3 oktober 2022

Quantumcomputers zorgen voor uitdaging rond informatiebeveiliging

Quantumcomputers hebben de toekomst, maar dat brengt ook vragen met zich mee op het gebied van dataveiligheid. De Radboud Universiteit speelt een rol in het vinden van antwoorden op die vragen, schrijft Innovation Origins.

Veel van onze technologie maakt gebruik van complexe versleutelingen, maar deze zijn door de komst van quantumcomputers niet altijd veilig meer. Voor deze nieuwe vorm van supercomputers is het namelijk heel simpel om de huidige versleutelingen te kraken. Daar moet een antwoord op komen. Een internationaal team van onderzoekers is daarom al bezig de overgang naar veilige datacommunicatie in het 'quantumtijdperk' in goede banen te leiden.

Namens de Radboud Universiteit doet Peter Schwabe hieraan mee. Hij is mede verbonden aan het Duitse Max Planck Instituut en werkt samen met Nederlande onderzoekers van de TU Eindhoven en het Centrum voor Wiskunde en Informatica. Ook al is het in een glazen bol kijken, een wereld met deze 'supercomputers' komt steeds dichterbij. Het is niet uitgesloten dat dit al binnen een periode van vijftien jaar gebeurt, stelt Schwabe.

Grote uitdaging

De uitdaging heeft alles te maken met het algoritme van de Amerikaanse wiskundige Peter Shor, die de zekerheid van de huidige cryptografie teniet wist te doen. Zijn quantumalgoritme slaagde erin de huidige databeveiliging te breken. Daarvoor is dus wel een quantumcomputer nodig.

Maar als die er is, kun je door de huidige beveiliging een streep zetten. De protocollen – voor bijvoorbeeld veilig e-mailverkeer, VPN, online bankieren en e-commerce – worden allemaal waardeloos. In vaktermen is het daarom nodig post-quantumschema's te ontwikkelen die (hopelijk) niet zijn aan te tasten door quantumcomputers.

Algoritmes gekozen

"Er is in 2016 een project gestart door het Amerikaanse National Institute of Standards and Technology (NIST), waarin een standaard ontwikkeld moet worden om digitale communicatie veilig te houden. Er zijn nu recent vier beveiligingsalgoritmes gekozen die bestand zijn tegen de rekenkracht van quantumcomputers", legt Schwabe uit.

De weg die de wiskundigen moesten gaan, was lang. Zes jaar geleden werd begonnen met 69 voorstellen. Daarvan zijn er dus nu vier overgebleven. Drie ervan focussen op een aanpak voor digitale handtekeningen. Dat zijn methodes voor het bevestigen van de juistheid van digitale informatie.

De andere geldt als standaard voor encryptie van publieke sleutels. Een publieke sleutel is een van de sleutels van zogenaamde 'asymmetrische cryptografie'. Bij deze vorm van beveiliging heb je twee sleutels nodig: een voor het vercijferen en een voor het ontcijferen van informatie. De publieke sleutel is degene die bedoeld is om uitgewisseld te worden met degene met wie je wil communiceren. De andere is geheim.

Bescherming tegen aanvallen

De vier winnende algoritmes gaan deel uitmaken van de standaard voor post-quantum cryptografie van NIST. Die is naar verwachting over twee jaar gereed. Er is volgens Schwabe gekozen voor meer dan één winnaar vanwege flexibiliteit. De uitverkoren algoritmes zijn gebaseerd op diverse onderliggende wiskundige problemen, met een verschillende performance, afhankelijk van waarvoor ze worden gebruikt.

"Waarom post-quantumcryptografie zo belangrijk is? Het gaat om de toekomst en het verleden. Denk aan regeringen of belangrijke diensten die zich met een upgrade van beveiliging moeten beschermen tegen toekomstige aanvallen."

Maar, zo waarschuwt Schwabe, het huidig internetverkeer dat nu wordt vastgelegd is ook kwetsbaar. Wat nu geldt als goed beveiligd, is dat in de nabije toekomst niet meer. Dan kan met behulp van quantumcomputers digitale communicatie uit het verleden alsnog worden gekraakt.

Fundamenteel onderzoek

Daarom moet je je nu al zorgen maken over iets wat pas over een aantal jaren speelt. Omdat bijvoorbeeld internetverkeer van nu dadelijk niet meer veilig is. De overgang naar een goede beveiliging gaat lange tijd duren. Standaardisatie, implementatie en adoptie zullen naar verwachting veel tijd in beslag nemen.

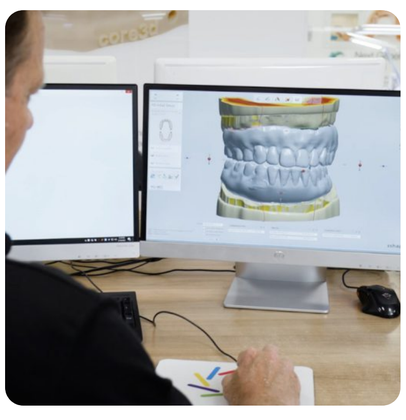
Het bijzondere aan het werk van Schwabe en zijn collega's is dat ze fundamenteel onderzoek verrichten, met als doel iets waar iedereen dadelijk in de praktijk mee krijgt te maken: veilige digitale communicatie in het quantumtijdperk. Dit helpt om gevoelige informatie nu al met post-quantum beveiliging te kunnen versleutelen, zodat deze ook in de toekomst veilig is.

Upgrades

De hiervoor benodigde wiskundige hoogstandjes zijn al snel te ingewikkeld om uit te leggen voor een niet ingewijd publiek. Maar een van de hobbels waarop de onderzoekers stuiten is het praktisch hanteerbaar houden van de algoritmes. Schwabe: "Er zijn afwegingen tussen beveiliging en bandbreedtevereisten, dat wil zeggen grootte en snelheid. Die variëren voor de verschillende benaderingen van post-qantum cryptografie."

Toch moet die beveiliging er komen. "Er zijn meer toepassingen waarbij men niet altijd beseft hoe belangrijk het is dat digitale communicatie veilig verloopt. In principe worden allerlei devices ontwikkeld met de garantie voor updates tijdens de gehele levensduur. Denk aan auto's, die tegenwoordig eigenlijk steeds meer computers op wielen zijn. Ook hiervoor geldt dat het configureren om een auto bij de tijd te houden, veilig moet blijven."

Meer over Health, Hightech, Food



Dit artikel delen

Schrijf u in voor onze nieuwsbrief

Samen werken we aan de toekomst van de regio Arnhem – Nijmegen – Wageningen. Ook op de hoogte blijven? Schrijft u zich dan in voor de maandelijkse update over The Economic Board en de regio.

Naam: Naam
Bedrijfsnaam: Bedrijfsnaam
E-mailadres: E-mailadres
Inschrijven

Inschrijven voor onze maandelijkse nieuwsbrief

Naam:
Naam

Bedrijfsnaam:
Bedrijfsnaam

E-mailadres:
E-mailadres

Inschrijven

Recente berichten

Arbeidsmarktinfarct als 'game stopper' voor innovaties nú samen aanpakken!
Quantumcomputers zorgen voor uitdaging rond informatiebeveiliging
Vijf interessante programma's en subsidiemogelijkheden (vierde kwartaal 2022)
GrondFest is de perfecte plek om met elkaar in gesprek te gaan over de energietransitie
Voor het eerst 3D-geprint klikgebit in Nederland

Toekomstige evenementen

Vakbeurs Energie
11 oktober - 08:00 - 13 oktober - 17:00
Smart Energy Solutions
11 oktober - 13:00 - 16:30
INNOVATE Meet-up Energy
12 oktober - 20:00 - 22:00
Innovatiefste Student van Nederland 2022
27 oktober
De Cirkel 2022
9 november - 16:00 - 19:00

Over Lifeport

Lifeport is een innovatienetwerk van overheid, kennisinstellingen en bedrijfsleven in de regio Arnhem – Nijmegen, met Wageningen. Hier groeien innovaties in de topsectoren Health, Hightech, Food en Energy en de cross-overs daartussen.

Sitemap

Over
Agenda
Nieuws
Vacatures
Parels
The Economic Board
Contact

Doe mee

Download Lifeport Toolbox 1