of door een speciaal hiervoor ingericht systeem. Die sleutel kan daarna weer gebruikt worden om de gegevens te ontsleutelen. Op deze manier ontstaat er een systeem waarbij de eigenaar van de gegevens eigenlijk geen omkijken meer heeft nadat hij zijn gegevens gedeeld heeft, maar hij blijft in staat om de toegang op een bepaald moment in de toekomst weer op te heffen.

> "Encryptie gebaseerd op attributen kan uitkomst bieden..."

Neem het heft in eigen hand

Als je niet helemaal zeker bent wat de aanbieder precies doet aan beveiliging van jouw gegevens, kan je er altijd nog voor kiezen om zelf enkele stappen te zetten om de veiligheid van je data te kunnen garanderen. Een mooi voorbeeld is het gebruik van bijvoorbeeld TrueCrypt, dat je in staat stelt om containers aan te maken waarbinnen alle opgeslagen bestanden worden versleuteld. Zo'n container is makkelijk online op te slaan in de cloud. Nadeel daarvan is wel dat je overal waar je toegang wilt tot je versleutelde gegevens, je de container in TrueCrypt moet openen. Een andere soortgelijke oplossing is Boxcryptor. Boxcryptor kan in combinatie met veel verschillende cloudopslagservices gebruikt worden en stelt de gebruiker in staat om individuele bestanden versleuteld op te slaan. Hierbij heb je dus geen last van het feit dat je een hele container dient te ontsleutelen voordat je bij je data kan.

Zoals beschreven zijn er de afgelopen tijd veel aanbieders van cloudopslag bijgekomen. Met welke daarvan je in zee gaat, is natuurlijk gebaseerd op persoonlijke voorkeuren en de functies die een aanbieder aanbiedt. Misschien speelt de veiligheid van je gegevens wel een hele belangrijke rol, en kies je ervoor om specifiek op zoek te gaan naar een aanbieder die dit goed voor elkaar heeft. Als je echter ultieme controle wilt over wat er gebeurt met jouw bestanden, kan je er nog voor kiezen om je eigen persoonlijke cloud op te zetten. Dit kan tegenwoordig al heel snel door ownCloud op je eigen server te installeren. OwnCloud biedt verschillende mogelijkheden voor het beheren van bestanden, en ondersteunt ook het delen van gegevens met bepaalde groepen personen.

Conclusie

Er zijn veel redenen om je data in de cloud te plaatsen. Zo biedt het een makkelijke manier om foto's te delen en overal te kunnen benaderen, en kan het daarnaast je productiviteit verhogen. Het is echter wel van belang dat je gegevens veilig opgeslagen worden. Deze moeten immers beschikbaar blijven, ook na technische problemen. Ook moeten je gegevens afgeschermd worden van buitenstaanders, maar wil je wel graag je foto's kunnen blijven delen met mensen die je toestemming geeft. De mogelijkheden die een opslagservice biedt wat betreft gegevensbescherming kunnen heel erg verschillen. Deze mogelijkheden hangen sterk samen met de architectuur van het systeem. Het is dus zaak om, als je om de veiligheid van je gegevens geeft, goed uit te zoeken hoe verschillende aanbieders met je gegevens omgaan. In het uiterste geval kan je er altijd nog voor kiezen om het heft in eigen handen te nemen, en een privécloud op te zetten, om zo de ultieme controle over je gegevens te kunnen blijven garanderen.

Bronnen

A history of cloud computing
http://www.computerweekly.com/feature/A-history-of-cloud-computing

Dropbox...opening my docs?
http://www.wncinfosec.com/dropbox-opening-my-docs/

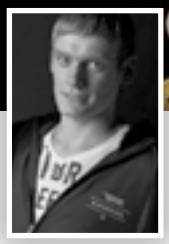
Security, Privacy and Trust in Cloud Systems
S. Nepal, M. Pathan (Springer, 2014)

Anatomy of a cloud storage infrastructure
M. Tim Jones

Securing the Cloud
Vic (J.R.) Winkler (Syngress, 2011)

Beveiliging op je telefoon

Zijn er dreigingen dan?



Door: Michel Brinkhuis
Redacteur I/O Vivat

In Nederland hebben zo'n 8 miljoen mensen een smartphone en daarnaast zijn er nog eens 6,5 miljoen tabletbezitters. Meer dan de helft van de bevolking heeft dus een dergelijk apparaat. Waar je je vroeger, met bijvoorbeeld een Nokia 3310, geen zorgen hoefde te maken over de beveiliging van je telefoon, behalve dan door een pincode in te stellen, is die tijd veranderd. Tegenwoordig kan iedereen van alles installeren op z'n telefoon en dat brengt natuurlijk beveiligingsrisico's met zich mee.

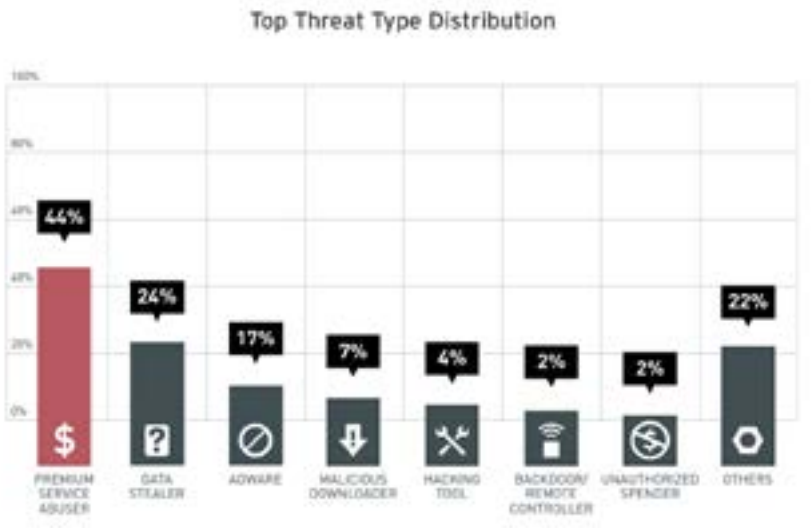
Per besturingssysteem

Uit documenten van de FBI blijkt dat Android veruit het besturingssysteem met de meeste malwaredreiging is. 79% Van alle malware komt voor op Android, tegen 19% nog op Symbian, gevolgd door iOS met slechts 0.7%. Er zijn grofweg twee mobiele dreigingen te onderscheiden: diefstal van informatie, en de gebruiker op kosten jagen. Diefstal van informatie ligt voor de hand: het zonder dat de gebruiker het weet opslaan van wachtwoorden of ontvangen berichten bijvoorbeeld. Sommige mobiele malware stuurt op de achtergrond dure SMSjes naar betaaldiensten, waardoor de telefoonrekening een stuk hoger kan uitvallen.

Het aantal mobiele bedreigingen groeit hard. Uit onderzoek van Trend Micro bleek dat het aantal Android-infecties in april van dit jaar nog op 561.000 lag, in mei steeg dit tot 639.000 en in juni lag het aantal al op 718.000 infecties. Dat is een aanzienlijke 'groeiversnelling': het duurde 3 jaar voordat er 350.000 geïnfecteerde apps werden gebruikt. In 22% van de gevallen gaat het om 'FAKEINST' malware. Dat is malware die SMSjes stuurt naar betaalde nummers. In de top 3 dreigingen staan verder OPFAKE (hetzelfde concept als de FAKEINST-malware) en SNDAPPS. Deze laatste vergaren allerlei informatie van de gebruiker en telefoon, zoals telefoonnummer, IMEI-nummer en e-mailadres. Deze gegevens zijn geld waard: in Rusland worden 1 miljoen telefoonnummers voor 70$ verhandeld. Een wat meer gepersonaliseerde database, dus telefoonnummers met persoonsgegevens, gaan illegaal voor zo'n 35$ per 1000 records van de hand. Het gaat in veel van de gevallen om specifieke situaties die in Rusland of omringende landen werken, omdat het daar heel eenvoudig is om een betaalde telefoondienst op te zetten. In Nederland zijn de risico's dat hier iets fout mee gaat een stuk kleiner.

Android master key vulnerability

Zowel Apple als Google bieden portals aan via waar apps kunnen worden gedownload. Het is echter ook mogelijk om buiten die 'stores' om applicaties op je telefoon te installeren. Met name bij Android is dat eenvoudig. Dat brengt risico's met zich mee, zoals de recent ontdekte 'Master key vulnerability' voor Android. De applicaties die op Android geïnstalleerd kunnen worden, worden verspreid als .apk-bestanden. Dit zijn echter gewoon .zip-archieven met een andere extensie. Probeer maar eens een



Figuur 1: Types bedreigingen voor Android-telefoons

.apk-bestand te openen met Winrar: je kunt dan gewoon zien welke bestanden er in zitten. Bij de installatie wordt er een lijst met checksums, te vinden in het bestand Manifest.mf, vergeleken met de checksums van de uitgepakte bestanden zelf. Nu blijkt het zo te zijn dat wanneer je twee bestanden met dezelfde bestandsnaam in het .apk-bestand stopt, het eerste bestand wordt geverifieerd door Android, maar het tweede bestand wordt geïnstalleerd. Zo kun je dus ongeverifieerde code installeren op Android. Dat kan natuurlijk door kwaadwillenden worden misbruikt. Inmiddels heeft Google dat lek al wel gedicht.

Hoe groot sommige bedreigingen voor bijvoorbeeld Android echt zijn is maar de vraag. In een presentatie van het Google Android Security Team laten de ontwikkelaars zien dat headlines in de media niet altijd helemaal weerspiegelen van wat er echt aan de hand is. Bij de eerder beschreven 'Master Key' kwetsbaarheid was een headline bijvoorbeeld '99% of devices vulnerable'. Dat klinkt heel indrukwekkend. Echter, volgens de statistieken die het team wist te vergaren werd de malware op minder dan één op de miljoen Android-telefoons geïnstalleerd. Een ander voorbeeld is Androrat, waarbij PCMag.com schreef: 'Android Remote Acces Trojan AndroRAT is Cheaper and More dangerous Than Ever'. Het aantal installaties van geïnfecteerde apps ligt volgens Google echter lager dan 1 op de 10 miljoen. En de meeste van die installaties worden vermoedelijk veroorzaakt door mensen die een betaalde app op illegale wijze gratis proberen te verkrijgen via andere portals dan de Google Play Store.

> "Hoe groot de dreigingen echt zijn is maar de vraag"

Malware as a Service

Er wordt onder andere misbruik gemaakt van fouten in besturingssystemen om er geld aan te kunnen verdienen. Dat blijkt uit bijvoorbeeld het bestaan van de FAKEINST-malware. Omdat er zo veel geld in die business omgaat, gaat men ook steeds professioneler te werk, met als gevolg een nieuwe 'tak van sport': Malware as a Service. Dit ontdekten de mensen achter het beveiligingsproduct LookOut op Android. Zij ontdekten de Russische diensten 'Jollybot' en DragonLady. Wat hier gebeurt is dat er een platform is waarop je een account kunt maken om affiliate te worden. Dat betekent dat over de inkomsten die voortkomen uit de door jou verspreidde apps met de malware van het platform jij een bepaald percentage ontvangt. Op die manier kun je geld verdienen met het verspreiden van geïnfecteerde apps, zonder dat je überhaupt hoeft te kunnen programmeren.

Andere beveiligingsrisico's

Het downloaden van apps uit ongeverifieerde bronnen blijkt dus een risicofactor te zijn. Maar ook zonder de installatie van 'foute software' loop je soms een risico. Recent bracht Apple de iOS7-update voor iPhones uit. Kort daarna ontdekten beveiligingsonderzoekers twee manieren om het toestel in gelockte toestand toch te kunnen gebruiken. Via het nieuwe 'control center' konden foto's worden gedeeld via bijvoorbeeld e-mail en vanuit de functie om 112 te bellen kon met een foefje ieder willekeurig nummer worden gebeld. Beide bugs werden snel door Apple opgelost, en middels een update over de toestellen verspreid.

Het aantal mensen dat momenteel zijn telefoon voorziet van dergelijke software is nog niet zo heel groot. Bloomberg maakte recent een rondje langs alle grote aanbieders van beveiligingsapps, en kwam op de volgende aantallen gebruikers uit: Kaspersky 1 miljoen, LookOut 45 miljoen, AVG 44 miljoen, McAfee 150 miljoen en NQ Mobile 372 miljoen. Symantec en Trend Micro wilden geen cijfers geven. Hoe dan ook, op een totaal van 4,5 miljard mobiele telefoons over de hele wereld valt het totaal aantal gedownloade apps nog heel erg mee.

Al met al vallen de dreigingen erg mee zolang je geen apps uit ongeverifieerde bronnen installeert en je besturingssysteem bijwerkt. Soms wil het echter wel eens voorkomen dat er tijdelijk toch geïnfecteerde software in een app-store terecht komt. Daarom is anti-malwaresoftware voor je mobiele apparaat geen overbodige luxe.

Figuur 2: Screenshot ' Malware as a Service'

Bronnenlijst

Ouderen massaal aan de Smartphone
http://www.nu.nl/tech/3505785/ouderen-massaal-tablet-en-smartphone.html

How is the mobile security business doing - don't ask
http://www.bloomberg.com/news/2013-09-04/how-is-the-mobile-security-business-doing-don-t-ask.html

Android Master Key vulnerability
http://nakedsecurity.sophos.com/2013/08/09/android-master-key-vulnerability-more-malware-found-exploiting-code-verification-bypass/

JollyBot: Malware as a Service Evolves
https://blog.lookout.com/blog/2013/09/10/jollybot-malware-as-a-service-evolves/

Alternatieve wachtwoorden

Zijn wachtwoorden dood?

Door: Jip Spel
Redacteur I/O Vivat

Afgelopen september zei Heather Adkins, Google's information security manager, tijdens een conferentie, TechCrunch Disrupt in San Fransisco, dat wachtwoorden dood zijn. Of dit komt door de opkomst van smartphones en tablets, waarbij het intoetsen van een wachtwoord op een klein scherm vervelend wordt, of dat dit komt doordat de veiligheid van wachtwoorden op zich in het geding komt, heeft Heather Adkins niet gezegd. Wel blijft de vraag, of er daadwerkelijk zoveel nadelen aan wachtwoorden kleven, en als wachtwoorden dan dood zijn, welke alternatieven er dan op komst zijn.

Tegenwoordig heb je voor veel verschillende services, zoals Facebook maar ook internetbankieren, een wachtwoord nodig. Aan deze wachtwoorden worden verschillende eisen gesteld. Een kort wachtwoord is immers makkelijker te kraken dan een lang wachtwoord. Probleem hierbij is dat een lang wachtwoord veel minder makkelijk te onthouden is dan een kort wachtwoord. Daarnaast zorgen deze verschillende eisen ervoor dat je voor de verschillende services ook verschillende wachtwoorden hebt. Dit zorgt weliswaar voor een betere beveiliging tegen hackers, maar zorgt wel voor het probleem dat je misschien vergeet welk wachtwoord je ook alweer waar had. Ook een lang wachtwoord voor alle diensten is geen oplossing, als deze gekraakt zou worden, heb je een probleem voor alle diensten die je gebruikt.

Een oplossing hiervoor is het gebruik van een password management tool. In deze tool sla je al je wachtwoorden gecodeerd op, er bestaat zelfs de mogelijkheid om de tool een wachtwoord voor je te laten genereren. Vervolgens kun je je wachtwoord opzoeken door in te loggen in de tool. Een voordeel hiervan is dat je niet meer het probleem hebt dat je verschillende wachtwoorden moet onthouden. Er kleeft echter ook een groot nadeel aan het gebruik van een password management tool: op het moment dat iemand op welke manier dan ook toegang krijgt tot jouw account in de password management tool, kan deze persoon overal bij. Het gebruik van wachtwoorden alleen is dus niet veilig.

Een aanvulling op het gebruik van een wachtwoord is dus gewenst. Google's tweestapsverificatie springt hierop in. Hierbij moet je eerst je wachtwoord invullen en vervolgens een toegangscode die je op je mobiel ontvangt. Voordeel hiervan is dat er naast het wachtwoord ook nog een fysiek apparaat nodig is om toegang te verschaffen tot je account. Ook is er nagedacht over een manier om toegang te krijgen tot je account als je bijvoorbeeld je mobiel verliest. Google heeft hiervoor een redelijk lange vragenlijst ontwikkeld waarbij er een aantal persoonlijke vragen worden gesteld. Als je als gebruiker genoeg vragen goed beantwoordt, zal je ook zonder mobiel toegang krijgen tot jouw account. Ook bij internetbankieren wordt veel gebruik gemaakt van tweestapsverificatie. Als je een transactie wilt uitvoeren, zul je je nogmaals moeten identificeren, bijvoorbeeld met behulp van tan-codes of een random reader.

Er bestaan ook vormen van authenticatie waarbij je geen wachtwoord hoeft in te voeren. Heather Adkins droeg dit tijdens het gesprek ook voor: biometrie, het gebruik van unieke persoonlijke kenmerken, zoals iriskenmerken, vingerafdrukken en het patroon van het netvlies. Op vliegvelden wordt de irisscan al veel gebruikt om je te identificeren. Maar ook bij de smartphones dringt het gebruik van biometrie door, zo heeft Apple bij zijn nieuwe iPhone de mogelijkheid ingebouwd om met je vingerafdruk je telefoon te ontgrendelen. Daarnaast zijn er ook bedrijven bezig met het gebruiken van stemherkenning als manier van authenticatie. Hierbij wordt een wachtwoordzin ingesproken. Deze is meestal tussen de zes en tien woorden lang en bevat veel verschillende soorten klanken. Op deze manier wordt een unieke stemafdruk gevormd die niet na te doen is. Een groot voordeel hiervan is dat je geen dure apparatuur nodig hebt zoals een vingerafdrukscanner. Er zijn echter ook nadelen aan stemherkenning, zo kun je iemand anders stem opnemen en dit afspelen, en is het mogelijk dat het niet werkt als je erg verkouden bent.

Motorola was afgelopen mei in het nieuws met de voorspelling dat wachtwoorden in de toekomst vervangen

zullen worden door armtattoos en authenticatiepillen. Bij de armtattoo zul je een soort barcode op je arm hebben die werkt met behulp van antennes en sensoren. Door deze in de buurt van bijvoorbeeld een scanner van de pinautomaat te houden, kun je betalen. Bij de authenticatiepil slik je bijvoorbeeld elke dag een pil. De sensoren in deze pil zullen geactiveerd worden door het zuur in je maag. Op deze manier wordt je lichaam een wandelende authenticatiebron.

Helaas zijn Motorola's armtattoos en authenticatiepillen nog in de ontwikkelingsfase, en kunnen ze dus ook nog geen oplossing bieden voor een ander probleem met wachtwoorden: ze zijn vaak lastig om in te voeren op een smartphone of tablet. De ontwikkelaars van smartphones en tablets zijn dan ook druk bezig met alternatieven hiervoor te vinden. Onder andere Microsoft en Apple hebben andere vormen van authenticatie ontwikkeld, die ervoor moeten zorgen dat de toegang tot je smartphone of tablet voor jou makkelijk te verkrijgen is.

Bij Microsofts afbeeldingswachtwoord kies je zelf een afbeelding en kan je vervolgens een willekeurige tekening hierop maken: je zet cirkels en pijlen bij dingen die jij belangrijk vindt. Microsoft is met dit alternatief gekomen omdat het intoetsen van een wachtwoord op een smartphone op een klein toetsenbord erg vervelend kan zijn. En qua veiligheid doet dit concept in principe niet onder voor het traditionele wachtwoord. Echter, uit recent onderzoek blijkt dat gebruikers vaak niet zo goed zijn in het maken van een willekeurige tekening. Vaak wordt ervoor gekozen om gezichten, ogen of objecten te omcirkelen. Hierdoor wordt het voor een hacker makkelijker om te achterhalen wat het afbeeldingswachtwoord was. Daarnaast zou je het afbeeldingswachtwoord ook kunnen achterhalen doordat er vette vingers op het scherm komen te staan.

> "Wachtwoorden zijn niet meer veilig genoeg..."

Ook Apple is druk bezig geweest met nieuwe vormen van authenticatie, zo heeft Apple een vingerafdruksensor in de nieuwe iPhone 5s geplaatst. Met deze sensor, die verwerkt zit in de home-knop, kun je snel en gemakkelijk je mobiel unlocken. Voor veel mensen zal dit een handige manier zijn om de gegevens van de mobiele telefoon te beveiligingen: geen codes meer die je moet onthouden, maar gewoon simpel je vinger langs de home-knop halen; de enige die de telefoon kan ontgrendelen, ben jij.

Belangrijk is echter te kijken naar de beveiliging van de opslag van jouw vingerafdruk: deze wordt immers op de telefoon opgeslagen, en is dus in principe voor hackers te verkrijgen. Een probleem wordt het als je vingerafdruk door iemand gehackt wordt en in verkeerde handen valt. Identiteitsfraude wordt hiermee mogelijk, en je kan een vingerafdruk niet zomaar wijzigen (zoals met een wachtwoord wel kan). Ligt jouw vingerafdruk op straat, dan kan dus iedereen die de technologie heeft om een kopie ervan te maken, zich als jou identificeren. Daarnaast schijnt het mogelijk te zijn om met een gekopieerde vingerafdruk, die bijvoorbeeld van een glas gekopieerd is en waarvan vervolgens een siliconen kopie is gemaakt, de smartphone te unlocken. Het is dus maar afwachten hoe veilig Apple's vingerafdrukdaadwerkelijk is.

Wachtwoorden zijn niet meer veilig genoeg als enige vorm van authenticatie doordat ze te makkelijk gekraakt kunnen worden. Echter zijn alternatieven of niet veilig of nog niet ontwikkeld. De meest veilige oplossing momenteel is een tweestapsverificatie, waarbij je via twee aparte wegen toegang krijgt tot de dienst waarvan je gebruikt wilt maken.

Armtattoo als alternatief voor wachtwoorden

Bronnen

Passwords are done
http://www.welivesecurity.com/2013/09/12/the-end-passwords-are-done-says-google-security-chief/

Fingerprints:
http://www.usatoday.com/story/cybertruth/2013/09/19/bounty-offered-to-hack-apples-fingerprint-sensor/2837541/

Biometrie
http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies

Alternatieve wachtwoorden
http://www.computerweekly.com/feature/Alternatives-to-passwords-Replacing-the-ubiquitous-authenticator

Motorola
http://www.welivesecurity.com/2013/05/31/motorola-predicts-passwords-will-be-replaced-by-arm-tattoos-and-authentication-pills/

Picture passwords
http://computertotaal.nl/apps-software/picture-passwords-in-windows-8-het-grote-onbenutte-potentieel-50190

Blijf 'onder de radar'

Beveilig bestanden en internetverkeer

Door: Michel Brinkhuis
Redacteur I/O Vivat

De artikelen in allerlei media over spionage door meerdere geheime diensten, zoals de Amerikaanse National Security Agency (NSA) en het Britse Government Communications Headquearters (GCHQ), zal menigeen niet ontgaan zijn. Zo blijken diensten als Gmail en Windows Live Mail actief in de gaten te worden gehouden, en worden er dagelijks miljoenen adresboeken van gebruikers van deze diensten opgeslagen. Recent waren er ook onthullingen dat zelfs encryptie-algoritmes niet meer 100% veilig zijn. Eén van de voornaamste zwakheden zou zitten in het, door de NSA zelf ontwikkelde, Dual_EC_DRBG-algoritme. Dit algoritme wordt gebruikt door random-number generators (rng). "Betrouwbare random number generators zijn belangrijk voor de werking van encryptie-algoritmes, maar deze rng blijkt om de tuin te leiden als een gebruiker een specifieke set cijfers kent.", zo meldde Tweakers.net in september.

In dit artikel nemen we een kijkje naar software die het mogelijk maakt om 'onder de radar' te blijven, ofwel je de mogelijkheid biedt je verkeer en bestanden te verstoppen voor mee-kijkers.

Internetverkeer

De 'NSA-leaks' begonnen met artikelen over het surveillanceprogramma PRISM, waardoor duidelijk werd dat de veiligheidsdienst internetverkeer in de gaten houdt. Eén van de meest genoemde opties om anoniem te kunnen internetten is The Onion Routing, ofwel TOR. Met deze software surf je via andere TOR-gebruikers naar een website, waardoor een website jouw bezoek niet kan afleiden maar enkel het ip-adres ziet van de zogenaamde exit node. Deze exit node is de computer die aan het einde van de reeks computers van jouw browse-verzoek staat. Als je via TOR op het internet gaat, dan haalt de TOR-client eerst een lijst op met IP-adressen van andere TOR-nodes. Vervolgens bepaalt de client-software een willekeurig pad langs een deel van deze clients. Hoewel TOR het lastig maakt om verkeer te monitoren, werd bekend dat de NSA zich hier ook mee bezig houdt. Men draait eigen servers, en via onder andere man-in-the-middle¬ aanvallen lokken ze mensen met niet-bijgewerkte Firefoxversies naar hun TOR-node, om ze aldaar te exploiten. *https://www.torproject.org/*

Steeds meer websites bieden de mogelijkheid om de website via HTTPS te benaderen. Stuur je bijvoorbeeld een tekst naar de website, bijvoorbeeld omdat je via Gmail een mailtje stuurt, dan wordt die tekst over een beveiligde verbinding naar de servers van Google gestuurd. Niet iedere website biedt echter standaard HTTPS aan, ook al ondersteunen ze het wel. Daarom heeft de Amerikaanse Electronic Frontier Foundation (EFF), die opkomt voor de digitale burgerrechten, in samenwerking met de mensen achter het TOR project een Firefox- en Chrome-plugin gemaakt genaamd HTTPS Everywhere. Deze plugin laadt de pagina via HTTPS ook al verwijst de website je zelf door naar http. *https://www.eff.org/https-everywhere*

Communicatie

Internet wordt natuurlijk veel gebruikt voor communicatie tussen personen. Facebook Chat en Google Talk worden door veel mensen dagelijks gebruikt. Maar hoe weet je zeker dat een conversatie tussen jou en de persoon aan de andere kant blijft? En hoe weet je zeker dat diegene aan de andere kant van de lijn echt is? Dat weet je bij deze diensten niet. Om een beveiligde chatsessie op te zetten kun je gebruik maken van de tool Off-the-Record (ORT). Niet alleen worden berichten versleuteld verstuurd, ook zit er een geavanceerd authenticatiemechanisme ingebouwd waarmee je de identiteit van de ontvanger vaststelt. Verder weet niemand na afloop van het gesprek zeker dat het ook echt heeft plaatsgevonden: tijdens het gesprek weet je dat, maar het is goed mogelijk dat iemand na het gesprek op wat voor manier dan ook extra berichten kan 'faken' waardoor het lijkt alsof jij ze verstuurde. OTR is een plugin die voor veel verschillende instant messaging-tools beschikbaar is, waaronder Pidgin. *https://otr.cypherpunks.ca/*

Eén van de bekendste voorvechters van online privacy is Kim Dotcom. Deze inwoner van Nieuw Zeeland met Duitse

roots werd eerder bekend door zijn succesvolle bestandsuitwisselingsdienst MegaUpload die door de Amerikaanse veiligheidsdiensten offline werd gehaald. Dat bracht hem op het idee om een nieuwe dienst te lanceren, waarbij bestanden die de gebruikers uploaden wel veilig zijn in het geval iemand toegang weet te krijgen tot de servers: Mega. De kracht van Mega zit in het feit dat de bestanden worden opgeslagen op servers die over de hele wereld staan. Het binnenvallen van één enkel datacenter zal dus niet voldoende zijn om de dienst offline te halen. Daarnaast worden bestanden versleuteld opgeslagen. De versleuteling vindt, in tegenstelling tot bij sommige andere diensten, niet serverside plaats, maar aan de kant van de gebruiker. Voordat je een bestand upload wordt het lokaal, middels Javascript, door je webbrowser geëncrypt en vervolgens pas geüpload. De keys worden alleen aan jou als gebruiker gegeven, en niet door Mega opgeslagen. *http://www.mega.co.nz*

Stel, je wilt geheimen communiceren met een landelijk dagblad. Hoe doe je dit op een manier dat er niet kan worden afgeleid dat jij de afzender bent? Daarvoor worden diverse mogelijkheden ontwikkeld. Recent lanceerden diverse Nederlandse nieuwsmedia het Publeaks.nl-project. Hiermee kun je als 'klokkenluider' anoniem bestanden uploaden en aanvinken welke media de bestanden moeten ontvangen. Het project gebruikt de open-source code van Globaleaks. Een ander project dat recent werd geadopteerd door de Amerikaanse Freedom of the Press Foundation is SecureDrop (voorheen Dead Drop). Dit is een open-source Python-platform, dat niet alleen het anoniem delen van documenten en berichten mogelijk maakt tussen instanties, maar het ook mogelijk maakt om contacten te onderhouden. Als je iets uploadt naar deze dienst krijg je een codenaam toegewezen, waarmee je later weer kunt terugkeren om te communiceren met de journalist. Hierbij ben je niet afhankelijk van e-mail en hoef je niet je echte identiteit op te geven. *https://pressfreedomfoundation.org/securedrop*

> "Bij PubLeaks kun je anoniem delen met de pers"

Lokale bestanden

Niet alleen wat je online uitspookt zal je willen beschermen. Het is ook goed mogelijk dat je de bestanden op je computer wilt beveiligen, al is het maar tegen diefstal of het moment dat je even je computer achterlaat terwijl je een kopje koffie scoort. Je kunt je bestanden encrypten met een programma als TrueCrypt. Deze gratis, en open-source, tool maakt het mogelijk om (delen van) je harde schijf te coderen. De kracht hiervan zit onder andere in het feit dat alles wordt versleuteld; ook de vrije ruimte. Daarnaast is het zelfs mogelijk om een 'hidden volume' aan te maken. Dit houdt in dat een buitenstaander niet eens kan zien dat er nog een versleuteld stukje harde schijf is bínnen het al versleutelde volume. Dit maakt het mogelijk om je bestanden écht te verbergen en te beveiligen voor de buitenwereld. *http://www.truecrypt.org/*

Beveiligde diensten vragen bijna altijd om een wachtwoord. Bovendien, het wordt aangeraden om bij elke dienst een ander wachtwoord te gebruiken. Lekt je wachtwoord bij de ene dienst, dan staan er niet ineens nog een heleboel andere deuren ook open. Dat resulteert in veel verschillende wachtwoorden. Die wil je waarschijnlijk op een veilige manier bewaren. De, zoals hij zelf schrijft, 'internationally renowned security technologist' Bruce Schneier heeft de tool Password Safe gemaakt. Hierbij worden wachtwoorden via het vrij beschikbare Twofish-algoritme opgeslagen. Ook dit programma is gratis en open-source. *https://www.schneier.com/passsafe.html*

Je computer barst van de tijdelijke bestanden als je een middagje over het internet hebt gesurft. Nu bieden browsers wel de mogelijkheid om tijdelijke bestanden te verwijderen, dat wil niet zeggen dat alles permanent is gewist. Met BleachBit kun je tijdelijke bestanden wél echt verwijderen. Na verwijderen worden deze bestanden namelijk overschreven met willekeurige data, waardoor je er zeker van bent dat niemand op je computer kan achterhalen welke websites er zijn bezocht. *http://bleachbit.sourceforge.net/*

Is nu alles wat ik doe verborgen?

Nee, zeker niet. Er zijn zoveel manieren waarop toegang kan worden verkregen tot dat wat je doet op je computer, dat het bijna niet mogelijk is om volledig 'onder de radar te vliegen'. Echter, je kunt wel je best doen om wat je wilt beveiligen goed te beveiligen.

Figuur 2: Schematische uitleg van TOR

//Column

Van Luís

Opleidingsdirecteur BIT en teamleider BWO F9

Door: Luís Ferreira Pires
Opleidingsdirecteur Business & IT

Sinds 1 augustus 2013 ben ik de nieuwe Opleidingsdirecteur (OLD) van de BIT-Bachelor- en Masteropleidingen. Mijn benoeming gaat samen met een overgang van deze opleidingen van de Faculteit MB naar de Faculteit EWI.

Ik vraag mij af of er een turbulentere periode te vinden zou zijn om OLD te worden. De overgang van MB naar EWI gaat al gepaard met de nodige bureaucratie en afstemmingen, en we zijn tegelijktijdig bezig met de invoering van het Twentse Onderwijs Model (TOM), die veel aandacht vraagt. Natuurlijk moet ik ook wennen aan deze nieuwe rol.

Bijna samen met deze nieuwe rol ben ik in september begonnen (samen met een goede vriend) als leider van de BWO F9, het voetbalteam van mijn zesjarige zoontje Caio. Ik zie dan ook een paar parallellen tussen deze twee nieuwe rollen.

Binnen de UT kennen we de relevantie van de BIT-opleiding voor de maatschappij, als een brug tussen de IT wereld en de businesswereld. Bovendien horen we van bedrijven dat ze professionals met het profiel van onze BIT-ers nodig hebben. Verder horen we dat bedrijven ontzettend tevreden zijn met onze BIT-afstudeerders. We moeten dit dus vaker aan de buitenwereld vertellen zodat de BIT-opleiding boven de '70 eerstejaars-norm' komt die in de wandelgangen wordt gehanteerd om het verschil tussen een kleine en een grote opleiding te bepalen.

Voor BWO F9 probeer ik ook elke week voldoende spelers op het veld te krijgen, door tijdig rond te mailen en eventueel invallers op te roepen. Tot nu toe is het gelukt om met een compleet team op het veld te staan.

Op de UT zijn we met zijn allen bezig met TOM, en dat betekent een ingrijpende herziening van het Bachelor onderwijs. De BIT Bachelor opleiding participeert in een aantal modules van de opleidingen Technische Informatica en Technische Bedrijfskunde, waardoor we samen schaalvoordeel kunnen halen. Maar hoe houdt een opleiding haar eigen identiteit als deze opleiding grotendeels uit modules van andere opleidingen bestaat?

We proberen dat met 'differentiatie' te bereiken, bijvoorbeeld met opdrachten en projecten die toegespitst zijn op het BIT-profiel. Dit moet dus in de gaten gehouden worden bij het ontwerp en de implementatie van modules waarin BIT-studenten participeren. De BIT varianten van de modules moet ook in lijn gebracht worden met de eindtermen van de opleiding, ook een taak voor de OLD.

Bij BWO F9 probeer ik structuur in het spel aan te brengen, zonder dat ze daardoor het plezier in het spelen verliezen (hun 'identiteit'). Dat lukt redelijk goed door eenvoudige maar duidelijke instructies te geven, zoals: 'jullie twee zijn onze verdedigers, jij bent onze spits en jullie lopen daartussen'.

Onze docenten werken met veel enthousiasme aan de ontwikkeling van onderwijsmateriaal en –activiteiten in het kader van TOM. In Module 1 heb ik vaak gehoord dat dit enthousiasme (kennelijk) heeft geresulteerd in een (te?) druk programma voor de studenten. De vraag is natuurlijk of dit klopt, of komt deze drukte van de overgang van de middelbare school naar de universiteit die ze ook zouden voelen in de pre-TOM periode? Drukte is een gevoel, vaak veroorzaakt door een volle agenda, een lange 'to do' lijst, of geen tijd om naar de kapper te gaan (gehoord van een paar studenten!), dus we moeten deze klachten serieus nemen. We moeten dus een reële inschatting maken van de studeerbaarheid van onze modules, en zorgen voor een betere afstemming tussen verschillende docenten binnen de modules. Hier gaan we ook aan werken.

Bij BWO F9 probeer ik ze op een positieve manier onder druk te zetten. Ik vertel ze dat als ze willen winnen dat ze hun best moeten doen, en dat doen ze ook, dus aan het eind van een wedstrijd krijgen ze in elk geval de complimenten (ook ranja, natuurlijk) en hopelijk de winst.

Bij BIT hebben ook de 'oude Bachelor' en de Masterstudenten, die net zo veel aandacht verdienen als onze eerstejaars. Deze studenten mogen niet de indruk krijgen dat we ze vergeten zijn, want dat zijn we niet.

Bij BWO F9 zijn ook alle spelers belangrijk. Dat vertel ik ze, en dat is ook zo!

Trouwens, BWO F9 heeft de eerste drie wedstrijden gewonnen en heeft een doelsaldo van 48 doelpunten. Morgen staat de thuiswedstrijd tegen de koploper op het programma!

Sinds 1994 is dr. Luís Ferreira Pires universitair hoofddocent aan de Universiteit Twente, momenteel bij de 'Services, Cyber-security and Safety' groep van de faculteit EWI. Luís werd op 7 april 1961 geboren in São Paulo (Brazilië), en sinds maart 1988 woont hij in Nederland. Hij heeft een ingenieursdiploma van 'Instituto Technológico de Aeronaútica' (São José dos Campos, Brazilië) en een Masterdiploma van 'Universidade de São Paulo' (São Paulo, Brazilië). In 1994 is hij bij de Universiteit Twente gepromoveerd.

Luís houdt van sporten, in het bijzonder voetbal, zoals elke typische Braziliaan. Luís is een fanatieke supporter van São Paulo FC, maar hij is ook regelmatig te vinden tussen de FC Twente supporters in de Grolsch Veste. Hij speelt tennis, de laatste tijd iets minder vanwege zijn knie. Hij is getrouwd en heeft drie kinderen: Elena (13), Melinda (11) en Caio (6).

Van de voorzitter

Met TOM, op de koffie

Door: Martijn Hoogesteger
Voorzitter I.C.T.S.V. Inter-Actief

Een nieuw jaar met veel veranderingen ten opzichte van vorig jaar. Voor eerstejaars is het altijd even wennen, de verandering van middelbare school naar universiteit. Ik kan me nog goed herinneren dat ik als eerstejaars mijn rooster zag en het niet kon laten om 'Vakantieee!' door mijn hoofd te laten gaan. Voor de huidige eerstejaars is dit wel wat anders. Zij zien een rooster dat aardig vol zit, en moeten daarmee hard aan de slag. We zien de meesten gelukkig wel meer op de bank zitten, het besef dat je op de universiteit een stuk vrijer bent, komt toch wel langzaam.

Het Twents onderwijsmodel is één van de belangrijke veranderingen dit jaar. In dit jaar geven we vanuit Inter-*Actief* extra aandacht aan het onderwijsvernieuwingen en letten we een beetje op de eerstejaars. Vooralsnog lijkt alles goed te gaan, zelfs met activisme. De commissiemarkt was druk bezocht en de interesselijsten zijn gevuld. Ik hoop heel veel eerstejaars dus binnenkort niet alleen over hun studie te spreken, maar ook over alle gave ervaringen die ze tegemoet gaan in hun activisme.

Een andere belangrijke verandering waar we dit jaar extra op letten, is er één die al langer aan het veranderen is: onze uitgaven aan koffie. Al jarenlang bestaat deze stijging, maar recentelijk is het tot een hoogte gekomen waarbij er wel wat belletjes gingen rinkelen. Veranderingen aan 'een gratis bakkie koffie bij Inter-*Actief*' willen we eigenlijk niet maken, dus onze uitgaven scherp in de gaten houden is waar het tijdelijk bij blijft. Tijdens een overleg over de koffie heeft Nick mij nog gerust kunnen stellen met een nieuwsbericht vanaf zijn smartphone: "Oh! Ik lees net dat de koffieoogst dit jaar goed is!". Hopelijk komt ook dit dus wel goed.

Ikzelf en de rest van mijn bestuur ondervinden ook een grote verandering. Van studerend student naar bestuur is een interessante beleving. Je bent met heel veel verschillende dingen bezig. Het rooster waar ik eerder over sprak, bestaat niet echt meer. Alles wordt van week tot week vastgesteld. De gedachte 'Vakantieee!' zou je door je hoofd kunnen laten schieten over een week ver in de toekomst, maar als die week er is, zit hij vol!

De laatste weken zat de planning vooral vol met constitutieborrels. Hier hebben we veel leuke mensen ontmoet en ervaringen opgedaan. Op de meeste borrels hebben we ook een welbekend liedje gezongen, op de melodie van "t is moeilijk bescheiden te blijven'. In tegenstelling tot de meeste oud-bestuurders hadden we echter nog geen motto die we achter dit mooie lied konden plakken. Geïnspireerd door de voorgenoemde punten die in ons bestuursjaar belangrijk zijn, hebben we 'Met TOM, op de koffie!' bedacht. Een mooie verwijzing naar de fout die we soms maken als iemand vraagt "Hoe is het met TOM?", namelijk denken dat het over een lid genaamd Tom gaat.

Martijn Hoogesteger,

Voorzitter I.C.T.S.V. 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 3 september voorzitter voor het jaar '13/'14 noemen.

Inter-*Actief*

//Column

USB 14.0

USB 14.0

Study Tour 2014

Smart Surroundings

Door: Jeroen Monteban
Voorzitter USB 14.0

Na een zeer geslaagde studiereis 2012, waarin deelnemers van Noodle in een aantal weken het verre Oosten hebben mogen verkennen, heeft de nieuwe studiereiscommissie de startblokken inmiddels alweer verlaten en wordt er druk getimmerd aan de weg die ons naar de volgende exotische bestemming moet gaan voeren. Onder de naam USB 14.0 en met het thema Smart Surroundings zal deze commissie een prachtige reis richting de Verenigde Staten en Brazilië neer gaan zetten!

Voor de eerstejaars, vergeetachtigen en andere onwetenden een korte introductie in het mooie concept van de studiereis. In het tweede kwartiel, een kleine wijziging ten opzichte van de vertrekperiode van voorgaande edities, van studiejaar 2014-2015 zullen wij met een enthousiaste groep mensen naar de Verenigde Staten en Brazilië afreizen om hier ruim drie weken lang kennis te mogen maken met verscheidene bedrijven en universiteiten. Het doel van deze reis is, naast het beleven van een onvergetelijke reis, het ontdekken van de cultuurverschillen tussen deze landen en ons eigen Nederland, en het kennismaken met grote informatie- en techniekbedrijven.

We zullen op onze reis verschillende steden aandoen: San Francisco, Los Angeles, Brasilia, São Paulo en Rio de Janeiro. We starten in de Verenigde Staten, waar we in Silicon Valley verschillende bedrijven zullen bezoeken. Garanties worden niet gegeven, maar we doen uiteraard ons best ook grote bedrijven als Microsoft en Google te bezoeken. Hierna vertrekken we via LA naar Brazilië, waar we verschillende steden bezoeken. We eindigen tenslotte in Rio, vanwaar de mogelijkheid geboden wordt op nareis te gaan.

De nareis is voor veel deelnemers een belangrijk deel van de studiereis, hoewel het officieel geen deel van de studiereis meer is. Na het eindigen van de officiële reis reizen veel deelnemers nog een tijdje door in het land van bestemming, in dit geval Brazilië. Het reisbureau dat onze reis regelt, zal verschillende verzorgde nareizen aanbieden, maar iedereen is natuurlijk vrij om er zelf op uit te trekken. Het ticket terug naar thuisbasis Holland zal uiteraard door de studiereis worden betaald, alle overige nareis-activiteiten zijn voor eigen rekening.

Nu het TOM-model menig student in de nek hijgt, hoor ik u allen denken: “En mijn studie dan?”. Vrees niet: de studiereis is naast leerzaam, leuk, interessant en spectaculair ook nog eens een volledige minor: International Management & Exploration. Naast de studiereis zelf zullen er drie vakken gevolgd moeten worden. Eén hiervan vindt plaats in het vierde kwartiel van dit studiejaar, de andere twee in het eerste kwartiel van studiejaar 2014-2015. Omdat het een minor is, is een vereiste voor deelname dan ook het bezitten van 60 EC bij aanmelding en 80 EC bij vertrek. Ook Masterstudenten zijn meer dan welkom op de studiereis en kunnen hier studiepunten uit slepen. Voor hetzelfde traject als de Minorstudenten zullen zij 10 EC krijgen.

Uiteraard moet deze reis ook betaald worden. Ten eerste is er een deelnemersbijdrage. Deze staat nog niet vast maar zal rond de €1000 zijn. Daarnaast zijn er inkomsten door middel van Contract Research. Dit houdt in dat jij als deelnemer voor eind Augustus 120 uur voor een bedrijf zult moeten werken. Het contact met bedrijven regelen wij: het maken van 120 uur is jouw taak!

Tot slot de commissie die dit alles mogelijk gaat maken:

> Jeroen Monteban 3e-jaars BIT
Voorzitter

> Tanja de Jong 4e-jaars INF
Penningmeester

> Kaspar Hageman 5e-jaars MTE
Onderzoekscoördinator

> Robin ten Buuren 5e-jaars SE
Externe betrekkingen

> Jeroen Vollenbrock 3e-jaars INF
Reiscoördinator

> Jochem Verburg 3e-jaars BIT
Reiscoördinator

Mocht je interesse in de studiereis gewekt zijn, bekijk dan onze website www.usb14.com en schrijf je hier in voor onze nieuwsbrief. Via deze brief wordt je op de hoogte gehouden van belangrijke ontwikkelingen. Heb je vragen, stuur dan een mailtje naar info@usb14.com of spreek één van de commissieleden aan.

We hopen jullie allemaal als deelnemers mee te mogen nemen. Wij hebben er zin in!

Privacy in aanbevelingssystemen

Personalisatie door beveiligde berekeningen

Door: Arjan Jeckmans
Vakgroep SCS

Aanbevelingssites, zoals Amazon of Imdb, geven waardevolle aanbevelingen over relevante producten en films. Maar waar komen deze aanbevelingen vandaan? Grote databases met gebruikersinformatie worden verzameld, om hier vervolgens mee te rekenen. Hierbij wordt de privacy van de gebruikers niet meegenomen. Is het niet mogelijk dezelfde functionaliteit te behouden zonder daarbij alle gegevens op tafel te gooien?

Om gepersonaliseerde aanbevelingen te genereren, vereisen aanbevelingssystemen informatie over de attributen, eisen of voorkeuren van de gebruiker. In het algemeen, hoe gedetailleerder de informatie gerelateerd tot de gebruiker is, hoe accurater de aanbevelingen voor de gebruiker zijn. Service-aanbieders van aanbevelingssystemen verzamelen grote hoeveelheden persoonlijke informatie om accurate aanbevelingen te waarborgen. Deze informatie dient beschermt te worden om de privacy van alle gebruikers te verhogen.

Een manier om de privacy te verhogen is door het gebruik van beveiligde berekeningen. Beveiligde berekeningen beschermen de informatie die wordt gebruikt tijdens het uitrekenen van de aanbevelingen door de vertrouwelijkheid van informatie te verstrekken, zowel tijdens de opslag als de berekening. Echter, hebben ze een overhead door het gebruik van cryptografie en beveiligde protocollen met meerdere partijen.

Als voorbeeld kan een verzoek voor aanbevelingen bij een bepaalde film beveiligd naar de service-aanbieder verstuurd worden. Deze verzamelt dan alle relevante informatie en combineert dit tot een aanbeveling (onder beveiliging). Wanneer de gebruiker de aanbeveling terug krijgt, kan deze de beveiliging eraf halen en de aanbeveling zien.

In ons onderzoek concentreren wij ons op het gebruik van beveiligde berekeningen om de privacy in aanbevelingssystemen te verhogen, waar we streven de berekeningen zo efficiënt mogelijk te maken. Om dit te realiseren, bouwen we specifieke beveiligde protocollen gebaseerd op homomorfe versleuteling (versleuteling waarmee gerekend kan worden) en beveiligde berekeningen met meerdere partijen. Elk protocol is afgestemd op het specifieke probleem dat wordt aangepakt met een minimum aan dure berekeningen en interacties.

Naast het efficiëntie probleem, zijn er nog meer uitdagingen. Omdat er gebruik wordt gemaakt van versleuteling, is er een partij nodig met de sleutel om deze versleuteling ongedaan te maken. Een versleuteld resultaat is immers nutteloos. De gebruiker die zijn eigen privacy wil waarborgen is een goede kandidaat. Dit geeft de gebruiker maximale controle over zijn gegevens. Zijn deze gegevens nodig in een berekening, dan dient de gebruiker wel aanwezig te zijn om te helpen met de berekening (alleen de gebruiker heeft de sleutel). Dit zorgt er weer voor dat de gebruiker continu online moet zijn, wat nou ook weer niet wenselijk is. Dan zou iedere gebruiker altijd zijn pc aan moeten laten staan. Er zijn verschillende trucs om dit op te lossen, zoals het machtigen van een andere partij de sleutel te gebruiken.

Een andere uitdaging is kwaadaardig gedrag van gebruikers. Als de privacy van de gebruikers beschermd wordt, dan is het moeilijker om te zien of een gebruiker zich wel gedraagt. Een gebruiker kan verkeerde gegevens invullen en zo het hele systeem overhoop gooien zonder dat dit opvalt. Bijvoorbeeld door een film het cijfer 100 te geven, terwijl het maximum een 10 is. Meer controle over de correctheid van de te berekenen functie, zonder daarbij de privacy te schenden, is soms moeilijk toe te voegen.

Daarnaast komen er in elk specifiek scenario nog meer uitdagingen om de hoek kijken. Het op een efficiënte manier overkomen van deze uitdagingen draagt bij aan betere en snellere oplossingen zodat in de toekomst de privacy van gebruikers gewaarborgd kan worden.

Tot die tijd zijn er nog genoeg uitdagingen om opgelost te worden en dient ook de efficiëntie verbeterd te worden. De aanbevelingssystemen van nu, werken nog op databases vol met zichtbare gebruikersinformatie. De aanbevelingssystemen van de toekomst waarborgen de privacy van de gebruikers zonder dat deze daarbij op functionaliteit hoeven in te leveren.

Meer info: http://scs.ewi.utwente.nl/ http://dies.ewi.utwente.nl/

//Advertorial

Bewustwording van informatiebeveiliging

Belangrijk voor consumenten en organisatie

Door: Willem de Boer & Jacco Wesselius
Senior consultant, Project manager, Technolution

Vroeger bewaarde men geld in een oude sok, paspoorten in de keukenla en dagboeken onder het hoofdkussen. Tegenwoordig staat ons elektronische geld op de bank, onze gegevens in verschillende databases en ons dagboek op social media. Het beveiligen van deze informatie kan niet meer door eenvoudigweg de voor- en achterdeur goed op slot te draaien.

We leven in een informatiemaatschappij. Zonder pasje kom je bijna nergens meer binnen en op internet hebben we meerdere accounts om te winkelen of deel te nemen aan fora en social media. Zo staat er op veel plaatsen informatie over ons geregistreerd. Helaas gaat niet elke organisatie even verantwoord met die gegevens om. Naïviteit is niet enkel voorbehouden aan de consument, die zelf via Facebook, Google en andere media persoonlijke informatie rondstrooit. Ook de overheid en het bedrijfsleven zijn zich vaak onvoldoende bewust van de risico's die ze lopen op het gebied van informatiebeveiliging. Dat kan gaan om een onschuldig voorval als het vinden van de miljoenennota (2011) en de kersttoespraak van de koningin (2012) door een getalletje in de oude URL te veranderen. Maar diezelfde overheid zet bij aanbestedingen voor bruggen of sluizen ook de complete systeemarchitectuur inclusief IP-adressen voor de bediening online. Informatie die iedereen mag downloaden, zonder enige vorm van 'pre-kwalificering'. Commerciële organisaties die over veel persoonlijke informatie beschikken zijn vaak doelwit voor hackers. Zo moest iedereen vorig jaar zijn wachtwoord van LinkedIn wijzigen. Hackers hadden de wachtwoorden op internet gepubliceerd en beschikten waarschijnlijk ook over de bijbehorende gebruikersnamen.

Data wildgroei

Hoewel ons veiligheidsbewustzijn zich langzaam maar zeker ontwikkelt, schrijdt de techniek met rasse schreden voort. Dankzij (draadloze) netwerktechnieken zijn koppelingen te maken tussen systemen en gegevens die vroeger niet mogelijk waren. Thuis koppelen we ons mobiele devices aan het netwerk, en bedrijven en instanties koppelen hun systemen aan elkaar, allemaal voor makkelijke en snelle informatie-uitwisseling. Elke koppeling levert weer nieuwe mogelijkheden op om verbanden te leggen en conclusies te trekken over bijvoorbeeld gedrag en gezondheid.

Verantwoord omgaan met data wordt dus steeds belangrijker. Maar nog voor je de beveiligingsvraag stelt, dien je je af te vragen: heb ik die data allemaal nodig? Veiligheidshalve is het verstandiger om zo min mogelijk data te genereren, zoals eerder te lezen was in het visieartikel van Objective 13. Wat er niet is, hoef je ook niet te beveiligen. Dus sla alleen de data op die echt noodzakelijk is voor de bedrijfsvoering of de functionaliteit van het systeem.

Informatie is business

Inmiddels is het niet meer zo eenvoudig om zo min mogelijk data te genereren, we leven immers in een informatiemaatschappij waarin het delen van data gewoon is geworden. Informatie speelt ook een economische rol. Bedrijven als Google, Facebook en Twitter leven van informatie. Zij hebben heel andere belangen en hebben dus ook een heel andere interpretatie van het fenomeen informatiebeveiliging. Voor hen is informatiebeveiliging eerder 'het veilig stellen van inkomsten'. Informatie is geld en daar ben je zuinig op. Zo zuinig dat ze zich eigenaar achten van de persoonlijke foto's en ontboezemingen die wij op ons eigen profiel plaatsen. Dat staat in de kleine lettertjes en daar is immers elke gebruiker mee akkoord gegaan.

Bewustwording

De consument zal zich meer bewust moeten worden van de risico's van sociale media. Via Twitter en Facebook leggen we onze ziel en zaligheid bloot. Veel mensen passen de zichtbaarheid van hun berichten niet aan en plaatsen alles publiekelijk zichtbaar, want zo is het uiteraard standaard ingesteld door het sociale medium. Bedenk dat iedereen dan kan meekijken: je collega's, je baas, je familie. Maar ook het dievengilde, dat ziet dat je op vakantie bent in Zuid-Frankrijk. En de verzekeraar die op Facebook vakantiekiekjes ziet waar je die dure zonnebril draagt die onlangs als verlo-

ren was geclaimd. Besef dat alles wat op internet belandt sowieso tot in eeuwigheid is terug te vinden in zoekmachinedata. Op zich is dit nog niet eens zo erg, zolang mensen zich er maar bewust van zijn. Maar wie wil over tien jaar nog steeds worden geconfronteerd met de getwitterde opmerking over de regering die nu zo onschuldig lijkt, maar in de toekomst ineens gevoelig ligt?

Verplichting versus keuze

Als consument vertrouwen we vrijwillig ons privéleven toe aan commerciële partijen, maar als burger gaan we met de hakken in het zand als de overheid een kilometerheffing, OV-chipkaart of elektronisch patiëntendossier invoert. De overheid legt ons beslissingen op, terwijl de klantenkaart van de supermarkt of de apps op onze smartphone onze eigen keuzes zijn. We staan er niet bij stil dat we via de klantenkaarten en apps heel veel inzicht in ons privéleven geven. De lange termijn risico's omtrent privacy wegen niet op tegen de korte termijn voordelen van een korting of een leuk gratis spelletje. Zo zit de menselijke psyche in elkaar. We nemen de meeste beslissingen op emotie en daar spelen bedrijven handig op in.

Verantwoord met data omgaan

Niet alle bedrijven die gegevens verzamelen, doen dat om er geld mee te verdienen. Maar zij hebben wel privacy gevoelige gegevens in beheer om hun taken uit te kunnen voeren. Ook deze bedrijven lopen risico's met informatiebeveiliging en/of schendingen van de privacywetgeving. Ze bedenken een fantastische app of interactief systeem waarmee ze (indirect) informatie van de gebruiker vergaren, zonder te beseffen dat ze privacy-regelgeving overtreden.

Imago-schade

Wie zich bij dataverwerking onvoldoende bewust is van zijn kwetsbaarheid, kan de mist ingaan en daarbij een forse deuk in het imago oplopen. Om imagoschade te voorkomen, stellen ze zeer hoge beveiligingseisen bij een nieuw ontwerp. Soms zelfs hoger dan voor de betreffende toepassing noodzakelijk is. "Wij willen niet in de krant komen met een verhaal over een hoogleraar die met een paar studenten in een uur ons product kraakt. Ook al is de winst van zo'n kraak marginaal, de imagoschade is enorm."

Het gevolg is dat relatief simpele producten toch behoorlijk duur kunnen worden vanwege de uitgebreide specificaties voor informatiebeveiliging. Terwijl het hierbij vooral om 'imagobeveiliging' gaat, dat wellicht meer kost dan dat het oplevert. Met behulp van de juiste technische keuzes tijdens het ontwerpen van het product, kan de optimale prijs/beveiliging-verhouding worden bereikt.

Alles is te kraken

Wie na al deze waarschuwingen denkt dat nu het gouden ei komt, moeten we helaas teleurstellen. Een universele oplossing is er niet, wel een universele stelregel: hoe goed de beveiliging ook is, uiteindelijk is alles (met heel veel geduld en kunde) te kraken. Een bijbehorende vuistregel is 'je doet het goed of je doet het niet'. 'Een beetje beveiligd zijn' is net zoiets als 'een beetje zwanger zijn', dat kan dus niet.

> "Je doet het goed of je doet het niet"

Informatiebeveiliging is een eeuwige wedloop tussen hackers en cryptografie experts. Qua techniek geven cryptoexperts actuele aanbevelingen. Maar wat je ook kiest, je weet dat het ergens in de toekomst weer gekraakt kan worden. Zeker in de continu veranderende wereld van connected elektronica, waar een product in een paar jaar is verouderd. Daarom moet je blijven evalueren. Is mijn beveiliging nog steeds toereikend? Helaas zijn er genoeg voorbeelden van producten waar we - om veiligheidsredenen - beter afscheid van zouden moeten nemen. GSM, GPRS en DECT zijn bijvoorbeeld zo lek als een mandje.

Beveiligen is anders denken

Veiligheidsdenken vraagt een andere manier van bekijken hoe een systeem misbruikt kan worden. Intuïtief gaan we uit van het goede in de mens. Gelukkig maar, in een normale samenleving is dat ook wenselijk. Echter, veiligheidsdenken vraagt het tegenovergestelde. Je hebt maar één persoon nodig die niet van goede wil is, ga daar dus ook vanuit. Breng risico's in kaart door naar kwetsbaarheden te kijken en maak een bewuste keuze voor de maatregelen die je vandaag-de-dag moet en kunt nemen. Vergeet vooral niet om over een paar jaar nog eens goed naar die risico's en keuzes te kijken: de technologie verandert en de keuzes van vandaag zijn morgen achterhaald.

Dit vraagt om bewustwording van de risico's, vandaag, morgen, volgend jaar: zowel bij consumenten als bij organisaties.

Telt mijn stem wel mee?

Een historische verkenning van de veiligheid van stemmethoden

Door: Stas Verberkt
Alumnus Computer Science (Information Security track) en Consultant Information Security

Hoewel er verhoudingsgewijs slechts weinig democratieën zijn geweest, hebben deze staten vele wijzen van stemmen gekend. Over de jaren is gewerkt met scherven, formulieren, machines en computers. Elk systeem is geplaagd door aanvallers die de uitslag naar hun hand wilden zetten. In Nederland is dit op fameuze wijze in het publieke debat gekomen door Rop Gongrijp en zijn comité "Wij vertrouwen stemcomputers niet".

De vraag die voor de wetenschap nog altijd overeind is blijven staan luidt: hoe bouwen wij een stemsysteem dat een grote mate van zekerheid biedt? Om deze vraag te beantwoorden is het verstandig om met de blik van een informatiebeveiliger naar de geschiedenis te kijken en ons af te vragen waar de sterke en zwakke punten van de geprobeerde methoden zitten.

Wanneer is een stemsysteem veilig?

Voordat een zinnig woord over de beveiliging van stemmingen gesproken kan worden is het nodig te bepalen wat van een stemsysteem verwacht wordt. In het algemeen wordt een vijftal vereisten waaraan voldaan moet worden erkend. Deze zijn de volgende: de correctheid, het sterke stemgeheim, de inclusiviteit, de authenticatie en de beschikbaarheid.

Om te beginnen dient een stemming correct te zijn. De uitslag moet corresponderen met de intentie van de stemgerechtigden. Hiermee wordt niet alleen bedoeld dat diegene wint waarvan de meeste burgers het stemvakje hebben ingekleurd, maar ook dat het de intentie was van die burgers om diegene te kiezen. Het zou immers een misverstand zijn om niet naar de gebruiksvriendelijkheid te kijken: een onbruikbaar systeem zal de democratie geen goed doen.

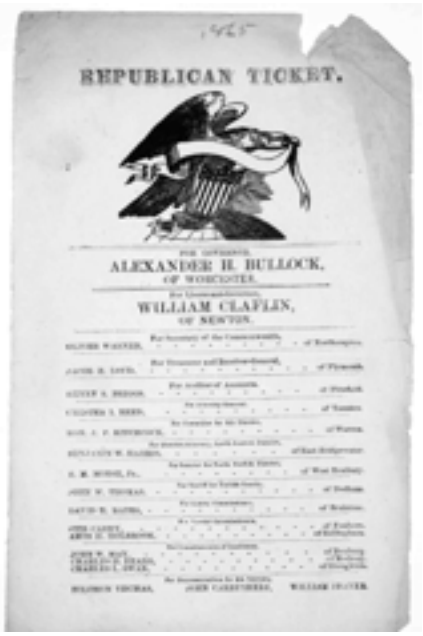
Ten tweede kennen wij het sterke stemgeheim: het dient onmogelijk te zijn voor een ander om te zien hoe jij gestemd hebt, zelfs als jij dat zou willen. Dit betekent niet alleen dat de privacy gewaarborgd is, maar ook dat het verkopen van een stem of het onder dwang uitbrengen van een bepaalde stem niet kan. Zeker nu is het sterke stemgeheim het moeilijkste vereiste om in de praktijk te brengen.

Als derde moeten stemmingen inclusief zijn. Iedere stemgerechtigde burger dient de kans te krijgen zijn stem uit te brengen. Zodoende bestaat een heel scala aan logistieke voorwaarden waaraan voldaan moet worden: genoeg stembureaus, lange openingstijden en heldere uitnodigingen.

Direct tegenover de inclusiviteit staat het vierde vereiste: elke stemmer moet geauthenticeerd worden alvorens hij stemt. Elke stemgerechtigde burger mag maximaal één stem uitbrengen.

De vijfde en laatste eis is van een andere aard en komt dan ook voort uit recentere ervaringen in de informatiebeveiliging: de beschikbaarheid. Simpel gezegd dient het systeem gebruikt voor de stemming beschikbaar te zijn gedurende de stemming. Zeker voor methoden die het Internet gebruiken is dit een zorgenkindje. Het tegengaan van een DDoS blijft immers een complex vraagstuk.

Met de vijf vereisten voor een stemming bepaald wordt het snel duidelijk waarom het opzetten van een werkend stemsysteem een van de moeilijkste opgaven is: de eigenschappen waaraan het systeem moet voldoen staan vaak lijnrecht tegenover elkaar. We verwachten



Figuur 1: Party Ticket (1865, Republican, Massachusetts, Wikipedia)

dat het systeem correct is, maar willen ondertussen ook een sterk stemgeheim. We verwachten authenticatie van de stemmers, maar vragen ook om inclusiviteit.

Daarentegen was de correctheid van Viva Voce redelijk goed gewaarborgd. Door de openbaarheid van de stemmen kon iedereen meeschrijven en zijn eigen conclusies trekken. Eveneens kon men met gemak meekijken met de medewerkers wat zij opschreven, wat ook nog eens redundant gebeurde.

Dat een stemming destijds niet inclusief was spreekt al uit het feit dat velen überhaupt niet stemgerechtigd waren. Daarnaast gebeurde het ook dat oppositieleden werden gedwongen thuis te blijven.

Stemmen met papier

De vervanger van het stemmen met de stem is het papieren stembiljet, de methode die wij nog altijd gebruiken. Over de jaren heen zal de papieren stemmethode op de meeste manieren aangevallen zijn. In het licht van de protesten tegen de elektronische stemcomputer lijkt deze wel heilig verklaard. Stemmen met papier kent echter ook haar zwakheden. Het is daarom ook belangrijk alle methoden kritisch tegemoet te blijven treden.

In het begin ging stemmen nog zonder gestandaardiseerde stembiljetten. Iedere stem was niets meer dan een aantal namen geschreven op een willekeurig stukje papier. In de Verenigde Staten kwamen al snel "party tickets". De twee grote partijen maakten gekleurde stembiljetten met daarop de namen van hun keuze. Op deze manier konden mensen het stemadvies van hun partij gemakkelijk opvolgen. Daarnaast was het aan de kleur zichtbaar dat jij de juiste partij stemde.

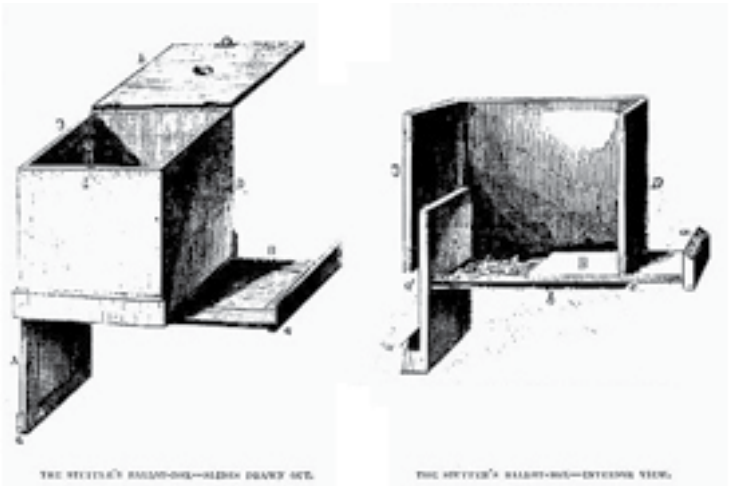
In het verleden is veel gefraudeerd met de stembus. Zo bestaan stembussen met een dubbele bodem of een tweede opening. Om fraude te voorkomen zijn glazen stembussen in gebruik geweest. Ook nu nog wordt vaak gebruikgemaakt van "stuffing" om te frauderen met verkiezingsuitslagen. In Nederland is tegenwoordig de stembus te controleren voor aanvang van de stemming.

"Door de geschiedenis zal het papieren-stembiljet het meest geplaagd zijn door aanvallers."

Viva Voce

Een van de vroegste manieren om te stemmen is "Viva Voce" – stemmen met de stem. In de prille Amerikaanse democratie verzamelde alle stemgerechtigde burgers zich op het dorpsplein. Daar zaten twee medewerkers van het stembureau die beiden de stemmen noteerden. Eveneens was een ander verantwoordelijk voor het omroepen van de stemmen. Iemand die zijn stem uit ging brengen zei simpelweg met luide stem zijn naam en zijn keuze. De twee schrijvers noteerden dit vervolgens onafhankelijk van elkaar op een lijst.

Het valt direct op dat deze vroege stemwijze totaal geen stemgeheim kent. Toen was het dan ook niet ongewoon dat de minderbedeelde stemgerechtigde burger een goede maaltijd of een stevige dreiging kreeg in ruil voor zijn stem. De koper of bedreiger kon vervolgens met gemak controleren of zijn slachtoffer inderdaad stemde als gevraagd.



Figuur 2: Stembus met dubbele bodem

Over Stas

Stas Verberkt (1988, Woerden) studeerde van 2007 tot 2012 informatica in Enschede. Tegenwoordig is hij consultant informatiebeveiliging bij Accenture. Hij heeft een cum laude MSc Information Security van het Kerckhoffs Institute.

Stas is actief binnen D66, waar hij onder andere voorzitter en oprichter is van de thema-afdeling Digitaal 66. Eveneens is hij associate member van de ALDE Party.

Tijdens zijn studie heeft Stas twee commissies bij Inter-Actief voorgezeten. Ook was hij vice-voorzitter van de Universiteitsraad van 2009-2010.

Stas schrijft regelmatig artikelen over informatiebeveiliging en politiek. Daarnaast onderhoud hij zijn persoonlijke weblog blog.digitalliberalism.eu.

Een creatieve aanval op het papieren-stembiljet is "vote chaining". Hier staat de aanvaller buiten het stembureau met een al ingevuld biljet. Middels omkoping of afpersing vraagt hij zijn slachtoffer dat biljet in de stembus te doen en het lege biljet van de stembus weer terug te brengen. Het lege biljet is voor de aanvaller het bewijs dat naar wens gestemd is.

Het zwakste punt van papier blijft de telling. Zeker bij handmatige tellingen is een foutmarge inherent, zeker wanneer dit gedaan wordt door aan het einde van een lange dag op het stembureau. Indrukwekkender zijn de zogenaamde "fingernail artists". Dit verwijst naar een aanval waarbij biljetten worden aangepast met behulp van een stukje grafiet onder de vingernagel. Hoewel dit vergezocht klinkt, bestaan veel verwijzingen naar deze vorm van fraude tijdens het tellen. Gelukkig zijn in Nederland de tellingen openbaar, al komen weinig mensen kijken.

"In de moderne tijd blijkt de smartphone een bedreiging van het stemgeheim."

Een moderner probleem met het papieren stembiljet is de smartphone. Tijdens de Tweede Kamerverkiezingen van 2012 deelde Femke Halsema een foto van haar ingevulde stembiljet publiekelijk op Twitter. Dit maakt pijnlijk duidelijk hoe het stemgeheim tegenwoordig niet meer zo sterk is.

Authenticatie op het stembureau

In Nederland heeft iedereen zijn identiteitsbewijs nodig om te mogen stemmen. Op deze manier kan gecontroleerd worden dat niemand meer dan één keer stemt. Gelukkig heeft bijna iedere Nederlander een identiteitsbewijs en kan elk ander deze relatief makkelijk aanvragen. Zodoende is ook de inclusiviteit vrij goed beschermd.

In Amerika hebben minder mensen een paspoort of rijbewijs. Daarnaast is in de Verenigde Staten vaak het inschrijven in het stemregister apart geregeld en niet via de basisadministratie. Tegen dit contrast wordt authenticatie op het stembureau opeens een stuk moeilijker en is de inclusiviteit ook minder vanzelfsprekend.

De bevolkingsgroep zonder identiteitsbewijs geldt als een aparte demografie. Veelal zijn dit armere mensen die dus eerder links zouden stemmen. De demografie komt ook kijken bij de locatie van het stembureau. In extreem dicht bevolkte gebieden is vaak meer armoede dan in "gewoon" stedelijk gebied. Wanneer men vervolgens in beide gebieden evenveel stembureaus plaatst, bestaat een kans dat de wachtrijen in het armere gebied zo erg worden dat een deel van de linkse stemmen niet meer uitgebracht wordt.

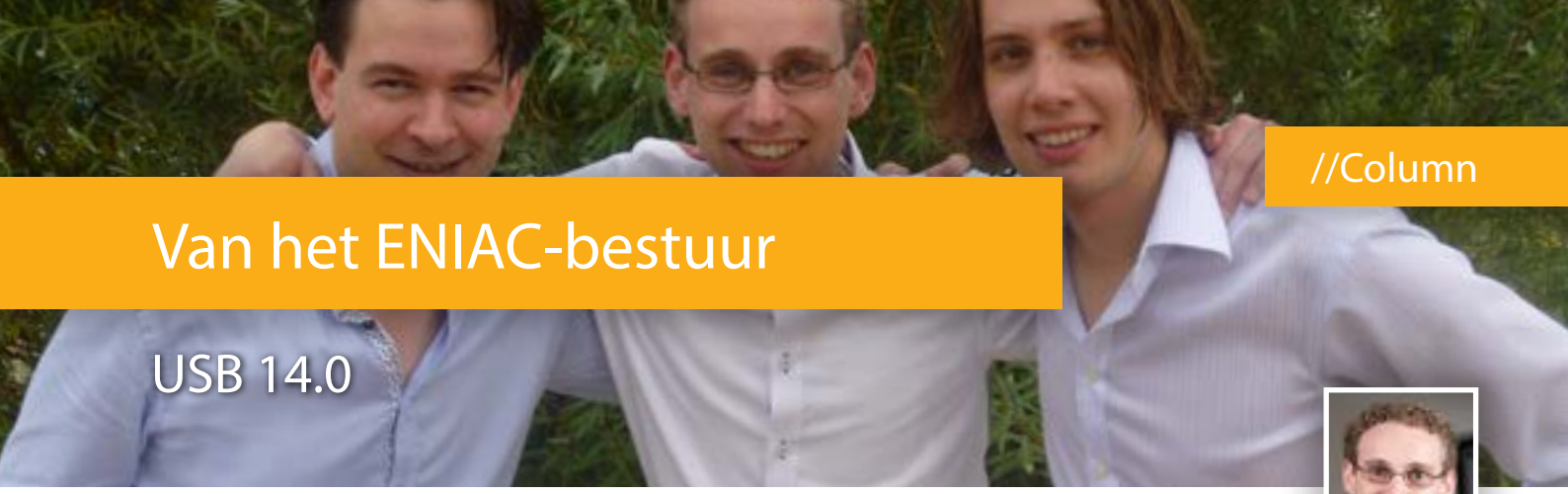
Tellen die stem!

Het hacken van elektronische stemcomputers is enorm spannend. Echter, het vernuft waarmee bij oudere stemmingen is gefraudeerd door de jaren heen is minstens zo interessant. In deze geschiedenis van bekende aanvallen op de klassieke methoden valt te zien hoe een stem vroeger ontnomen werd. Wellicht kunnen we een volgende keer de methoden van de 20e en de 21e eeuw aanpakken…

Figuur 1: Glass Ballot Box (1884, Wikipedia)

Bronnen

Broken Ballots - http://press.uchicago.edu/ucp/books/book/distributed/B/bo13383590.html



Van het ENIAC-bestuur

USB 14.0

Door: Johan Noltes
Voorzitter ENIAC

Het is een koude avond eind 2013. Terwijl mijn bestuursgenoten toevallig beide genieten van een welverdiende vakantie in een warmer deel van deze wereld, denk ik terug aan hoe het twee en een half jaar geleden allemaal begon. Tijdens de EWI-Trip verdeelden wij met elkaar op een terrasje in Praag de bestuursfuncties, en spraken onze ambities voor de vereniging uit. Nu, ruim twee jaar later, zijn we bijna aan het einde van onze periode, en zoeken we alweer bijna naar opvolgers. Als ik terug denk aan onze resultaten, realiseer ik me opeens hoe internationaal georiënteerd wij als alumni en als vereniging zijn.

Kijken we bijvoorbeeld naar het jaarboek dat ENIAC eerder dit jaar uitbracht, dan zien we daarin een mooie lijst met alumni in het buitenland. Maar een opvallender signaal vond ik de betrokkenheid van deze buitenlandse alumni bij de vereniging. Gezien de hoge portokosten mailden we onze internationale leden met de vraag of ze het jaarboek wel wilden ontvangen. De reacties waren overweldigend: meer dan de helft reageerde actief met het verzoek om het jaarboek op te sturen.

Ook onze oproep om deel te nemen aan de accreditatie van de Informaticaopleidingen riep internationale reacties op. Gezien de moderne technologie zou een videoconference geen belemmeringen voor digitale aanwezigheid moeten geven, maar de visitatiecommissie vond het steunen op deze 'nieuwe technologie' toch net iets te eng.

Als vereniging proberen we een buitenlandreis tijdens de studie ook te stimuleren. Dit jaar reikten we voor het eerst sinds lange tijd weer het ENIAC Scholarship uit. Op onze website lees je de maandelijkse blog de avonturen van Mark en Jonas op de Chung-Ang University in Seoul, Zuid Korea. Zij waren de gelukkigen die het scholarship toegekend kregen door de beoordelingscommissie. Een commissie die natuurlijk voor de meerderheid uit in het buitenland wonende leden bestond.

Ik vraag me af hoe het komt dat onze actieve informatici zo internationaal bezig zijn. Komt het omdat de technologie uit ons vakgebied ons eenvoudiger in contact brengt met de rest van de wereld? Of vindt deze internationale oriëntatie toch zijn oorsprong in onze studie?

Op het moment dat ik deze column schrijf, maakt de nieuwe studiereiscommissie van Inter-Actief – USB 14.0 – haar thema en bestemmingen bekend. Volgend jaar reizen 30 studenten naar de VS en Brazilië, om bedrijven te bezoeken rond het thema 'smart surroundings'. Het zou me niet verbazen dat deelnemers aan een studiereis toch nét iets meer geïnternationaliseerd zijn dan de gemiddelde student. Laten 25 jaar aan studiereizen bij Inter-Actief dan toch haar sporen in de historie na?

Ik hoop daarom dat ik via deze column studenten kan enthousiasmeren om deel te nemen aan een dergelijke reis. Maar ook om alumni te motiveren om hun bijdrage te leveren. Want met onze internationale achtergrond kennen wij ongetwijfeld interessante bedrijven, universiteiten of onderzoeksinstellingen die een waardevolle toevoeging kunnen zijn aan deze reis naar twee continenten aan de andere kant van de wereld.

Met een bereik van 1000 studenten en 900 alumni moeten er toch weer mooie samenwerkingen kunnen ontstaan? Ik zie nu al uit naar de dagverslagenbundel van de nieuwe studiereis!

Johan Noltes, voorzitter

Johan Noltes is voorzitter 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 activitei- ten 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.

Johan Noltes
voorzitter@eniac.utwente.nl