Bestrijding kwantumgevaar IT-systemen in internationaal perspectief

Dr. ir. Marc Stevens

Senior onderzoeker Cryptology Group

NWO-I Centrum Wiskunde & Informatica

BIZ & IT —

NSA preps quantum-resistant algorithms to head off crypto-apocalypse

Quantum computing threatens crypto as we know it. The NSA is taking notice.

DAN GOODIN - 8/21/2015, 1:02 PM

VS: Transitie naar kwantum-veilig

VS als eerste in actie:

- 2015 NSA wil transitie naar kwantum-veilige cryptografie
- 2016 NIST start internationale competitie
  voor digitale handtekeningen & encryptie
  - NIST FIPS standaarden verplicht
    voor gehele Fed. overheid & IT-leveranciers

- 2022 NIST kondigt 4 draft standaarden aan, 2024 klaar op papier
  (ontworpen o.a. door CWI NXP TU/e)
- 2022 Wet Quantum Computing Cybersecurity Preparedness Act

President Biden Signs Quantum Computing Cybersecurity Preparedness Act

BY MATT SWAYNE • DECEMBER 22, 2022 • NATIONAL

VS: Transitie naar kwantum-veilig

2022 Wet Quantum Computing Cybersecurity Preparedness Act

Horizon: mitigeer kwantum risico voor 2035

Acties: voor alle overheidsorganisaties:

1. **Inventarisatie**
   - Wijs Inventaris & Migratie lead aan (binnen 30 dagen)
   - Inventariseer (volgens normen van OMB/CISA)
2. **Jaarlijks rapporteren**
   - Inventaris cryptografische systemen (mei ‘23)
   - Rapporteer geschatte kosten transitie (juni ‘23)
3. **Plan migratie & start uitvoering**
   - 1 jaar na OMB/NIST nieuwe standaarden (‘25)
   - Gedirigeerd samen met OMB vanwege interoperabiliteit
   - Nu al testen met pre-standaarden

EU: Transitie naar kwantum-veilig

DE-BSI / FR-ANSSI / NL-NBV

- Volgen veelal NIST standaardisatie

- Verantwoordelijk voor Normen & certificering IT voor *gerubriceerde informatie*

- Voor gehele overheid & bedrijfsleven:
  - Generiek advies kwantum-veilige cryptografie & migratie
    1. **Vorm** migratieteam en start met **inventarisatie**
    2. **Planning**: maak tijdspad op basis van risico afweging
    3. **Executie**:
       - Standaarden & kennis nog niet klaar
       - Test met pre-standaarden

EU: Transitie naar kwantum-veilig

Knelpunten die de transitie kunnen vertragen in NL/DE/FR/EU:

1. Overheidsinstellingen zijn zelf verantwoordelijk voor migratie strategie
2. Tekort aan centrale sturing voor interoperabiliteit tussen IT-systemen en tussen overheidsinstellingen
3. Geen centraal migratie expertise centrum voor toegespitste adviezen & oplossingen
   - Moeilijker om kennis samen te brengen en nieuwe kennis te ontwikkelen
4. Expertise is schaars & nog onvolledig
   - Meer educatie nodig
5. Geen gestelde horizon voor bedrijven
   - AVG? …

Gevaar in Blindspots

- Internationale focus op *digitale handtekeningen & encryptie*
  - Veruit het belangrijkste voor digitale samenleving !

- Echter sectoren zitten vast aan eigen protocol standaarden
  - Internet: TLS, DNSSEC, IPsec, VPN, …
  - Banken: EMV, Telecom: 5G, Smart grid
  - Overheid: DigiD, eHerkenning, …
  - Nieuwe sector-specifieke standaarden moeten ontwikkeld worden!
  - NIST standaarden mogelijk niet geschikt voor sector-specifieke eisen
    - Inventariseer & plan
    - Begin zo snel mogelijk: mogelijk nieuw onderzoek oplossing nodig!

Gevaar in Blindspots

- Andere cryptografie is ook kwantum onveilig
  - Met name geavanceerde privacy-versterkende cryptografie
    - Polymorfe identiteiten & pseudonymen
    - Homomorfe encryptie
    - Blockchain/DLT technieken & applicaties

- Vervangde cryptografie moet veelal nog ontwikkeld worden!
- Inventariseer
  & investeer in onderzoek toekomstbestendige oplossingen!

Conclusie

Sinds 2015 is Verenigde Staten een leider in de transitie naar kwantum-veilige IT

Nederland mist centraal beleid voor transitie:

- Voor: IT gehele overheid
- Voor: bedrijven duidelijkheid in relevante wetgeving (AVG, …)
- Door: **horizon voor kwantum-veilige beveiliging**
- Door: **korte termijn acties**: inventarisatie, stappenplan, middelen vrijmaken, educatie

Gevaar in blindspots:
Slechts digitale handtekeningen & encryptie niet genoeg!

- Nieuwe sectorspecifieke standaarden: banken, telecom, energiemeters, …
- Nieuwe geavanceerde cryptografie: o.a. DigiD IRMA Herkenning BLOCKCHAIN
- Actie: **inventariseer** & **investeer**: **nieuw onderzoek nodig**

Achtergrond: Cryptografie

- **Symmetrisch**: beide partijen hebben **dezelfde geheime sleutel**
  - Bijvoorbeeld: Encryptie, Authenticatie
  - Probleem: hoe komen ze aan een gedeelde geheime sleutel?
  - Impact kwantum beperkt: mogelijk grotere sleutels aangeraden

- **Asymmetrisch**: Elke partij heeft een **publieke sleutel** en een **geheime sleutel**
  - Encryptie kan met publieke sleutel, decryptie met geheime sleutel
  - Handtekening zetten met geheime sleutel, controleren met publieke sleutel
  - Dé oplossing voor grootschalige internet communicatie
  - Kwantum onveilige oplossingen: gebaseerd op RSA, ECC
  - Kwantum veilige oplossingen: gebaseerd op roosters, hashes, codes

Achtergrond: Quantum Key Distribution

Quantum Key Distribution (QKD)

- **Quantum** protocol om sleutels uit te wisselen
- Vergelijkbaar met sleutel uitwisselen via koerier, maar dan met bijv fotonen
- Afluisteren is destructief: fotonen komen niet aan
- Vereist nog steeds authenticatie mbv extra crypto (sym of asym)
- Slechte schaalbaarheid voor IT systemen:
  - Vereist dure quantum infrastructuur: glasvezel & end-point apparatuur
  - Kan niet over standaard IT infra: netwerkkabels of radio (wifi, mobiel)
  - Mogelijk geschikt voor site-2-site oplossingen
  - Niet geschikt voor gros van IT systemen
    - communicatie tussen backend en applicatie op device (pc, laptop, mobiel) gaat veelal via standaard IT infrastructuur
- Alle grote beveiligingsdiensten raden nu QKD af voor eigen overheid (zie quotes volgende slides)

Achtergrond: Quantum Key Distribution

US-NSA

NSA does not support the usage of QKD or QC to protect communications in National Security Systems:

1. QKD is only a partial solution
2. QKD requires special purpose equipment
3. QKD increases infrastructure costs and insider threat risks
4. Securing and validating QKD is a significant challenge
5. QKD increases the risk of denial of service

DE-BSI

1. Post-quantum algorithms are much more flexible, as they can be implemented in existing infrastructure, they are more cost-effective, do not require secret pre-distributed keys and offer end-to-end security
2. QKD is subject to some restrictions and is therefore only suitable for certain application scenarios
3. Standards, for example on protocols, and certified products are still lacking
4. QKD should only be used in hybrid mode with classical and post-quantum key agreement schemes

https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Brochure/quantum-safe-cryptography.html?nn=916626

Achtergrond: Quantum Key Distribution

FR-ANSSI

1. The use of state-of-the art classical cryptography including post-quantum algorithms is by far the preferred way to ensure long-term protection of data, as it is the only technology choice that offers the functional properties needed in modern communication systems
2. Deployment constraints specific to QKD hinder large-scale deployments with high practical security
3. The cost incurred by the use of QKD should not jeopardize the fight against current threats to information systems

UK-NCSC

1. NCSC advice is that the best mitigation against the threat of quantum computers is quantum-safe cryptography
2. NCSC does not endorse the use of QKD for any government or military applications
3. NCSC cautions against sole reliance on QKD for business-critical networks, especially in Critical National Infrastructure sectors
4. More research is needed to understand how QKD protocols can be implemented and integrated into these complex systems of classical components, such that the whole system is secure against an appropriate threat model

https://www.ssi.gouv.fr/uploads/2020/05/anssi-technical_position_papers-qkd.pdf
https://www.ncsc.gov.uk/pdfs/whitepaper/quantum-security-technologies.pdf