

12

ZOMER 2011

UPDATE

WWW.MADISON-GURKHA.COM

.....

DE COLUMN 2

Walter Belgers

HET NIEUWS 3

- Sponsoring EuroBSDCon 2011
- Beveiliging open source-systeem tiqr
- HACK.LU 2011
- Eindhoven is uitgeroepen tot slimste regio ter wereld

HET INZICHT 4-5

Tim Hemel over de risico's rondom het gebruik van mobiele apparatuur

DE HACK 6-7

Laurens Houben vertelt over het (on)veilig gebruik van publieke netwerken

DE KLANT 8

Openhartig gesprek met twee medewerkers van SURFnet:
Harold Teunissen en Joost van Dijk

HET INTERVIEW 9

IT-wetenschapper Karsten Nohl van de Universiteit van Virginia over het af luisteren van GSM- verkeer

HET VERSLAG 10

Black Hat Sessions, Part IX:
The Human Factor

HET COLOFON 11

.....



Het internet is overal

Het doet me deugd dat u onze Update aan het lezen bent. Misschien leest u hem op papier, misschien digitaal. Misschien zelfs wel vanaf uw vakantieadres. Overal ter wereld kunt u via internet de Update downloaden. Het internet is overal.

De opkomst van het internet bracht een revolutie teweeg. De daarop volgende revolutie was die van "always on". Gebruikers die niet meer inbelden, maar altijd online bleven via ADSL of kabel. Momenteel is de volgende revolutie aan de gang: de overgang van internet thuis naar internet dat je meeneemt. Dankzij smartphones kunnen we continu overal online blijven, met een hele nieuwe industrie als gevolg: die van de social media.

Dankzij social media is de sociale cirkel rondom iemand niet meer een fysieke cirkel, maar is deze virtueel geworden. Vroeger kwam je, als je in de trein stapte, in een fysieke andere sociale omgeving. Tegenwoordig grijpen mensen in de trein naar hun smartphone om hun eigen sociale cirkel weer bij zich te hebben.

De komst van mobiel internet heeft ook gevolgen voor de manier waarop u IT regelt in uw organisatie. Vroeger hadden medewerkers thuis geen, of in ieder geval andere computerapparatuur dan op kantoor beschikbaar was. Er was daarom een manier van werken op kantoor en een manier van werken thuis.

Nu iedereen thuis van (ruwweg) dezelfde technologie gebruikt maakt als op kantoor, leeft de verwachting dat alles op kantoor op dezelfde manier werkt. En daar wringt de schoen een beetje. Beveiligen houdt vaak in dat je wat aan functionaliteit moet inleveren. Het verbieden van USB-sticks verhoogt de beveiliging, maar is wel lastig. Dat soort maatregelen konden vroeger nog wel genomen worden, maar aangezien vrijwel iedereen thuis probleemloos met USB-sticks kan werken, wordt het erg lastig om medewerkers te laten inzien wat de beveiligingsrisico's zijn die dat met zich meebrengt. Vooral als het "meestal" goed gaat.

Met de komst van smartphones gaat het nog een stap verder. Medewerkers willen hun werk kunnen doen vanuit een niet-werkomgeving, op hun eigen apparatuur. Dat is uit bedrijfsoogpunt misschien prettig, maar ook dit brengt risico's met zich mee. Vroeger kon dit nog wel beheersbaar gehouden worden door zelf een oplossing in te richten met voldoende beveiligingsmaatregelen, zoals een "laptop van de zaak", maar smartphone-gebruikers willen gewoon met hun bestaande apparaat kunnen werken.



We staan daarom voor een uitdaging. Hoe krijgen we dit soort zaken veilig, als de bedrijfsapplicaties op een niet door ons beheerd apparaat draaien? Er zijn wel technieken die hier kunnen helpen, maar het risico zal uiteindelijk hoger worden. Vandaar dat het belangrijk is om het interne bedrijfsnetwerk goed op te zetten en veilig te houden.

Mobiele apparaten bieden natuurlijk ook interessante nieuwe mogelijkheden. Met de komst van het internet heeft vrijwel elk bedrijf gericht op consumenten, een selfservicewebsite opgezet. Daar kunnen klanten inloggen en hun gegevens inzien en wijzigen, producten aanschaffen, etc. Momenteel nemen we de stap van websites naar mobiele applicaties. Zo staat de applicatie "Appie" van een bekende grootgrutter in de Nederlandse top-3 van mobiele applicaties. Gebruikers kunnen hiermee een recept aanklikken, waarop de ingrediënten automatisch geselecteerd worden, desgewenst gesorteerd op de looproute door de winkel.

Smartphones bieden verder een interessante mogelijkheid om bestaande beveiligingssystemen, die GSM-technologie gebruiken, uit te faseren. GSM-verkeer en met name SMS-verkeer is vaak relatief eenvoudig af te luisteren. Zie hiervoor ook het interview met Karsten Nohl elders in deze Update. Door de twee-factor authenticatie deels via internet te laten lopen, waarbij goede versleuteling wordt gebruikt, kan dit risico vermeden worden. SURFnet heeft onlangs "tiqr" geïntroduceerd met dat precies als doel. Zie de rubriek "De Klant" waarin Harold Teunissen en Joost van Dijk hier openhartig over spreken.

Wij merken bij onze klanten een groeiende vraag naar onderzoeken van apparatuur die medewerkers bij zich dragen (zoals laptops en smartphones). Ook zien we een groeiende markt voor onderzoeken naar smartphone-applicaties. De groei van het aantal van zulke applicaties is niet tegen te houden. Als u zich er nog niet meer bezig houdt, bereid u dan wel alvast voor, want het komt eraan, ook voor u.

Walter Belgers
Partner, Principal Security Consultant

Eindhoven is uitgeroepen tot slimste regio ter wereld

Eindhoven is op 3 juni 2011 in New York uitgeroepen tot Intelligent Community of the Year 2011. Na een spannende finale werd Eindhoven als winnaar gekozen uit een selectie van zeven genomineerden, waaronder Dublin en Windsor-Essex. Volgens medeoprichter Louis Zacharilla van het Intelligent Community Forum (ICF) is Eindhoven "een voorbeeld voor een nieuwe manier van denken over samenwerking en regionale ontwikkeling".



Madison Gurkha is blij om haar steentje hieraan bij te kunnen dragen. Wij erkennen dat specialisatie, kennisopbouw en ontwikkelingen noodzakelijk zijn en delen graag onze kennis met de maatschappij door het verzorgen van presentaties, opleidingen, artikelen en onze bijdrage aan open source projecten. Deze prestatie is niet alleen iets om als regio trots op te zijn maar is ook nuttig omdat het nog meer interessante bedrijvigheid, investeringen en creativiteit aantrekt.



Sponsoring EuroBSDcon 2011

EuroBSDcon is een conferentie voor gebruikers en ontwikkelaars van op BSD gebaseerde systemen. In oktober 2011 wordt de tiende editie van deze technische conferentie gehouden. EuroBSDcon streeft ernaar om de beste technische papers en presentaties beschikbaar te stellen om ervoor te zorgen dat de laatste ontwikkelingen in onze open source-gemeenschap worden gedeeld met het grootst mogelijke publiek.

Wij steunen de doelstellingen van EuroBSDCon en sponsoren dit project dan ook van harte.

Kijk voor meer informatie op <http://2011.eurobsdcon.org>.

HACK.LU 2011

Op 19 t/m 21 september vindt de zevende editie van Hack.lu plaats in het Parc Hotel Alvisse te Luxemburg. Hack.lu is een open conventie/conferentie, waar men kan discussiëren over computerbeveiliging, privacy, informatietechnologie en de culturele/technische gevolgen hiervan op de samenleving. De eerste dag worden er verschillende workshops gegeven, waaronder die van Walter Belgers. In zijn workshop "lockpicking" leert hij je hoe je, door middel van fijne metaalstaafjes, een hangslot zonder forceren kan openen. De volgende twee dagen staan in het teken van interessante lezingen.

Kijk voor meer informatie en om je in te schrijven op <http://2011.hack.lu>

Beveiliging open source-systeem tiqr

Het open source project is in september 2010 gestart door SURFnet en is gebaseerd op open standaarden voor veilige authenticatie ontwikkeld door het Open Authentication Initiative (<http://www.openauthentication.org>).



SURFnet wil graag een second opinion krijgen over de security. Het doel van het onderzoek is om te checken of de hele architectuur van het systeem klopt. Worden de sleutels wel netjes opgeslagen op de server bijvoorbeeld? Maar ook om te kijken naar zaken waar wellicht bij de implementatie nog niet aan gedacht is.

De zogeheten "Crystal Box Application Audit", inclusief inspectie van de broncode en een design review met threat analysis, is volledig uitbesteed aan Madison Gurkha.

Zie ook het interview met Harold Teunissen en Joost van Dijk over het tiqr-project elders in deze Update.

Nieuwe platforms bieden nog weinig beveiligingsbewustzijn

Met het slimmer worden van telefoons is de wereld een stuk interessanter geworden. We kunnen foto's die met de camera op de telefoon zijn gemaakt, direct online zetten, we kunnen kijken of we de bus bij de dichtstbijzijnde halte nog kunnen halen dankzij de GPS-ontvanger en we kunnen boze vogels met een katapult afschieten naar kleptomane varkens.

Dit wordt allemaal mogelijk gemaakt door software en zoals we al jaren iedere dag weer merken: software zorgt voor risico's.

Nu zou het niet zo'n probleem zijn als we met onze telefoon alleen het spelletje Angry Birds zouden spelen, of wat surfden op het web om de laatste roddels over een BN'er te bekijken, maar we gebruiken onze telefoon ook voor zaken waarbij gevoelige informatie een rol speelt. Het is dus belangrijk dat we ons bewust zijn van de risico's die het gebruik van een smartphone met zich meebrengt.

Eén van de voordelen van de smartphone is het bedieningsgemak. Iedereen kan de basisfuncties van een telefoon wel gebruiken en als ons kleine neefje heeft uitgelegd hoe je moet websurfen of dat leuke spelletje moet spelen, dan lukt het ook wel om de telefoon geavanceerder te gebruiken. Dit bedieningsgemak is tegelijkertijd een valkuil, omdat mensen niet kunnen zien of begrijpen wat er 'onder water' gebeurt.

Veiligheid

De diverse fabrikanten van smartphone platforms vertellen ons vaak dat hun platform veilig is; maar zelfs al klopt die bewering, dan is deze bescherming beperkt. Een iPhone app is bijvoorbeeld alleen te installeren na goedkeuring van Apple.

Diverse applicaties zijn al geweigerd omdat ze informatie van de telefoon zouden stelen. Maar hoe betrouwbaar is deze controle? Uit eigen ervaring weet ik hoe ingewikkeld het kan zijn om een applicatie te onderzoeken op veiligheid en dat een programmeur een achterdeur in een programma er onschuldig uit kan laten zien.

Het Android platform doet niet aan dergelijke controles, maar legt de verantwoordelijkheid bij de gebruiker. Applicaties moeten voor het installeren vertellen welke permissies ze willen hebben ('deze applicatie wil het telefoonboek kunnen lezen') en de gebruiker dient dit goed te keuren. Het probleem daar is tweeledig: aan de ene kant is het permissiemodel niet nauwkeurig genoeg. Je kunt een applicatie bijvoorbeeld wel toegang geven tot het telefoonboek, maar wat er met deze gegevens gebeurt weet je niet. Aan de andere kant snappen veel gebruikers niet wat deze permissies inhouden of lezen er vluchtig overheen. Het nog complexer maken van het permissiemodel zal ze niet helpen.

Tot zover zijn dit niet echt nieuwe problemen. We zien deze zaken immers ook bij gewoon computergebruik en dat vertrouwen we ook, dus waarom zouden we nu ineens extra voorzichtig moeten doen met onze smartphones?

Vertrouwen

Er is een aantal redenen waarom we extra moeten opletten. Ten eerste bieden de smartphone platforms expliciet de mogelijkheid om data te delen tussen applicaties, meer dan bij het PC-platform zoals we dat kennen. Het is daardoor aantrekkelijk voor applicatiebouwers om van deze functionaliteit gebruik te maken. Daarnaast hebben de mobiele platforms een voor veel programmeurs nieuw beveiligingsmodel, waardoor er weinig ervaring is op het gebied van het maken van veilige applicaties. Een ander beveiligingsmodel geeft een ander soort aanvallen, waarvan men zich nog niet bewust is. Ten derde zien we op desktopcomputers virusscanners en persoonlijke firewalls. Vooralsnog zijn deze nog geen gemeengoed op smartphones. Hoewel ze wel bestaan, wordt het gebruik ervan niet afgedwongen. Voor desktop PC's zien we in een organisatie vaak een beveiligingsbeleid, maar een beleid opstellen voor smartphones is een stuk lastiger. De gebruikte smartphone is immers vaak eigendom van de gebruiker zelf en daarom is het moeilijk eisen te stellen aan de installatie hiervan. Daarnaast is er nog weinig bekend over de technische risico's van een smartphone. Als deze al worden genoemd, dan betreft het vaak maatregelen die voorkomen dat informatie lekt wanneer men het toestel verliest. Over virusscanners en het gebruik



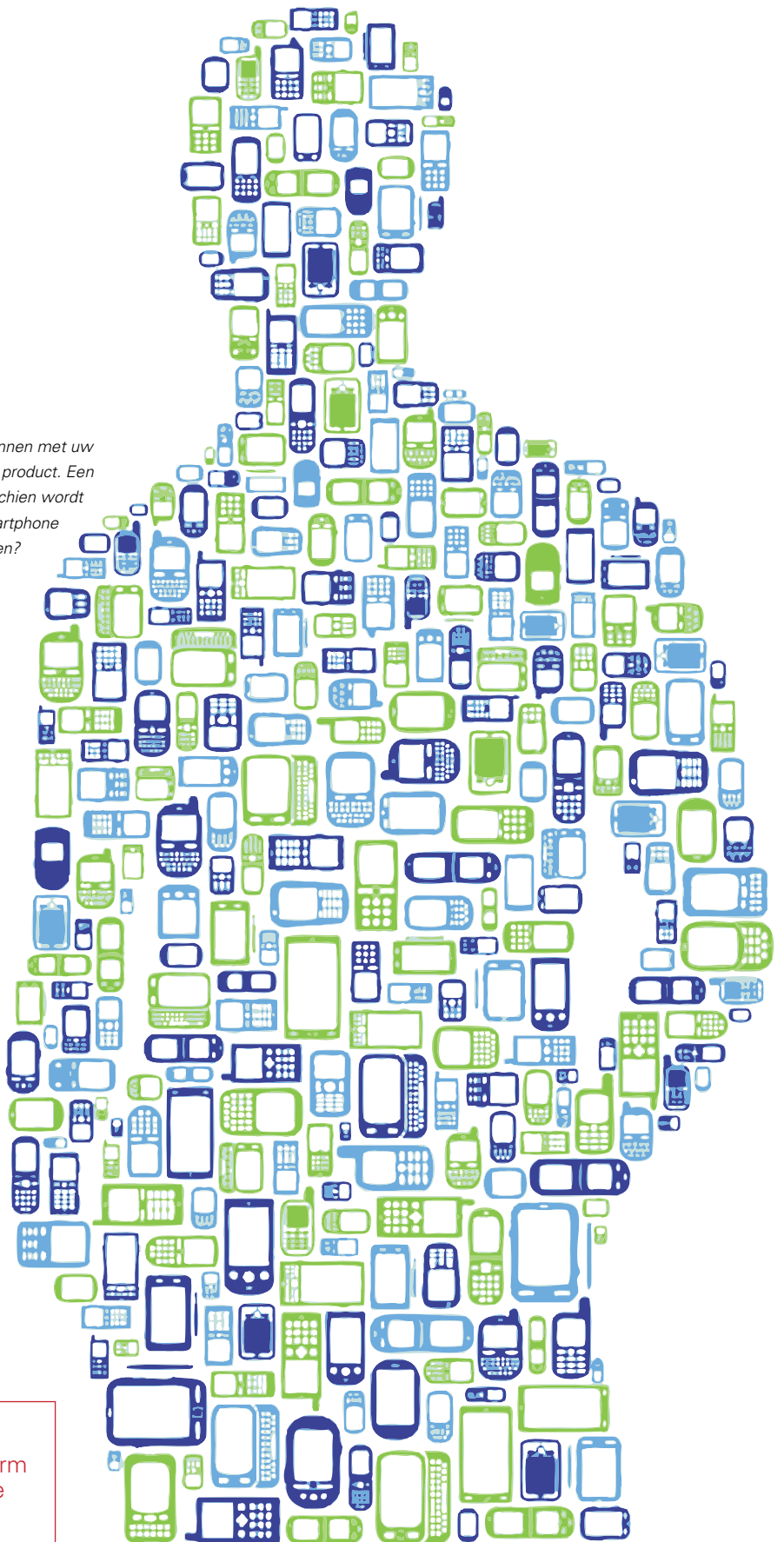
Hierboven ziet u twee zogenaamde QR-codes. Deze kunt u scannen met uw smartphone om vervolgens meer informatie te krijgen over een product. Een van de twee codes is te goeder trouw, maar de andere...? Misschien wordt u wel doorgestuurd naar een kwaadaardige website die uw smartphone voorziet van malware. Welke van de twee is veilig om te scannen?

van beveiligde netwerkverbindingen wordt niet gesproken. Dat brengt ons bij het laatste kenmerk van mobiele apparatuur: de netwerk-omgeving is in principe niet te vertrouwen. Het goed controleren van de netwerkbeveiliging is daarom nog belangrijker dan we zijn gewend op onze PC. Het feit dat ik op mijn Nokia telefoon de lijst van vertrouwde certificaten niet makkelijk kan zien (als ik het al kan zien), geeft aan hoe vaak gebruikers deze functionaliteit willen gebruiken.

Kortom, we zien weliswaar de risico's die we al kennen, maar de omgeving en de platforms zijn zodanig nieuw dat er nog weinig beveiligingsbewustzijn is op dit gebied. Voorsnog dienen we de makers van programma's te vertrouwen dat zij geen kwaadaardige handelingen uithalen op onze telefoons en dat ze hun applicaties goed beveiligen. En uiteraard dienen we hier zelf ook goed op te letten. Bijvoorbeeld door het interpreteren van QR-codes.

TIP

Zorg dat u een applicatie gebruikt die de inhoud van de QR-code eerst op het scherm toont, zodat u kunt kiezen wat u met deze QR-code doet.



Datapakketjes door de lucht

Je bent aan het wachten op je vlucht met een kopje koffie erbij of je zit bijvoorbeeld in je hotelkamer en merkt dat er gratis WiFi aanwezig is. Dat is handig, kun je alsnog bij je zakelijke e-mail, internet bankieren, Facebook en andere zaken waar je je dagelijks mee bezig houdt. Maar hoe veilig is het nu om je privé- en werkgegevens over publieke netwerken te versturen als een handig persoon met een draadloze netwerkkaart eenvoudig mee kan luisteren?

Wat kan er gebeuren?

Herinnert u zich nog het artikel "Lucratieve handelswaar" uit Update 11? Hierin beschrijf ik wat er met persoonsgegevens kan gebeuren zodra deze in verkeerde handen valt. Deze persoonsgegevens gaan vaak grotendeels onversleuteld over het publieke WiFi-netwerk. Leesbaar voor eenieder die met minimale IT-kennis een sniffer-tool kan starten om vervolgens al het verkeer af te luisteren. Wanneer je gebruik maakt van onversleutelde protocollen zoals HTTP (voor het browsen), POP en SMTP (voor e-mailverkeer), Telnet en FTP (voor communicatie naar servers), dan gaat alle verkeer in leesbare tekst door de lucht. Die handige tooltjes op uw smartphone voor het versturen van berichtjes, opvragen van het saldo, inloggen bij webdiensten etc., versleutelen die het verkeer? Hier heeft u vaak geen invloed op en is het een kwestie van vertrouwen dat alles veilig wordt verzonden.

De Volkskrant voerde enige tijd geleden een onderzoek uit naar de veiligheid van publieke draadloze netwerken. Een VWO-leerling toonde toen aan dat het mogelijk is om al het verkeer van en naar de hotspots over zijn laptop om te leiden. Vervolgens kon hij met andere software HTTPS-verkeer meelezen. Binnen enkele minuten leverde een sniff op het gratis WiFi-netwerk van Schiphol Plaza wachtwoorden van ING, Facebook en Gmail op. Er wordt in de media aandacht geschonken aan het feit dat WiFi-netwerken vaak onveilige configuraties bevatten, maar zijn de gebruikers zich bewust van deze gevaren en doen ze er ook iets mee?

Is het strafbaar?

Dat is een vraag waar meerdere antwoorden en ideeën over bestaan. IT-jurist Arnoud Engelfriet heeft het op zijn weblog www.isusmentis.com beschreven. Hij zegt het volgende:

"Het opzettelijk en wederrechtelijk met een technisch hulpmiddel aftappen of opnemen van gegevens die voor iemand anders bedoeld zijn, is een strafbaar feit: 1 jaar cel, 16.750 euro (art. 139c lid 1). Dit wordt soms gegevensdiefstal genoemd, alhoewel dit formeel gesproken onjuist is: gegevens kunnen niet worden gestolen zoals fietsen of geld. Daarnaast zijn er speciale regelingen over het af luisteren, opnemen of aftappen van gesprekken tussen mensen. In een woning of besloten ruimte mogen geen gesprek-

ken worden opgenomen zonder toestemming. Gesprekken daarbuiten mogen niet heimelijk en met een technisch hulpmiddel opgenomen of afgeluisterd worden."

Een uitzondering op deze wet zijn de "vrije signalen".

"Het ontvangen van vrije signalen uit de ether is niet verboden, tenzij je een 'bijzondere inspanning' moet leveren om de signalen te kunnen interpreteren.

De bovengenoemde strafbepaling over het aftappen of opnemen van datacommunicatie geldt niet altijd. Er is een uitzondering gemaakt voor het opvangen van door middel van een radio-ontvangapparaat ontvangen gegevens (art. 139c lid 2). Het ontvangen van vrije signalen uit de ether is immers een Europees grondrecht (art. 10 van het Europees Verdrag voor de Rechten van de Mens (PDF)).

Wordt "een bijzondere inspanning" geleverd, of een niet toegestane ontvanginrichting gebruikt, dan is er echter toch sprake van strafbaar af luisteren. Een bijzondere inspanning kan bijvoorbeeld zijn het af luisteren van de encryptie-sleutel of het zich voordoen als de werkelijke ontvanger (denk aan het spoofen of vervalsen van een MAC-adres)."

Het af luisteren van onversleuteld internetverkeer lijkt dus tussen wal en schip te belanden. Het lijkt strafbaar omdat het af luisteren van persoonsgegevens betreft, maar volgens de wet valt het net buiten het strafbare gebied. Het vonnis zal uiteindelijk bij een rechter liggen of het strafbaar is of niet.

Hoe doen ze het?

Er zijn diverse open source tools die vrij beschikbaar zijn waarmee het mogelijk is om eenvoudig het draadloze verkeer te sniffen. Ik zal enkele voorbeelden geven.

Frans Kollée schreef in Madison Gurkha Update 11 over het opzetten van 'valse' netwerken om gebruikers te lokken. Dit kan met de set tools die samen het KarMetasploit-framework vormen. Zodra gebruikers verbonden zijn met het netwerk is het kinderlijk eenvoudig om het verkeer af te luisteren. Om deze moeite te besparen is het ook mogelijk om met het grafische programma Wireshark al het draadloze verkeer binnen het bereik van je netwerkaart af te luisteren en op te slaan. Het is dan wel noodzakelijk dat je je draadloze netwerkaart in een zogenoemde 'promiscuous' mode brengt waardoor deze naar al het verkeer luistert in plaats van alleen naar het verkeer dat voor hem bestemd is. Je krijgt nu alle datapakketjes te zien die door de lucht gaan. Hierin kun je vervolgens zoeken en sorteren totdat je de gegevens ziet die je graag wilt hebben.

In 2010 bracht Eric Butler het tool Firesheep uit. Dit deed hij uit protest tegen de grotere webdiensten omdat zij hun gebruikers niet goed zouden beschermen. Het tool is een Firefox-addon die je kunt installeren en vervolgens op het netwerk snijft naar ingelogde gebruikers op onder andere de volgende applicaties: Amazon, Cisco.com, Cnet, Facebook, LinkedIn, Flickr, Foursquare, Google, Gowalla, Live, Twitter, Vimeo, Wordpress, Yahoo en anderen. Firesheep geeft aan wanneer een gebruiker op het netwerk is ingelogd op één van de eerder genoemde pagina's en vervolgens kun je door op de melding te dubbelklikken de sessies overnemen. Je hebt dan niet direct de gebruikersnaam en het wachtwoord in handen, maar je bent wel ingelogd als deze gebruiker.

Hoe kun je het voorkomen?

Er zijn diverse oplossingen om veilig op een publiek netwerk te internetten. Eén van deze oplossingen is met behulp van een VPN-tunnel. Je zet dan een versleutelde verbinding op naar een computer die je vertrouwt, bijvoorbeeld bij je thuis. Over deze versleutelde verbinding verstuurt je de data zodat deze niet te sniffen is vanaf het netwerk. Dit vergt enige configuratie, maar je hoeft er geen expert voor te zijn. Op het internet staan diverse handleidingen over hoe je een VPN-tunnel op kunt zetten naar je thuiscomputer.

Mocht je geen VPN-oplossing voor handen hebben en toch gebruik moeten maken van een publiek netwerk, denk dan goed na over wat je doet op het internet. Nieuws kijken is geen probleem, maar log beter niet in bij je persoonlijke data zoals webmail en internet bankieren. Let altijd goed op dat wanneer je toch moet inloggen, je gebruik maakt van een HTTPS-verbinding. Dit herken je aan het slotje in je browser.

Klein detail: controleer wel of je een HTTPS-verbinding hebt met het juiste systeem.



Firesheep in werking



Dit keer in deze rubriek geen anoniem interview zoals u gewend bent, maar een diepte interview over het actuele open source-project voor veilige en toch ook makkelijke authenticatie. We gingen hier voor in gesprek met Harold Teunissen (l), afdelingshoofd middleware services/security officer, en Joost van Dijk (r), technisch productmanager en mede verantwoordelijk voor de ontwikkeling van tiqr.

SURFnet

Wat doet SURFnet?

Harold: SURFnet zorgt dat onderzoekers, docenten en studenten eenvoudig en krachtig samen kunnen werken met behulp van ICT. Eigenlijk is SURFnet een 'facilitator' voor samenwerking. Zie ook www.surfnet.nl.

Mobility wordt steeds belangrijker. Hoe speelt SURFnet in op de mogelijkheden hiervan?

Harold: Op dit moment zijn we bijvoorbeeld aan het kijken naar de integratie tussen WLAN en UMTS/LTE, waarmee studenten en medewerkers van hoger onderwijs- en onderzoeksinstellingen overal in Nederland netwerktoegang hebben met elk (mobiel) device, zonder daarvoor iets extra's te hoeven doen. Verder hebben we al jaar en dag het concept 'eduroam', wat geauthenticeerde toegang biedt tot een wereldwijd wireless-LAN. Op dit moment zijn we aan het kijken of we eduroam naast scholen en universiteiten, ook kunnen aanbieden op commerciële hotspots.

SURFnet heeft tiqr ontwikkeld. Hoe is deze ontwikkeling tot stand gekomen?

Joost: Voor een aantal gevoelige applicaties gebruiken wij one time passwords per sms. Vorig jaar zijn er doorbraken geweest in het stukmaken van GSM-encryptie waarbij is aangetoond dat het mogelijk is om de SMSjes uit de lucht te plukken en zo de 'one time passwords' te stelen. Hier wilden we iets anders voor bedenken. Bij veel andere methodes, zoals een SecurID hardware-token van RSA of een via sms toegestuurde code, moet je nog een complexe code invoeren op je computer. Een ander alternatief is het gebruik van PKI USB-tokens, die je moet aansluiten

op de computer. Daarvoor zijn echter speciale drivers nodig en dus installatierechten. We zochten daarom iets dat veiliger is dan SMS authenticatie, maar dat wel op je telefoon draait, want die heb je altijd bij je. Twee jaar geleden zijn we begonnen met een project "Mobile PKI". Dat gaat over authenticatie op basis van je SIM-kaart. De applicatie op de SIM-kaart leest de challenge en genereert op basis van de secret op de SIM een response die vervolgens wordt teruggestuurd naar de server. Omdat het allemaal op de SIM plaats vindt is het dus heel veilig. Het pad is beschermd, de SMSjes worden gecrypt, dus daar is goed over nagedacht. Een probleem is dat de SIM-kaart eigendom is van de operator. Zonder operator kunnen wij daar niks mee en helaas is Nederland niet erg voortvarend in het aanbieden van SIMs waar de applicatie al op staat. Omdat we daar niet op willen wachten, hebben we een alternatief bedacht: een programmaatje dat op je telefoon draait en min of meer hetzelfde doet.

We hebben toen gekeken naar twee belangrijke features die je daarvoor kunt gebruiken. In plaats van een challenge van een scherm over te tikken, gebruiken we de camera van de telefoon zodat de camera de challenge leest. Deze technologie is gewoon voorhanden in de vorm van QR-codes. En in plaats van iets wat je op het scherm ziet van je mobiele telefoon en dat vervolgens moet over-tikken in een browser, kan je telefoon het ook rechtstreeks naar de webserver sturen. Deze technologieën hebben we samen gebruikt om een challenge – response mechanisme in software op je telefoon te bouwen. Dat hebben we tiqr gedoopt.

Hoe werkt tiqr?

Joost: Het is makkelijk en veilig. Je hebt twee zaken nodig, je smartphone met de tiqr-applicatie en een PIN-code. Dus iets dat je hebt en iets dat je weet. Op deze manier kom je aan 2-factor authenticatie. Bij registratie berekent de tiqr-app een secretkey. Om in te loggen lees je met je camera een QR-code in. In de QR-code zit een challenge gecodeerd. Na het invoeren van de PIN-code wordt een response berekend en naar de website gestuurd, die het antwoord verifieert en het aanmelden toelaat. De PIN-code wordt gebruikt om het secret te crypten. Dus als je je telefoon kwijtraakt en deze in handen komt van een slimme hacker, dan kan hij elke bit dat er op staat uiteindelijk te pakken krijgen, maar gezien het feit dat deze allemaal gecrypt zijn heeft hij hier in principe niks aan.

Joost: Er is nog een ander scenario dat we ondersteunen. Noem het 'step up' authenticatie. Stel dat iemand geauthenticeerd is via SURFfederatie, dus die is ingelogd bij zijn eigen instelling. Dan kan het zijn dat de site wat extra zekerheid wil, om bijvoorbeeld een transactie uit te voeren. Dit zou ook met tiqr kunnen. Het aardige daarvan is dat, omdat de gebruiker al is ingelogd, we gebruik kunnen maken van nog een feature van telefoons: 'push notifications'. Dat doen we door de challenge rechtstreeks naar de telefoon te sturen. Op de telefoon zie je dan een pop-up die bijvoorbeeld vraagt "deze bank wil graag een transactie authenticeren". Daar kun je dan mee akkoord gaan, eventueel gekoppeld met een PIN-code. Daarna wordt de response teruggestuurd. Je hoeft dan dus niet eens meer een QR-code te scannen. We hebben dit alles open source gemaakt en het is te downloaden via www.tiqr.org.

De beveiligingsaudit van tiqr is uitbesteed aan Madison Gurkha. Wat zijn de ervaringen tot nu toe?

Joost: Dit is de eerste keer dat ik jullie zelf inhuur. Wat me opvalt is dat degenen die de scan hebben uitgevoerd snel to the point kwamen en zich snel hebben ingewerkt in de code. Al heel snel kwamen er gedetailleerde vragen. Ik was daar wel bang voor, het gaat in dit geval toch over een wat obscuurdere programmeertaal Objective-C, maar dat heeft deze personen in ieder geval niet tegengehouden om zich de materie snel eigen te maken. Toen ik hoorde wat er tijdens het onderzoek gedaan werd, vond ik het interessant dat ze de boel op die manier op pijnbank legden.

Karsten Nohl

How did you get into reverse engineering hardware?

At university, where I got my degree in cryptography. I wanted to design new cryptography for mobile applications but there didn't seem to be a need for it. The industry had already solved all the problems. To motivate the work on new cryptography I wanted to show that old cryptography was broken by reverse engineering it. We spent a couple of years on RFID and then went into mobile communication.

Back then, not many people were looking into reverse engineering hardware. Did people think it was too hard to do?

The approach of hardening systems by trying to break them, what we do as penetration testers, really only exists within computer science, not in engineering. When protection measures move from software to hardware, they left the realm where they were constantly challenged by people who get academic rewards for breaking something. It took some hackers to bring that back. Computer science people agree that it is not evil to point out flaws if doing so makes systems better in the long run.

You built tools to help reverse engineering chips. Did many people start using those tools?

The tools are being used, but not by a great number of people yet, mostly at universities. It may be that people still think it's a lot of work. But I think breaking hardware is easier than breaking software.

You first looked at RFID systems like Mifare, and later DECT and GSM. Why these?

We are mostly working with technology that is popular and old. Most new systems are based on good cryptography and good authentication protocols that were reviewed heavily. We don't expect much low-hanging fruit in these systems. But anything that has been out there 20 years and hasn't got any updates, is almost certainly broken. We almost feel obligated to do this quality assurance step 20 years later.

Should technology have an expiry date?

Yes, especially security technology. With the progress we're making in security, it does not make sense to have a system being used for more than 10 years, and even that is



stretching it. People are now discussing the chips and techniques to be used in ID-cards for the next 10 years, while it is not understood how much better chip-attacks will be in 10 years. It's hard to build a system now that can make guarantees for such a long period.

Why did your demonstration of intercepting and decrypting a live phone conversation at the CCC conference last December have such an impact, do you think?

The public component made a huge difference, but also the price component. We used four phones that cost 50 euro combined, so now it becomes possible to do war-driving (driving around intercepting calls), which happened with WiFi before. I expect many people to take this capability and start snooping on innocent people. This possibility is finally waking people up, seeing themselves as a target. They didn't consider themselves a target when only the government could listen in.

How did the network operators react?

Some phone companies see this as a chance to create better networks. We created the publicity that makes security valued by the public and quality operators take it as a chance to distinguish themselves from lesser quality operators. There is one operator in Germany that started the race, they implemented all the countermeasures we suggested in December and they are now waiting to see if we can break it.

What can people do to protect themselves better from GSM attacks?

Using GSM less for security related applications, not exchanging unencrypted data over GPRS, voice calls or SMS. What would have more impact, though, is to go out and ask for more security from the operators. They have the means to provide this. Demanding more protection will protect you better in the long run.

How can non-tech people ask the right questions?

The public needs to know that the risks can be mitigated. There is still time for the operators to put in countermeasures. I know of a small one that implemented the countermeasures in just a few months. If the management is convinced that their customers want it, it doesn't take too much effort to do. And now is the right time to do it. When the war-driving starts, we will have casualties.

Suppose all operators implement fixes, do you have ideas about new kinds of weaknesses?

If the operators choose to implement single fixes to prevent further attacks, this will start an arms race. If they are going to implement real security like A5/3 encryption, it will probably take a few years for cryptanalysts to find flaws. Another area, people are already researching, relates to the networks. The information is sent over microwave links and over the SS7 signaling network and these are being tested right now. The connections have no encryption at all. We also look at a related research field at the moment: data radio. GPRS is ancient technology, like GSM. In a couple of countries, you can already intercept GPRS-data. More on that later this summer.

Do you break hardware security on request of customers?

I am leading a research lab (Security Research Labs) in Berlin that offers risk management services. Large companies ask us which technology they should be using. We can make transparent to them what the risks are and which architecture and technologies they should use. We use a pool of knowledge to provide these services. The knowledge creation through research is always the first step in the process.

In de rubriek "Het Verslag" laten wij u delen in onze ervaringen tijdens conferenties, seminars en trainingen. Deze keer doet Daniël Dragičević verslag van de Black Hat Sessions, Part IX: The Human Factor.

HET VERSLAG

foto's Walter Belgers en Arjen van den Berg



Black Hat Sessions Part IX

Op 26 april 2011 vond de "Black Hat Sessions Part IX" plaats in congrescentrum De Reehorst te Ede. Het thema van de negende editie van dit jaarlijkse congres dat door Array Seminars en Madison Gurkha is georganiseerd was 'The Human factor'.

Tijdens deze zonovergoten dag kwam een groot aantal geïnteresseerden bijeen om zich te laten informeren over de menselijke aspecten op het gebied van informatiebeveiliging. De conferentie werd ook dit jaar geopend door dagvoorzitter **Walter Belgers** (Madison Gurkha). De eerste keynote, getiteld "Cybercriminaliteit en digitale burgerrechten" werd gegeven door **Ot van Daalen**, Directeur van Bits of Freedom. In zijn keynote sprak hij over de Nationale Cyber Security Strategie (NCSS) en hoe deze op gespannen voet staat met onze digitale burgerrechten. Treffend in zijn presentatie was de conceptuele verwarring die rondom cyber security bestaat. De brede definitie zoals gebruikt in de NCSS doet vermoeden dat zowel de aard als de omvang van het probleem niet duidelijk is.

Security Awareness

De tweede lezing zou volgens het programma verzorgd worden door schrijfster en columniste **Karin Spaik**. Helaas kon zij wegens ziekte deze dag niet aanwezig zijn. Jammer dat we deze waardevolle spreek-

ster hebben moeten missen, maar gelukkig was **Hans Van de Looy** (Madison Gurkha) zo flexibel om zijn presentatie naar voren te schuiven. In zijn presentatie "Security Awareness" ging hij in op de problemen en bedreigingen op het gebied van informatiebeveiliging. Trojans, bugs, phishing en identiteitsdiefstal zijn een aantal van die bedreigingen. Daarnaast sprak Hans over het nut van veelgebruikte technieken als antivirus, firewalls, intrusion detection en cryptografie. Echter, omdat techniek niet altijd het complete antwoord biedt, zal de aandacht ook en misschien wel steeds meer naar de menselijke factor moeten uitgaan.

Live hacking demo

Na een korte koffiepauze verzorgden **Ralph Moonen** en **Arthur Donkers** (ITSX) een aantal live hacking demo's. Hierin lieten ze onder andere zien hoe netwerkverkeer kan worden onderschept waarbij bruikbare gegevens als netwerknamen (SSID's), gebruikersnamen en wachtwoorden kunnen worden buitgemaakt. Ook gingen de heren in op het kraken van GSM en DECT.



n in small,
ms –



Andrew MacPherson



Hiervoor werd een live gesprek tussen twee bezoekers in de zaal via DECT onderschept en afgespeeld. Tot slot werd er gesproken over de veiligheid van RFID: een techniek die gebruikt wordt in toegangspassen, de OV-chipkaart en identiteitsbewijzen. Het was boeiend om te zien hoe een paspoort van een bezoeker uit de zaal tijdens een demo werd uitgelezen.

It's all about you

Na de uitgebreide lunch en het bezoeken van de informatiestands, was het de beurt aan de Zuid-Afrikaanse spreker **Andrew MacPherson** van Paterva. In zijn keynote "Me, Myself and Maltego" gaf hij meer inzicht in de applicatie Maltego en de informatie die hiermee uit open bronnen kan worden gehaald. Na een introductie van de applicatie, zoekresultaten, diagrammen en transforms, gaf Andrew een aantal

indrukwekkende demonstraties waarbij hij door het combineren van online en offline informatie een zeer precies beeld van personen, hun leefomgeving en vriendenkring schetste.

Cybercrimebestrijding in Europa

In de middag sprak **Jaap van Oss** van het High Tech Crime Center van Europol tijdens zijn presentatie "Malware and Mules" over de bestrijding van cybercrime in Europa. Hierbij werd ingegaan op het "cybercrime business model", waarin identiteitsdiefstal, oplichting en het witwassen van geld centraal staat. Ook sprak Jaap over de verschillende onderzoeksterreinen als malware-onderzoek, onderzoek naar financiële sporen, infiltratie in criminele organisaties en de uitdagingen die deze vorm van criminaliteit met zich mee brengt. Hij benadrukte dat samenwerking tussen verschillende teams,

instanties en landen de sleutel is tot het tegengaan van de georganiseerde misdaad.

Social Engineering – Theorie en Praktijk

Als laatste sessie heb ik de presentatie van mijn collega's **Fans Kollée** en **Laurens Houben** bijgewoond. Zij verzorgden een lezing "Social Engineering – Theorie en Praktijk" waarin de definitie en de basisaspecten achter Social Engineering werden uiteengezet. De theorie werd afgewisseld met video's en voorbeelden. Tijdens de sessie werd een zeer geslaagde opdracht uit de praktijk besproken, waarin veel van deze basisaspecten naar voren kwamen.

Met een kort afsluitingswoord bedankte Walter Belgers ten slotte iedereen voor zijn/haar aanwezigheid in de vorm van een borrel in de wintertuin. Volgend jaar wordt de BHS voor de tiende keer georganiseerd, ik kijk nu al uit naar deze speciale editie.

HET COLOFON

Redactie

Tim Hemel
Laurens Houben
Remco Huisman
Frans Kollée
Maayke van Remmen
Ward Wouts

Vormgeving & productie

Hannie van den Bergh /
Studio-HB

Foto cover

Digidaan

Contactgegevens

Madison Gurkha B.V.
Postbus 2216
5600 CE Eindhoven
Nederland

T +31 40 2377990

F +31 40 2371699

E info@madison-gurkha.com

Redactie

redactie@madison-gurkha.com

Bezoekadres

Vestdijk 9
5611 CA Eindhoven
Nederland

Voor een digitale versie van de Madison Gurkha Update kunt u terecht op www.madison-gurkha.com. Aan zowel de fysieke als de digitale uitgave kunnen geen rechten worden ontleend.

Safe?



Goede IT-beveiliging is niet zo eenvoudig als vaak wordt beweerd. Bovendien blijkt keer op keer dat deze beveiliging van strategisch belang is voor organisaties. Alle IT-beveiligingsrisico's moeten op een acceptabel niveau worden gebracht en gehouden. Professionele en gespecialiseerde hulp is hierbij onmisbaar. Kies voor kwaliteit. Kies voor de specialisten van Madison Gurkha.

Your Security is Our Business

tel: +31(0)40 237 79 90 - www.madison-gurkha.com - info@madison-gurkha.com