**Jury Report**
**Dutch Cyber Security best Research Paper Award (DCSRP Award) 2021**
**Award Ceremony: 19 May 2022**

## 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. 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 of SIG CS and Jury

The Dutch Cyber Security Best Research Paper (DCSRP) award has been organized annually since 2015. It is awarded to the best recent technical research paper published by Dutch researchers. In the previous years the award was steered by first the (former) public-private Dutch ICT Innovation Platform on Security and Privacy (IIP-VV), and, from 2017, by the (former) Dutch cybersecurity platform higher education & research (dcypher). In 2021, the Dutch cyber security special interest group SIG CS that represents all Dutch academic institutions where Cyber Security is carried out from a computer science perspective has taken the responsibility for co-organizing the award, jointly with the NWO and former dcypher representatives for continuity.
Each year the organizing body receives a collection of research papers as a result of a call for nominations distributed in the wide research community. Every year an international jury is composed with the task to independently assess eligible, high quality cybersecurity research papers. Thanks to the advice from SIG CS members, this year an international and multi-disciplinary Jury was composed, consisting of three well-respected scientists in the cyber security field. The Jury evaluated all papers based on the following criteria: (i) Quality and quantity of paper contributions; (ii) Real world impact; and (iii) Quality of the publication venue.
Out of 9 submitted papers, the Jury, under the technical chairmanship of SIG CS members Dr. Regazzoni and Dr. Gadyatskaya, selected the Top Three papers, out of which the winner was chosen.

## FUSION Event

The DCSRP 2021 award is presented at the (postponed) FUSION Event. The Corona pandemic forced the organizers to move the FUSION event from November 2021 to May 2022. At this event, the partners INTERSCT and ACCSS collectively organize a series of (physical) events on one day. A ''fusion" of different cyber security-related events occurs, even with slightly different and also overlapping target groups. It also is a fusion of different cyber security disciplines, and different parts of the knowledge chain. Collectively the partners and their members are seeking a more cyber secure future by organizing themselves now. This event represents a continuity of the cyber security research ecosystem in the Netherlands, building on top of a strong fundament of community developed by the former dcypher.

Within a dedicated DCSRP 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 determines which paper ranks as the very best out of this set. The main author(s) and presenter of this paper receive the "Dutch Cyber Security best Research Paper Award" certificate, together with a bonus check. Sponsors of the DCSRP-Award 2021 are KPN Security, represented by Eduard Hoekx and Compumatica Tesorion, represented by Ries van Son.

**A message from the Jury members**

The DCSRP award is an important prize for Dutch scientists. The papers submitted this year show that the Netherlands play an important role in international security research, and Dutch researchers produce excellent scientific results in the cyber security arena.

The Jury members were happy to see that the papers were accompanied by shared and independently evaluated artifacts. This is very important for the research community. Another strong aspect of some submissions was their accessibility to a wider audience, including students. It is essential that research findings are disseminated to students, and going an extra mile in making accessible short videos and tutorials is highly appreciated.

Finally, the Jury members noted that the majority of the papers were dealing with attacks, while it would be nice to also have a focus on defenses, since our society and industry needs both, complete awareness of attack strategies and effective techniques to mitigate them.

**Winning research papers**

Winner: Paper #07

***TRRespass: Exploiting the Many Sides of Target Row Refresh***

Authors: Pietro Frigo, Emanuele Vannacci, Hasan Hassan, Victor van der Veen, Onur Mutlu, Cristiano Giuffrida, Herbert Bos, and Kaveh Razavi

Published at: IEEE Symposium on Security and Privacy 2020 (S&P'20)

Link: https://doi.org/10.1109/SP40000.2020.00090

Motivation by the nominator:

After an initial onslaught of high-profile RowHammer attacks, CPU and DRAM vendors scrambled to deliver what was meant to be the ultimate hardware solution against RowHammer: Target Row Refresh (TRR). In fact, it was considered powerful enough that DRAM vendors started advertising their DDR4 as absolutely "Rowhammer free". Except they were wrong. After two years of reverse engineering, TRRespass revealed that TRR does not stop Rowhammer at all. Using a fuzzer exploring TRRespass' many-sided Rowhammer patterns, it turns out that modern DRAM chips from all major vendors are even more vulnerable than ever. This research has already had a strong impact in practice. First, it has concretely demonstrated current on-DIMM Rowhammer mitigations are insufficient and Rowhammer will remain a major threat for years to come. This has already prompted vendors such as Intel to deploy targeted Rowhammer countermeasures. Second, the DRAM industry's consortium (JEDEC), has formed a RowHammer working group to develop mitigations and testing strategies inspired by the TRRespass fuzzer. Finally TRRespass has received prestigious awards from both the academic (Best Paper at IEEE S&P and Top Picks Honorable Mention at IEEE Micro) and the technical (Pwnie Award for Most Innovative Research at BlackHat USA) security communities.

Jury's assessment:

This paper demonstrates the very important role of security researchers today. RowHammer attacks have been known for a while, and industry has claimed that they have been largely fixed. However, the authors of this paper demonstrated in their very thorough study that this claim is simply not true. Some defenses touted for RowHammer attacks are disabled in practice, and our systems are now even

more vulnerable. The strong message that this paper sends is that security by obscurity does not work, and to achieve better security, industry should be more **open** with the research community. Therefore, the impact of this paper in industry is extremely substantial.
This recent publication in an A* (top tier) computer security conference has gained more than 50 citations to day, demonstrating its relevance and impact in the community.

Runner up: paper #02
***A Highly Accurate Query-Recovery Attack against Searchable Encryption using Non-Indexed Documents***

Authors: Marc Damie, Florian Hahn, and Andreas Peter
Published at: 30th USENIX Security Symposium (USENIX Security 2021)
Link: https://www.usenix.org/conference/usenixsecurity21/presentation/damie

Motivation by the nominator:
Searchable encryption is a promising approach to store data on a remote server in encrypted form while still allowing for the efficient search on this data without revealing the search queries in the clear. Efficient schemes typically leak the access pattern (= sequence of identifiers of all data items that match the search query) and the search pattern (= sequence of identifiers of search queries), which can be exploited in query-recovery attacks to reveal the cleartext query of an encrypted search. Existing attacks make strong assumptions on the attacker's background knowledge. The nominated paper describes the first query-recovery attack that works under very mild assumptions while achieving comparable or even higher accuracies than the state-of-the-art. The authors show how certain countermeasures can be implemented to mitigate the described attack. Unfortunately, these countermeasures lead to losses in search performance, hindering practical deployment of searchable encryption. Therefore, the described attack further complicates the open research question on how to balance security with efficiency requirements in searchable encryption. The research follows the principles of open science and is fully reproducible. Because of this, it also passed the USENIX Artifact Evaluation: https://github.com/MarcT0K/Refined-score-atk-SSE.

Jury's assessment:
This is a strong attack paper on symmetric searchable encryption schemes that achieves real impact with real-world deployments. This is also an excellent example of rigorous foundational research.
It is commendable that this paper follows the open science principles and has passed the independent artifact evaluation process. The effort put by the authors into transparency and reproducibility of their research allows other researchers to build on their results. The Jury highlighted that this is very important for the community.

Runner up: paper #06
***Speculative Probing: Hacking Blind in the Spectre Era***

Authors: Enes Goktas, Kaveh Razavi, Georgios Portokalidis, Herbert Bos, and Cristiano Giuffrida
Published at: ACM Conference on Computer and Communications Security 2020 (CCS'20)
Link: https://doi.org/10.1145/3372297.3417289

Motivation by the nominator:
The BlindSide attack shows that in the Spectre era, attackers armed with a single memory corruption vulnerability are able to "hack blind" without triggering even a single crash. That is, given a simple buffer overflow in the kernel and *no* additional information leak vulnerability, BlindSide can mount blind brute-force attacks in the *speculative execution domain* to repeatedly probe and derandomize

the kernel address space, craft arbitrary disclosure gadgets, and enable reliable exploitation. This works even in the face of strong defenses, e.g., fine-grained ASLR (FGKASLR), execute-only memory, and state-of-the-art Spectre mitigations. It had immediate impact and led to grsecurity (behind major innovations like ASLR and NX) developing a new CFI defense against BlindSide. BindSide shows for the first time that blind attacks are effective even against crash-sensitive targets like the kernel, with practical exploits ranging from root password hash leaks to arbitrary code execution. Generalizing both speculative execution attacks and traditional software exploitation, BlindSide shows it no longer suffices to consider threat models in isolation and is the first combined attack where the combination is *greater* than the sum of its parts. For this reason, it was recognized by the larger security community with the Pwnie Award for Most Innovative Research

Jury's assessment:
This paper provides an important generalisation of the speculative attacks that gained attention in recent years. In this systematic study the researchers bring together many findings from the Spectre era. It demonstrates a new kind of speculative attacks, and the community needs to develop new defenses against it.
Additionally, this paper is very accessible and easy to be read and followed also for readers not very familiar with the topic. The authors have made an effort in making the content accessible by a wider audience creating videos and artifacts, which is commendable. The Jury believes that this paper will have a big impact in security education, and it is very likely that the paper and the associated material will be highly used by students to learn the topic. Overall, the work is an excellent example of communicating science beyond the paper itself.

**Jury Members Dutch Cyber Security Research Paper Award 2021**

**Prof. dr. Sascha Fahl**
*Professor CISPA Helmholtz Center for Information Security, DE*

Sascha Fahl studies the intersection of computer security and privacy with human factors particularly. Professor Fahl is interested in investigating end users, operators, developers and designers of computer systems and their interdependencies with computer security and privacy mechanisms. His research involves large-scale analyses of the Internet and software repositories to understand the huge challenges humans face when interacting with computer security and privacy mechanisms.

*more at https://saschafahl.de/*

**Prof. dr. Patrick Schaumont**
*Professor in Computer Engineering at Worcester Polytechnic Institute (WPI), USA*

Patrick Schaumont is Professor of Computer Engineering at the Vernam Lab of Worcester Polytechnic Institute in Massachusetts, USA. His research interests are in design and design methods of secure, efficient and real-time embedded computing systems. He was also visiting researcher at the National Institute of Information and Telecommunications Technology (NICT) in Japan and at Laboratoire d'Informatique de Paris 6 in Paris in France. He served as program co-chair for several conferences in cryptographic and secure engineering, including CHES, HOST, ASHES, and FDTC.

*more at https://schaumont.dyn.wpi.edu/schaum//*

**Dr. Magnus Almgren**
*Associate professor at Chalmers university of technology, SE*

Magnus Almgren is an associate professor at Chalmers university of technology in the department of computer science and engineering. His research interests include system security, in particular intrusion detection systems, machine learning in security, and security suitable for IoT and other types of cyber-physical systems. He is a member of the editorial board for the International Journal of Information Security and the steering committee for DIMVA and NordSec.

*more at http://www.cse.chalmers.se/~almgren/index.html*

**Technical Chairs Dutch Cyber Security Research Paper Award 2021**

**Dr. Francesco Regazzoni**
*Assistant professor at Informatics Institute University of Amsterdam, NL*

Francesco Regazzoni is assistant professor at University of Amsterdam. He obtained his Ph.D. degree from Università della Svizzera italiana in 2010, and his M.Sc. degree in Computer Engineering from Politecnico di Milano in 2003. Dr. Regazzoni has been visiting researcher at NEC Labs America, Ruhr-Universitat Bochum, EFPL Lausanne, and Nanyang Technological University Singapore, and assistant researcher at Universitè Catholique de Louvain and Delft University of Technology. His research interest are in side channel attacks, design automation for security, and lightweight cryptography.

*more at https://www.uva.nl/en/profile/r/e/f.regazzoni/f.regazzoni.html*

**Dr. Olga Gadyatskaya**
*Assistant professor at the Leiden Institute of Advanced Computer Science, NL*

Olga Gadyatskaya is an assistant professor at the Leiden Institute of Advanced Computer Science. She works on a variety of cyber security topics, ranging from security risk management and threat modeling to mobile security and secure software development. Her main goal is to make organisations more secure by improving their security management practices, helping them to secure their software and systems, providing them insights into cyber threats, and assisting them in making decisions about cyber security.

*more at https://ogadyatskaya.github.io/*