

Juryrapport

Internetscriptieprijs Internet & Technische Wetenschappen 2016

Nederland wil zich internationaal graag profileren als een safe place to do business, om meer bedrijvigheid in de digitale economie aan te trekken. Niet alleen heeft ons land snelle internetverbindingen en grote datacenters, maar ook hebben wij onze digitale beveiliging op orde. Dat is de boodschap die graag afgegeven wordt.

Om deze mooie ambitie enige geloofwaardigheid te geven moeten veel partijen samenwerken en hun zaakjes ook daadwerkelijk op orde hebben. Jurylid Bart Jacob is zelf lid van de nationale Cyber Security Raad en ziet daar hoe belangrijk digitale hygiëne is. Een cruciale rol in het “schoon” houden van het digitale speelveld in Nederland is weggelegd voor SIDN, de Stichting Internet Domeinregistratie Nederland, die verantwoordelijk is voor het uitgeven van webadressen, zoals khmw.nl. Die uitgifte wordt in de praktijk geregeld via zogenaamde registrars, waarvan er wereldwijd zo'n 1500 actief zijn in 27 landen. Het registeren van een domeinnaam in Nederland is voor een groot deel een geautomatiseerd proces, waardoor soms willekeurige reeksen letters en cijfers als domeinnaam aangevraagd worden. Het is belangrijk ervoor te waken dat er geen “foute” webadressen uitgegeven worden.

Maar wat is “fout” en hoe herken je dat? Dit is het onderwerp van de masterscriptie van Moritz Müller van de Universiteit Twente. De domeinen worden “fout” genoemd als ze gebruikt worden voor phishing, spam of DDOS, voor botnets, of voor andere kwaadaardige activiteiten. De scriptie van Moritz beschrijft een zoektocht naar karakteristieken voor zulke webdomeinen en beschrijft een tool dat hij zelf gebouwd heeft om foute domeinen automatisch te kunnen vinden. Dit is nieuw en nog niet eerder gedaan voor het .nl domein.

De jury is onder de indruk van deze scriptie. Om te beginnen is de scriptie bijzonder zorgvuldig geschreven en vormgegeven, en daarmee een plezier om te lezen. Er wordt uitgebreid gebruik gemaakt van de beschikbare literatuur, hetgeen duidt op belezenheid en kennis van zaken van de auteur. Wij academici waarderen zo iets. De scriptie bevat een goede omschrijving van het DNS systeem, van verschillende vormen van misbruik, en van de karakteristieken daarvan. Daarnaast heeft de schrijver de opgedane kennis ondergebracht in een eigen tool, waarmee in de grote hoeveelheid gegevens gezocht kan worden naar phishing websites in het bijzonder.

Deze tool maakt gebruik van dataclassificatie, en is een toepassing van “big data” in het security domein. Het is geschreven in de programmeertaal Python, en heeft geen gladde user-interface, maar werkt gewone vanaf de command-line. Zo zien wij informatici het toch het liefst. Deze tool, SIDeKlck genaamd, is erg succesvol bij het detecteren van kwaadaardige domeinen wanneer de registratie-informatie als uitgangspunt genomen wordt, maar werkt minder overtuigend wanneer gekeken wordt naar de DNS-opvragingen bij een Authorative Name Server (AuthNS). Dat laatste is misschien een beetje jammer. Maar op een hoger plan is het een teken van goed onderzoek, waarbij duidelijk onderbouwd wordt wat wel werkt en wat niet.

Kortom, alle lof voor Moritz Müller zelf, voor de begeleiders Andreas Peter van de Universiteit Twente en Maarten Wullink van SIDN. Onze felicitaties met deze prijs!

Prof. dr. J.C.M. Baeten, algemeen directeur Centrum Wiskunde & Informatica Amsterdam, hoogleraar theory of computing Universiteit van Amsterdam

Prof. dr. B.P.F. Jacobs, hoogleraar beveiliging en correctheid van programmatuur Radboud Universiteit Nijmegen

De jury vergaderde op 15 februari 2016 onder leiding van Prof. dr. G. van Dijk, oud-secretaris natuurwetenschappen KHMW; daarnaast waren ter vergadering aanwezig de secretaris geestes- en maatschappijwetenschappen, Prof. mr. A. Soeteman, en secretaris Mevr. Drs. S. van Manen (notulen).