Jury report Dutch Cyber Security best Research Paper Award (DCSRP Award) 2017

Background

In the last 20 years, the Dutch information security community grew from a handful of brilliant mathematicians to a large community of cybersecurity researchers with representatives from many of the technical and the social sciences. The Netherlands Organisation for Scientific Research (NWO) and the European Commission have provided over a hundred million Euros of funding in long term Dutch cybersecurity research. This has led to dozens of new businesses, hundreds of highly skilled employees in all major corporations, government departments and universities, and thousands of scientific publications and patents.

Role dcypher and Jury

In 2015 the public-private Dutch ICT Innovation Platform on Security and Privacy (IIP-VV) decided to introduce a new and prestigious prize for the best recent Dutch scientific cybersecurity research paper. IIP-VV board members designed the nomination and assessment process. As of 2015, every year an international jury is formed and accepts the task to assess eligible, i.e. recent non-commercial scientific cybersecurity research papers, which were received as a result of a call for nominations.
The yearly ICT.OPEN conference is an excellent place with the right audience to present a series of top research papers and to announce the award winning paper and its main author!
In 2017 for the third time the best research paper contest was held.
The dcypher advisory council, like the IIP-VV board in previous years, came up with a long list of possible (foreign) jury members. Based on this list the dcypher bureau composed the 2017 Jury, consisting of three well-respected scientists in the cybersecurity field.
This Jury, under technical chairmanship of the director dcypher, selected the Top Three out of twelve papers nominated by seven different Dutch knowledge institutions.

'Peaks of Dutch Cyber Security Research'

The thematic session on cyber security, part of the ICT.OPEN 2017 conference program, is scheduled March 21nd 2017 and is titled '*Peaks in cybersecurity and privacy*'. The objective of this session is to demonstrate the progress and achievements in the execution of recent cybersecurity research.

Within the '*Peaks of Cyber Security Research*' session the main authors of the research paper Top Three present their paper. Each presenter receives a "Dutch Cyber Security Research Paper Award" certificate, signed by Jury members.

The Jury not only selects the Top Three, but also determined which paper ranks as the very best out of this set of three. The main author and presenter of this paper receives the "Dutch Cyber Security **best** Research Paper Award" certificate, together with a special € 500,- bonus cheque donated by IBM.

ICT.OPEN 2017 is a conference organized by NWO and IPN. The thematic session on cyber security is organized by dcypher (Dutch cybersecurity platform higher education & research). The Dutch Cyber Security best Research Paper Award 2017 is sponsored by IBM.

Jury report Dutch Cyber Security best Research Paper Award (DCSRP Award) 2017

Research Paper Top Three

Paper title: Flush, Gauss and Reload – a Cache Attack on the BLISS Lattice-Based Signature Scheme
Presenter: Andreas Hülsing, Technical University Eindhoven
Authors: Leon Groot Bruinderink, Andreas Hülsing, Tanja Lange, Yuval Yarom
Published at: CHES 2016, the conference on Cryptographic Hardware and Embedded Systems; CHES 2016 had an acceptance ratio of 30/148.

Motivation by Tanja Lange:
This paper presents the first side-channel attack on a lattice-based signature scheme, one of the strongest contenders for signature schemes that resist attacks by quantum computers. The attack determines which cache lines are accessed during sampling from a discrete Gaussian distribution and combines that information over several signatures into a big system of equations that are true up to a small error. Finally, this system is solved with the help of the so called LLL algorithm, deploying lattices as an attack tool. The attack applies to all proposed ways of sampling discrete Gaussians.

Jury's assessment:
The Jury considered this a very interesting and well written research paper, describing novel research in the area of post-quantum cryptograpy. It was noticed and appreciated the paper was accepted at a very relevant and highly ranked conference. The reseach resulted in a proof-of-concept implementation with a high probability of being a successful attack.

Paper title: Complete addition formulas for prime order elliptic curves
Presenter: Joost Renes, Radboud University Faculty of Science, Mathematics, and Computer Science
Authors: Craig Costello and Lejla Batina
Published in: Advances in Cryptology - EUROCRYPT 2016 - 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part I, pages 403–428, 2016

Motivation by Lejla Batina:
This is the first paper of Joost in his 1st year as a PhD student. He published it at the top crypto/security conference (Eurocrypt) and he is the main contributor to this work as evident from him being put as the first author (not following the alphabetic order). As a follow-up he was invited for an internship with Microsoft Research, which is very exceptional achievement for a 1st year PhD student.

Jury's assessment:
This interesting paper describes novel research. This paper in particular stands out because it was accepted at Eurocrypt, which is a top-tier conference, and because the main author was only in his first PhD year when he cooperated with Microsoft Research on this paper. The Jury considered this an excellent piece of work, with a broad impact, as can be illustrated by the receipt of an invitation for an internship at Microsoft, following the publication of this paper.

Paper Title: Drammer: Deterministic Rowhammer Attacks on Mobile Platforms
Presenter: Victor van der Veen, VU University, Computer Systems Section

Jury report Dutch Cyber Security best Research Paper Award (DCSRP Award) 2017

Authors: Victor van der Veen, Yanick Fratantonio, Martina Lindorfer, Daniel Gruss, Clémentine Maurice, Giovanni Vigna, Herbert Bos, Kaveh Razavi, Cristiano Giuffrida
Published in: CCS 2016, October 24-28, 2016, Vienna, Austria,
https://vvdveen.com/publications/drammer.pdf

Motivation by Herbert Bos:
With DRAMMER, Victor demonstrated that it is possible to trigger Rowhammer bit flips on widespread ARMbased platforms and exploit such bit flips to deterministically (and thus reliably) compromise an entire system without relying on any special features. Victor showed this is all possible thanks to only two standard features present in all modern commodity platforms: Direct Memory Access (DMA) buffer management (which grants an attacker direct memory access to easily trigger bit flips) and buddy page frame allocation (which allows an attacker to easily predict physical memory reuse to target bit flips on securitysensitive targets). A combination of these techniques is quite scary: a malicious app running on millions of mobile devices today and on billions of Internet of Things (IoT) devices tomorrowcan reliably gain root privileges on vulnerable targets without an easy fix given the hardware nature of the issue.
Google was the first to realize the impact of DRAMMER and gave an award to Victor's proofofconcept exploit as part of the Android Security Reward Program. The joined effort between VU and the Android Security Team resulted in improved ARM/Android security and also sparked a discussion between Linus Torvalds and Alan Cox on the Linux Kernel mailing list. The conclusion was that mitigation in software is not possible. Hence, we expect DRAMMER to prompt hardware manufacturers to provide additional protection in hardware.

Jury's assessment:
This is a very interesting paper, published at ACM CCS, one of the top 4 security conferences, a tier-1 venue with high impact. The paper has a large international team of authors, which further fosters collaboration, with Victor van der Veen as the leading author, which shows the key role the Dutch team had in this research. The proposed mitigation in the paper requires hardware modification or replacement (in the worst case scenario, for the Rowhammer component). Results have thus a broad and long lasting impact. The interest in DRAMMER even extended beyond academia and open source, including the hacker community as well as government and industry. It received extensive traditional media coverage, in more than 20 countries, from magazines to television as well as high profile web media.

The Winner
Jury members, who individually ranked and collectively decided on the quality of all research papers received, appreciated the response by the Dutch research community on the call for nominations, resulting in twelve paper nominations. Out of the Top Three as presented today, one paper deserves the predicate **best** Dutch Cyber Security Research Paper.

The Award winning paper is: **Drammer: Deterministic Rowhammer Attacks on Mobile Platforms,** by Victor van der Veen et al.

Jury report Dutch Cyber Security best Research Paper Award (DCSRP Award) 2017

Jury members

Drs. Jan Piet Barthel, Chairman Jury Dutch Cyber Security Research Paper Award 2017
dcypher/NWO

Jan Piet Barthel is Director of dcypher, the Dutch platform for cybersecurity higher education and research and also program manager cyber security research within the Netherlands Organisation for Scientific Research (NWO), the main funding organisation for scientific research in the Netherlands.
more at https://www.dcypher.nl/en/content/drs-jp-jan-piet-barthel

Prof. Dr. Stefan Katzenbeisser
Techische Universität Darmstadt

Since 2012 Stefan Katzenbeisser is Professor at the Techische Universität Darmstadt. His research activities focus on Cryptographic protocols (design, analysis), Cryptographic techniques for noisy and fuzzy data, Physically Unclonable Functions, Privacy Enhancing Technologies, Watermarking, Digital Rights Management, Copyright Protection and Steganography and Covert Channels
more at https://www.seceng.informatik.tu-darmstadt.de/people/katzenbeisser/

Dr. Lorenzo Cavallaro
ISG, Royal Holloway, University of London.

Lorenzo Cavallaro is a Reader (Associate Professor) of Information Security in the School of Mathematics and Information Security at Royal Holloway. His research focuses largely on systems security and he has founded and is leading the recently-established Systems Security Research Lab (S2Lab), which builds on program analysis and machine learning to devise novel techniques to protect systems from a broad range of threats, including those perpetrated by malicious software. Prior to joining Royal Holloway, Lorenzo was a Post Doctorate researcher in the Systems & Security group at Vrije Universiteit Amsterdam, the Security Group at UC Santa Barbara and a long-term Visiting Scholar at Stony Brook University. He publishes and sits in program committees of well-known and premiere security conferences, and his research is funded by the UK EPSRC, McAfee, and Royal Holloway.
more at http://s2lab.isg.rhul.ac.uk/~sullivan

Dr. Nele Mentens
KU Leuven

Nele Mentens obtained a Ph.D. in Engineering Science with the title "Secure and Efficient Coprocessor Design for Cryptographic Applications on FPGAs". Since 2014, she is an associate professor at KU Leuven and an academic staff member of the COSIC research group. Her research interests are in the field of cryptographic coprocessors in secure embedded systems, partial/dynamic reconfiguration of FPGAs, design automation for cryptographic hardware/software,...
more at http://homes.esat.kuleuven.be/~nmentens