Bescherming & Privacy vanaf de grond op

Transacties op het Internet, die betrouwbaar en mogelijk versleuteld moeten zijn, beginnen meestal met het opzoeken van het IP-adres waarmee dan de verbinding wordt opgezet. IP adressen worden opgezocht in het Domain Name System (DNS): het telefoonboek van het internet. Zo'n DNS zoekopdracht (DNS-query) is van oorsprong onbeveiligd en publiek.

Om bescherming en privacy voor **eindgebruikers** vanaf het allereerste begin te waarborgen, moeten we de DNS transacties meenemen in het beveiligingsdomein. De eerste stap hiertoe is DNSSEC, waarmee de authenticiteit en de juistheid van de ontvangen gegevens kunnen worden gecontroleerd. Maar om ook de privacy van meet af aan te waarborgen, moeten ook de DNS-servers zelf worden geverifieerd en de transacties ermee versleuteld.

De zwakste schakel

Van oudsher worden versleutelde verbindingen gewaarmerkt door zogenaamde Certificate Authorities (CA's). Zij verklaren door middel van een digitale handtekening dat de versleutelde verbinding voor de **DNS naam** valide is. Jammer genoeg kunnen alle, ten minste 1482[1], CA's in staan voor elke DNS naam. Deze garantie is dus zo sterk als de zwakste van deze 1482 schakels.

Met DNS-based Authentication of Named Entities (DANE [RFC6698]) kan hier iets aan gedaan worden. Hiermee staan domeinnaamhouders zelf in voor hun eigen DNS namen voor versleutelde verbindingen (met behulp van DNSSEC) en zijn hiervoor niet meer afhankelijk van een derde partij.

Living on the Edge

Om vanaf de grond op bescherming en privacy voor alle versleutelde transacties te bewerkstelligen, moeten zowel DANE als DNS Privacy [RFC7858] zo dicht als mogelijk bij de eindgebruiker kunnen worden gerealiseerd. Dus tenminste op het systeem van een eindgebruiker, maar misschien zelfs nog dichterbij, tot in de applicatie die wordt gebruikt. De omstandigheden, daar aan de randen van het Internet, zijn divers en vaak niet optimaal. Beschikbaarheid van DNSSEC wordt vaak gehinderd door goedkope, niet standaard-compliant, middleboxes (modems en zo).

De getdns library, Stubby & de getdns API specificatie

getdns is een DNS resolver library voor applicaties. Applicaties hebben met behulp van de getdns library beschikking over betrouwbare DNSSEC validatie (voor DANE), zelfs in de lastigste omgevingen (middels DNSSEC Roadblock Avoidance [RFC8027]). De ontwikkeling van getdns is hand in hand gegaan met de ontwikkeling van de DNS privacy standaard [RFC7858]. getdns heeft dan ook de meest volledige en geoptimaliseerde DNS Privacy implementatie [2]. getdns heeft een systeem component waarmee ook de DNS Privacy van legacy applicaties gewaarborgd wordt: Stubby [3].

getdns is een implementatie van de getdns Application Programmers Interface (API) specificatie, die is geïnitieerd door participanten van de IETF en is geredigeerd door Paul Hoffman. In 2013 heeft Allison Mankin (destijds bij Verisign Labs) het initiatief genomen om deze specificatie te implementeren in een samenwerking met NLnet Labs en NO Mountain Software. Momenteel wordt getdns verder ontwikkeld in een samenwerkingsverband van NLnet Labs met Sinodun. Veel van de mensen van het eerste uur (waaronder Allison Mankin) dragen nog steeds actief bij aan de ontwikkeling van getdns.

getdns, above and beyond

getdns ziet momenteel een snelle toename in gebruik, vanwege de introductie van de Privacy enabled DNS resolver infrastructuur van Quad9.net en Stubby als het beste software component om hier gebruik van te maken[4]. Één van de doelstellingen voor de toekomst is dan ook verdere verbetering van de toepasbaarheid en kwaliteit van de Privacy DNS functionaliteit, onder andere door: Meer schaalbare manieren om authenticiteit van DNS servers te verifiëren[5,6], maar ook door manieren te vinden om blokkeren van Privacy DNS service tegen te gaan[7].

Ook is er een nieuw initiatief, voor een library in de geest en gebruik makend van getdns, die applicaties in staat zal stellen internet verbindingen op te zetten waarbij automatisch alle moderne standaarden worden gebruikt: de Connect by Name library. Deze library zal onder de motorkap onder andere de volgende standaarden toepassen: Private DNSSEC gevalideerde DNS lookups, Happy Eyeballs (positieve discriminatie van IPv6), versleuteld met TLS geverifieerd met DANE.

[1] Eckersley, Peter, and Jesse Burns. "An observatory for the SSLiverse." *Talk at Defcon* 18 (2010).
[2] https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status
[3] https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Daemon+-+Stubby
[4] https://labs.ripe.net/Members/stephane_bortzmeyer/quad9-a-public-dns-resolver-with-security
[5] https://tools.ietf.org/html/draft-ietf-dprive-dtls-and-tls-profiles
[6] https://tools.ietf.org/html/draft-ietf-tls-dnssec-chain-extension
[7] Make traffic unblockable issue on github: https://github.com/getdnsapi/getdns/issues/370