Juryrapport
Internetscriptieprijs 2016
Internet & Technische Wetenschappen

Quantum computing is een van de grote wetenschappelijke onderwerpen van dit moment, waar wereldwijd door overheden veel geld in gestoken wordt. Om quantum computing te realiseren zijn verschillende technische doorbraken nodig, waar fysici hard aan werken. In Nederland gebeurt dat vooral in Delft, waar men een internationale koppositie heeft.

Hoewel er dus nog geen echte quantum computers zijn, bestaat de wiskunde van quantum computing al wel. Op theoretisch niveau kan geanalyseerd worden wat een eventuele quantum computer zou kunnen doen. Dat is tegelijkertijd goed en slecht nieuws voor het vakgebied computerbeveiliging. Het is slecht nieuws omdat een aantal veelgebruikte public key crypto systemen, zoals RSA, kwetsbaar zijn voor quantum computers. Die computers kunnen namelijk bepaalde operaties, zoals het factoriseren van priemgetallen veel sneller uitvoeren dan traditionele computers. Het goed nieuws is dat met quantum computers ook nieuwe algoritmen mogelijk zijn, zoals quantum key exchange.

Doordat quantum computers "slecht" nieuws zijn voor public key crypto systemen is er een nieuwe onderzoeksrichting ontstaan die "post quantum crypto" heet. Het gaat daarbij om het ontwikkelen van nieuwe algoritmen die bestand zijn tegen quantum computing. Dat wil zeggen: ze blijven veilig ook als fysici er ooit in slagen een quantum computer te bouwen.

Dit gebied post quantum computing is in korte tijd enorm gegroeid en heeft tot veel nieuwe ideeën geleid. Zo hebben twee Nederlandse onderzoekers, Peter Schwabe en Leo Ducas, samen met twee buitenlandse collega's het afgelopen jaar de Internet Defense Prize gewonnen (van 100.000 dollar) voor een nieuw algoritme "new hope". Dit wordt nu geïmplementeerd in de Chrome browser van Google. Peter Schwabe heeft hier overigens ook de Dutch Prize for ICT Research 2017 gewonnen. U ziet, dit post quantum crypto is een goed onderwerp als u in de prijzen wil vallen.

Zo ook de kandidaat van vandaag, **Simon de Vries** van de Universiteit Twente. Ook hij heeft een implementatie gemaakt van een bestaand post quantum public key algoritme, namelijk McEliece, in OpenVPN. Eigenlijk is niet McEliece geïmplementeerd, maar een variatie die Niederreiter genoemd wordt, maar dat terzijde. Deze VPN software wordt door de Nederlandse overheid en door veel andere partijen gebruikt voor het beveiligen van hun verbindingen. Deze implementatie is een van de twee bijdragen van deze scriptie.

De andere bijdrage van de scriptie zit in het analyseren van hoe de paramaters voor Niederreiter het beste gekozen kunnen worden. Het nadeel van Niederreiter is dat de sleutels erg groot zijn, namelijk meer dan een megabyte. In de scriptie wordt deze sleutellengte met 35% gereduceerd door een gedetailleerde analyse van een bekende aanval met gebruik van Shor, waardoor de parameter zuiniger gekozen konden worden. Hierbij is voortgebouwd op een suggestie van de Eindhovense cryptograaf Dan Bernstein.

Simon de Vries schreef zijn scriptie getiteld *Achieving 128-Bit Security. Against Quantum Attacks In Openvpn* in het kader van zijn masterstudie Computer Science (Kerckhoffs Master

program in computer security) aan de Universiteit Twente en in nauwe samenwerking met het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De jury is zeer onder de indruk van deze ver boven de andere inzendingen uitstekende scriptie en kent de Internetscriptieprijs Internet en Techniek, beschikbaar gesteld door Greenhost, met veel genoegen aan Simon de Vries toe.

Prof. dr. J.C.M. (Jos) Baeten, algemeen directeur Centrum Wiskunde & Informatica Amsterdam, hoogleraar theory of computing Universiteit van Amsterdam
Prof. dr. B.P.F. (Bart) Jacobs, hoogleraar beveiliging en correctheid van programmatuur Radboud Universiteit Nijmegen

De jury vergaderde op 2 maart 2017 onder leiding van Prof. dr. G. van Dijk, oud-secretaris natuurwetenschappen KHMW; daarnaast namen deel aan de vergadering Prof. mr. A. Soeteman, secretaris geestes- en maatschappijwetenschappen en Drs. S. van Manen, secretaris (notulen).