

Juryrapport

KNVI Scriptieprijs voor Informatica en Informatiekunde 2017

1^e prijs Jos Wetzels (Technische Universiteit Eindhoven)

KINTSUGI Identifying & addressing challenges in embedded binary security

Bij het nomineren van kandidaten voor scripties wil de indiener wel eens overdrijven. Deze keer was geen uitzondering. Vertaald vanuit het Engels ging het ongeveer als volgt: “De afstudeerscriptie van Jos Wetzels is niet alleen de beste afstudeerscriptie die ik heb mogen begeleiden, het is zelfs de beste afstudeerscriptie die ik ooit in mijn leven heb gezien.” Het houdt ook niet op: “Het aantal resultaten en de diepgang, de uitgebreidheid en precisie van de realisatie en validatie, de kwaliteit van wat er getoond is, het aantal en de accuratesse van de referenties (480) zie je alleen maar bij een heel goed proefschrift”.

Inderdaad, nogal overdreven, maar volgens de jury niet buitengewoon veel. Jos Wetzels heeft een uitzonderlijke prestatie geleverd, en de juryleden waren unaniem in hun oordeel, en ook zonder noemenswaardige discussie. Dit was de evidente nummer 1.

Waar gaat het om? Computers zijn kwetsbare apparaten, vooral als ze zijn aangesloten op het internet. Laten we vaststellen dat er nog maar heel weinig computers zijn die niet aangesloten zijn op het internet. Dat netwerk biedt allerlei mogelijkheden om een computer te besmetten met programmatuur die je er niet op wilt hebben, in het bijzonder programmatuur die de oorspronkelijke werking teniet doet. Normaal gesproken kun je op allerlei manieren bescherming bieden, vooral door hardwarematige barricades op te werpen die besmettingen vaak afdoende tegen kunnen houden. Echter, hele kleine computers, zoals dikwijls ingebed in auto's, robots, uw elektriciteitsmeter, TV's, bewakingscamera's, moderne deursloten en pacemakers, hebben deze hardware beschermingen niet, of anders in mindere mate. Daar is domweg geen ruimte voor, of vereist teveel van een systeem om er goed gebruik van te maken. Voor deze minder beschermde computers moeten speciale maatregelen genomen worden. Feitelijk komt het erop neer dat je moet voorkomen dat specifieke programmatuur ingebracht door een aanvaller überhaupt uitgevoerd kan worden. Dat dit relevant is, zal snel duidelijk worden als u zich realiseert dat veruit het overgrote deel van computers juist tot deze categorie van kwetsbaren behoren. Daar komt mogelijk de komende jaren verandering in, maar zover is het nog lang niet. Tot dan zullen we het moeten doen met technieken gericht op het minder kwetsbaar maken van wat er momenteel voorhanden is.

Jos Wetzels heeft verschillende technieken geanalyseerd en vervolgens geïmplementeerd om een aanvaller dwars te zitten. Zonder hier in allerlei details te treden is het bijzondere dat het gaat om technisch geavanceerde technieken die diep inzicht vereisen in computersystemen om ze succesvol te implementeren. Het is al bijzonder dat een promovendus deze inzichten heeft; nog indrukwekkender is dat een afstuderende masterstudent zover komt. Als dit vervolgens nog in de volledige breedte en diepte uitgemeten wordt in een scriptie, reflecterend aan de hand van een volledige beschouwing van wat er reeds gerapporteerd is in de wetenschappelijke literatuur, dan is het voor elke jury wel helder wie er op 1 komt te staan.

Gedeelde 2^e prijs Anna Latour (Universiteit Leiden)

Incremental algorithms for solving stochastic constraint optimisation problems with probabilistic logic programming

De afstudeerscriptie van Anna Latour richt zich op “constraint optimisation” problemen. Dit zijn problemen waarbij er aan meerdere voorwaarden (“constraints”) voldaan moet worden om tot de best mogelijke oplossing te komen. Een voorbeeld van een dergelijk probleem is het inroosteren van docenten, klaslokalen en scholieren op een middelbare school. De best mogelijke inroostering houdt zo goed mogelijk rekening met de beschikbaarheid van docenten en lokalen. Anna’s scriptie handelt over zogenaamde stochastische constraint optimisation problemen, waarbij de voorwaarden een zekere waarschijnlijkheid hebben. Bijvoorbeeld: er is een kans van 50% dat een docent op een gegeven tijdstip beschikbaar is. Een speciaal voor stochastische constraint optimisation problemen ontwikkelde programmeertaal vereist een specificatie van de voorwaarden en de optimalisatie, waarna het programma automatisch zoekt naar een oplossing. Voor de meeste optimalisatieproblemen levert de stap van specificatie naar het automatisch zoeken problemen op, vanwege de benodigde computerkracht. Interessante of nuttige problemen vereisen enorm langdurige berekeningen, waardoor toepassing in de praktijk niet mogelijk is.

Anna Latour heeft een methode voorgesteld waarbij de specificatie van de voorwaarden en de optimalisatie in stapjes wordt opgedeeld. Het zoeken naar oplossingen geschiedt daardoor ook in stapjes, hetgeen resulteert in een enorme reductie in de benodigde rekentijd. Experimenten tonen aan dat de voorgestelde methode superieure resultaten oplevert in vergelijking met de oorspronkelijke inefficiënte methode.

Ondanks de complexiteit van het onderwerp, is Anna Latour er in geslaagd om een prettig leesbare scriptie te schrijven, met een heldere argumentatie en uitleg. De jury is onder de indruk van de kwaliteit van het werk en van de wijze waarop Anna het onderzoek heeft uitgevoerd.

Gedeelde 2^e prijs Paul Marcelis (Technische Universiteit Delft)

Frame Loss Characterisation and Data Erasure Coding for LoRaWAN

Het internet der dingen komt er aan. We vinden het al heel normaal dat we op afstand de verwarming thuis kunnen regelen, maar straks vinden we het ook doodnormaal dat onze fiets ons waarschuwt als die verplaatst wordt. Zeker als je dacht dat je hem op slot gezet had. Evenzo verwachten we straks dat het riool ons vertelt dat er een opstopping op komst is, of dat een akker aan de boer rapporteert dat het echt de hoogste tijd wordt om te gaan rooien wegens de hoge vochtigheid van het land.

Dit soort meldingen maken gebruik van een speciaal draadloos netwerk, LoRaWAN geheten. Een pracht van een netwerk dat tot zelfs 15 km afstand berichten kan verzenden zonder tussenkomst van allerlei apparatuur. Helaas is het ook een bijzonder onbetrouwbaar netwerk en moeten we rekening houden met wel 85% kans dat een bericht niet aankomt. Moeder Natuur heeft het nooit op draadloze communicatie gehad, en zeker niet als je denkt er 15 km ongehavend mee weg te komen. Daar gaat je fiets.

Paul Marcelis heeft gekeken hoe we die betrouwbaarheid kunnen vergroten. De essentie van zijn oplossing ligt in meesturen van zoveel extra informatie, dat als je bericht als gatenkaas aankomt, de ontvanger toch nog het oorspronkelijke bericht kan herstellen. Hij heeft daarvoor een eigen methode ontwikkeld en is volgens het boekje te werk gegaan: een gedegen literatuurstudie, een goede theoretische onderbouwing, een pracht van een algoritme, wat vervolgens ook nog eens geïmplementeerd is en aan experimenten blootgesteld. Het is de combinatie van deze elementen, en vooral gegeven dat het een waarlijk moeilijk onderwerp betreft, dat de jury ertoe bracht hem te eren met een prijs.

Prof. dr. C.M. (Catholijn) Jonker, hoogleraar interactie intelligence group Technische Universiteit Delft

Prof. dr. E.O. (Eric) Postma, hoogleraar kunstmatige intelligentie Tilburg University

Prof. dr. ir. M.R. (Maarten) van Steen, hoogleraar informatica Universiteit Twente, wetenschappelijk directeur ICT Onderzoeksinstituut Universiteit Twente

De jury vergaderde op 18 oktober 2017 onder leiding van Prof. mr. A. Soeteman, secretaris geestes- en maatschappijwetenschappen (voorzitter i.v.m. verhindering van de secretaris natuurwetenschappen); daarnaast waren ter vergadering aanwezig Drs. S. van Manen, secretaris en S. de Boer (notulen).