Veilig(er) internet

Ton Valkenburgh

De oorsprong van internet ligt bij een opdracht van het Amerikaanse ministerie voor een robuust netwerk. Uit het hieruit ontstane ARPANET is internet ontstaan.

Bij het ontwerp van internet is veiligheid een ondergeschoven kindje geweest.

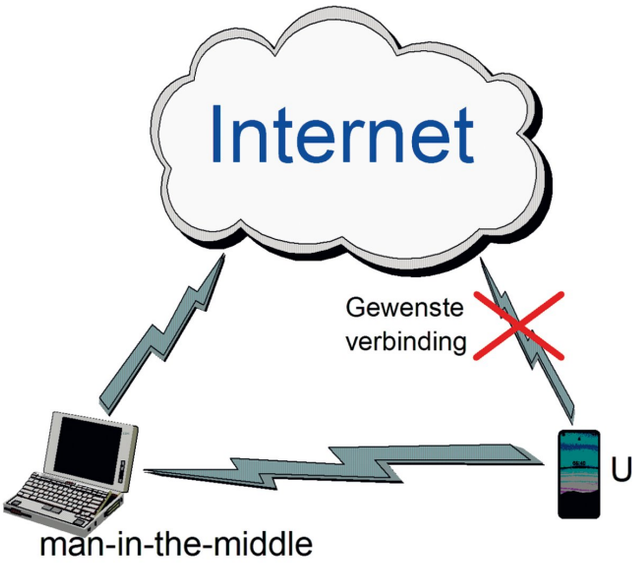
Inleiding

Nu veiligheid en privacy steeds belangrijkere onderwerpen zijn geworden, komen daar oplossingen voor. Helaas laat het invoeren nog wel eens op zich wachten. Wat dat betreft lijkt het op de invoering van IPv6.

Domeinnaamservers

Een veiligheidszwakte bij internet is de manier waarop een sessie wordt opgezet. We zijn allemaal gewend namen te gebruiken voor bijvoorbeeld een website. Deze naam moet worden omgezet in een fysiek IP-adres. Hiervoor gebruiken we domeinnaamservers: het zogenaamde domeinnaamsysteem (DNS).

In het internet zijn de domeinnaamservers gekoppeld. Als u een internetverbinding opzet wordt de naam van de gewenste site naar de domeinnaamserver van uw internetprovider gestuurd. In de domeinnaamserver wordt deze naam omgezet in een fysiek IP-adres, bijvoorbeeld 23.45.7.100. Deze berichten zijn gewoon leesbaar.



Man-in-the middle

Als een wifi-toegangspunt met een identieke naam uw verbinding heeft overgenomen, kunnen al uw gegevens worden opgevangen en meegelezen. Een zogenaamde ‘man-in-the-middle’. Het kan trouwens ook een vrouw zijn. Om dit meelezen te voorkomen is een aantal oplossingen bedacht met ieder hun voor- en nadelen.

DNSSEC

DNSSEC (link 1) is een uitbreiding op het domeinnaamsysteem. Het verhelpt een aantal kwetsbaarheden, maar niet alle. De met DNSSEC ingevoerde uitbreiding voegt een digitale handtekening toe aan de DNS-informatie. Hierdoor is een controle mogelijk op de juistheid van het verkregen IP-adres. Alle informatie is hier nog steeds zichtbaar.
Hierdoor is het mogelijk de zichtbare informatie te gebruiken, bijvoorbeeld om gerichte reclame aan te bieden. Mede daarom zijn er nog meer veiligheidsopties uitgewerkt. Niet alle internetserviceproviders hebben trouwens DNSSEC ingevoerd.

DNS over HTTPS

De juiste manier om naar een website te gaan is met het https-protocol. De verbinding tussen de browser en de website is dan versleuteld. Helaas ondersteunen nog niet alle websites dit. Het verbreidt zich wel steeds meer, omdat het ondersteunen hiervan een hogere ranking in de zoekresultaten van Google geeft. De verbindingsopbouw is echter niet versleuteld. Als deze ook zou zijn versleuteld, was uw privacy beter gewaarborgd.

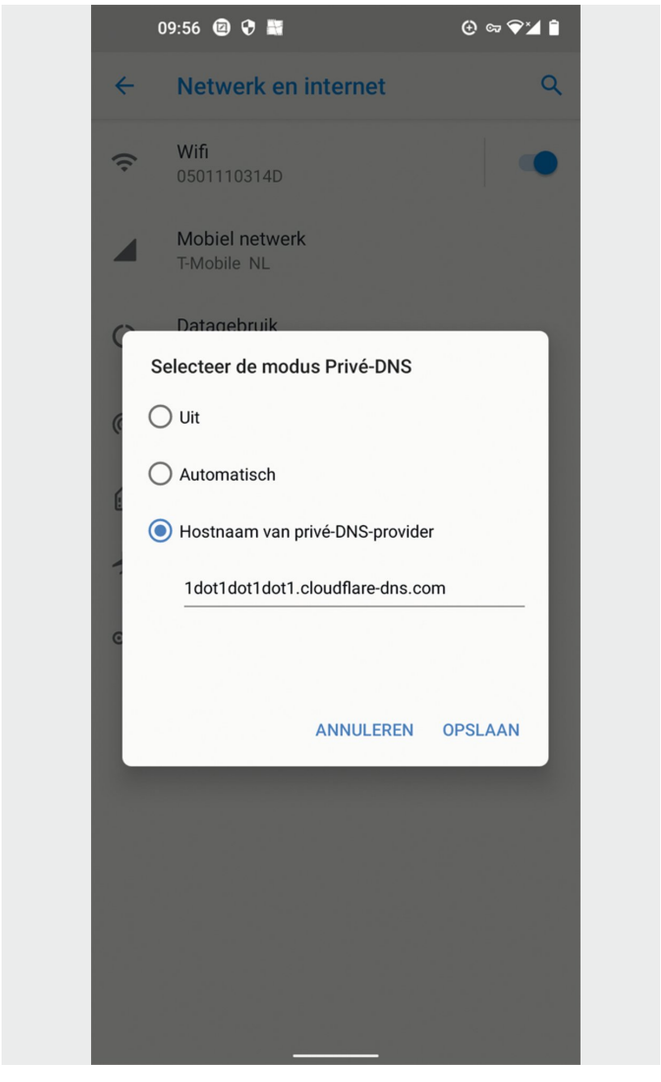
Normaal wordt voor de sessieopbouw het User Datagram Protocol (**UDP**) gebruikt. Bij DNS over HTTPS (**DoH**) wordt echter het Transmissie Control Protocol (**TCP**) gebruikt over een versleutelde verbinding. Daardoor zijn transmissiefouten te corrigeren. Ook wordt de DNS-informatie versleuteld. Het resultaat is een betrouwbaardere verbindingsopbouw met grotere veiligheid en privacy. DoH gebruikt poort 443. De standaardpoort voor https.
DoH wordt o.a. standaard door Firefox ondersteund.

Bij *Opties* > *Algemeen* > *Netwerkinstellingen* > *DNS over HTTPS inschakelen* kiest u een DNS-service die het protocol ondersteunt. Bij Linux vindt u het bij *Bewerken* > *Voorkeuren* > *Algemeen* > *Netwerkinstellingen*.
Het instellen in de browser op een mobiel is lastiger, maar er is ook een eenvoudige oplossing. Gebruik de hieronder genoemde *DNS over TLS* en installeer voor alle zekerheid de add-on *HTTPS-Everywhere*. Dit geeft dezelfde beveiliging als *DNS over HTTPS*.

Ondersteuning voor DoH is nog vrij beperkt en u vindt het vooral bij wereldwijdwerkende grote providers als Google, Cloudflare en NEXTDNS (link 2).
Google kiezen zou hier het paard achter de wagen spannen

zijn; de DNS-provider ziet namelijk wel het IP-adres. Een uitgebreide lijst van DNS-providers die het ondersteunen is te vinden bij link 3.
Het nadeel van deze oplossing is dat het alleen voor sessies met het https-protocol werkt en niet voor bijvoorbeeld uw mailsessies.
Helaas wordt op dit moment de Server Name Indication (SNI) nog niet versleuteld. Hierdoor is de hostnaam waarmee men wil verbinden nog zichtbaar. Mozilla werkt op dit moment aan een oplossing voor Firefox (link 4).

DNS over TLS



Bij DNS over TLS (**DoT**) gaat de opbouw van de sessie via een versleutelde TCP-verbinding. De opgebouwde verbinding is echter alleen versleuteld als de betreffende toepassing dat ondersteunt, bijvoorbeeld uw mailprogramma of browser.

Als u uw ‘standaard’ programma’s wilt gebruiken heeft u dus een programma nodig dat DoT ondersteunt.

Voor Windows, Mac-OS en Linux zijn programma’s beschikbaar om deze functie te vervullen.
In de thuissituatie kan de functie ook worden geleverd door de router.

De FRITZ!Box-router ondersteunt het vanaf versie 7.2 (link 5). Het voordeel bij een dergelijke oplossing is dat het gelijk voor alle apparaten binnen het thuisnetwerk werkt.

DoT gebruikt poort 853.
Sommige firewalls blokkeren standaard deze poort.

Voor buitenshuis zal het per mobiel apparaat moeten worden ingesteld. Juist hier is het belangrijk. Onderweg is de kans op een man-in-the-middle bij openbare netwerken namelijk groter. Android ondersteunt het standaard sinds versie 9.0. Ook vanaf iOS 14 zijn er oplossingen met apps uit de store.

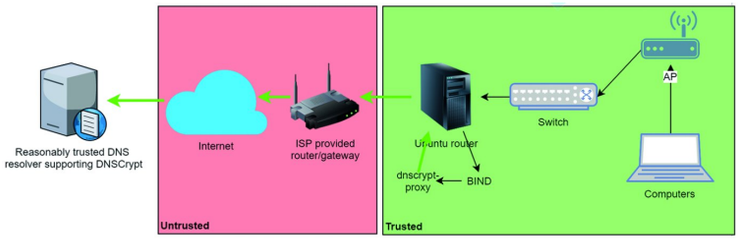
Voor Android klikt u op:*Instellingen* > *Netwerk en internet* > *Geavanceerd* > *Privé-DNS*.
Selecteer Hostnaam van privé-DNS-provider en vult hier een domeinnaam in van de gewenste provider.
Bijvoorbeeld voor: **Cloudflare**
1dot1dot1dot1.cloudflare-dns.com

Voor een aantal andere providers zie link 2.

Voor iOS is een app nodig. Grote providers bieden hiervoor apps aan in de Apple-store.

DNSCrypt

DNSCrypt is een ander protocol voor versleutelde autorisatie met DNS-servers. Het heeft het nooit gebracht tot een officiële norm. Er zijn echter wel DNS-servers die het ondersteunen.



Conclusie

Voor mobiele apparaten, zoals smartphones, is een veilige verbinding met internet belangrijk. Bij het gebruik van openbare netwerken is het belangrijk om de man-in-the middle te elimineren. De hier beschreven methodes maken uw verbinding veiliger. Nog niet alle benodigde functies zijn even makkelijk te configureren.
Op dit moment is het aantal DNS-servers die deze functies ondersteunen beperkt. Het is daarom te hopen dan het snel standaard wordt bij alle internetserviceproviders.

In een volgend artikel wil ik de oplossingen voor DoT bij pc en laptop behandelen.

Links

1. https://www.sidn.nl/cybersecurity/dnssec-uitleg
2. https://www.privacy-tools.nl/providers/dns-domein-providers/
3. https://dnscrypt.info/public-servers/
4. https://blog.mozilla.org/security/2021/01/07/encrypted-client-hello-the-future-of-esni-in-firefox/
5. https://www.der-windows-papst.de/2020/09/25/dns-over-tls-fritzbox-aktivieren/