Publicatie : New Scientist special
Datum : 28 feb 2021 Regio : Nederland Pagina : 30 Bereik : -1
cm2 : 856 Frequentie : incidenteel AVE : € 4538,00 Oplage : 15.000

Klaar voor het postquantum tijdperk

Hoe meer ons leven zich in de digitale wereld afspeelt, hoe groter het belang van digitale veiligheid wordt. Bij het CWI werken **Marten van Dijk** en **Ronald Cramer** samen met hun onderzoeksgroepen hard om te zorgen dat onze bankrekeningen niet worden leeggehaald, we veilig op een virtuele desktop kunnen werken en staatsgeheimen niet op straat belanden.

Tekst: Fenna van der Grient

Alle gevoelige digitale communicatie wordt versleuteld verstuurd. Zo kunnen kwaadwillenden geen informatie onderscheppen of aanpassen. Op die manier kunnen we veilig online bankieren en kunnen burgers, bedrijven en inlichtingendiensten veilig communiceren over internet. De huidige versleutelmethoden zijn zelfs voor de allersnelste supercomputers onkraakbaar. Maar de ontwikkeling van de quantumcomputer vormt een groot gevaar voor deze versleutelmethoden. Zo'n quantumcomputer rekent op een compleet andere manier, waardoor hij de versleutelingen wél kan kraken. Mocht er dus over een tijdje een quantumcomputer zijn met voldoende rekenkracht, dan zijn opeens alle huidige versleutelmethoden onveilig.

Daarom bereidt Ronald Cramer, hoofd van de Cryptology-onderzoeksgroep, ons voor op dit zogeheten postquantumtijdperk. De meningen zijn nogal verdeeld over op welke termijn dit een bedreiging gaat zijn. Volgens de één is er over twee jaar een quantumcomputer die onze huidige versleutelmethoden kan kraken, volgens de ander speelt dit pas over honderd jaar.

Staatsgeheimen

Toch is het zaak om er in alle gevallen op tijd bij te zijn. Ten eerste omdat het een hoop tijd kost om nieuwe versleutelmethoden volledig door te ontwikkelen, zodat je zeker weet dat ze in alle situaties veilig zijn. Vervolgens moet je ze ook nog implementeren. Maar er speelt ook nog iets anders. Bij de meeste communicatie is vooral veiligheid op korte termijn vereist: je moet bijvoorbeeld op dit moment een veilige verbinding met je bank kunnen aangaan om geld over te maken. Als blijkt dat die verbinding over een paar jaar niet meer veilig zal zijn, dan kun je tegen die tijd overstappen op een ander systeem. Vanaf dat moment worden nieuwe banktrans-

Publicatie : New Scientist special
Datum : 28 feb 2021 Regio : Nederland Pagina : 30 Bereik : -1
cm2 : 856 Frequentie : incidenteel AVE : € 4538,00 Oplage : 15.000

acties op een andere manier versleuteld. Een mogelijke aanvaller kan dan niks meer met een bankverbinding die een jaar geleden tot stand is gebracht.

Voor zaken die voor langere tijd geheim moeten blijven, zoals staatsgeheimen of gezondheidsgegevens, is het een ander verhaal. Cramer: 'Zelfs als je denkt dat er pas over vijftig of honderd jaar een quantumcomputer is, dan is het goed dat je er nu mee bezig bent. Alles wat je in de komende decennia versleutelt moet namelijk nog lang daarna veilig zijn.'
Als een kwaadwillende nu een versleuteld staatsgeheim op zijn harde schijf heeft staan, kan hij dat gewoon bewaren en over vijftig jaar, als er een quantumcomputer is, met gemak ontcijferen. Als die informatie op dat moment nog steeds gevoelig is, hebben we een probleem. Informatie die voor langere tijd gevoelig blijft, moet dus eigenlijk nú al op zo'n manier versleuteld worden, dat die zelfs over tientallen jaren nog niet te kraken is. Daarom ontwikkelt Cramer met zijn onderzoeksgroep nieuwe standaardmethoden voor versleuteling die bestand zijn tegen aanvallen van quantumcomputers.

Virtuele omgevingen

Als je al je gegevens goed kunt versleutelen en dus veilig kunt communiceren ben je al een heel eind, maar je bent er nog niet. Meestal wil je namelijk ook nog iets doen met die gegevens: berekeningen uitvoeren of de gegevens verwerken met een programma bijvoorbeeld. Tegenwoordig gebeurt dat lang niet meer altijd op een computer of server die in je werkkamer of in het bedrijfspand staat. Berekeningen, programma's en applicaties worden steeds vaker in de cloud uitgevoerd. Daar zitten voordelen aan: in plaats van dat elk bedrijf zelf een heleboel servers moet hebben staan, delen we alle servers uit datacenters met z'n allen. Heel efficiënt, maar een berekening die in een virtuele omgeving plaatsvindt, is een stuk gevoeliger voor aanvallen dan een berekening die op je eigen afgesloten computer plaatsvindt.

> Een berekening die in een virtuele omgeving plaatsvindt, is een stuk gevoeliger voor aanvallen

Veilige eilandjes

De onderzoeksgroep Computer Security onder leiding van Marten van Dijk houdt zich bezig met de vraag hoe je in zo'n virtuele omgeving toch veilig berekeningen uit kunt voeren. 'De kans is groot dat iedereen in de toekomst een virtuele desktop heeft,' aldus Van Dijk. 'Als daar privacygevoelige informatie of concurrentiegevoelige software op staat, wil je niet dat die gaat lekken.' Wat het ingewikkeld maakt, is dat als je in zo'n omgeving gaat rekenen, je allemaal tussenliggende resultaten krijgt. Die moet je binnen die virtuele omgeving opslaan, en daarmee zijn ze kwetsbaar voor aanvallen van buitenaf. Van Dijk: 'We kijken bijvoorbeeld hoe we binnen zo'n omgeving kleine stukjes van de berekeningen geïsoleerd van alle andere kunnen uitvoeren. Je creëert dan een soort veilige eilandjes. Zelfs als een aanvaller toegang heeft gekregen tot je hele virtuele omgeving, dan zijn die eilandjes nog steeds veilig. Met een slimme combinatie van hardware en software kun je dat voor elkaar krijgen.'

Gesimuleerde Zeus

Een andere uitdaging is een situatie waarin je met meerdere partijen samen een berekening wilt uitvoeren. Stel bijvoorbeeld dat je met verschillende partijen, die elkaar niet vertrouwen, gevoelige informatie wilt verwerken, zonder dat de andere partijen die informatie te zien krijgen. Je kunt bijvoorbeeld denken aan een digitale verkiezing. Hierbij stemt iedere partij, en levert zo dus een brokje informatie in. Al die stemmen samen moeten op een of andere manier verwerkt worden in een gezamenlijke uitslag: wie heeft de meeste stemmen, en hoeveel zijn dat er?

Cramer en collega's ontwikkelen systemen om dit soort berekeningen tussen meerdere partijen mogelijk te maken. Hierbij streven ze een fictief ideaalbeeld na: 'In het ideale geval geven alle betrokken partijen hun informatie aan een bemiddelaar die volledig te vertrouwen is, laten we die Zeus noemen,' zegt Cramer. 'Nou waren de Griekse goden ook niet altijd te vertrouwen, maar laten we even aannemen dat dat wel zo is,' lacht hij. Zeus doet daar een berekening mee, en deelt de uitkomst met alle partijen: de uitslag van de verkiezingen.'

In de praktijk beschik je niet over zo'n bemiddelaar, dus moet je Zeus simuleren. Dit kun je doen door een netwerk te creëren tussen alle partijen, dat als geheel fungeert als een soort Zeus. Iedere partij doet een deel van de berekeningen, communiceert met de andere partijen en voert tests uit. Dat alles samen zorgt voor de gevraagde uitkomst, zonder dat partijen vertrouwelijke informatie van de andere partijen onder ogen krijgen. 'Er zit een hoop wiskunde achter, maar eigenlijk is het ook een beetje magie, dat dat op deze manier kan,' lacht Cramer. 'Het mooie is dat bij een netwerk van ten minste drie partijen, zelfs een oneindig krachtige computer dit systeem niet kan breken.' ■

Fysieke systemen

Het belang van digitale veiligheid speelt ook een grote rol bij fysieke systemen. Zo worden de Deltawerken en het elektriciteitsnetwerk bijvoorbeeld met digitale systemen bestuurd. Als kwaadwillenden daar op kunnen inbreken, zijn de gevolgen desastreus. Daarnaast halen we allemaal steeds meer intelligente systemen in huis, waarvan we ook niet willen dat iemand die kan kraken. Van Dijk ontwikkelt met zijn onderzoeksgroep methoden om dit soort systemen zo goed mogelijk te beveiligen.