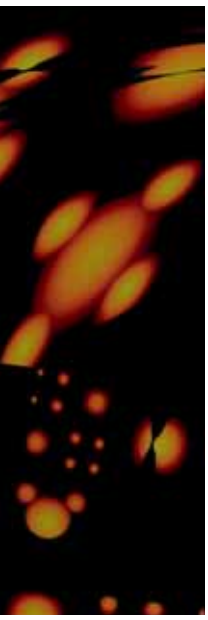

Zekerder dan ooit:

DNS als database

Rick van Rein

In het verleden beschreven we al eens een paar bijzondere systemen die in speciale toepassingen als database kunnen worden gezien; we bezagen DNS als gedistribueerd en decentraal beheerde database; en we bespraken certificaten als gedistribueerd en zekerheid biedende vormen van samenhangende data. Recent zijn die systemen min of meer samengekomen, in de vorm van DNSSEC.

De klassieke database zoals die bijvoorbeeld van Oracle of MySQL AB afkomstig is, bestaat uit een centrale server, of tegenwoordig een cluster van machines dat als geheel zo'n centrale server simuleert. Voor heel veel bedrijfsinterne systemen is dat de aangewezen architectuur, maar uiteraard past het niet bij alle gevallen.

Er zijn situaties waarin het beter is data te distribueren, bijvoorbeeld om het dicht bij de bron te houden, en hooguit via caching te voorkomen dat er al te veel netwerkverkeer optreedt. DNS en LDAP zijn voorbeelden van zulke systemen. In geval van DNS (en in mindere mate bij LDAP) is het zelfs zo dat het beheer van de gegevensset ook kan worden verdeeld tussen verschillende partijen.

Anders dan bij SQL-gebaseerde systemen gaat het bij dit soort databases om informatie die niet vaak verandert. Het wordt min of meer read-only benaderd, met slechts af en toe updates. Hoewel veranderingen binnen de scope van beheer snel genoeg door kunnen worden gegeven, geldt dat niet vanzelf bij de relaties naar clients; er wordt gewerkt met de aanname dat de vorige versie van de data voldoet, totdat de client opnieuw gegevens opvraagt.

Het moge duidelijk zijn dat we het niet hebben over de klassieke database. De trade-off pakt anders uit, maar daarom is het niet minder interessant om deze alternatieve paradigma's serieus te nemen als we data willen delen.

Toepassingen

LDAP is een zogeheten directory. Je slaat er hiërarchisch geordende gegevens in op, bijvoorbeeld volgens de bedrijfsstructuur of via de opbouw van je bibliotheek. LDAP is echter niet het hoofdonderwerp van dit artikel, dat is het systeem van DNS dat er enigszins op lijkt. DNS wordt meestal voor technische doeleinden gebruikt, maar hoeft daar niet altijd tot beperkt te blijven.

De informatie is geïndexeerd op domeinnaam en daar kan Jan en alleman over meepraten tegenwoordig; een e-mailadres of website is heel gewoon als identifier voor een persoon of een bedrijf. En binnen de DNS-infrastructuur zijn sub-bomen opgehangen voor speciale indexen, zoals ENUM voor telefoonnummers en ARPA voor IP-adressen. Als je dus maar op de goede plek begint dan kunnen we van alles kwijt in de DNS-infrastructuur.

Laten we ENUM als voorbeeld nemen. Stel dat je telefoonnummer +31.6.543210 is, dan zou je dat in ENUM terugvinden met de naam 0.1.2.3.4.5.6.1.3.e164.arpa. De eigenaar van een telefoonnummer kan zo'n domein registreren en er allerhande informatie onder stoppen; denk daarbij aan een soort visitekaartje: een telefoonnummer via SIP, een faxnummer of voicemail, de website van je bedrijf, een certificaat of PGP-sleutel, enzovoort.

Voor gewone namen in DNS lopen de toepassingen overigens ook uiteen; het algemene telefoonnummer voor een bedrijf, SRV records voor een telefooncentrale met 'nummers' die gelijk zijn aan mailadressen, een SSL-certificaat voor de veilige website en ga zo maar door. Bijzonder interessant is ook remote toegang tot de shell van een database; dat kan bijzonder goed worden dichtgetimmerd met SSH, waarvoor de server-side key dan in DNS kan worden opgenomen ter controle door de SSH-client.

DNS is dus flexibel op diverse fronten:

- indexes voor mens & machine;
- diverse voorgedefinieerde soorten data;
- gedistribueerde opzet & beheer;
- robuust, failsafe.

Waar de beperkingen van het min of meer read-only gedrag van DNS dus geen beperking vormen, en de toepassing aansluit bij het soort dingen dat in het algemeen in DNS thuishoort, is het een bijzonder interessante optie.

Maar nu veilig!

Het probleem met al dit soort data is de veiligheid ervan. DNS is zo lek als een mandje, en als een kraker als eerste een antwoord geeft op een DNS-vraag van iemands PC, dan overtuigt dat die PC. Sterker nog, er zijn tegenwoordig aanvallen bekend waarmee de DNS-resolvers van een ISP overtuigd kunnen worden van een antwoord dat me uitkomt. Het kan weken of maanden duren, maar het is zeker dat de resolver van de ISP uiteindelijk voor de bijl gaat.

Als de DNS-resolvers van een grote ISP overtuigd raken dat de centrale database van een groot bedrijf op iemands zolderkamer staat dan zijn de rapen gaar en de kersen zuur. De kraker kan dan de informatiestromen onderweg aftappen, analyseren en eventueel gewijzigd doorgeven. Dat zou genoeg moeten zijn om elke informatiemanager badend in het zweet wakker te maken, terwijl hij bijt in zijn kussen of roept om zijn moeder. Maar de huidige situatie met DNS is werkelijk zo ernstig.

Nu is pas kort bekend hoe dit soort aanvallen praktisch verwezenlijkt kunnen worden, maar het algemene stramien van dergelijke aanvallen is al veel langer bekend, en daarom is al jaren gewerkt aan een oplossing. Die oplossing heet DNSSEC. Het zien van de concreet uitvoerbare problemen zal bij menig internetgebruiker een schrikreactie geven, maar de mensen die werkelijk aan de infrastructuur werken zien er ook wel voordelen aan dat een theoretisch maar belangrijk lek nu eindelijk tractie krijgt en opgelost wordt. DNSSEC wint dan ook stormenderhand aan domein. Eindelijk!

DNSSEC werkt met controleerbare handtekeningen op DNS-data. In wezen is het niet zo heel anders dan het certificatensysteem voor veilige websites, behalve dat het nooit een pop-up wegens foute DNS-data zal leveren; in plaats van fouten te melden verdwijnt een onveilig domein gewoon uit de lucht. Dat is cru, maar het voordeel voor de eindgebruiker is dat er serieus zal worden gezorgd voor degelijke infrastructuur, want niemand wil graag van het Internet af vallen. En dat betekent dat er een heel bruikbare, veilige infrastructuur aan zit te komen.

Veilige toepassingen

De voordelen van DNSSEC voor het type toepassingen dat zich in DNS thuis voelt is enorm. Want in DNS zoek je data op die elders zijn gepubliceerd, door een ander die je mogelijk niet kent. Dankzij DNSSEC vindt minimale verificatie plaats op deze gegevens.

Het is goed te beseffen dat er nog jaren ondersteuning voor niet-ondertekend DNS zal blijven. Terwijl fout ondertekende domeinen letterlijk verdwijnen, zal een niet-ondertekend domein gewoon zichtbaar blijven. Het onderscheid tussen een juist ondertekend domein en een niet-ondertekend domein is echter op applicatieniveau te onderscheiden, en een daarop gespitste toepassing kan dus kiezen om alleen nog veilige verbindingen op te bouwen. Dan verdwijnt alle oude DNS alsnog van het Internet dus.

Afbeelding 1: Browsers die klagen over foute certificaten helpen de veiligheid niet echt vooruit. Bovendien is het erkenningsproces achter certificaten 'tenenkrommend' onveilig. Het hele systeem is te ingewikkeld voor eindgebruikers, en dit soort meldingen zal meer kwaad dan goed doen. Het probleem is dat certificaten op naam zijn, maar verder los van de infrastructuur van het Internet staan. Als een certificaat onder een domeinnaam wordt gepubliceerd en ondertekend is met DNSSEC, dan kan het veel eenvoudiger omdat het validatiepad van DNSSEC dan het verband met de infrastructuur zeker stelt. Nu maar hopen dat de browserwereld deze kans oppakt!

Een erg interessante toepassing kan zijn wanneer elke webserver een *self-signed* certificaat opneemt in DNS, met ondertekening in DNSSEC. Zodra het gemeengoed wordt dat browsers dit accepteren kunnen we de poeha van certificaatmakers verder afschaffen. Leuker nog: dit kan ook worden gedaan met persoonlijke certificaten, voor veilige e-mail. Zowel X.509 als PGP kennen hier structuren voor in DNS. En als het niets kost. waarom dan niet? Het is professioneler dan een *disclosure* onderaan elke e-mail!

Ook bijzonder nuttig is een SSH-sleutel in DNS, met ondertekening in DNSSEC. Thuisgebruikers van een applicatie moeten vaak bij de database kunnen. Dat kan via een VPN (die het hele bedrijfsnet ontsluit bij de gebruiker thuis) of alleen voor de databaseconnectie via een SSH-tunnel. Dat merkt de applicatie niet, die wordt alleen naar het lokale eindpunt van de tunnel gestuurd. Als SSH dan vervolgens de SQL-verbinding beveiligt zal daar bij *first contact* een pop-up verschijnen die geen enkele thuisgebruiker zal controleren. Daarentegen, als DNSSEC is toegepast en de SSH-software voldoende nieuw is, dan zal die pop-up uitblijven en zullen alleen problemen tot pop-ups leiden!

Het idee van internettelefonie is spannend, en zeker als e-mailadressen ook gaan werken als mobiele telefoonnummers, zoals met SIP gebruikelijk is. Als het contactadres via DNS opgezocht moet worden dan is het wel zo prettig als die contactgegevens

authentiek zijn, zodat een concurrent het gesprek niet kan overnemen. Ook kan het prettig zijn wanneer telefonie versleuteld wordt, zeker in Nederland afluisterland. Voor de sleutels die nodig zijn voor versleuteling kan dankzij DNSSEC nu ook een aftapvrije optie worden gekozen. Wel zo handig om niet te hoeven rekenen op een lekvrije overheid voor commercieel gevoelige zaken zoals de toekomstvisie van je bedrijf.
Als ik niet uitkijk raak ik op hol. Waarom worden bedrijfsgegevens niet in een ENUM-achtig visitekaartje opgenomen onder kvk.nl, geordend op registratienummer? Veel andere organisaties kunnen iets dergelijks doen – bijvoorbeeld de Belastingdienst, die van bedrijven verlangt dat ze buitenlandse BTW-nummers controleert, maar die geen automatiseerbare procedure biedt om dit te vereenvoudigen. Allerhande publieke registers kunnen zich ervoor lenen om via DNS, met bekrachtiging van DNSSEC, toegankelijk te worden gemaakt. Een enorm potentieel aan innovaties lacht ons toe.

Hoe werkt DNSSEC?

De veiligheid van DNSSEC is hiërarchisch georganiseerd, net als DNS. Helemaal aan de top vinden we het root-domein "." waaronder de bekende top-level domains vallen (COM, NL, ORG, enzovoort) en ook enige minder bekende (ARPA voor IP- en telefoonnummers). Daar weer onder vallen gewone domeinnamen die een losse domeineigenaar kan bezitten en alles daar weer onder kennen we als subdomeinen, die onder verantwoording van de domeineigenaar kunnen worden aangemaakt en zo nodig opgezet voor onafhankelijk beheer (zoals BAKKER.ORVELTE.NEP).
Het root-domein "." is sinds half juli ondertekend, en de sleutel waarmee dat is gedaan wordt verspreid via de kanalen van goed met elkaar bekend zijnde infrastructuurbeheerders. Deze sleutels worden handmatig ingebracht in de DNS-resolvers waarvan een gewone PC meestal afhankelijk is. Als het goed is bouwt je ISP het binnenkort in; maar vraag dat vooral na, want ze staan niet allemaal te popelen om onopgemerkte veiligheid in te bouwen.
De domeinen onder het root-domein werden altijd al via een delegatie gevonden; er zijn daarvoor verwijzingen vanuit de root naar de DNS-servers voor een domein. Die worden nu onder DNSSEC vergezeld van een handvat naar de sleutels die de data onder zo'n domein als authentiek ondertekenen. Het doorverwezen domein kan dan zelf de handtekeningen plaatsen, mits het gebeurt met een sleutel waarvoor het handvat bij de doorverwijzing staat. Er is speciale software ontworpen om dergelijke processen te begeleiden, met OpenDNSSEC en BIND als bekendste voorbeelden en ZKT als saillante extra optie.

Een DNS-resolver bouwt vanuit het vertrouwde startpunt voor de root "." een vertrouwenspad op naar de concrete gegevens die opgevraagd zijn door een DNS-client. Als dat pad expliciet aangeeft dat de data niet ondertekend zijn, dan zullen de data worden teruggezonden zoals dat altijd is gedaan. Als ergens op het pad een fout in de ondertekening zit, dan zal worden teruggemeld dat de gevraagde data niet bestaan. Als het hele pad klopt, dan zal de gevraagde informatie worden teruggerapporteerd, vergezeld van een speciale AD-vlag die aangeeft dat het om authentieke informatie gaat.

Organisaties die DNSSEC implementeren, ofwel die hun domeinen gaan ondertekenen, dienen dat met hun registrar af te stemmen. Hoewel nog lang niet alle registrars dit kunnen, zal het er langzaamaan wel van komen. Het is nu al mogelijk om voor bepaalde top-level domeinnamen (zoals ORG) een domeinnaam te registreren voor beveiligde data. Voor het implementeren zelf zal een organisatie ofwel op de registrar moeten vertrouwen, of het in eigen beheer regelen met software zoals OpenDNSSEC, BIND of ZKT. Dat laatste is overigens niet eenvoudig, zoals op de DNSSEC blog van SURFnet uit de doeken wordt gedaan.
Vanwege het hiërarchische karakter van DNSSEC moeten alle tussenliggende lagen vanuit "." ondersteuning bieden voor DNSSSEC. Voor de meeste Nederlandse toepassingen betekent dit dat het NL-domein ondertekend moet worden. Op het moment van dit schrijven wordt hier hard aan gewerkt; het zou bij het verschijnen van dit blad in kannen en kruiken moeten zijn.

Samenvatting

Voor bepaalde speciale gevallen (stabiele, publieke informatie) kan DNS een zeer interessante wijze van publicatie zijn. Dat geldt voor zaken uit de infrastructuur van een netwerk, maar ook voor bepaalde persoons- of bedrijfsgebonden informatie, zoals de informatie op visitekaartjes.
Het probleem met DNS was altijd de zeer beperkte veiligheid, maar nu het hele Internet DNSSEC aan het adopteren is verdwijnt dat probleem als sneeuw voor de zon. Het wordt hierdoor steeds interessanter om DNS te overwegen als publicatiekanaal voor automatisch verwerkbare gegevens.

Links

DNSSEC
Achtergrondinformatie in het whitepaper op http://dnssec.nu/ en de blog
- *Voor uitrol van DNSSEC als toegeleverde dienst op https://dnssec.surfnet.nl/*
- *DNSSEC platform voor Nederland op www.dnssec.nl/*
- *Informatie over DNSSEC voor de DNS root op www.root-dnssec.org/*

ENUM, telefoonnummers in DNS: www.enum.nl/ met als registrar-voorbeeld www.regeljeenum.nl/

Standaarden: Certificaten in DNS in RFC 4398, SSH-keys in DNS in RFC 4255, ENUM in DNS in RFC 3761 en uitbreidingen daarop.

Software voor het controleren van DNSSEC op ondersteunende domeinen is Unbound: www.unbound.net/ of BIND www.isc.org/software/bind met een HOWTO op https://dnssec.surfnet.nl/?p=212

Software voor het publiceren van domeinen onder DNSSEC is te vinden op www.dnssec.org/ of www.isc.org/software/bind of www.hznet.de/dns/zkt/

Rick van Rein
Dr. ir. H. van Rein (rick@openfortress.nl) is ontwikkelaar en beheerder bij OpenFortress Digital signatures.