Nieuws

AIVD komt volgend jaar met handleiding voor kwantumveilige communicatie

maandag 19 september 2022, 16:34 door **Redactie**, 11 **reacties**

De AIVD zal volgend jaar in samenwerking met TNO en het Centrum voor Wiskunde en Informatica (CWI) een handleiding publiceren voor de overstap naar kwantumveilige communicatie. Daarnaast zullen zowel overheid als bedrijfsleven snel met de migratie moeten beginnen om op de dreiging van kwantumcomputers voorbereid te zijn. Dat laat **staatssecretaris Van Huffelen** van Digitalisering vandaag weten op Kamervragen van de VVD.

Aanleiding voor de vragen was berichtgeving dat het Amerikaanse National Institute of Standards and Technology (NIST) **vier encryptie-algoritmes** heeft gekozen die tegen de rekenkracht van kwantumcomputers zijn opgewassen. "Op welke wijze borgt u tijdig met oplossingen te komen tegen de komst van kwantumcomputers zodat inwoners van Nederland veilig digitaal kunnen communiceren en persoonsgegevens en bedrijfs- en staatsgeheimen goed beveiligd kunnen blijven?", zo wilde VVD-Kamerlid Rajkowski weten.

Volgens Van Huffelen brengt de kwantumcomputer risico's met zich mee op het gebied van informatiebeveiliging. "Sommige cryptografische standaarden die nu veilig worden geacht, zullen door de komst van kwantumcomputers niet meer veilig zijn, waaronder cryptografie die nu veelvuldig wordt gebruikt voor het beveiligen van internetverkeer", aldus de staatssecretaris. "Informatie die gedurende een langere periode vertrouwelijk moet blijven, waaronder staatsgeheimen, moet daarom zo snel mogelijk al beschermd worden tegen store now, decrypt later-aanvallen."

Zowel overheid als bedrijfsleven zullen daarom moeten migreren naar kwantumveilige communicatie. "Deze migratie is omvangrijk, en zal zo snel mogelijk gestart moeten worden om op tijd voorbereid te zijn op de dreiging van quantumcomputers", stelt Van Huffelen. Om bij deze migratie te helpen zal de AIVD in samenwerking met TNO en het CWI een "Quantum Migratie Handleiding" publiceren die overheden, bedrijven en burgers kunnen gebruiken als handvat voor de overstap naar quantumveilige communicatie. De handleiding beschrijft de verschillende doelgroepen en bijbehorende technische stappen die genomen kunnen worden.

Verder meldt de staatssecretaris dat er binnen de verschillende ministeries wordt gewerkt aan een gezamenlijke aanpak van de dreiging van kwantumcomputers. Daarnaast werken experts en cryptologen van de Rijksoverheid ook nauw samen met experts uit de private sector en wetenschap. "Hierbij wordt breder gekeken naar het vraagstuk dan sec de ontwikkeling van cryptografie, maar ook de implementatie in beveiligingsproducten, standaardisering en migratie-adviezen. Die brede inzet moet de komende jaren leiden tot adviezen en producten die overheid, bedrijven en burgers kunnen gebruiken om zich te beveiligen tegen de dreiging van kwantumcomputing", meldt de staatssecretaris.

Rockstar bevestigt inbraak op systemen en diefstal van vertrouwelijke data
School stuurt kinderen naar huis wegens datalek na Microsoft Office-migratie

Reacties (11)

19-09-2022, 16:57 door Anoniem — Reageer met quote

AIVD, amerika ?, backdoor zeker.

19-09-2022, 17:57 door Anoniem — Reageer met quote

Nee hoor

Alle info over hoe NIST tot de nieuwe standaarden is gekomen, dat alles is openbaar. Niet alleen het proces, maar ook de keuzes en de technologie. Wetenschappers uit de hele wereld hebben hieraan bijgedragen.

19-09-2022, 18:09 door Anoniem — Reageer met quote

> *Door Anoniem:* AIVD, amerika ?, backdoor zeker.

In onze provincie vind je inderdaad America.
Maar ik neem aan dat hier geen backdoor gevonden wordt...:-)
https://nl.wikipedia.org/wiki/America_%28Limburg%29

19-09-2022, 18:29 door Anoniem — Reageer met quote

Weet iemand nog hoe Alan Turing de enigma code brak terwijl er een hele zaal wiskundigen met hele mooie diplomas er enkel over zaten te theroretiseren (als Alan niet zo eigenwijs was geweest, nu nòg waarschijnlijk)????

19-09-2022, 18:55 door Anoniem — Reageer met quote

dit heeft niets met AIVD .te maken.
zo als voor kwantum PC bestaat nog geen beveilig software
mag men zich daar wel eerst in verdiepen.

19-09-2022, 22:25 door Anoniem — Reageer met quote

> *Door Anoniem:* Weet iemand nog hoe Alan Turing de enigma code brak terwijl er een hele zaal wiskundigen met hele mooie diplomas er enkel over zaten te theroretiseren (als Alan niet zo eigenwijs was geweest, nu nòg waarschijnlijk)????

Als er één iemand was die vooraan in een zaal wiskundigen zit (en hoort) was het wel Alan Turing.

Ik weet niet waar jij het narratief "Turing was een praktische hacker terwijl de theoreten nog zaten te dromen" vandaan gehaald hebt , maar dat is echt totaal onjuist .
Het beeld van "eigenwijs" snap ik ook niet - hij was een tijd hoofd van 'Hut 8' , de cryptografische sectie van Bletchley Park die werkte aan de 'Naval enigma' .
Voor een verhaal van een "maverick" die naast/buiten de "gevestigde orde" om resultaten haalt moet je echt iemand anders zoeken .

Theoretiseren was de core competentie van Turing - en hij had dus ook alle mooie diploma's - M.Sc King's College Cambridge, PhD wiskunde van Princeton .

Je kunt zelfs wel stellen dat zijn werk aan de theoretische informatica (Universal Turing Machine, halting problem) een grotere en bestendiger 'claim to fame' is dan het werk aan de Enigma.

Een internet vol informatie, en toch slagen mensen erin om zich ervoor af te sluiten en een bekende naam te hangen aan een onzin verhaal omdat het verhaal ze aanspreekt .
Je geloof zeker ook dat Einstein slecht was op school ? [hint : nee - jarenlang beste van de klas]

20-09-2022, 00:55 door Anoniem — Reageer met quote

Grappig.

Tegen de tijd dat er werkelijk functionele quantum computers actief worden, kunnen ze opnieuw beginnen.

Alsof je een SHA-256 handleiding schrijft voor de Eniac.

Even wachten!.. Pizza!!!...

20-09-2022, 09:51 door Anoniem — Reageer met quote

> *Door Anoniem:* Weet iemand nog hoe Alan Turing de enigma code brak terwijl er een hele zaal wiskundigen met hele mooie diplomas er enkel over zaten te theroretiseren (als Alan niet zo eigenwijs was geweest, nu nòg waarschijnlijk)????

Alan Turing was zelf een wiskundige met heel mooie diploma's. Hij kon de enigma-code breken juist omdat hij een uitstekende theoreticus was die bovengemiddeld goed snapte waar hij mee bezig was.

Gisteren om 22:25 heeft iemand hetzelfde in meer detail geschreven.

In het dagelijks taalgebruik wordt het woord theorie vaak gebruikt als iets dat tegenover de praktijk staat. In de wetenschap is dat heel anders, daar beschrijft een theorie de werkelijkheid. Als een theorie blijkt te botsen met de werkelijkheid dan gaat men hard op zoek naar een theorie die wel klopt. Theorieën staan niet los van de praktijk, ze geven ons begrip van de werkelijkheid weer en zijn de basis voor het toepassen van kennis in de praktijk. En reken maar dat dat ook geldt voor hoe Alan Turing en zijn team de enigma-code kraakten.

20-09-2022, 12:31 door Anoniem — Reageer met quote

> *Door Anoniem:* Weet iemand nog hoe Alan Turing de enigma code brak terwijl er een hele zaal wiskundigen met hele mooie diplomas er enkel over zaten te theroretiseren (als Alan niet zo eigenwijs was geweest, nu nòg waarschijnlijk)????

Die heeft Alan nooit (zelfstandig) gebroken. graag de credits geven aan degene die het verdient 'Around December 1932 Marian Rejewski, a Polish mathematician and cryptologist at the Polish Cipher Bureau, used the theory of permutations, and flaws in the German military-message encipherment procedures, to break message keys of the plugboard Enigma machine.'
@https://en.wikipedia.org/wiki/Enigma_machine#Breaking_Enigma - Alan's naam wordt alleen als referentie gebruikt!

20-09-2022, 19:52 door Anoniem — Reageer met quote

> *Door Anoniem:* Grappig.
>
> Tegen de tijd dat er werkelijk functionele quantum computers actief worden, kunnen ze opnieuw beginnen.
>
> Alsof je een SHA-256 handleiding schrijft voor de Eniac.
>
> Even wachten!.. Pizza!!!...

Dat kan je dan ook maar beter doen. Een pizza eten. En niet meer.
OK. Ik ben nu niet aardig. Laat ik me verbeteren.

De kennis dat een quantum computer de huidige asymmetrische algoritmes (op basis van Priemgetallen) kan breken is een resultaat dat de Amerikaans wiskundige Shor heeft beschreven (Shor's algoritme) (kijk even op https://nl.wikipedia.org/wiki/Algoritme_van_Shor en vandaar kan je ook meer gegevens vinden.)

Shor's algoritme zegt niets over de door NIST geselecteerde algoritmes die quantum proof zijn.

Voor het begrip.
Elk algoritme en elke sleutellengte kan in theorie worden gebroken.
Het rekenkracht van een computer is bepalend of die theorie in de praktijk kan worden omgezet.
Als de rekenkracht van een computer in staat gaat zijn om een sleutel te breken, dan besluit men tot langere sleutellengtes. als je dit spel wilt zien, kijk dan eens op keylength.com. Daar zie je modellen waarmee de houdbaarheid in tijd van sleutellengtes voor verschillende soorten algoritmes wordt bepaald (eigenlijk: geadviseerd, gedemonstreerd).

Daartegenover staat dat niet alleen breken van een sleutel heel veel tijd kost (als het goed is ;-)
Ook het vercijferen/ontcijferen van een bericht kost tijd (veel minder dan het breken). De tijd die versleutelen/ontcijferen kost mag weer niet te lang worden. Dat zou veroorzaken dat nieamnd meer comfortabel een computer kan gebruiken. Je kan dus niet ongestraft de sleutellengtes eindeloos groot maken. Daarom zal er een balans moeten zijn tussen de vercijfer/ontcifer tijd en het breken van een sleutel.

De wet van Moore zegt iets over hoe snel de rekenkracht kan toenemen. Ook de wet van Moore geeft daarom informatie over de noodzakelijke lengte van sleutels.

Bovenstaande geldt ook voor quantum computers versus quantum resilient algoritmes
(dit weet ik niet zeker; iemand die het beter weet, laat je horen)

20-09-2022, 21:14 door Anoniem — Reageer met quote

> *Door Anoniem: Vandaag, 19:52*
>
> Dat kan je dan ook maar beter doen. Een pizza eten. En niet meer.
> OK. Ik ben nu niet aardig. Laat ik me verbeteren.

Valt wel mee, vind ik. Wilde er ook nog een regel over de Wet van Moore aan spenderen voor de duidelijkheid, niet gedaan.

Mijn punt is meer dat de quantum computer nog in de kinderschoenen staat en nog niet weten hoe het zich zal ontwikkelen, dus ook niet hoe het in praktijk toegepast gaat worden.

Waardoor het schrijven van die handleiding voorbarig is. Wel een interessant leerproject.

Reageren

Ondersteunde bbcodes

Je bent niet ingelogd en reageert "**Anoniem**". Dit betekent dat Security.NL geen accountgegevens (e-mailadres en alias) opslaat voor deze reactie. Je reactie wordt **niet direct geplaatst** maar eerst gemodereerd. Als je nog geen account hebt kun je hier direct een account aanmaken. Wanneer je Anoniem reageert moet je **altijd** een captchacode opgeven.

Nieuwe code
Herhaal code:
Preview Reageren