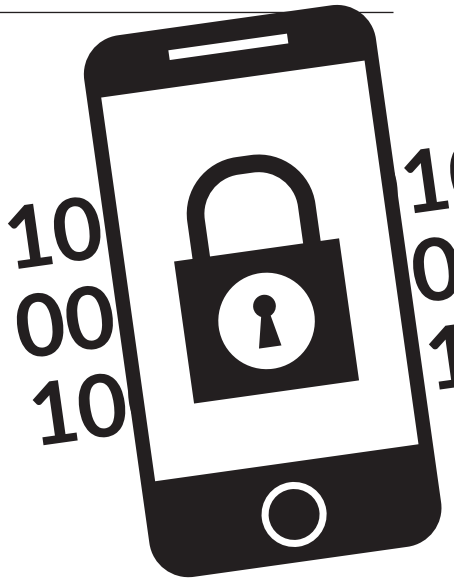
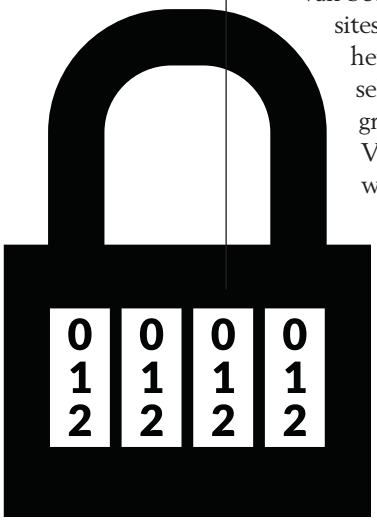


Het belang van cryptografie voor de samenleving

EEN KWESTIE VAN TOEVAL

WE ZIJN GEWEND AAN WINKELEN VIA INTERNET, GELD UIT DE MUUR EN SMARTCARDTOEPASSINGEN ZOALS OV-CHIP EN BETAAL-TV. WEINIG MENSEN REALISEREN ZICH ECHTER WELKE TECHNOLOGIE NODIG IS OM ERVOOR TE ZORGEN DAT DERGELIJKE TOEPASSINGEN VEILIG ZIJN. TECHNOLOGIE IS ECHTER EEN TWEESNIJDEND ZWAARD EN STEEDS MEER CYBERINCIDENTEN HALEN HET NIEUWS. DIT ARTIKEL GEEFT AAN WELKE BEVEILIGINGSMOGELIJKHEDEN CRYPTOGRAFIE BIEDT EN WAAROM DE KWANTUMCOMPUTER DIE BEVEILIGING ONDER DRUK ZET.

door Henk-Jan van der Molen beeld Shutterstock



Als we online een goede aanbieding hebben gevonden, kunnen we meestal meteen afrekenen. Dat houdt de kosten laag voor de leverancier, die op zijn beurt zijn marktaandeel kan vergroten door zijn klanten het prijsvoordeel te geven. Tegelijkertijd mogen cybercriminelen geen kans krijgen om misbruik te maken van betalingsgegevens. Vandaar dat sites de data beveiligen die via het internet worden uitgewisseld, herkenbaar aan het groene 'slotje' in de adresbalk. Voor het inloggen op een webwinkel moet je als klant een identiteit en een wachtwoord invoeren. Meestal bestaat de identiteit uit het e-mailadres van de klant, die de leverancier koppelt aan het klantaccount. De klant kiest daarna zijn wachtwoord, waarmee hij later opnieuw kan inloggen op de website. Webwinkels moeten dus ook de opslagen klantgegevens geheimhouden. Ondertussen heeft Europa de Algemene verordening gegevensbescherming (AVG) aangenomen, die eist dat privacygevoelige data 'aantoonbaar goed beveiligd' zijn. Maar hoe veilig is die beveiliging eigenlijk?

... CRYPTO, ANYONE?

Je kunt wachtwoorden rechtstreeks opslaan in de klantendatabase, maar dan kunnen databasebeheerders die wachtwoorden uitlezen. De wet van Murphy geeft aan dat als er een kans is dat iets fout kan gaan en je wacht lang genoeg, dan gaat het een keer fout.
Gelukkig kan cryptografie die kans op misbruik van wachtwoorden fors verminderen met zogenaamde hashfuncties. Een hashfunctie vertaalt een invoertekst naar een pseudo-willekeurige tekst met een vaste lengte, zodanig dat het bijzonder lastig is om vanuit de output de input te bepalen. Daarom kan de hashwaarde van

AUTEUR

HENK-JAN VAN DER MOLEN
heeft elektrotechniek en ICT-systeemontwikkeling gestudeerd. Hij werkt inmiddels 25 jaar in de ICT-branche, waarvan de laatste 15 jaar in het vakgebied van informatiebeveiliging en privacy. Naast een reguliere baan werkt hij onder andere als freelancedocent bij de Security Academy.

In het post-kwantumtijdperk zijn veel asymmetrische encryptiemethoden niet langer veilig

een wachtwoord wel veilig worden opgeslagen in de klantendatabase. Als de klant opnieuw inlogt, wordt het ingevoerde wachtwoord gehasht en vergeleken met de opgeslagen hashwaarde van zijn wachtwoord in de database. Als beide hashwaarden gelijk zijn, is de kans bijna 100% dat die persoon het juiste wachtwoord heeft ingevoerd. Met nadruk 'bijna 100%', omdat bijvoorbeeld de MD5-hashfunctie élke invoer converteert naar 16 bytes. Er zijn bijvoorbeeld meer 20-karakterwachtwoorden uit cijfers, leestekens, hoofd- en kleine letters te maken dan er past in 16 bytes.
Een hashfunctie kan dus dezelfde output produceren, ook al verschilt de input. De veiligheid blijft echter gegarandeerd zolang het praktisch onmogelijk is om vanuit een hashwaarde het wachtwoord te reconstrueren. Maar er is meer nodig dan een goede hashfunctie, zoals SHA-256. In 2012 bemachtigden hackers de LinkedIn-database met alle gebruikersnamen en gehashte wachtwoorden. Veel mensen kiezen een makkelijk wachtwoord. '123456' is al jaren het meest gebruikte wachtwoord. Het bleek dat de meest voorkomende hashwaarden van wachtwoorden in de LinkedIn-database goed overeenkwamen met de Wachtwoord Top 20.
Hoe moet het dan wel? Je voegt 'zout' toe aan de invoer van de hashfunctie. Per gebruiker genereer je een willekeurig getal dat je toevoegt aan het ingevoerde wachtwoord. Daarna sla je de hashwaarde met de zoutwaarde op in de database. Doordat iedere gebruiker een willekeurige zoutwaarde heeft, kun je geen top 20 van wachtwoordhashes meer maken.

PROBLEMEN BIJ GROOTSCHALIG GEBRUIK VAN SYMMETRISCHE ENCRYPTIE

Al eeuwen is het mogelijk vercijferde informatie uit te wissen als twee partijen samen een cryptosleutel afspreken. Omdat beide partijen dezelfde sleutel gebruiken, wordt dit symmetrische encryptie genoemd. Maar als we eisen dat de sleutel van Alice en Bob anders moet zijn dan tussen Alice en Chris, lopen we tegen een probleem aan: het aantal tweetallen dat je uit een groep kunt trekken, neemt snel toe als de groep groter wordt. Voor een gebruikersgroep van 10 personen zijn 45 sleutels nog voldoende. Maar als de groep gebruikers toeneemt tot 1.000 personen, zijn er al 499.500 symmetrische sleutels nodig. Op landelijke schaal wordt de verstrekking van symmetrische sleutels (via een ander medium dan het internet!) en het sleutelbeheer onbetaalbaar.

DE OPLOSSING: PUBLIC KEY INFRASTRUCTURE

Sinds 1970 is er een alternatief voor symmetrische encryptie ontwikkeld die bekendstaat als public key infrastructure. (PKI). Iedere gebruiker heeft een sleutelpaar met een publieke en een geheime

sleutel. Als Bob aan Alice een bericht wil sturen, downloadt hij de publieke sleutel van Alice en vercijfert daarmee zijn bericht. Alice is dan de enige die Bobs bericht kan ontcijferen met haar geheime sleutel. Het asymmetrische RSA-algoritme werkt bijvoorbeeld zo: je neemt twee willekeurige priemgetallen (p, q) die je met elkaar vermenigvuldigt om de zogenaamde modulus (N=p*q) te berekenen, zoals 11 en 13. Daarna kies je een ander priemgetal als onderdeel van de openbare sleutel (e), zoals 7. Als laatste stap zoek je het resterende deel (d) van de geheime sleutel, die voldoet aan een rekenkundige voorwaarde, zoals 103.

De wiskundige magie van PKI-encryptie is dat als je tekst vercijfert met de publieke sleutel (e, N), dan kun je die ontcijferen met de geheime sleutel (d, N) en vice versa.

PKI blijft veilig zolang de priemfactoren (p, q) van de openbare modulus N geheim blijven. In de praktijk zijn p en q getallen met honderden cijfers. Een computer kan het product N=p*q snel berekenen, maar om uit die N weer p en q te halen, is een heel langdurige rekenoperatie. Tenminste, voor een conventionele computer.

KWANTUMCOMPUTER

De steeds toenemende rekenkracht maakte het al nodig dat encryptiesleutels periodiek worden verlengd om informatie geheim te houden. Het volume aan mogelijke sleutelwaarden moet zo groot zijn dat cybercriminelen met 'brute force'-aanvallen alleen met heel veel geluk en toeval de beveiliging kunnen doorbreken. Zodra er echter een kwantumcomputer met voldoende rekenkracht ontwikkeld wordt, ontstaat een trendbreuk die direct grote invloed heeft op de lengte van symmetrische sleutels en de asymmetrische encryptiemethoden. De kwantummechanica stelt dat een elementair deeltje zich in superpositie of meerdere toestanden tegelijk kan bevinden. Met twee mogelijke toestanden tegelijk neemt met elk toegevoegd deeltje het aantal toestanden van de deeltjesverzameling met een factor 2 toe. In een kwantumcomputer kan een zogenaamde qubit gelijktijdig 0 en 1 zijn. De rekenkracht van een kwantumcomputer is dus exponentieel evenredig met het aantal qubits. Met voldoende qubits kan een kwantumcomputer sommige rekenproblemen veel efficiënter oplossen dan conventionele computers, zoals factorisatie, het zoeken in grote databases en het simuleren van moleculaire bindingen. Kwantumdeeltjes zijn inherent wispelturig en het is bijzonder moeilijk om meerdere qubits zolang stabiel te houden dat je ermee kunt rekenen. Met wetenschappelijk onderzoek lukt het om steeds meer qubits langer te stabiliseren. Intel en IBM kondigden begin 2018 chips aan met 49 en 50 qubits. Na 50 logische qubits komen we in het 'quantum supremacy'-gebied en kunnen we zo'n kwantumcomputer niet meer simuleren op een conventionele computer.

POST-KWANTUM-ENCRYPTIE

In het post-kwantumtijdperk (PQ) zijn veel asymmetrische encryptiemethoden niet langer veilig. Vanuit lopende onderzoeken en competities zijn al enkele asymmetrische PQ-encryptiemethoden ontwikkeld waarvoor nog geen efficiënte kwantumrekenmethode bestaat, maar die vergen meer rekenkracht en soms veel langere sleutels. Met voldoende lange sleutels zijn bestaande methoden zoals AES en SHA voorlopig nog veilig.

We moeten dus de ontwikkeling van de kwantumcomputer proactief monitoren. Momenteel worden al grote hoeveelheden vercijferde bestanden verzameld, met het idee dat een kwantumcomputer die later kan ontcijferen. Als je zeker wilt weten dat informatie ook na circa 2025 geheim blijft, moet je dus nu al PQ-encryptiemethoden gebruiken. Van technologie kun je nooit de veiligheid bewijzen, maar alleen de onveiligheid. De AVG eist een 'aantoonbaar goede beveiliging', wat hier betekent: faseer cryptografie (zoals eerder SSL) zó snél mógelijk uit nadat die onveilig is gebleken. Een goede beveiliging vraagt dus om flexibiliteit.