Juryrapport
Kees Schouhamer Immink Prijs 2019

Laureaat: Dr. ir. R.M. (Roland) van Rijswijk-Deij, NLnet Labs & Universiteit Twente

Het Domain Name System, ofwel kort DNS, is verantwoordelijk voor het vertalen van de webadressen waar we mee vertrouwd zijn, bijvoorbeeld ns.nl, naar de interne IP adressen in het Internet, in dit geval het adresnummer 176.34.128.145. We moeten erop kunnen vertrouwen dat een indringer niet stiekem een ander IP adres injecteert in plaats van het werkelijke IP adres van de website die we willen bezoeken. Dit is belangrijk omdat bijvoorbeeld cybercriminelen met valse, maar bijna echt lijkende websites, gebruikers allerlei persoonlijke data afhandig kunnen maken. Lang werd gedacht dat dit vertaalsysteem veilig was. Groot was dan ook de schrik toen enkele jaren geleden werd aangetoond dat de caches die werden gebruikt om het DNS sneller te maken, tegelijk een achilleshiel waren en dat het toch mogelijk was om in te breken.

Het antwoord van de Internetgemeenschap was de introductie van een veiliger systeem, genaamd DNSSEC, waarbij versleuteling van de informatie moet zorgen voor authenticiteit en integriteit van de DNS-data, waardoor zekerheid wordt verkregen dat de website die aangegeven is ook de juiste is die op het scherm verschijnt. Brede uitrol van DNSSEC gaat echter moeizaam omdat door het toevoegen van encryptie de lengte van de boodschappen significant toeneemt, waardoor het web trager worden. Verder kan DNSSEC worden gebruikt voor grootschalige vijandige aanvallen op websites, de zogenaamde Distributed Denial of Service (DDoS) attacks, waardoor deze onbereikbaar worden.

Het onderzoek van Roland van Rijswijk-Deij is gericht op het oplossen van dit probleem. Allereerst heeft hij door middel van grootschalige metingen en modelmatige analyse de tekortkomingen van DNSSEC in kaart gebracht en onderbouwde oplossingen voorgesteld. De blijvende impact van dit onderzoek blijkt uit het feit dat het werk van Roland van Rijswijk-Deij tot wijzigingen in de Internet standaarden heeft geleid en dat hij daarvoor in 2015 en 2017 is onderscheiden met de Applied Networking Research Prize.

Een tweede belangrijke bijdrage van Roland van Rijswijk-Deij is dat hij heeft aangetoond dat de toepassing van een andere methode van versleuteling van de DNS-data die gebaseerd is op Elliptic Curve Cryptography (ECC) kan bijdragen aan een beter acceptatie van DNSSEC. Deze methode heeft significant kleinere boodschappen, maar heeft als nadeel dat de ontcijfering twee ordes van grootte langer duurt dan de huidige methode van versleuteling. Roland toont echter in zijn proefschrift aan dat dit in de praktijk niet tot onoverkomelijke problemen hoeft te leiden.

Het onderzoek van Roland van Rijswijk-Deij zou niet mogelijk zijn geweest zonder grootschalige metingen aan het DNS-systeem. Hij heeft een meetplatvorm ontwikkeld, genaamd “openINTEL” dat in staat is dagelijks 60% van alle DNS-domeinnamen te meten zonder het DNS-systeem noemenswaardig te verstoren. Dit systeem is van grote waarde voor verder onderzoek en is publiek beschikbaar.

De jury is unaniem van mening dat het onderzoek van Roland van Rijswijk-Deij bij uitstek voldoet aan de criteria van de Kees Schouhamer-Immink prijs: inventiviteit, efficiëntie en schaalbaarheid, creativiteit, maatschappelijke relevantie en wetenschappelijk perspectief.

Prof. dr. C.M. (Catholijn) Jonker, hoogleraar interactie intelligence group Technische Universiteit Delft
Prof. dr. B.P.F. (Bart) Jacobs, hoogleraar beveiliging en correctheid van programmatuur Radboud Universiteit Nijmegen
Prof. dr. ir. H.J. (Henk) Sips, hoogleraar programmatuuraspecten van parallelle en gedistribueerde systemen Technische Universiteit Delft

De jury vergaderde op 5 november 2019 onder leiding van Mr. C.G.A. van Wijk, oud-bestuurslid KHMW. Tevens waren ter vergadering aanwezig Prof. dr. A.P. IJzerman, secretaris natuurwetenschappen KHMW en Drs. S. van Manen, secretaris.