De perfecte oplossing is er nog niet

KWANTUMVEILIGE ALGORITMEN VOOR DNSSEC

DE KWANTUMCOMPUTERS KOMEN ERAAN. EN DAT HEEFT GEVOLGEN VOOR BIJNA ALLE CRYPTOGRAFISCHE ALGORITMEN DIE OP DIT MOMENT WORDEN GEBRUIKT OM HET INTERNET TE BEVEILIGEN. DNSSEC, DE BEVEILIGINGSUITBREIDING VAN HET DOMAIN NAME SYSTEM (DNS), MAAKT OOK GEBRUIK VAN ZULKE ALGORITMEN. AAN WELKE VOORWAARDEN MOETEN NIEUWE ALGORITMEN VOOR DNSSEC VOLDOEN OM OOK IN DE KWANTUMTOEKOMST INGEZET TE KUNNEN WORDEN?

door Moritz Müller beeld Shutterstock

KWANTUMCOMPUTERS WERKEN ANDERS DAN DE HUIDIGE COMPUTERS. In plaats van bits, die de toestand van één of nul kunnen aannemen, werken kwantumcomputers met qubits, die zich in meerdere toestanden tegelijk kunnen bevinden. Hierdoor kunnen kwantumcomputers bepaalde computationele problemen efficiënter oplossen dan de hedendaagse computers. Deze computationele problemen worden als basis gebruikt voor de cryptografische algoritmen om DNS-berichten te signeren, bijvoorbeeld Elliptic Curve en RSA. Dankzij het gebruik van die algoritmen in DNSSEC kan iedereen op het internet verifiëren of een inkomend DNS-bericht het oorspronkelijke bericht is en achterhalen of er onderweg mee is geknoeid. Kwantumcomputers hebben in potentie de capaciteit om dergelijke cryptografische algoritmen met behulp van het algoritme van Shor binnen een paar uur of dagen te kraken, in plaats van de honderden jaren die huidige computers nodig hebben. Voor DNSSEC betekent dit dat een aanvaller een man-in-the-middle-aanval zou kunnen uitvoeren: een DNSSEC-gesigneerd antwoord (met bijvoorbeeld het IP-adres van een site als www.belastingdienst.nl) onderscheppen, het IP-adres in het DNS-antwoord wijzigen en vervolgens het antwoord opnieuw signeren. Het slachtoffer ziet dan geen verschil tussen de handtekening op het oorspronkelijke bericht en de handtekening die de aanvaller heeft toegevoegd aan het gemanipuleerde bericht. Als gevolg daarvan kan het slachtoffer worden omgeleid, bijvoorbeeld naar een phishingsite.

WEDSTRIJD NIST

Gelukkig bestaan er nog computationele problemen die ook voor kwantumcomputers niet snel op te lossen zijn. Deze kunnen dus worden gebruikt voor de cryptografische algoritmen die nodig zijn voor DNSSEC. Het National Institute of Standards and Technology (NIST) in de VS heeft een wedstrijd uitgeschreven die moet leiden tot de standaardisering van ‘kwantumveilige’ algoritmen.

DNS-BERICHTEN KUNNEN MAAR BETER NIET WORDEN GEFRAGMENTEERD

Dat wil zeggen: algoritmen die ook in het tijdperk van de kwantumcomputer nog voldoende beveiliging bieden.

VEREISTEN VOOR KWANTUMVEILIGE DNSSEC-ALGORITMEN

SIDN Labs, TNO, NLnet Labs en de Universiteit Twente hebben gezamenlijk onderzocht of de algoritmen die aan de NIST-wedstijd meedoen, ook geschikt zijn voor gebruik in DNSSEC. Daarvoor hebben de onderzoekers eerst vier vereisten gedefinieerd waaraan kwantumveilige algoritmen moeten voldoen om voor gebruik in DNSSEC in aanmerking te komen.

1. Handtekeninggrootte

Omdat bij ieder gesigneerd DNS-bericht een DNSSEC-handtekening wordt verzonden, is de eerste vereiste: kwantumveilige algoritmen moeten handtekeningen kleiner dan 1.232 bytes genereren. Metingen tonen namelijk aan dat DNS-berichten die groter zijn, meer kans lopen om niet goed te worden verzonden. Het DNS maakt voor het overbrengen van berichten tussen resolvers en autoritatieve nameservers voornamelijk gebruik van UDP. Een DNS-bericht moet dus in één UDP-datagram passen. Doet het dat niet, dan bestaat het risico dat het bericht als gevolg van fragmentatie niet goed wordt verzonden. In het DNS werkt dat als volgt: als een recursieve resolver een query naar een autoritatieve nameserver stuurt, geeft de resolver aan wat de maximale ondersteunde antwoordgrootte is. Als het antwoord groter is, vraagt de autoritatieve nameserver de resolver om het opnieuw te proberen, maar dan met TCP in plaats van UDP.

Dit proces is echter foutgevoelig. Het is bijvoorbeeld mogelijk dat de resolver of de autoritatieve nameserver TCP niet ondersteunt of dat een middlebox alleen DNS-berichten toestaat die met UDP worden verstuurd. Zelfs als de resolver aangeeft een bepaalde datagramgrootte te ondersteunen, kan het zijn dat de onderliggende netwerklaag dit niet doet.

NIST-wedstrijd moet leiden tot de standaardisering van ‘kwantum-veilige’ algoritmen

In dat geval deelt de netwerklaag het antwoord op in kleinere fragmenten, waarbij de kans groter is dat ze niet goed aankomen, bijvoorbeeld door firewalls die gefragmenteerde pakketten droppen. Na verloop van tijd probeert de resolver het opnieuw via TCP, maar ook dat lukt dan vaak niet. DNS-berichten kunnen dus maar beter niet worden gefragmenteerd.

2. Validatiesnelheid

Resolvers moeten kwantumveilige algoritmen net zo efficiënt kunnen valideren als de huidige algoritmen. Aangezien bij elk DNS-antwoord een handtekening wordt verzonden, moet een resolver voor elk bericht dat hij van een autoritatieve nameserver ontvangt, ook de handtekening valideren. Dat betekent dat drukke resolvers (bijvoorbeeld van een ISP of een dienst als Google Public DNS) duizenden antwoorden per seconde moeten valideren. Bovendien is de verwachting dat dit aantal in de toekomst stijgt, omdat het gebruik van DNSSEC nog steeds toeneemt.

3. Signeersnelheid

Ook de snelheid waarmee records worden gesigneerd, mag niet lager liggen dan die van de huidige algoritmen.
In DNSSEC hoeft de operator van een zone, records alleen te ondertekenen als de inhoud van de zone wijzigt. Voor .nl worden bijvoorbeeld ieder halfuur gemiddeld zo’n 11.000 nieuwe handtekeningen gegenereerd. In sommige gevallen moeten records on-the-fly worden gesigneerd en dan kunnen hogere signeersnelheden nodig zijn.

4. Sleutelgrootte

Met DNSSEC worden publieke sleutels slechts af en toe verzonden om de handtekeningen op afzonderlijke antwoorden te valideren. Een resolver vraagt doorgaans bijvoorbeeld slechts één keer per uur om de publieke sleutels voor de miljoen populairste domeinnamen. Anders dan reguliere DNS-berichten kunnen DNS-berichten met publieke sleutels daarom wel groter zijn dan 1.232 bytes.

KWANTUMVEILIG?

Welke algoritmen die aan de NIST-wedstrijd deelnemen, voldoen aan bovenstaande vereisten? Drie ervan genereren in ieder geval een handtekening die kleiner is dan 1.232 bytes: Falcon-512, Rainbow-Ia en RedGeMSS128. Als we deze langs de meetlat van de overige vereisten leggen, leidt dat tot het overzicht in figuur 1.
Ter vergelijking, de huidige algoritmen die vaak in DNSSEC worden gebruikt, hebben de kenmerken zoals vermeld in figuur 2.
Om de kwantumveilige algoritmen te testen, signeerden de onderzoekers in een testomgeving een willekeurig bericht van 86 bytes en valideerden ze de handtekening. Vervolgens registreerden ze hoeveel tijd beide stappen innemen. Dit proces herhaalden ze een paar duizend keer om mediane verwerkingstijden te kunnen berekenen. Uit hun metingen concluderen de onderzoekers dat alle drie de onderzochte algoritmen efficiënt genoeg zijn voor de meeste DNSSEC-toepassingen. De validatiesnelheid van de resolver in hun testopstelling is daar in ieder geval hoog genoeg voor. De grootte van de sleutels en de handtekeningen zijn echter minder hoopgevend. Hoewel Falcon-512 handtekeningen genereert die kleiner zijn dan 1.232 bytes, ontstaan er mogelijk problemen bij key-rollovers. Een DNS-record wordt namelijk vaak met de oude en de nieuwe sleutel gesigneerd, wat bij Falcon-512 een pakket van 1,4 kB oplevert en daarmee een hoger risico op pakketverlies. Rainbow-Ia en RedGeMSS128 genereren op hun beurt weliswaar zeer kleine handtekeningen, maar hun publieke sleutels zijn weer te groot om in een DNS-bericht te passen.

Algoritme	Publieke sleutel	Handtekening	Handtekening/sec	Validaties/sec
Falcon-512	0,9 kB	0,7 kb	~3.300	~20.000
Rainbow-I_a	158 kB	66 B	~8.300	~11.000
RedGeMSS128	375 kB	35 B	~500	~10.000

Figuur 1

Algoritme	Publieke sleutel	Handtekening	Handtekening/sec	Validaties/sec
EdDSA Ed22519	32 B	64 kB	~26.000	~8.000
RSA-2048	0,3 kB	0,3 B	~1.500	~50.000

Figuur 2

CONCLUSIE

Samenvattend stellen de onderzoekers dat geen van de onderzochte algoritmen perfect is voor DNSSEC. Falcon-512 voldoet theoretisch gezien weliswaar aan alle eisen, maar in de praktijk kunnen er wel degelijk problemen ontstaan.
Een oplossing daarvoor zou zijn alle DNS-berichten via TCP te verzenden, maar dit is onhandig omdat onduidelijk is of de nameservers van grote TLD’s en drukke resolvers in staat zijn om grote aantallen TCP-verbindingen efficiënt af te handelen. Dit heeft te maken met de enorme hoeveelheid informatie die servers dan moeten bijhouden om de verbindingen in stand te houden. Rainbow-Ia en RedGeMSS128 lijken meer geschikt voor DNSSEC, maar dan moet er wel een andere, betrouwbare manier worden gevonden om publieke sleutels te verzenden. Omdat de publieke sleutels van deze twee algoritmen niet in een DNS-bericht passen, is het volgens het onderzoeksteam een optie om deze sleutels in segmenten op te splitsen en ieder segment onder een apart domeinnaamlabel te publiceren. Daarvoor moet wel aanvullende informatie aan de berichten worden toegevoegd die de segmenten bevat, zodat een resolver ze weer kan samenvoegen tot één sleutel. Het voordeel is dat de sleutel in-band via het DNS-protocol kan worden verzonden. Het nadeel is dat een resolver meerdere query’s moet verzenden om de sleutel te verkrijgen. Dat vergroot de kans op pakketverlies.
Een alternatief is daarom om publieke sleutels out-of-band buiten het DNS om te verzenden. Resolvers ontvangen dan niet de sleutel zelf, maar alleen een URL. Via een ander protocol, bijvoorbeeld HTTP, kan de resolver de sleutel vervolgens ophalen. Hiervoor moet de resolver wel HTTP ondersteunen en moeten beheerders van nameservers aanvullende hostingservices voor sleutels aanbieden.

ALGORITMEN EVALUEREN

Als vervolgstap willen de onderzoekers de algoritmen evalueren die op dit moment geschikt lijken voor DNSSEC en hoe ze in de praktijk kunnen worden toegepast.
Het onderzoeksteam stelt dat het hoe dan ook zaak is om zo snel mogelijk plannen te maken voor de transitie naar kwantumveilige algoritmen. Het duurde immers ook bijna tien jaar voordat eerdere signaalalgoritmen op grote schaal werden ingezet.

Drukke resolvers valideren duizenden antwoorden per seconde

REACTIES EN BIJDRAGEN

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

AUTEUR

MORITZ MÜLLER is research engineer bij SIDN Labs. Hij schreef deze bijdrage in samenwerking met Jins de Jong (TNO), Maran van Heesch (TNO), Benno Overeinder (NLnet Labs) en Roland van Rijswijk-Deij (NLnet Labs en Universiteit Twente).