Achtergronden bij DNS-versleuteling

Datum
23 november 2018 (versie 1.0)

Auteur(s)
Marco Davids

Pagina
1/3

Classificatie
Publiek

Contact
sidnlabs@sidn.nl

Contact
T 026 352 5500
support@sidn.nl
www.sidn.nl

Bezoekadres
Meander 501
6825 MD Arnhem

Postadres
Postbus 5022
6802 EA Arnhem

DNS Privacy is een 'hot topic' binnen de internetgemeenschap en diverse innovaties ter verbetering van de privacy van DNS zagen de afgelopen jaren het levenslicht. We vergelijken in dit document verschillende technieken en gaan in een begeleidende blog dieper in op de controverse rondom één ervan, namelijk DNS over HTTPS (DoH).

1 Inleiding

De afgelopen jaren werkte de IETF-community aan het verhogen van de veiligheid van het DNS-protocol. DNSSEC is hier het beste voorbeeld van. 2 gebeurtenissen waren van doorslaggevende invloed op deze ontwikkelingen.

1.1 Kaminsky-aanval

De adoptie van DNSSEC kreeg in 2008 een behoorlijke impuls na de zogenaamde 'Kaminsky aanval'. Via die aanval kunnen relatief eenvoudig DNS-antwoorden worden vervalst (DNS spoofing). Wat eerst een voornamelijk theoretisch risico was, veranderde plotsklaps in een reële bedreiging. DNSSEC garandeert de integriteit van DNS-antwoorden waardoor antwoorden niet vervalst kunnen worden en spoofing nagenoeg onmogelijk wordt. Inmiddels is ruim 53% van alle ruim 5,8 miljoen .nl-domeinnamen met DNSSEC beveiligd.

1.2 Snowden-onthullingen

Na de onthullingen van Edward Snowden (2013) kwamen privacy en het afluisteren van internetverkeer, al dan niet door statelijke actoren, weer volop in de belangstelling. Snowden lekte geheime informatie over de vermeende spionageactiviteiten van zijn toenmalige werkgever, de NSA.

De IETF, waar internetstandaarden tot stand komen, besloot daarop om bij het ontwikkelen van standaarden nog meer aandacht te besteden aan 'afluisterbaarheid' en privacy.

En zo kon het gebeuren dat er opnieuw gekeken werd naar het DNS-protocol. Want hoewel DNS inmiddels tegen DNS spoofing was beveiligd met behulp van DNSSEC, kende het als een van de laatste protocollen nog geen versleutelde variant. Dat wil zeggen; wie mee kan kijken met het verkeer, kan precies zien welke DNS-vragen er worden gesteld. En wie dat kan, leert ontzettend veel over het internetgedrag van de gebruiker.

De hernieuwde aandacht voor privacy initieerde een reeks nieuwe ontwikkelingen op het gebied van DNS privacy. Een manier om privacy te verbeteren is het versleutelen van het DNS-verkeer.

2 Voordelen van DNS-versleuteling

Bij DNS-encryptie, versleuteling dus, kunnen derden niet meer meekijken om te zien welke DNS-vragen er over de lijn gaan. Dit draagt bij aan de privacy van de gebruiker, want vrijwel elke activiteit op het internet wordt voorafgegaan door een DNS-lookup en wie die kan

meekijken, krijgt dus een uitstekende indruk van het surfgedrag van de gebruiker in kwestie. Voor de volledigheid; wie aan de uiteinden van de versleutelde verbinding zit, bijvoorbeeld wie de resolver draait, heeft die inzage nog wel. Dit is overigens wat Oblivious DNS (ODNS), hierboven reeds kort genoemd, probeert te verhelpen.

Impliciet kent DNS-versleuteling nog 2 voordelen:

Omdat het verkeer versleuteld is, is het niet zomaar te wijzigen. Versleuteling kan dus, vergelijkbaar met DNSSEC, ook helpen tegen het vervalsen (spoofen) van DNS-antwoorden. Maar dat geldt alleen als de versleuteling 'end-to-end' wordt toegepast. Dat gaat voorlopig niet gebeuren. Tot die tijd is versleuteling geen vervanging voor DNSSEC, maar zijn beide technieken complementair aan elkaar. De komst van DNS-versleuteling is volgens experts wel een mogelijke aanjager voor de verdere adoptie van DNSSEC (en daarop leunende standaarden zoals DANE).

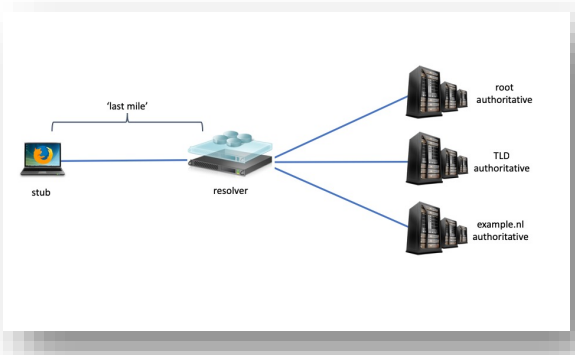
Het 2e impliciete voordeel van DNS-versleuteling is, dat hiermee het zogenaamde 'source address spoofing' kan worden tegengegaan. Deze vorm van IP spoofing, (niet te verwarren met DNS spoofing), wordt vaak gebruikt bij DDoS-aanvallen. Deze zogenaamde 'DNS-amplification attacks' zijn bij tijd en wijle een behoorlijke plaag op het internet waarbij ze veel hinder veroorzaken.

Een laatste voordeel is dat de TCP-gebaseerde DNS-versleutelingsmethoden geen last meer hebben van zogenaamde 'truncated' DNS-antwoorden. Maar daar staat flink wat meer IP-overhead als nadeel tegenover.

3 Verschillende vormen van DNS-versleuteling

Er zijn de afgelopen tijd verschillen paden bewandeld die geleid hebben tot verschillende oplossingsrichtingen. We zetten de belangrijkste DNS-versleutelingstechnieken kort op een rij. Primair beschermen deze technieken de 'last mile', dat wil zeggen het pad tussen die cliënt (stub) en de resolver (zie afbeelding 1). Daar waar dit anders is, wordt dit vermeld.

Ze kunnen in theorie ook werken voor het pad tussen resolver en authoritative server, maar dat is qua standaardisatie en schaalbaarheid nog een paar stappen verder en momenteel nog niet aan de orde.



Afbeelding 1

Het overzicht is niet compleet. Zo laten we QNAME Minimisation buiten beschouwing, omdat hierbij strikt genomen geen sprake is van versleuteling. In plaats daarvan wordt DNS-privacy daar bereikt door andersoortige DNS-vragen met daarin niet meer detail dan strikt noodzakelijk. Ook laten we Oblivious DNS (ODNS) buiten beschouwing. Ook hierbij is geen sprake van versleuteling, bovendien is ODNS nog slechts een zeer pril gedachtenexperiment.

3.1 DNSCrypt en DNSCurve

Encryptie van DNS-verkeer, zodat het tegen afluisteren is beschermd, is niet nieuw en er werd al voor 'Snowden' mee geëxperimenteerd. Zo is er een al langer bestaand idee, genaamd DNSCrypt, dat wordt ondersteund door enkele grote spelers zoals OpenDNS, Quad9 en bijvoorbeeld de Yandex webbrowser, maar opvallend genoeg is dit protocol nooit naar de IETF gebracht voor standaardisatie, als is het al volledig uitgewerkt sinds 2013.

DNSCrypt werkt zowel via TCP als UDP en gebruikt standaard poort 443, maar stuurt daar geen HTTPS-verkeer over. Er zijn dus geen TLS (-stack) en geen X.509 certificaten nodig. Het beschermt het pad tussen de cliënt (stub) en de resolver.

Een andere techniek is DNSCurve en werkt eveneens via UDP en TCP. DNSCurve is evenmin gestandaardiseerd

in de IETF, al is er wel een draft gemaakt. Het kent vrij weinig toepassingen in het wild. DNSCurve werkt 'hop-by-hop' tussen resolvers en authoritative nameservers. De standaard beschermt dus niet de 'last mile' tussen cliënt (stub) en resolver. Het kan worden gezien als concurrent van DNSSEC, met dien verstande dat DNSSEC end-to-end is en geen DNS-versleuteling doet (niet manipuleerbaar, wel afluisterbaar).

3.2 DNS over TLS (RFC7858, 2016) en DNS over DTLS (RFC8094, 2017)

DNS over TLS werkt standaard over TCP-poort 853. En zoals de naam al doet vermoeden, wordt het DNS-verkeer verpakt in een versleutelde TLS-verbinding. Enkele van de grote publieke DNS-providers ondersteunen het al, zoals Quad9 en CloudFlare 1.1.1.1. En er is ook cliënt-software, zoals bijvoorbeeld Stubby. DNS afhandelen via TCP vereist veel meer overhead, wat een uitdaging is. Daarom is er ook een poging gedaan om DNS over DTLS te standaardiseren. Dus over DTLS, dat UDP gebaseerd is. Er zijn hiervan echter geen werkende implementaties bekend.

3.3 DNS over HTTPS (RFC8484, 2018)

DNS over HTTPS (DoH) is een techniek waarbij het DNS-verkeer versleuteld wordt in de vorm van 'gewoon' HTTPS- of HTTP/2-verkeer, dat we ook al kennen van websites (met het fameuze slotje). TCP dus. De standaard is opmerkelijk snel tot stand gekomen en heeft wat stof doen opwaaien. Opvallend snel boden grote spelers, zoals Google Public DNS en Cloudflare, maar ook bijvoorbeeld Quad9, ondersteuning. Google heeft het ingebouwd in zijn nieuwste versie Android 9 "Pie" en de Chromebrowser wordt er ook op voorbereid. CloudFlare bracht een app uit, om hun dienst op Android en iOS beschikbaar te maken. En webbrowsermaker Mozilla heeft het zelfs al ingebouwd in zijn FireFox browser en noemt deze feature de 'Trusted Recursive Resolver' (TRR). Ze hebben daarvoor een samenwerkingsverband afgesloten met CloudFlare.

3.4 DNS over QUIC (draft)

QUIC (of, zoals het in de toekomst misschien gaat heten; HTTP/3) is een nieuw transportprotocol met ingebouwde versleuteling. Er is een draft in ontwikkeling die DNS over QUIC beschrijft. QUIC werkt over UDP. Het is daardoor efficiënt en heeft minder overhead. Het is het beste van 2 werelden, tussen traditioneel DNS over UDP en nieuw DNS over TLS. Daarom heeft deze oplossing veel potentieel. Het protocol is specifiek gericht op verkeer tussen de cliënt (stub) en de recursieve resolver, maar dat kan in de toekomst nog veranderen.

4 Resumerend

We hebben gelezen dat er goede redenen zijn om meer privacy aan te brengen in het DNS-protocol. En hoewel er al een aantal initiatieven liepen, zorgden de Snowden-onthullingen voor een extra opleving en voor nieuw IETF-standaardisatiewerk. De meeste methodieken gaan uit van DNS over een versleuteld pad. En hoewel de ontwikkelingen nog volop in beweging gaan, zien we een bescheiden adoptie voor DNScrypt, een wat grotere adoptie voor DNS-over-TLS en een opvallend snelle adoptie van DNS-over-HTTPS (DoH).

Over die laatste, opmerkelijke ontwikkeling van DoH en de controverses die daarmee gepaard gaan, hebben we een blog geschreven met extra duiding. Dit artikel dient daarbij als technisch achtergrondartikel.