Verslag vanaf grote afstand

Conferenties Blackhat en Defcon – augustus 2008

Maarten Veltman

In dit artikel leest u over twee conferenties, die afgelopen zomer plaatsvonden in Las Vegas, in de staat Nevada, Verenigde Staten. Het gaat om de jaarlijkse Blackhat-USA-briefings en de aansluitende Defcon-hackerbijeenkomst. De auteur was hier niet zelf bij aanwezig, maar heeft voor u zijn verslag gebaseerd op publicaties naar aanleiding van beide gelegenheden.

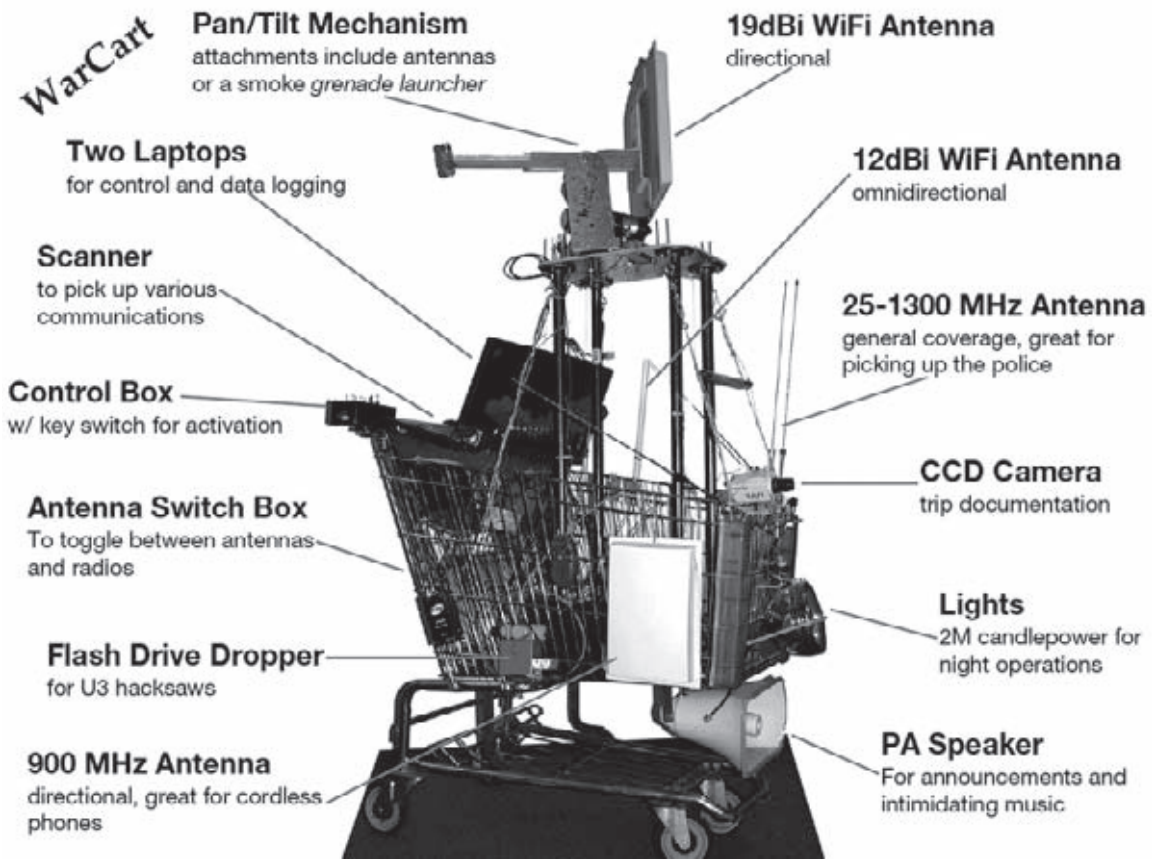
ing. M. (Maarten) Veltman RE is sinds 2000 werkzaam bij het ministerie van Defensie als senior IT-auditor bij de Audit Dienst Defensie.

Dit verslag van Blackhat en Defcon is gebaseerd op gepubliceerde presentaties, audio- en video-opnamen [6ed45c] [ytnj59]. De presentaties (pdf) zijn vrij beschikbaar op internet. Op het moment van schrijven is tevens een beperkt aantal audio- en video-opnamen gratis beschikbaar. Tegen betaling is al het audio- en videomateriaal van beide conferenties verkrijgbaar. [3zbdw8]. Geduld wordt in deze beloond, want na zes maanden wordt ook het audio- en videomateriaal vrijgegeven op internet.
In dit artikel is gekozen om internetverwijzingen via tinyurl.com te laten lopen. Als voorbeeld: om de referentie [6n6apw] via internet te raadplegen, gaat u naar http://tinyurl.com/6n6apw.
Voor de duidelijkheid: de cijfers 0 en 1 worden niet gebruikt (dit zijn dus de letters o en l).

Blackhat en Defcon

Defcon, een driedaagse bijeenkomst, werd dit jaar al weer voor de zestiende keer georganiseerd en is inmiddels uitgegroeid tot een *mega-event* met meer dan 8000 deelnemers vanuit de hele wereld. Tijdens Defcon, dat verwijst naar het Amerikaanse Defensie alertheidniveau, worden de klok rond een groot aantal hackerpresentaties, -wedstrijden, diverse vormen van entertainment, *socials* en feesten gehouden. Een bekende wedstrijd tijdens Defcon is bijvoorbeeld het Capture the Flag (CTF), waarbij hackers hun kennis en kunde kunnen laten zien door op speciaal daartoe ingerichte netwerk-/systeemomgeving in te breken en *the flag* te veroveren. Een ander vermakelijk onderdeel is *spot the fed*, waarbij het aanwezige publiek vermeende agenten van de FBI, CIA of andere buitenlandse diensten aanwijst, waarna op ludieke wijze ondervraging op het podium plaatsvindt. Een indruk en uitslag van een aantal *events* zijn terug te vinden op de website van Defcon [5eln8], enkele filmpjes zijn te vinden via onder andere You Tube (geef als zoekopdracht 'Defcon 16'). Daar waar de toegang tot Defcon afgestemd is op het budget van Amerikaanse pubers en studenten (toegangskosten 120 dollar), is Blackhat gericht op deelnemers uit het (internationale) bedrijfs- en overheidsleven (toegangskosten 1700 dollar). Daarnaast is het mogelijk om enkele dagen Blackhat-cursussen te volgen, over onderwerpen op het gebied van bijvoorbeeld webapplicatie-penetratie-*testing*, *IT forensics* en *reverse engineering*. Kleinere versies van Blackhat worden overigens sinds enkele jaren ook in Japan en Europa (Amsterdam) georganiseerd.

Samen zijn Blackhat en Defcon goed voor meer dan honderd presentaties, verdeeld over verschillende parallelle *tracks*.



Een omgebouwde winkelwagen, ter illustratie van 'war carting' [6n6apw] slide 82.

Beide conferenties overlappen elkaar echter op diverse fronten. De organisatie is bijvoorbeeld in dezelfde handen en ook een aantal sprekers staat op beide conferenties. Tijdens de bijeenkomsten wordt inhoudelijk gediscussieerd over nieuwe (theoretische) bedreigingen en kwetsbaarheden. Maar ook wordt er voortgeborduurd op bekende hackertechnieken en aanvalsmethoden. Om sommige presentaties te kunnen volgen, moet je al aardig thuis zijn in de materie. Voor een IT-auditor is het echter al prettig om te weten wat de laatste bedreigingen, risico's en ontwikkelingen zijn. Het zelf kunnen uitvoeren van de aanvallen of in detail doorgronden van de informatie is niet voor elke auditor nodig.

Beide conferenties vormen daarnaast ook een goed moment voor het lanceren van nieuwe *hacker tools*. Met deze tools kan soms met een enkele druk op de knop een gecompliceerde aanval volledig geautomatiseerd uitgevoerd worden. Een overzicht (overigens niet volledig) van uitgebrachte tools is terug te vinden op internet [5kj29v].

In the picture

Nagenoeg elk jaar gebeurt er iets tijdens een van beide conferenties, dat de aandacht krijgt van de internationale pers. Zo werden dit jaar enkele Franse journalisten verwijderd van Blackhat, nadat zij wachtwoorden van collega's hadden afgeluisterd op het voor de conferentie aangelegde persnetwerk [6n6apw]. Overigens is het afluisteren van gebruikersnamen en wachtwoorden van deelnemers één van de bekende onderdelen op Defcon, waarna deze (deels afgedekt) gepubliceerd worden op de *wall of sheep*. Het mag duidelijk zijn dat na publicatie van je eigen gegevens je natuurlijk als *security professional* niet meer serieus genomen wordt.

Ook een door de rechter verboden presentatie van enkele MIT-studenten over onveiligheden in het elektronische vervoersbewijs in Boston, kreeg door dit verbod juist extra aandacht. De presentatie is uiteindelijk niet gehouden, maar vervangen door een presentatie van een Nederlandse journalist met als boodschap de vrijheid van meningsuiting. De oorspronkelijke verboden, studentikoze, aansprekende, illustratierijke presentatie [3hwzql] 'Anatomy of a subway hack' is overigens, evenals de video van de presentatie die als vervanging diende [3sulel] op internet geplaatst.

De verboden presentatie is een uiterst informatieve demonstratie van hackermethodieken, waaronder *social engineering* (handig 'gebruik'maken van het menselijk gedrag en handelen) en *reverse engineering* (het ontleden van de werking van een product zonder ontwerpschema's en details). Een grappig detail in deze presentatie is de introductie van een nieuwe 'war'-techniek, na *war dialing* en *war driving*, wordt *war carting* geïntroduceerd. Hierbij wordt gedoeld op een enigszins opzichtige, omgebouwde winkelwagen vol met elektronica (zie illustratie).

Overigens was dit niet de enige presentatie waarin een 'war'-techniek uitgewerkt werd. Op Defcon was een volledige presentatie gewijd aan het idee en de uitwerking van *war ballooning*. Hierbij is een grote ballon met helium uitgerust met scanapparatuur voor het in kaart brengen van onveilige draadloze netwerken [3rr5rs].
Niet alleen door tussenkomst van de rechter zijn dit jaar presentaties op Blackhat geannuleerd. Een onderzoeker die gaten in de beveiliging in diskencryptiesoftware van Apple wilde demonstreren, heeft vlak voor de conferentie een *non-disclosure agreement* met Apple ondertekend. Ook medewerkers van Apple zelf hebben zich naar verluidt teruggetrokken als spreker uit Blackhat [5sa6sd].

In de aanloop van Blackhat was verder veel aandacht voor de aangekondigde presentatie van Dan Kaminsky, waarin hij het inmiddels befaamde Kaminsky-DNS-lek zou toelichten. Details over zijn bevindingen lekten echter uit, enkele weken voordat hij zijn presentatie kon geven. Door misbruik te maken van de door Kaminsky ontdekte kwetsbaarheid kunnen kwaadwillenden het systeem beïnvloeden, waarmee de vertaling van internetnamen (zoals www.cnn.com) in een IP-adres (bijvoorbeeld 157.166.226.26) plaatsvindt. Meer over het DNS-probleem volgt later in dit verslag.

Onderwerpen

Gelet op het grote aantal presentaties is het ondoenlijk om elke presentatie afzonderlijk te behandelen. Voor de beeldvorming volgt hierna, soms op hoofdlijnen en een andere keer wat gedetailleerder, een indruk van de diversiteit aan onderwerpen en presentaties tijdens beide conferenties.

- Ontwikkelingen op het gebied van *rootkits*. Het begrip verwijst naar geplaatste achterdeuren in besturingsystemen, waarmee opdrachten uitgevoerd worden met de hoogste rechten. De rootkit-programmatuur zorgt ervoor dat het gebruik en de aanwezigheid ervan verborgen blijven. Op internet zijn al enkele jaren kant-en-klare rootkits te verkrijgen voor bijvoorbeeld Microsoft Windows en Unix-platformen. De presentaties dit jaar hadden betrekking op andere platformen, zoals het MacOS-besturingssysteem [3fcsbg], NetBSD [4z6zw7], maar ook platformonafhankelijke rootkits (SMM) stonden op de agenda [4vq68a].
- *Tunneling* is een techniek waarbij protocollen of informatie verpakt wordt in andere protocollen of verkeersstromen. Naast legitieme toepassing (bijvoorbeeld IPSEC) kleeft er ook een duistere kant aan deze techniek. De techniek kan gebruikt worden om *firewalls* of *intrusion detection*-programmatuur te misleiden of om informatie naar buiten te sluizen. Dit jaar werden weer een nieuwe tool [65x4gf] en mogelijkheden voor de inzet gepresenteerd [3rpha3].
- Social networks zoals LinkedIn en Facebook staan nu enkele jaren sterk in de aandacht en groeien nog jaarlijks. Het kon natuurlijk niet uitblijven dat ook op dit gebied het nodige beveiligingsonderzoek zou plaatsvinden. Onder de kop 'Satan is on my friends list' worden de mogelijkheden voor het beïnvloeden en misbruiken van dergelijke toepassingen uiteengezet [3r5fap].
- Ontwikkelingen met betrekking tot het hacken van draadloze netwerken. De aandacht verschuift van access point naar de *clients* [443nns]. Maar ook nieuwe ideeën om beperkt toegankelijke locaties te scannen op de aanwezigheid van draadloze netwerken. Het concept komt neer op het herprogrammeren van een Apple iPhone en deze uitrusten met *wireless* scanprogrammatuur en een accu, voor het garanderen van een langdurige stroomvoorziening. Deze telefoon wordt vervolgens via de post verstuurd en komt op plekken en distributiecentra waar normaal gesproken niemand bijkomt. De hacker kan vervolgens verbinding met de telefoon maken en gegevens uitlezen en verbindingen leggen met aangetroffen netwerken [46dd6b].
- Onderzoekers hebben mogelijkheden gevonden om het authenticatiemechanisme van beveiligingssoftware, welke direct tijdens het opstarten van een systeem geactiveerd wordt, te doorbreken. Voor het doorbreken van deze zogenoemde *pre-boot* authenticatiesoftware maken de onderzoekers gebruik van eigenaardigheden van de BIOS-*keyboard buffer*. Er wordt gedemonstreerd dat deze onvercijferde wachtwoorden met de nodige trucs en tools uitgelezen kunnen worden in het geheugen. Een overzicht van vastgestelde kwetsbare BIOS-versies en authenticatiesoftware is te vinden op [3fa9np].
- Een presentatie over de mogelijkheden van het doorbreken van CAPTCHA-mechanismen. CAPTCHA staat voor 'Completely Automated Public Turing test to tell Computers and Humans Apart'. CAPTCHA's zijn de moeilijk leesbare *random* karakters in de verschijningsvorm van een *bitmap* die een internetgebruiker moet intypen om ergens toegang toe te krijgen. Het mechanisme is bedoeld om zeker te stellen dat daadwerkelijk een menselijke gebruiker toegang vraagt en daarmee de toegang door geautomatiseerde programmatuur te bemoeilijken. Er blijkt een markt te zijn voor het doorbreken van het CAPTCHA-mechanisme [46vkwo].
- Hardwareleveranciers nemen onderdelen, zoals chips, af van verschillende partijen overal ter wereld. Indien er inadequaat toezicht plaatsvindt op de herkomst, integriteit en productieproces van deze onderdelen kan dat tot beveiligingsproblemen leiden. Dat hiervan niet alleen in theoretische zin sprake van is, laten enkele onderzoekers van een universiteit zien. De presentatie gaat in op *hardware trojans*, waarmee gedoeld wordt op het herprogrammeren van logische componenten en deze uit te rusten met trojans. Als voorbeeld wordt een AES-encryptieapparaat genomen, waarbij na bepaalde *user input* het sleutelmateriaal via een verborgen kanaal verstuurd wordt. Een videodemonstratie en toelichting is te vinden op [495j6a].
- De digitale reclameborden *(billboards)* naast en boven de weg en op bedrijfspanden zijn een bekende verschijning. De mogelijkheid van het overnemen van de aansturing en daarmee het aanpassen van de tekstmeldingen, is een aansprekend onderwerp. Stapsgewijs geven hackers aan hoe ze

te werk zijn gegaan om de aansturing van een billboard over te nemen en welke varianten er bestaan [5x8mlt].
- Niet alleen IT-technologie en software wordt in Las Vegas besproken, ook technieken met een hardere kant passeren de revue. *Lockpicking* is daar een voorbeeld van. Lockpicking is de verzamelbegrip gericht op het openen van sloten, zonder originele sleutel. De bekende gerenommeerde Amerikaanse *high-end* slotenmaker Medeco en de sloten die zij leveren, staan in de presentatie centraal [3rhagc].
- Steeds vaker worden tijdens een netwerkanalyse in een onbekende netwerkomgeving Virtual Machines (VM) aangetroffen. Geschikte middelen om bijvoorbeeld tijdens een penetratietest deze VM aan de tand te voelen, ontbreken. In de presentatie 'hacking Virtual Machines' is een aanzet gemaakt voor het pentesten van deze omgevingen en is een aantal ondersteunende tools aangekondigd [4mjnuj].
- Een overzicht van de verschillende aanvalsmethoden, beschikbare hacking tools en mogelijke tegenmaatregelen voor VLAN-netwerkaanvallen (OSI laag 2) [3zbjke].
- Het vinden van kwetsbaarheden in Voice over IP (VOIP)-implementaties met behulp van een nieuwe tool, genaamd VoIPER [4vz52p].

Er waren ook diverse onderwerpen die dit jaar verder uitgediept werden. Voorbeelden daarvan zijn SCADA, *smartcards*, het IOS-besturingssysteem van Cisco en eigenlijk ook de DNS-problematiek.

SCADA

SCADA was dit jaar een populair onderwerp. SCADA staat voor 'Supervisory Control And Data Acquisition' en heeft betrekking op het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines in grote industriële systemen [4oh35w]. Voorbeelden van dergelijke systemen zijn waterbeheersing-, elektriciteits- en verkeerssystemen. Het onderwerp trok vorig jaar veel aandacht op Blackhat en dit jaar werd daar op voortgeborduurd. De onderzoekers presenteren de problemen waar ze tegenaan liepen bij de inzet van zogenaamde *fuzzer* tools. Met een fuzzer worden pakketten verstuurd, die niet voldoen aan de protocolspecificaties. De wijze waarop de ontvangende systemen omgaan met deze afwijkende, niet verwachte data is afhankelijk van de implementatie en kan 'verrassende' effecten opleveren. Het meest voorkomende effect bij de toepassing van fuzzers is een *denial of service*, een blokkade of *crash* van het systeem. Daarnaast kan bijvoorbeeld een authenticatiemechanisme doorbroken worden. Een van de aanbevelingen die de onderzoekers geven, is het treffen van maatregelen tegen het injecteren van data in het controlnetwerk. De presentatie en verwijzing naar de toegepaste fuzzer tools zijn te vinden via [3edlq8].

Een andere presentatie op het gebied van SCADA betreft een *modbus netwerkscanner* [4h7cdw]. De tool scant het netwerk op de aanwezigheid van SCADA-gebaseerde apparaten. Nog een andere presentatie [449la5] geeft een *overview* van SCADA, incidenten al dan niet natuurlijk met SCADA-systemen en de ontwikkelingen in de beveiliging van SCADA. Ook wordt stilgestaan bij de mogelijkheid om SCADA-communicatie via radiokanalen af te luisteren en de inzet van war dialing om modems te traceren.

Smartcards en MiFARE

Ook kwetsbaarheden en mogelijkheden voor het aanvallen van smartcards en MiFARE (in Nederland de OV-chipkaarttoepassing) stonden dit jaar weer in de belangstelling. Naast de eerder genoemde verboden presentatie over de zwakheden in het elektronische vervoersbewijs in Boston, werd er nog meer gediscussieerd over mogelijkheden voor het hacken van smartcards. Een van de presentaties ging bijvoorbeeld over het gestandaardiseerde communicatieprotocol APDU (Application Protocol Data Unit). APDU-commando's zorgen voor de gegevensuitwisseling en opdrachten tussen *smartcard device* en *host* (systeem van een eindgebruiker). Het bedrijf Compass licht in een presentatie de ontwikkeling en inzet van een hardwareapparaat toe. Dit apparaat zit als het ware tussen de client-server-communicatie-uitwisseling (*man-in-the-middle*) en kan zodoende de APDU-communicatie onderscheppen. Middels een *proof of concept* zet Compass vervolgens uiteen wat de mogelijkheden zijn voor het verkrijgen van sleutelmateriaal. Zie [4nvscj].

Cisco IOS-onderzoek

Een grote speler in de router- en *switch*-netwerkbranche is Cisco. Het besturingssysteem waarmee deze routers en switches uitgerust zijn, is het Cisco IOS (Internetwerk Operating System).
Een presentatie van Information Risk Management gaat in op de ontwikkeling van *shellcode* voor het IOS-platform. Met het begrip shellcode wordt een klein stukje softwarecode bedoeld, waarmee een kwetsbaarheid uitgebuit wordt en bijvoorbeeld een *shell of commandline* opgestart wordt. Shellcode is een bekend hackerbegrip voor Windows- en Unix-platformen, maar is nog relatief onbekend binnen de wereld van netwerkcomponenten en de daarop aanwezige besturingssoftware. Een van de gepresenteerde mogelijkheden betreft het maken van een IOS-distributie met achterdeuren. Zie [3t3om4].

De bekende hacker FX beschrijft de ontwikkelingen die doorgemaakt worden op het gebied van IOS-forensisch onderzoek. FX geeft aan dat er tienduizenden verschillende IOS-versies in omloop zijn. Hij verwacht dat hackers door aanscherping van beveiligingsmaatregelen op Windows- en Unix-platformen zich meer en meer gaan richten op deze systemen. FX pleit in zijn presentatie voor het activeren van *core dumps* (registratie van onder meer registers en het geheugengebied). Tijdens een crash worden deze core dumps automatisch gegenereerd. Aan de hand van deze core dumps kan achteraf bepaald worden, waardoor de crash veroorzaakt is. Voor een succesvolle aanval, die niet leidt tot een crash, zal dat echter weinig waarde hebben en zal teruggevallen moeten

worden op onhandige en beperkt aanwezige auditing mechanismen en analysetools. In IOS kunnen core dumps echter niet alleen tijdens een crash gegeneerd worden, ze kunnen ook middels een commando op aanvraag gegenereerd worden. Het door FX bedachte *framework* komt neer op het centraal archiveren van deze getriggerde core dumps, om deze vervolgens geautomatiseerd te analyseren.
Een uiteenzetting van de achtergrond van het framework is te vinden op [49cdsj].

De Kaminsky Code – Black Ops 2008, Dan Kaminsky

Wat een publicitair klapstuk had moeten worden, lekte enkele weken voor de Blackhat-conferentie uit. Hoewel er al veel over geschreven is, volgt nu toch nog even een korte samenvatting van het probleem.
Dan heeft begin 2008 een aantal kwetsbaarheden gevonden in het mechanisme dat zorgdraagt voor de vertaling van internetdomeinnamen (zoals www.cnn.com) in IP-adressen (zoals 157.40.103.22). Het mechanisme dat deze vertaling realiseert, heet het Domain Name System (DNS) en is, gelet op haar toepassing, cruciaal voor de juiste werking van het gehele internet. Binnen de DNS-inrichting is sprake van twee typen servers. De *Authoritative nameservers* en de *Recursive nameservers*. De Authoritative nameservers hebben de leiding in het vertalen van adressen die vallen onder het eigen regime (*zone*). De Recursive nameserver bevraagt de authoritative nameserver en neemt de ontvangen informatie op in zijn *cache*, zodat een bevraging (*resolving*) van hetzelfde adres in de toekomst sneller verloopt. Een internetnaam waarvoor de caching nameserver nog geen IP-adresvertaling heeft, zal derhalve door de Recursive nameserver middels een verzoek (*request*) bij de authoritative nameserver opgevraagd worden. De kwetsbaarheid schuilt in het kunnen beïnvloeden van de informatie die door de recursive nameserver in zijn cache opgenomen wordt.
Dan nu het probleem in een technische notendop. Het beveiligingsmechanisme waarmee legitieme DNS-antwoorden (*reply*) onderscheiden kunnen worden van malafide antwoorden, is een zogenaamde *transaction* ID (TXID). Het TXID is een random getal tussen de 0 en 65534. Alleen de echte DNS-nameserver kent dit getal, omdat dit in het verstuurde DNS-verzoek opgenomen is. Een antwoord met een afwijkend TXID wordt dan ook niet als een legitiem antwoord door de server geaccepteerd. Om van deze vertrouwensrelatie misbruik te maken, is het de kunst om het juiste getal (TXID) te raden. Gelet op het beperkt aantal mogelijke TXID (64k), is dat op zich geen onmogelijke taak. Een ander mechanisme binnen de DNS-specificaties om enige mate van veiligheid te introduceren, is het meegeven van een geldigheidsduur van een ontvangen reply. Deze geldigheidsduur wordt aangeduid met de TTL-waarde (Time to Live). Een eenmaal bevraagde DNS-naam kan zo bijvoorbeeld dagenlang opgenomen blijven in de cache (tot 655 dagen), wat in principe de mogelijkheden voor misbruik beperkt. De aanvaller zal namelijk, indien hij niet het juiste TXID gebruikt heeft, moeten wachten totdat deze TTL verstreken is.

De door Dan gevonden kwetsbaarheid bestaat uit een combinatie van de volgende drie probleempunten:

1) de aanvaller maakt misbruik van de tijd die nodig is tussen de nameservers om een adres te bevragen. De aanvaller heeft hierbij het voordeel (lees: een voorsprong), omdat hij zelf een adres-resolve kan initiëren. De aanvaller kan daarbij gelijktijdig een vervalst antwoord versturen (op zijn eigen vraag), met daarin een vervalst random TXID-nummer. Dit pakket komt, vanwege het gelijktijdig versturen, altijd eerder aan bij de resolving nameserver dan het legitieme reply-pakket;
2) er zijn voor de aanvaller geen beperkingen om meerdere TXID's te proberen. Diegene die namelijk het eerste met het correcte TXID reageert, wint. Een dergelijke situatie wordt ook wel een *race condition* genoemd. Het aantal pogingen van een aanvaller is dus afhankelijk van de tijd die de recursive DNS-server moet wachten op een antwoord van de authoritive DNS-server.

Deze mogelijkheden tot beschikking hebbend, kan de bescherming die het TXID levert, theoretisch doorbroken worden. Het TXID betreft namelijk, zoals eerder aangegeven, een 16 bit (64k) veld.

Wat resteert is de beveiliging die het TTL-mechanisme introduceert. Of toch niet?

3) De TTL-waarde blijkt alleen geldig te zijn voor de volledige domein naam (FQDN) die bevraagd wordt. Bij een bevraging van een subdomein (zoals 1.foo.com, 2.foo.com, et cetera) heeft de aanvaller weer een nieuwe kans. De aanvaller hoeft, als hij de race verliest, in dat geval dus niet te wachten op het verstrijken van de TTL. Indien de aanvaller het juiste TXID voorspeld heeft van een bevraging van een subdomein, dan wordt de informatie die gekoppeld is aan deze reply door de nameserver gebruikt. Let wel, dit is dus informatie waarover de aanvaller de controle heeft, deze heeft hij namelijk zelf in het vervalste antwoord pakket opgenomen. Een van de mogelijke antwoorden is een doorverwijzing naar een andere authoritive nameserver. Dan licht in zijn presentatie toe hoe een aanvaller ervoor kan kiezen om in de succesvol voorspelde resolving reply (bijvoorbeeld naar DNS name 559.foo.com) aan te geven dat de server (559.foo.com in het voorbeeld) niet bekend is, maar dat het adres opgezocht moet worden bij www.foo.com, dat zich bevindt op het adres van de aanvaller (door Dan 'bait and switch' genoemd). Alle verzoeken voor resolving van www.foo.com komen nu uit bij de aanvaller.

Het voorgaande is een mooi staaltje van creativiteit en kennis van zaken. Een uitgebreide technische analyse en illustratie van de werking van DNS en de Kaminsky-kwetsbaarheid is overigens te vinden op [4ted6j]. De presentatie van Dan zelf is te vinden op internet [67uklz], evenals de video [5vqaoe].

Dan behandelt vervolgens diverse scenario's om te demonstreren wat de mogelijkheden en gevolgen zijn van deze kennis. Te denken valt aan het overnemen van de adressering van een *top-level domain* (zoals .com), maar ook specifieke DNS-informatie voor de e-mailafhandeling (MX-*records*) zijn te beïnvloeden. Een ander potentieel doelwit is volgens Dan het SIP-berichtenverkeer, wat een belangrijke pijler vormt voor Voice over IP (VOIP). Het mag duidelijk zijn, mogelijkheden te over. De ernst van de situatie blijkt ook wel uit de afgegeven waarschuwingen van diverse instanties, waaronder het Nederlandse GovCERT [4sha7j].

Een voorgestelde oplossing is de toepassing van *source port randomization*. Hierbij is de geldigheid niet alleen afhankelijk van het TXID-veld, maar ook van een random IP source-poortnummer. Deze combinatie vergroot het aantal mogelijke combinaties substantieel en verkleint de kans dat het juiste replypakket door de aanvaller verstuurd wordt. Ook dit blijkt echter niet de ultieme oplossing, door het versturen van een groot aantal vervalste pakketten (4 GB aan data) en de aansluiting op een *backbone*, is ook dit mechanisme te doorbreken.

Ten slotte

Beide conferenties kunnen, zeker voor de technische auditors onder u, zeer interessant zijn. Zowel Blackhat als Defcon vormen voor de IT-auditor een uitgelezen kans om zicht op en gevoel bij actuele bedreigingen en risico's te krijgen. De presentaties worden direct na de conferentie op internet geplaatst, zodat je jezelf, ook zonder fysieke aanwezigheid, direct inhoudelijk op de hoogte kunt stellen. Voor het zelf ervaren van de Blackhat-briefings hoeft u gelukkig niet ver weg of lang te wachten. In april 2009 wordt namelijk alweer de Europese versie van de Blackhat-briefings gehouden in Amsterdam. Helaas moet u het dan wel zonder de beleving van Defcon doen. ■