

TLS 1.3

VEEL SNELLER EN VEILIGER DAN VOORGANGER

Ondersteuning onveilige standaarden gestopt

De nieuwe versie 1.3 van TLS is aanzienlijk beter dan zijn voorganger. Invoering is niet eenvoudig, maar grote browsers als Safari en Chrome zijn er al mee aan de slag. Rob van der Staaij zet de verbeteringen op een rij.

door Rob van der Staaij beeld Shutterstock



HET VERSLEUTELLEN VAN COMMUNICATIEVERBINDINGEN IN OPENBARE NETWERKEN is een van de belangrijkste maatregelen om de vertrouwelijkheid van digitale informatie te waarborgen die van a naar b wordt verstuurd. Steeds meer websites ondersteunen die functionaliteit. Gevestigde namen zoals Google sporen het gebruik ervan aan. Terecht, want de middelen die cybercriminelen tot hun beschikking hebben om informatie te onderscheppen, worden steeds verfijnder en geavanceerder.

SPECIFICATIES

Een van de bekendste specificaties voor het tot stand brengen van een versleutelde communicatieverbinding is SSL/TLS (Secure Sockets Layer/Transport Layer Security). Dit levert onder meer het welbekende hangslotje op in de adresbalk van browsers. De twee specificaties worden vaak in één adem genoemd of ook wel samengevat onder de noemer SSL, maar in feite is TLS de opvolger van SSL. Deze laatste is volkomen verouderd en zou niet

meer moeten worden gebruikt. Alle versies ervan vertonen namelijk ernstige kwetsbaarheden, waarvan de beruchte POODLE (Padding Oracle On Downgraded Legacy Encryption) een van de bekendere is. Ook de eerdere versies van TLS vertonen kwetsbaarheden. De op dit moment gangbare versie is TLS 1.2, maar zelfs deze versie is niet gevrijwaard van kwetsbaarheden. SLOTH (Security Losses from Obsolete and Truncated Transcript Hashes) is de verzamelnaam voor een reeks kwetsbaarheden die de server zouden kunnen dwingen verouderde en te manipuleren standaarden te gebruiken voor het verifiëren van digitale handtekeningen. Daarmee worden in potentie allerlei typen man-in-the-middleaanvallen mogelijk. Inmiddels is TLS 1.3 beschikbaar gekomen die de zwakheden van de voorgaande versies verhelpt en ook een aanzienlijk betere performance kent. TLS 1.3 is in augustus 2018 door de Internet Engineering Task Force (IETF) gepubliceerd als

RFC 8446 en biedt flinke verbeteringen ten opzichte van TLS 1.2. Die verbeteringen hebben niet alleen betrekking op de security. Ook de efficiency is onder handen genomen.

SECURITY

TLS 1.3 levert een verbeterde beveiliging doordat verouderde en regelrecht onveilige encryptie- en hashingstandaarden niet meer worden ondersteund. Voorbeelden hiervan zijn DES, 3DES, RC4, MD5 en SHA-1. Omdat deze en andere kwetsbare standaarden niet meer worden toegestaan, kunnen ze ook niet meer door minder ervaren beheerders en ontwikkelaars worden geïmplementeerd, iets wat met TLS 1.2 wel mogelijk is. In samenhang met het voorgaande moet het verplicht gebruik van 'perfect forward secrecy' (ook wel kortweg 'forward secrecy' geheten) worden genoemd. Dit is een eigenschap die ervoor zorgt dat de sleutel voor het genereren en uitwisselen van symmetrische encryptiesleutels steeds wordt ververs. Dit maakt het onmogelijk



**HANDSHAKE
TUSSEN CLIENT EN
SERVER VEREIST
AANMERKELIJK
MINDER STAPPEN**

om voorafgaande symmetrische sleutels te herleiden en daarmee vorige berichten te achterhalen. Deze eigenschap is slechts optioneel in de voorgaande versies van TLS. TLS 1.3 benut hiertoe de standaard Ephemeral Diffie-Hellman (EDH). Deze encryptiestandaard maakt slechts eenmalig gebruik van een sleutel om de symmetrische encryptiesleutels te genereren en te distribueren waarmee uiteindelijk de te versturen informatie wordt versleuteld. Bij het afsluiten van de sessie wordt de sleutel weer afgedankt. In oudere versies van TLS wordt daarentegen vaak gebruikgemaakt van statische sleutels voor het genereren en uitwisselen van symmetrische encryptiesleutels. Een aanvaller zou met het onderscheppen van een dergelijke sleutel alle daarmee versleutelde informatie kunnen achterhalen. Het beperken van de uit te wisselen informatie die nodig is voor de handshake (zie verderop) zorgt eveneens voor verbetering van de beveiliging, omdat hiermee het aantal mogelijkheden voor een aanvaller om de sessie te manipuleren afneemt.

PERFORMANCE

TLS 1.3 is een stuk sneller dan TLS 1.2 doordat de handshake die plaatsvindt tussen de client en de server aanmerkelijk minder stappen vereist. In TLS 1.2 kan de tijd die nodig is voor de handshake oplopen tot een halve seconde, een eeuwigheid in de wereld van digitale communicatie. Let wel: de eigenlijke communicatie is dan nog niet eens begonnen. De TLS-handshake dient om de communicatie tussen de client (bijvoorbeeld een browser) en de server (bijvoorbeeld een website) mogelijk te maken en omvat de volgende functies:

- Authenticatie van de partijen die met elkaar gaan communiceren (voor de server is dit verplicht, voor de client optioneel). Dit gebeurt door middel van digitale certificaten.
- Maken van afspraken over de toe te passen encryptiealgoritmen en -parameters.
- Genereren en uitwisselen van encryptiesleutels. De encryptiesleutels die

voor het eigenlijke versleutelen van de te versturen data worden gebruikt, zijn gebaseerd op symmetrische encryptiestandaarden zoals AES. Het genereren en uitwisselen ervan gebeurt met behulp van asymmetrische encryptiestandaarden zoals RSA en Diffie-Hellman. Daarnaast ondersteunt TLS 1.3 een modus die bekendstaat als de zogeheten zero round trip time (afgekort 0-RTT). Deze modus maakt het mogelijk om de handshake geheel over te slaan indien deze al eerder heeft plaatsgevonden, bijvoorbeeld wanneer een browser verbinding maakt met een website die recentelijk al eerder bezocht is. Dit verbetert de performance nog verder, maar introduceert ook een potentiële kwetsbaarheid. Een aanvaller zou met een zogeheten replay attack alle informatie van de voorgaande handshake kunnen onderscheppen om die opnieuw te presenteren aan de server tijdens de 0-RTT. Voorlopig is dit een theoretische kwestie waarvan de praktijk zal moeten uitwijzen in hoeverre dit reëel is.

AUTEUR



ROB VAN DER STAAIJ
(rstaaij@gmail.com) is
eigenaar van Stysec B.V.
(stysec.nl) en als associate
verbonden aan Strict
Consultancy (strict.nl)

REACTIES EN BIJDRAGEN

Voor reacties en
nieuwe bijdragen van
IT-experts:
Tanja de Vrede
020-2356415
t.d.vrede@agconnect.nl

ENCRYPTIEMETHODES

Ter opfrissing wordt hier een beknopte uitleg gegeven van de meest gangbare methoden van versleuteling. Al deze methoden maken deel uit van de TLS-specificatie.

SYMMETRISCHE ENCRYPTIE

Bij symmetrische encryptie wordt een identieke sleutel gebruikt voor zowel versleutelen als ontsleutelen. Een uitdaging hierbij is dat de sleutel op een veilige wijze moet worden gedeeld met de partij met wie vertrouwelijke informatie wordt uitgewisseld. In de praktijk wordt hiervoor meestal asymmetrische encryptie toegepast (zie hieronder). Symmetrische encryptie is aanmerkelijk sneller dan asymmetrische encryptie en daarom meer geschikt voor het versleutelen van grote hoeveelheden data. Dat is de reden dat voor het versleutelen van data in communicatieverbindingen symmetrische encryptie wordt toegepast. De belangrijkste standaard is AES (Advanced Encryption Standard).

ASYMMETRISCHE ENCRYPTIE

Hierbij worden twee verschillende sleutels gebruikt: een publieke sleutel en een priv sleutel. Zoals de naam al aangeeft, kan de publieke sleutel vrij beschikbaar worden gesteld. De priv sleutel moet echter strikt geheim worden gehouden. Beide sleutels kunnen worden gebruikt voor zowel versleutelen als ontsleutelen, maar wat is versleuteld met een bepaalde sleutel, kan alleen nog maar met de andere sleutel van hetzelfde sleutelpaar worden ontsleuteld en vice versa. De sleutels zijn wiskundig aan elkaar gerelateerd, maar sluiten elkaar uit. Net als symmetrische encryptie kan asymmetrische encryptie worden gebruikt voor het waarborgen van de vertrouwelijkheid van informatie. Hiervoor wordt de publieke sleutel van de ontvangende partij gebruikt.

Ontslutelen vindt plaats met de priv sleutel van de ontvanger. Daarnaast wordt deze methode toegepast voor het borgen van de authenticiteit van informatie (digitale handtekening). Hiervoor wordt de priv sleutel van de partij gebruikt die de informatie verzendt. Verificatie vindt vervolgens plaats met de publieke sleutel van diezelfde verzender.

Een groot nadeel van asymmetrische encryptie is de complexiteit ervan. Deze methode is veel trager dan symmetrische encryptie; een processor heeft er grote moeite mee. Daarom is asymmetrische encryptie eigenlijk alleen maar geschikt voor het versleutelen van kleine stukjes digitale informatie, bijvoorbeeld symmetrische encryptiesleutels. Als standaarden kunnen RSA (Rivest Shamir Adleman), ECC (Elliptic Curve Cryptography) en Diffie-Hellman worden genoemd.

PUBLIC KEY INFRASTRUCTURE

Een public key infrastructure (PKI) is het geheel aan componenten, processen en standaarden dat de volgende doelstellingen kent:

- Uitgeven van publieke sleutels.
- Waarborgen dat publieke sleutels zijn verbonden aan rechtmatige eigenaren. Dit kunnen zowel individuen zijn als organisaties.
- Verifi ren dat publieke sleutels echt en valide zijn.

Publieke sleutels worden uitgegeven (en ingetrokken) door een certificatautoriteit (CA). Dit gebeurt door middel van digitale certificaten. Een digitaal certificaat bevat naast de publieke sleutel alle informatie die nodig is om de echtheid en validiteit van die publieke sleutel te kunnen verifi ren, zoals de digitale handtekening van de certificatautoriteit.

INVOERING

Het invoeren van TLS 1.3 heeft veel voeten in de aarde, omdat applicaties en netwerkcomponenten hiervoor moeten worden aangepast. Toch zal het waarschijnlijk niet lang duren voordat deze specificatie breed beschikbaar is. Leveranciers van applicaties willen niet de indruk wekken achter te lopen op de ontwikkelingen en zullen daarom haast maken met de implementatie van TLS 1.3. Belangrijke browsers zoals Chrome, Firefox, Safari en Samsung Internet ondersteunen de specificatie inmiddels; een aantal webserver- en cloudplatforms eveneens, zoals NGINX en Cloudflare.

AANDACHTSPUNTEN

Het is goed om te bedenken dat TLS alleen de communicatieverbinding tussen twee partijen beveiligt. Zodra de digitale informatie op de plaats van bestemming (bijvoorbeeld een website) is aangeland, wordt de versleuteling ervan opgeheven en is het voor de client niet meer zichtbaar wat er met de informatie gebeurt. Met andere woorden, TLS zegt niets over de betrouwbaarheid van de partij waarmee de informatie wordt gedeeld. Iedereen, criminele organisaties niet uitgezonderd, kan een website opzetten en een officieel digitaal certificaat aanvragen dat als basis dient voor de met TLS versleutelde verbinding. Daarmee zal de betreffende website vertrouwd ogen. Ook kan een cybercrimineel nog steeds een man-in-the-middleaanval uitvoeren waarbij het legitieme digitaal certificaat wordt onderschept terwijl het van de server naar de client wordt verstuurd om vervolgens te worden vervangen door een vals certificaat. Dit kan worden ondervangen door een effectieve maatregel die we kennen als ‘certificate pinning’. Hierbij wordt de client vooraf geconfigureerd met informatie over welk digitaal certificaat wordt verwacht van de server. Als het digitale certificaat niet met deze informatie overeenkomt, zal de client de sessie voortijdig afbreken. 