19-CSRE-045

Jury Report
Dutch Cyber Security best Research Paper Award (DCSRP Award) 2019

Background

In the last 25 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. In recent years these funds were provided through NWO's cybersecurity programs, the Veni and Vici instrument and European instruments like H2020 and CHIST-ERA. 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.

Award conditions, role dcypher and Jury

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.
In 2019 the best research paper contest is held for the fifth time. 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).
Every year an international jury is composed with the task to assess eligible, high quality cybersecurity research papers. Thanks to the advice of the dcypher advisory council, again this year the dcypher bureau was able to compose an international 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 9 papers nominated by eight different Dutch research institutes.

ICT.OPEN 2019 conference

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!
The thematic session on cybersecurity & privacy, part of the ICT.OPEN 2019 conference program, is scheduled March 20th 2019. The objective of this session is to demonstrate the progress and achievements in the execution of recent cybersecurity research. Within the 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 selected the Top Three, but also determined which paper ranks as the very best out of this set. The main author(s) and presenter of this paper receives the "Dutch Cyber Security best Research Paper Award" certificate, together with a bonus cheque donated by IBM and KPN.

ICT.OPEN 2019 is a conference organized by NWO and IPN. The Dutch Cyber Security best Research Paper contest 2019 is organized by dcypher and the associated award is sponsored by IBM and KPN.

19-CSRE-045

Jury Report
Dutch Cyber Security best Research Paper Award (DCSRP Award) 2019

Research Paper Top Three

1. Paper title (paper 07):
Grand Pwning Unit: Accelerating Microarchitectural Attacks with the GPU ("GLitch")

Author: Pietro Frigo, Cristiano Giuffrida, Herbert Bos, Kaveh Razavi
Published at: IEEE Security & Privacy ("Oakland")

Motivation by Herbert Bos
It is our pleasure to nominate "GLitch", published at IEEE Security & Privacy 2018 for the DCSRP Award, one of the most (if not the most) influential papers to come out of the VUSec group at VU Amsterdam in 2018. GLitch has 15 citations and counting on Google questioned whether this could be done from the browser at all. While fully stopping GLitch is impossible as it is rooted in hardware, Google and Mozilla reacted by disabling various browser features to make the attack harder, impacting billions of browsers. GLitch is the first effort to show that CPU vendors must consider microarchitectural attacks when adding new components such as GPUs into their SoC. Given the scientific and societal impact, we firmly believe that GLitch deserves the DCSRP award. Scholar, was nominated for the CSAW's Best Practical Research Award, won the Code Blue Award, and appeared in a wide range of online and offline media (including WIRED, BleepingComputer, ArsTechnica, Hacker News, Security Affairs, etc.). Microarchitectural attacks from JavaScript have become one of the most worrying attack vectors of our time: even a single malicious ad can remotely compromise users. In response, the community has scrambled to deploy browser mitigations to stop them. At first sight, the effort was successful and all attacks were mitigated. However, GLitch shows that, not only attacks are still possible, but can even be made more efficient and even on mobile devices that were previously thought to be immune. In particular, GLitch demonstrates for the first time that performing remote (browser-based) microarchitectural attacks on mobile platforms is feasible. These attacks are really hard on the ARM CPUs of commodity mobile devices. Specifically, triggering the widespread Rowhammer vulnerability in DRAM seems impossible with the way ARM CPU caches are designed. They are slower than their x86 counterpart and try to randomly evict entries to allocate new ones. This makes it difficult to craft efficient and predictable DRAM access patterns for Rowhammer exploitation on mobile devices. GLitch's browser-based attacks are enabled by the WebGL interface, which allows one to run programs on integrated GPUs present on all ARM System-on-Chips (SoCs) next to the CPU. This is how you can play fancy games in your browser without quickly draining your battery. The problem was that, before GLitch, nobody knew how these GPUs actually worked. The hardware vendors are very secretive about the design in order to protect their market share. GLitch used a large number of analysis programs to reverse engineer the internal architecture of these GPUs. This led to the key insight that GPU caches are much faster and more predictable than their CPU counterparts, allowing even JavaScript-based Rowhammer attacks on mobile phones for the first time. At a higher level, GLitch is the first effort to concretely demonstrate the perils of the WebGL interface in modern browsers. However, the results go well beyond that. Exploring the attack surface of GPUs further, GLitch shows that one can use them to bypass state-of-art mitigations and build novel microarchitectural attacks. The GLitch exploit uses this knowledge to build the first practical, hardware-based attack in the browser. The impact of this achievement is extremely high.

Jury Report
Dutch Cyber Security best Research Paper Award (DCSRP Award) 2019

Jury's assessment:
The paper deals with a very interesting subject and demonstrates the security implications of a vulnerability associated to Graphics Processor Units (GPUs), widely employed in almost all mobile processors. More precisely, it demonstrates how an attack can be launched based on the identified vulnerability.
This research presents yet another way of exploiting remote microarchitectural attacks from the GPU. This technically highly advanced work, shows the fragility of our complex systems when it comes to security. The researchers followed a novel angle by demonstrating that this type of attacks affects System-on-Chips in a much wider sense than perhaps previously thought.
Since CPUs were already clearly in need for some redesign, this work also has impact on the development of future GPUs. As a consequence results of this work have deep transformational impact in industry, leading to changes in widely used products.
After publication in an A (top tier) computer security conference this research attracked lots of attention, received wide media coverage as well as an award.*

2. Paper title (paper 04):
CSIDH: An Efficient Post-Quantum Commutative Group Action

Authors: Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes
Published at: *Asiacrypt 2018, LNCS 11274, pp. 395-427*

Motivation by Tanja Lange
Post-quantum cryptography is one of the hottest areas in cryptography right now as all systems need to switch to alternatives that resist attacks by quantum computers. Research has produced good candidates for signatures and encryption/key encapsulation mechanism (KEM) schemes. However many applications currently use the Diffie-Hellman (DH) key exchange and some features of it are missing post-quantum alternatives. This paper presents the first practical non-interactive key exchange in post-quantum cryptography, deliverying a full replacement for DH. The system uses supersingular isogenies in a novel way and gives a complete study from mathematical theory to practical implementation. The paper already prompted several follow-up papers, including two building new cryptographic protocols on top of Commutative SIDH (Supersingular isogeny Diffie-Hellman) or CSIDH, highlighting the practical importance.

Jury's assessment:
The paper presents a very important development in the field of post-quantum cryptography, delivering a key exchange protocol replacing the existing Diffie-Hellman protocol, thereby tremendously simplifying the transition process. The proposed scheme is based on supersingular isogenies and thus providing post-quantum guarantees. The level of technical complexity and achievement of this research are high. Not only a detailed theoretical analysis and mathematical proofs are provided, but also a proof of concept.
The research was published on Asiacrypt, an A conference. Many researchers around the world are looking for replacement candidates of the current constructs. While it remains to be seen if this approach will be adopted in future systems, the mere proposal of such a construct has already had substantial research impact.

19-CSRE-045

Jury Report
Dutch Cyber Security best Research Paper Award (DCSRP Award) 2019

3. Paper title (paper 08):
XMSS: Translation Leak-aside Buffer: Defeating Cache Side-channel Protections with TLB Attacks

Authors: Ben Gras, Kaveh Razavi, Herbert Bos, Cristiano Giuffrida
Published at: USENIX Security 2018

Motivation by Herbert Bos
It is our pleasure to nominate "TLBleed", published at USENIX Security 2018 for the DCSRP Award, one of the most (if not the most) influential papers to come out of the VUSec group at VU Amsterdam in 2018. TLBleed has 7 citations and counting on Google Scholar, has its own Wikipedia page (made by others) similar to other high-profile attacks such as Spectre, Meltdown, and Foreshadow, led to a host of longer presentations at hacker conferences such as BlackHat USA, and was also presented by independent leading researchers such as Jon Masters (RedHat) at FrOSCon. TLBleed was quickly "Slashdotted" and articles appeared in numerous online and offline magazines and podcasts, such as The Register, ArsTechnica, ZDnet, SecurityNow, etc. TLBleed exposes an entirely new side-channel attack that bypasses all existing defenses. In particular, it shows for the first time, that the community's fixation on side-channel attacks and defenses based solely on CPU caches is wholly insufficient. Other shared resources, in this case the TLB, are just as amenable to powerful information disclosure attacks. The subsequent explosion in the news was difficult for the authors to contain, while the measures taken by operating system maintainers were as unexpected as they were rigorous. For instance, RedHat, warned that SMT should be treated with care and hyperthreads come with security risks. More importantly, Theo de Raadt, the OpenBSD project leader, decided that since TLBleed exposed a fundamental hardware vulnerability with no easy fix, OpenBSD would disable simultaneous multithreading ("hyperthreading") completely on Intel processors from now on. Huge! More technically, TLBleed developed novel techniques to leak cryptographic keys under different constraints compared to existing cache side channels. Traditionally, attackers break cryptographic keys using cache side channels, by monitoring which cachelines are used by the victim: the cryptographic code processes the key bit by bit and executes different code (in different cache lines) for a 1 than for a 0. Since the cache is shared, the attackers can tell which cachelines were used by looking at which of their own cache lines are still/again in the cache. In contrast, TLBleed demonstrated that attackers do not even need to see code accesses ("the victim program executed code that maps to this cache set, so I know what it is doing"), but can suffice by observing data accesses in the TLB ("the victim accessed a data page that maps to a specific TLB set") to recover secret keys. Likewise, it proved that there is no need to observe spatial differences ("the victim program first executed code that maps to a cache line in cache set X and then code that maps to a cache line in cache set Y, so I know that the first bit of the key is a 1 and the second is a 0"). Instead, even if the victim accessed the code that is spatially indistinguishable (all routines are on the same page), we can still determine what code is executing by looking at temporal differences. While the signal looks very noisy at first glance, TLBleed demonstrates that picking apart the signal and reconstructing the key can be done in practical real-world settings by using supervised machine learning techniques. Given the scientific and real-world impact, as well the novel findings and techniques, we firmly believe that TLBleed deserves the DCSRP2019 Award.

19-CSRE-045

Jury Report
Dutch Cyber Security best Research Paper Award (DCSRP Award) 2019

Jury's assessment:

The paper describes how translation lookaside buffers (TLBs) can be exploited to leak sensitive information even when CPU cache activity is protected by state-of-the-art cache side channel protections. A prototype implementation TLBleed is also provided that can be exploited to leak a secret key, and RSA-key reconstruction.

The paper presents an interesting new angle for cache side channels, in particular dismantling some countermeasures that were previously believed to be sufficient. This type of work helps to further confirm that our current CPU designs are inherently insecure. It proceeds (in a very clever and complex way!) along the path of previous work – most of the novelty is in building the concrete exploit. ~~The attack vector is limmited to local adversaries.~~ The level of technical achievement is high, requiring a wide set of skills.

This paper has been published in a top tier venue for computer security an had substantial transformational impact in industry, leading to changes in widely used products (operating systems). The impact resulted in important media coverage.

19-CSRE-045

Jury Report
Dutch Cyber Security best Research Paper Award (DCSRP Award) 2019

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

Final conclusion of the Jury
The Jury used three criteria for their assessment: level of technical achievement, impact in real world and publication venue, and all three papers came out just great.
The Jury was very impressed about the TLBleed paper (paper 08), however in their opinion the contribution of this paper is less transformational (more incremental) than that of the other paper, coming from the VU security group, about the microarchitectural attacks with the GPU (paper 07).

You could say the 2019 research paper contest showed two winners, the microarchitectural attack paper and the post-quantum cryptography paper. However the Jury had to, and made a choice between these two.
In the discussion between the factual realized substantial impact of the GPU paper and the great potential impact of the post-quantum paper, in a very close race, the Jury decided to call:

An Efficient Post-Quantum Commutative Group Action written by Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes

as the winner of the dcyphers's DCSRP 2019

The Jury realizes that the world is looking at new cryptographic solotions for the post quantum future and highly appreciats the potential impact of this paper, and the horizon of new research that this opens.

Jury Report
Dutch Cyber Security best Research Paper Award (DCSRP Award) 2019

Jan Piet Barthel (MSc)

Chairman Jury Dutch Cyber Security Research Paper Award 2019, Director dcypher, The Hague

Jan Piet Barthel is Director of the Dutch platform for cybersecurity higher education and research and also 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. Flavio D. Garcia

Professor of Computer Security EPSRC Fellow School of Computer Science University of Birmingham, UK

Flavio Garcia is Professor of Computer Security EPSRC Fellow School of Computer Science. His research interests revolve around Automotive Security, Embedded devices security, Cryptanalysis and reverse engineering, RFID security and privacy and Privacy Enhancing Technologies.
more at https://www.cs.bham.ac.uk/~garciaf/

Prof. Dr. Cas Cremers

Faculty member at the CISPA Helmholtz Center (i.G.) in Saarbruecken, Germany

Cas Cremers obtained his PhD in 2006 from Eindhoven University of Technology in the Netherlands. From 2006 to 2013 he was a postdoctoral researcher, and senior researcher and lecturer, at ETH Zurich in Switzerland. In 2013 he moved to the University of Oxford where he became (full) Professor of Information security in 2015. In 2018 he joined the CISPA Helmholtz Center i.G.
more at https://cispa.saarland/people/cas.cremers

Dr. Katerina Mitrokotsa

Associate professor Dep. of Computer Science and Engineering Chalmers, University of Technology Sweden

Formerly, Katerina held positions as a visiting professor at the department of Computer Science at ETHZ, a visiting associate professor at Tokyo Institute of Technology a senior researcher (Marie Curie fellow) at EPFL. She has been active both in European and National research projects. Her research interests revolve around RFID Security & Privacy, Distance bounding protocols, Intrusion Detection & Response, Privacy-Preserving Biometrics, Security in Wireless Ad hoc Networks Machine Learning for Security and Privacy-preservation.
more at http://www.cse.chalmers.se/~aikmitr/