Hoe vooral de implementatie sneller zou kunnen

DNSSEC-ALGORITMEN: DE LANGE WEG VAN STANDAARDISATIE TOT GEBRUIK

CRYPTOGRAFISCHE SIGNEERALGORITMEN VORMEN DE KERN VAN DNSSEC. OM DE BEVEILIGING VAN HET DNS OP PEIL TE HOUDEN, MOETEN DEZE ALGORITMEN REGELMATIG WORDEN VERVANGEN. IN DE PRAKTIJK BLIJKT DIT EEN LANG EN MOEIZAAM PROCES TE ZIJN. HOE KOMT DAT? EN, BELANGRIJKER NOG: KAN DIT PROCES WORDEN VERSNELD?

door Moritz Müller beeld Shutterstock

DNS SECURITY EXTENSIONS, KORTWEG DNSSEC, IS DE CRYPTOGRAFISCHE BEVEILIGING VAN HET DOMAIN NAME SYSTEM (DNS), waarmee de vertaling van domeinnamen naar IP-adressen en vice versa wordt geregeld. DNSSEC beschermt de DNS-informatie, waardoor gebruikers de garantie hebben dat hun internetverkeer op de juiste plaats terechtkomt. Cryptografische signeeralgoritmen vormen de kern van DNSSEC.
Door krachtigere computers en meer geavanceerde cryptoanalyse komt het echter regelmatig voor dat deze algoritmen niet langer voldoende veiligheid bieden. DNSSEC-implementaties moeten daarom andere algoritmen gaan gebruiken. Maar de weg van standaardisatie van een nieuw algoritme voor DNSSEC tot aan de daadwerkelijke toepassing ervan is lang en hobbelig. Welke barrières komen we tegen en hoe kunnen we in de toekomst sneller op veiligere algoritmen overstappen?

BREED SCALA

DNSSEC ondersteunt een breed scala aan cryptografische signeeralgoritmen, uiteenlopend van moderne, op Edwards curve-gebaseerde algoritmen, zoals Ed25519, tot algoritmen die uit de jaren negentig stammen, zoals DSA/SHA1. De meeste domeinnamen onder .nl zijn gesigneerd met RSA/SHA-256 of ECDSA. Hetzelfde geldt overigens voor andere domeinnamen.

VAN STANDAARDISATIE TOT GEBRUIK

De route van het standaardiseren van een nieuw algoritme tot aan de ingebruikname ervan bestaat grofweg uit de volgende drie stappen.

STAP 1: EEN NIEUW ALGORITME STANDAARDISEREN

Voordat een algoritme in DNSSEC kan worden gebruikt, moet dit algoritme

Overstappen op kwantumveilige algoritmen is een bittere noodzaak

binnen de Internet Engineering Task Force (IETF) – een internationale, open gemeenschap die zich bezighoudt met de evolutie van de internetarchitectuur en de soepele werking van het internet – worden gestandaardiseerd als Request for Comments (RFC). Dit zijn documenten die de protocollen en andere aspecten van het internet beschrijven.
In het verleden duurde het één tot vier jaar om nieuwe algoritmen te standaardiseren. Uit de mailinglistarchieven van de IETF blijkt dat algoritmen over het algemeen meer kans hebben om gestandaardiseerd te worden wanneer ze ook echt een verbetering bieden. Denk bijvoorbeeld aan het bieden van meer veiligheid, maar ook betere prestaties of kleinere handtekeningen.

STAP 2: HET ALGORITME INTEGREREN IN DE DNS-SOFTWARE

Uiteindelijk moet de DNS-software een nieuw algoritme kunnen gebruiken voor het signeren, terwijl resolvers de handtekeningen moeten kunnen valideren.
Voor de uitvoering van deze cryptografische functies maakt de DNS-software gebruik van bibliotheken, meestal OpenSSL en GnuTLS. Alleen als deze bibliotheken het nieuwe algoritme ondersteunen, kan de DNS-software hiervan gebruikmaken. Oftewel, de bibliotheken kunnen de implementatie van een nieuw algoritme in de weg staan.

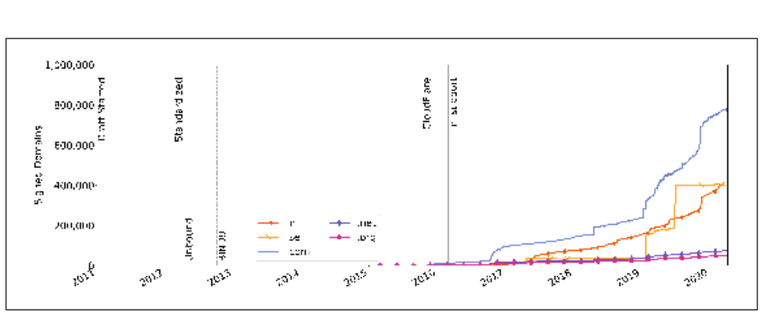
STAP 3: HET ALGORITME IN GEBRUIK NEMEN

Bibliotheken zijn helaas niet het enige obstakel. DNS-operators, registrars en registry's moeten het nieuwe algoritme ondersteunen: ze moeten de publieke sleutel of een hash daarvan publiceren, zodat resolvers de handtekening kunnen valideren.

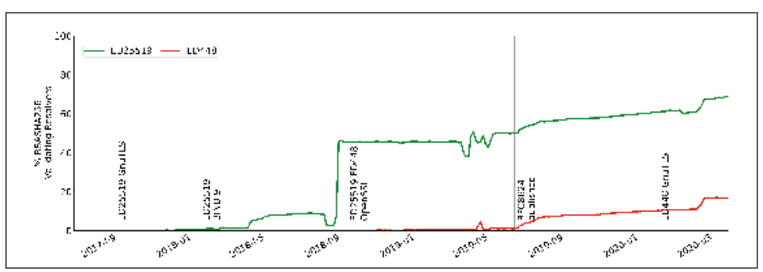
Als we kijken naar de algoritmen die het meest recent aan DNSSEC werden toegevoegd, Ed25519 en Ed448, blijkt dat het vooralsnog niet erg opschiet met die ondersteuning. Ruim drie jaar na hun standaardisatie zijn ze beschikbaar via de meestgebruikte cryptobibliotheken, maar worden ze nog steeds niet ondersteund door veel van de populairste DNS-operators en registrars. Hieronder vallen ook registry's die verantwoordelijk zijn voor topleveldomeinen (TLD's).
Dit betekent dat klanten van die registry's niet kunnen upgraden naar Ed25519 of Ed448, ook al wordt Ed25519 naar verwachting het aanbevolen standaardalgoritme.

STAP NAAR GROOTSCHALIG GEBRUIK

Als al deze stappen zijn genomen, is het interessant om te zien hoelang het duurt voordat een nieuw algoritme ook echt gebruikt wordt door domeinen, en resolvers in staat zijn om het algoritme te valideren.
Hiervoor hebben we met behulp van het meetplatform OpenINTEL gekeken naar het aantal domeinnamen onder de TLD's .com, .net, .org, .nl en .se dat wordt gesigneerd met ECDSAP256.
Na de standaardisatie in 2012 duurde het nog ruim vierenhalf jaar voordat de eerste 100.000 domeinnamen met dit algoritme werden gesigneerd.
De belangrijke aanjagers waren grote DNS-operators die al hun domeinnamen gingen signeren met ECDSAP256, waardoor de adoptie een stuk sneller ging.
De early adopters van dit algoritme waren echter de kleine providers.



Figuur 1: Aantal domeinnamen getekend met ECDSAP256 sinds in 2011 met het ontwerp ervan werd begonnen.



Figuur 2: Aandeel van resolvers die ED25519 en ED448 kunnen valideren. De ondersteuning wordt gemeten met RIPE Atlas.

Daarnaast zijn de meeste resolvers niet onmiddellijk in staat om nieuwe algoritmen te valideren. Het upgraden neemt ook tijd in beslag (zie figuur 2). Ruim drieënhalf jaar na de standaardisatie van dit nieuwe algoritme in april 2017, wordt Ed25519 door 72% van de valideerende resolvers in onze dataset ondersteund. Alle grote leveranciers van DNS-resolvers ondersteunen het algoritme echter al sinds begin 2018. Domeinnaambeheerders die Ed25519 willen implementeren, kunnen daar dus beter nog even mee wachten totdat de resolverondersteuning dichter bij de 100% ligt. Anders zijn hun domeinnamen niet optimaal beschermd.

OBSTAKEL

Overschakelen op een ander algoritme wordt door domeinbeheerders nog steeds gezien als een obstakel. Dergelijke 'algoritme-rollovers' kunnen storingen veroorzaken als ze niet met beleid worden uitgevoerd. Zo zijn er gevallen bekend van domeinnamen waarbij DNSSEC-signering eerst helemaal werd uitgeschakeld voordat er met ECDSAP256 werd gesigneerd.
Maar de (onterechte) angst om op andere algoritmes over te schakelen, kan leiden tot onveilige situaties. Zo worden sommige domeinnamen nog steeds gesigneerd met algoritmen die SHA-1 gebruiken. Dit wordt al geruime tijd als onveilig beschouwd. Er is sprake van zowel beheerders die het overschakelen op een ander algoritme te lastig vinden, als beheerders die de overstap naar veiligere algoritmen domweg niet noodzakelijk achten.

SUCCESFACTOREN VOOR IMPLEMENTATIE

Op basis van bovenstaande bevindingen kunnen een aantal succesfactoren worden gedestilleerd die de implementatie van een nieuw algoritme kunnen versnellen.
Ten eerste moet de internetgemeenschap het nieuwe algoritme vertrouwen. Het helpt bijvoorbeeld als een algoritme al wordt gebruikt in andere protocollen, zoals TLS. Daarmee neemt de kans toe dat de standaardisatie van DNSSEC soepel verloopt.
Ten tweede moeten DNS-operators, registrars en registry's door de gemeenschap worden aangemoedigd om het nieuwe algoritme ook te ondersteunen. Als ze merken dat er vraag naar is, wordt de kans groter dat ze ondersteuning toevoegen. Aan de andere kant moeten DNS-operators streven naar optimale veiligheid en hun systemen en domeinnamen up-to-date houden.
Ten derde moet het zo eenvoudig mogelijk worden gemaakt om het algoritme voor een domeinnaam te vervangen door een ander. Gelukkig is de DNS-software inmiddels dusdanig geavanceerd dat het mogelijk is om een algoritme-rollover grotendeels te automatiseren.

KWANTUMTOEKOMST

Met het oog op de toekomst wordt het nog belangrijker om voor een snellere implementatie van algoritmen te zorgen. Er zullen dan cryptografische signeeralgoritmen nodig zijn die ook niet door kwantumcomputers gekraakt kunnen worden. Overstappen op kwantumveilige algoritmen is dan een bittere noodzaak om de veiligheid van DNS te kunnen blijven garanderen.

In het verleden duurde het één tot vier jaar om nieuwe algoritmen te standaardiseren

AUTEUR

MORITZ MÜLLER
Moritz Müller is research engineer bij SIDN Labs. Hij schreef deze bijdrage in samenwerking met Willem Toorop (NLnet Labs), Taejoong Chung (Virginia Tech), Jelte Jansen (SIDN Labs) en Roland van Rijswijk-Deij (NLnet Labs en Universiteit Twente). Dit artikel is gebaseerd op het onderzoekspaper 'The Reality of Algorithm Agility: Studying the DNSSEC Algorithm Life-Cycle'.