Jury Report
Dutch Cyber Security best Research Paper Award (DCSRP Award) 2020
Award Ceremony: 28 September 2020

Background

In the last decennia, 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. In recent years these funds were provided through NWO's cybersecurity programs, the Veni and Vici funding instruments and EU instruments like H2020 and CHIST-ERA. This has led to new businesses, hundreds of highly skilled employees in all major corporations, government departments and universities, and thousands of scientific publications.

Award history, conditions, role dcypher and Jury

Cybersecurity researchers from all over the world are searching for yet unknown vulnerabilities, for new and better detection or prevention techniques, for aspects that negatively or positively impact our cybersecurity behavior. Cybersecurity research in The Netherlands is of high level. Frequently Dutch research papers are accepted at prestigious international conferences.

In 2015 the (former) public-private Dutch ICT Innovation Platform on Security and Privacy (IIP-VV) introduced a new and prestigious award for the best recent Dutch scientific cybersecurity research paper. The tradition of organizing this contest was taken over by the Dutch cybersecurity platform higher education & research (dcypher) in 2017. Each year the organizing body receives a bunch of research papers as a result of a wide spread call for nominations.
The paper contest is open for recent non-commercial scientific cybersecurity research papers, where the main responsibility of the research lies within (a) Dutch research institute(s).
In many cases the papers are a result of a PhD study. For the PhD student it is an honor to get nominated and be selected to present his/her paper. For a country like The Netherlands it is extremely important to deliver sufficient numbers of scientifically trained cybersecurity experts each year to the Dutch society, including industry.

In 2020 the best research paper contest is held for the sixth time. Like previous years an international jury was composed, consisting of three well-respected scientists in the cybersecurity field, with the task to assess eligible, high quality cybersecurity research papers. The Jury, under technical chairmanship of the director dcypher, selected a Top-4 out of 10 papers received and nominated by 8 different Dutch research institutes. Selection criteria for the jury are:

- Substantiveness of the technical achievement;
- Real-world impact (e.g. transformational impact in industry);
- Quality of the venue where the paper was published.

As usual the Jury does not only select a small set of top papers, but also determines which paper ranks as the very best out of this set. Each paper presenter, representing the team of authors, receives a "dcypher Dutch Cyber Security Research Paper Award" certificate, signed by Jury members. The main author(s) and presenter of the paper scored number one receives the "**dcypher best Dutch Cyber Security Research Paper Award**" certificate, together with a bonus cheque. Sponsors of the DCSRP-Award 2020 are KPN Security and Compumatica.

dcypher mini Symposium 2020

The **dcypher best Cyber Security Research Paper Award** will be presented on Monday 28 September 2020. This year the best paper presentations and award ceremony are part of the (virtual) dcypher mini Symposium (https://www.dcypher.nl/dcypher-mini-symposium). In previous years paper presentations, as well as the announcement of the award winning paper, took place at the annual ICT.OPEN conference. The Covid-19 outbreak resulted in a cancellation of this conference. To avoid skipping this years ceremony, also realizing that presentations were already prepared when the cancellation was announced, dcypher decided to make the DCSRP session part of a special dcypher mini Symposium. Within this session main authors of the research paper Top-4 present their paper.

Cyber Security Research Paper Top-4

1. Paper title (paper 09):

CSI NN: Reverse Engineering of Neural Network Architectures Through Electromagnetic Side Channel

Authors: Lejla Batina (RUN), Shivam Bhasin (NTU), Dirmanto Jap (NTU), Stjepan Picek (TUD)
Published at: Proceedings of the 28th USENIX Security Symposium

Motivation by Lejla Batina (RUN)

Deep learning (DL) has already been used to improve side-channel analysis (SCA). This paper is the first one to consider the opposite direction, basically using SCA to reverse engineer implementations of neural net architectures. We demonstrate that a side-channel attacker is capable of learning proprietary information from an ARM Cortex-M3 microcontroller using neural networks. This platform is often used in pervasive applications such as wearables, surveillance cameras etc. Several companies have contacted us about this work related to the protection of their IP and products as neural network implementations of today typically contain no protection against side-channel analysis and fault injection. This research is a collaboration of Radboud University, the Technical University of Delft (Batina and Picek) and Nanyang Technological University, Singapore (Bhasin and Jap). This work was presented at the USENIX Security Symposium 2019.

Jury's assessment:

This Dutch - Singaporean research is about a novel approach: executing and studying side-channel attacks capable of leaking information about neural networks. The research team used these attacks to reverse engineer neural network architectures.
The Jury calls the new application of side-channel attacks very interesting, since the protection of deep learning IP is an emerging problem. This research potentially opens new research directions.
What remains a little unclear is how realistic the size of the evaluated neural networks is.
This important paper was published at a top security conference.

2. Paper title (paper 07):

Self-Encrypting Deception: Weaknesses in the Encryption of Solid State Drives

Authors: Carlo Meijer (Radboud University Nijmegen) and Bernard van Gastel (Open University of the Netherlands)

Published at: IEEE Security & Privacy 2019

Motivation by Hugo Jonker (Open University)

Hereby, we submit the paper Self-Encrypting Deception: Weaknesses in the Encryption of SSD's (Solid State Drives) for your consideration for the Dutch Cyber Security best Research Paper 2020 award. This paper presents the culmination of a two-year effort by Carlo Meijer (Radboud University Nijmegen) and Bernard van Gastel (Open University of the Netherlands) into research and world-wide, coordinated vulnerability disclosure. In this work, Carlo and Bernard investigated the security of so-called self-encrypting drives, and found that the security underlying the promise of such drives was razor-thin. They found that "for multiple models, it was possible to bypass the encryption entirely, […] without knowledge of password or keys." In short: the security of self-encrypting drives could not be relied upon. The relevance of this work is extraordinary. A commonplace security mechanism was thoroughly investigated and found to be lacking to such an extent, it could no longer be relied upon. This finding necessitated that many institutions world-wide reviewed and updated their security policies – and changed the encryption of their drives. Finally, we remark that this two-man effort was executed completely within the Netherlands, by a team of two researchers. As such, we believe it makes this paper an excellent candidate for the DCSRP 2020 award.

Jury's assessment:

This paper, about serious security issues in SSD encryption, was presented at a top security venue and received considerable attention in the news. The vulnerabilities discovered are mainly due to the bad design and implementation of the self-encryption devices, rather than the use of novel analysis techniques or crypto concepts. Nevertheless this relatively small team of two researchers has proven, in a relatively short period of time, to be able to dive deep into SSD encryption. They disclosed a significant weakness in a high technical knowledge effort, by using reverse engineering of the firmware.
This paper demonstrates a false sense of security provided by hardware encryption. In bypassing encryption the team executed a devastating attack (full recovery of data without password knowledge). The real world impact of this paper is high: 60% of SSD's are affected. This represents a large number of devices!

3. Paper title (paper 06):

RIDL: Rogue In-flight Data Load

Author: Stephan van Schaik, Alyssa Milburn, Sebastian Österlund, Pietro Frigo, Giorgi Maisuradze, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida

Published at: IEEE Security & Privacy 2019

Motivation by Herbert Bos (VUSec)

If there was one VUSec paper that made headlines in 2019, it was RIDL (Rogue In-flight Data Load), which was covered by media around the world -- including the New York Times. The reason is that RIDL represents a new and very dangerous class of speculative execution vulnerabilities that has not been fixed even today, 1.5+ years (!) after it was first reported to Intel. Intel itself admits the seriousness and has so far awarded 6 CVEs and $127,000 in bounties to VUSec. However, the paper is even more important from a research perspective. First, it shows that the problems with speculative execution were not just a one-off issue, but rather fundamental problems deeply ingrained in the design of CPUs -- making them difficult to fix (witness the two rounds of broken mitigations released by Intel so far). Second, it reveals, for the first time, how attackers can leak sensitive speculative information without relying on memory addresses. Third, it shows that all attempts to fix such vulnerabilities with spot mitigations are broken and have made our computers much slower since 2018, without much real gain in security. Finally, it shows important aspects of modern CPUs that have hitherto remained secret via novel reverse engineering techniques. It is for these reasons that RIDL was accepted with 2 ‘Strong accepts’ and an ‘Accept’ at IEEE S&P (the highest paper score in 2019).

Jury’s assessment:

The VUSec RIDL paper became a highly visible paper presented at leading security conferences, with already 38 citations. Speculative execution attacks are an intriguing new class of attacks revealing dangerous vulnerabilities which are difficult to fix. These type of attacks break any security boundary, can also be exploited from the browser, and raise important questions about current mitigation strategies and disclosure processes. Apart from presenting a new set of CPU attacks, the paper also provides a fundamental study of the underlying problems. With this paper the VUSec team won the second place in the 2019 CSAW (“See SAH”) Applied Research Competition, showing this work has strong practical impact.

4. Paper title (paper 05):

Exploiting Correcting Codes: On the Effectiveness of ECC Memory Against Rowhammer Attacks

Authors: Lucian Cojocar, Kaveh Razavi, Cristiano Giuffrida, Herbert Bos
Published at: IEEE Security & Privacy 2019

Motivation by Herbert Bos (VUSec)

In 2014, researchers from CMU showed that it is possible to flip bits in 87% of deployed DRAM by merely accessing memory very quickly. This Rowhammer vulnerability, originally thought to be a reliability problem, turned into a massive security headache as researchers, including members of the VUSec team in Amsterdam, showed that you can pretty much compromise every device, from cloud servers all the way to mobile devices. However, before our ECCploit work, the common belief in the security community was that ECC memory provides adequate (i.e., strong probabilistic) protection against Rowhammer bit flips and that Rowhammer was essentially a solved problem on ECC-equipped server platforms. In contrast, ECCploit shows deterministic Rowhammer attacks are not only possible on ECC-equipped platforms, but can be as powerful as the existing Rowhammer attacks on non-ECC systems. ECCploit also details a 2-year long reverse engineering effort that uncovered details and vulnerabilities on commodity ECC implementations, including side-channel vulnerabilities that, combined with novel insights into data-dependent Rowhammer patterns, make ECC-aware Rowhammer attacks possible. For these reasons, ECCploit has been widely recognized by the community, with extensive media coverage (Wired, Ars Technica, etc.) and the Best Practical Paper Award at IEEE S&P 2019, one of the most recognized venues in security.

Jury's assessment:

The paper presents the first Rohammer attack on error-correcting code (ECC) memory, which use has been considered a viable defense strategy before. The attack resulted from an intense reverse engineering effort. The common belief was that ECC memory mitigates Rowhammer exploits. Demonstrating this belief was not sustainable resulted in winning the Best Practical Paper Award at IEEE S&P. The practicality of this research was also shown by uncovering details and vulnerabilities on commodity ECC implementations.
Given the fact that ECC memory is not the solution, also the Jury realizes there is still an open problem. More research is needed in how to defend against this type of attacks.
This ECC paper was presented at a top security venue, and in no time already 14 citations could be counted.

The Winner

Jury members, who individually ranked and collectively decided on the quality of ten research papers received, appreciated the response by the Dutch research community on dcypher's call for nominations. Out of the Top-4 as presented today at the dcypher mini Symposium, one paper deserves the predicate **best** Dutch Cyber Security Research Paper and has earned the dcypher best Cyber Security Research Paper **Award** 2020.

Final conclusion of the Jury
(presented by Martina Lindorfer on behalf of the other jury members):

In the discussion between jury members, considering the assessment criteria, and the diversity of topics, the Jury ultimately decided to recognize a top-4 of excellent papers instead of a top-3.

However, the Jury unanimously agreed that out of these four there was one paper really outstanding with huge scientific and real world impact. It was tough for the other three to compete with this one. While the other three are excellent runner ups, the winning paper can be called the pinnacle of the Amsterdam VUSec research team on CPU attacks. They discovered a real new class of attacks. In many aspects the research was a big learning experience for the research team as well as for the cybersecurity community, often dealing with dilemma's around disclosure. INTEL gave the team a hard time. Media attention was impressive and well spread.

In short, the Jury selected:

RIDL: Rogue In-flight Data Load

Stephan van Schaik, Alyssa Milburn, Sebastian Österlund, Pietro Frigo, Giorgi Maisuradze, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida

as the winner of the dcypher DCSRP Award 2020

Jury DCSRP Award 2020

Drs. Jan Piet Barthel

Chairman Jury Dutch Cyber Security Research Paper Award, Director dcypher, NL

Jan Piet Barthel is founder and present Director of the Dutch platform for cybersecurity higher education and research. He combines this with the role of lead 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.linkedin.com/in/jan-piet-barthel-4839b38*

Prof. Anja Lehmann

Hasso Plattner Institute

From February 2020 Anja Lehmann is Professor of Cyber Security and Identity Management at the Hasso-Plattner Institute and University of Potsdam in Germany. Till then she is a researcher in the Foundational Cryptography group at IBM Research – Zurich, where she works on the design of cryptographic protocols with provable security guarantees. Before joining IBM, she obtained her PhD in 2010 from Darmstadt University of Technology.

more at *https://www.linkedin.com/in/anja-lehmann-342563101*

Dr. Martina Lindorfer

Assistant Professor in the Security and Privacy Group, TU Wien

Martina Lindorfer is a tenure-track Assistant Professor in the Security and Privacy Group at TU Wien (Technische Universität Wien, formerly known as Vienna University of Technology) in Vienna, Austria. She is also a key researcher at SBA Research, the largest research center in Austria which exclusively addresses information security. Lindorfer's research interests focuses on systems security, in particular mobile security and privacy, and malware analysis.

more at *https://martina.lindorfer.in/*

Prof. Davide Balzarotti

Professor Eurecom Graduate School and Research Center, Sophia Antipolis

Davide Balzarotti is a Professor (Professeur des université) at the Eurecom Graduate School and Research Center, located in Sophia Antipolis on the French riviera. His research interests include most aspects of system security and in particular the areas of binary and malware analysis, reverse engineering, computer forensics, and web security. He is a member of the Order of the Overflow - the team which is currently organizing the DefCon Capture the Flag competitionanalysis.

more at *http://www.eurecom.fr/en/people/balzarotti-davide*