Jury Report Dutch Cyber Security best Research Paper Award (DCSRP Award) 2018

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 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 2018 the best research paper contest is held for the fourth 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 Five out of 15 papers nominated by eight different Dutch research institutes.

ICT.OPEN 2018 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, part of the ICT.OPEN 2018 conference program, is scheduled March 20th 2018. 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 Five 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 Five, 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.

Jury Report Dutch Cyber Security best Research Paper Award (DCSRP Award) 2018

ICT.OPEN 2018 is a conference organized by NWO and IPN. This year the thematic session on cyber security is organized by CSng (CyberSecurity next generation scientists) with the support of dcypher (Dutch cybersecurity platform higher education & research).
The Dutch Cyber Security best Research Paper contest 2018 is organized by dcypher and the associated award is sponsored by IBM.

Research Paper Top Five

1. Paper title: **Economic Factors of Vulnerability Trade and Exploitation**
Presenter: Luca Allodi (on video)
Author: Luca Allodi, Eindhoven University of Technology
Published at: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (ACM CCS 2017)

Motivation by Sandro Etalle
Dr. Luca Allodi infiltrated a prominent, segregated (Russian) cybercrime market to study the underground economy of cyber-attack acquisition. This required 6+ months of committed research efforts.This paper is the first to quantitatively link cybercrime economics with actual risk of attack 'at scale', and provides evidence-based estimates of the effect of vulnerability characteristics on market activity and odds of exploitation. In doing so, this paper goes well beyond current allegations on “attacker economics”, and paves the way for future research on attack development, risk metrics, defensive strategies, as well as standard practices for cyber-risk management. Aware of the difficult nature of this data, Luca spent more than 3 years prior to this study in thoroughly understanding the market dynamics. This was an exceptional effort in scientific rigorousness, that goes well against the “publication fever” of publishing all interesting data as soon as available. I think this aspect should be rewarded in itself. Remarkably, this is also acknowledged by a CCS reviewer, that states to be “also impressed by the analysis methodology”. Further, this paper received international media attention, and is the only one-author paper at ACM CCS'17, which only reinforces the perceived quality of security research in the Netherlands.

Jury’s assessment:
The Jury considered this an intriguing paper about an exciting study (or “cool work”) with high impact on specific branches of security research. Amongst the results: a detailed analysis of hidden aspects of cybercrime, a very thorough statistic approach resulting in a better understanding of the functioning of this dark market; less need to speculate. The Jury admired the fact that the author was able to infiltrate into this exploit-as-a-service market. Given the fact this is a study on one specific market, and might be hard to reproduce, the impact on broad society is limited. Luca Allodi deserves more compliments, since he has done most of his research on his own, and presented his paper at a highly ranked conference ACM CCS’17. Not amazing that this study received international media attention!

Jury Report Dutch Cyber Security best Research Paper Award (DCSRP Award) 2018

2. Paper title: **ASLR on the Line: Practical Cache Attacks on the MMU**
Presenter: Ben Gras
Authors: Ben Gras and Kaveh Razavi et al., VU University Amsterdam
Published at: NDSS

Motivation by Herbert Bos:

Introduction

Despite papers in many other tier-1 venues, for the VUSec security group at Vrije Universiteit Amsterdam, 2017 was probably the year of "ASLR on the Line". This award-winning paper, published originally at NDSS and awarded no fewer than 4 CVEs and a Pwnie Award, shows that one of the most common and most important defenses against exploitation, Address Space Layout Randomization (ASLR) is fundamentally broken for all systems. As soon as attackers are able to execute any code on the victim machine, even if it is just some JavaScript in a web browser, they can break the randomization offered by ASLR. The issue is strongly related to the way in which modern processors translate virtual addresses into the physical addresses used by the hardware. These transactions are at the heart of modern processors and the way they take place are essential to the performance offered by modern computer systems. In other words, fixing this vulnerability in software is not possible without suffering a tremendous performance impact, well beyond what anyone would consider acceptable. The conclusion is that one of our prime defenses against software exploitation is fundamentally broken on all modern processors. Ben Gras and Kaveh Razavi personally verified that it is effective on all 25+ CPU architectures that we tried.

Breaking ASLR from the browser

With stack protection and non-executable stack/data sections, ASLR is one of three core defenses implemented in common operating systems such as Windows, Linux, *BSD, Android, and MacOS. Moreover, the non-executable stack/data sections are also pointless. Likewise, many even more powerful defenses now proposed in the research community depend on ASLR at heart. Break ASLR and you break all them. Being able to do this from native code would be bad already, but what the paper demonstrates is that attackers can even do this from JavaScript in a browser, the code that powers almost every popular website today. If an attacker is able to lure the victim to a malicious website, or place a malicious ad on a legitimate one, the client's browser is at threat from our attack.

Unpatchable

Specifically, it shows that ASLR is broken due to how modern CPUs use caching, hence the name of the attack: AnC (A SLR n ot C ache). Unlike other side channels that have become popular in recent years, there is no practical patch for AnC. Where common side channels such as existing cache attacks target the way the process addresses memory and thus can typically be mitigated by changing the way memory is laid out, AnC side channels the Memory Management Unit (MMU) itself a hardware unit. It represents some of the core operations of the CPU and cannot be easily fixed by redesigning processes or operating systems. In that way, it resembles the Meltdown/Spectre vulnerabilities that recently generated such

furore, except that the performance cost of fixing AnC will be even (much) higher than the proposed Meltdown/Spectre fixes.

Pwnie Award for Most Innovative Research

The novelty and seriousness of the AnC technique received wide-spread recognition from the wider infosec community and even won the prestigious Pwnie Award for Most Innovative Research at a ceremony during the Black Hat conference in Las Vegas. Likewise, the vulnerability was slashdotted and led to worldwide coverage in WIRED, The Register, and media from Australia to Europe, and from Japan to the US. All the major browser vendors responded to our suggestions to at least make the attack harder. We worked directly with Apple's Product Security Team to harden the Safari browser which Apple generously acknowledged. The interest for AnC is still very strong and we have presented the work in many invited presentations at conferences such as Black Hat, CCC, ESSoS, Hardwear.IO, SummerCon, etc. This, combined with the awards, shows the impact of the paper on both the academic and non-academic community.

Jury's assessment:

This interesting paper, presented at a tier-1 conference, describes excellent and innovative research. The authors reached a great result by discovering how caches leak data in a most surprising way. Recent Spectre vulnerabilities show that the identified hardware-related threats are more important and more prevalent than initially thought to be. The paper has more than 34 citations in Google Scholar but its impact is broader than information security research, because the study shows every browser has unpatchable vulnerabilities. The Jury considered this an excellent piece of work, performed by a single Dutch research group, with a broad impact. The many prices won and the impressive media coverage demonstrate this.

3. Paper Title: **The Dynamics of Innocent Flesh on the Bone: Code Reuse Ten Years Later**

Presenter: Manolis Stamatogiannakis

Authors: Victor van der Veen and Dennis Andriesse et al., VU University Amsterdam

Published at: CSS17

Motivation by Herbert Bos:

Introduction

Ten years ago at CCS07, Hovav Shacham published a paper, The Geometry of Innocent Flesh on the Bone, that had a profound impact on the security community. Previously, researchers assumed that an attacker should inject (shell-)code in a vulnerable program and have the program execute it. However, this was getting harder as the programs stack and data areas were made non-executable. Shacham showed that instead you could just reuse the instructions already present after all, there are plenty of them and all are executable. Everything changed. Code reuse became the dominant exploitation technique and all follow-up research, be it offensive or defensive, followed Shachams approach.

Geometry

Jury Report Dutch Cyber Security best Research Paper Award (DCSRP Award) 2018

The approach was intuitive: attackers would first examine the program binary using static analysis to examine the layout of the code (its geometry) to detect simple code snippets (gadgets) to reuse in an attack, and then, at attack time, chain them together to create a malicious payload. Ever more advanced defenses both in academia and industry aimed for exactly that threat model: an advanced static analysis to find suitable gadgets. Every security conference brought more techniques to make this analysis more difficult and counter increasingly sophisticated attacks, in the hope that one day we would make the wiggle room so small and defenses so strong that static analysis could no longer bear fruit for attackers.

Questioning the assumptions

Ten years later, the Newton paper is the first to re-examine the original assumptions in Shachams paper. Simply said: real attackers do not care about finding gadgets, or about constructing powerful Turing-complete machines out of them. Nor are they interested in the limits of static analysis. All they want is to execute a sensitive system call that allows them to pwn the victim. Why would they limit themselves to static analysis?

Dynamics rather than geometry

Newton shows that even a modicum of dynamic analysis allows attackers to bypass the most advanced defenses effortlessly. The idea behind Newton is extremely simple. Intuitively, it runs the target program, say a webserver, with the simplest possible input (e.g., a single request) and then tracks where all the bytes that the attacker can modify with the vulnerability end up. For instance, it may be that a byte under the attackers control determines which system call the program makes, or which arguments are passed to a system call. The attacker has no idea how those bytes got there, and does not care. As long as the attacker manages to execute the right system call with the right arguments, the exploit is done. No advanced analysis needed. Newton bypasses all known advanced defenses developed in the past decade. It forces the security community to return to the drawing board and radically changes the defenses to also incorporate an attacker using dynamic analysis. At the CCS conference, Victor was presenting the paper in a special session, that as a token of honor, had Hovav Shacham himself introduce the work and lead the discussion. In our opnion, the paper represents the most significant step in a decade of frantic research in the wake of the original code reuse paper, and the start of a whole new direction in security research.

Jury's assessment:

Very interesting research, resulting in a well written, impressive paper. Extremely relevant work. Their elegant and novel attack strategy was published at the highly ranked CCS 2017 conference. During 10 years a code-reuse strategy based on static analysis was used. In the study a radically novel strategy is introduced, called the Newton framework, based on static and dynamic analysis, knowing that during a decade attackers succeeded in bypassing classic protections.

Jury Report Dutch Cyber Security best Research Paper Award (DCSRP Award) 2018

4. Paper Title: **Herding Vulnerable Cats: A Statistical Approach to Disentangle Joint Responsibility for Web Security in Shared Hosting**

Presenter: Samaneh Tajalizadehkhoob

Authors: Samaneh Tajalizadehkhoob, Delft University of Technology, Tom Van Goethem, imec-DistriNet, KU Leuven, Maciej Korczyński, Delft University of Technology, Arman Noroozian, Delft University of Technology, Rainer Böhme, Innsbruck University, Tyler Moore, The University of Tulsa, Wouter Joosen, imec-DistriNet, KU Leuven, Michel van Eeten, Delft University of Technology

Published at: CCS '17 Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security

Motivation by Michel van Eeten:

This paper presents the first study that combines a comprehensive measurement of security practices in the global shared hosting market and statistically estimates the impact of different practices on abuse rates. This paper also presents a unique approach to empirically disentangling the responsibility and influence of providers in fighting web compromise. When the defenses fall short and resources are compromised, hosting providers are regularly faulted for not doing enough to forestall compromise. While hosting providers play a key role, their ability to prevent abuse is constrained by the security practices of their own customers, especially in shared hosting where customers operate under restricted privileges and providers retain more control over configurations. The paper answers the question of what providers can realistically achieve in terms of preventing abuse.

Jury's assessment:

This measurement paper addresses an important topic; it is based on a large study, among others resulting in very useful guidelines for hosting providers. A clever analysis allows results to be drawn from the things that can be measured, without assuming that the things that were measured were inherently important. Results were presented at a top conference, the scientific significance is relatively limited, but the (societal) impact is high.

5. Paper Title: **Millions of targets under attack: a macroscopic characterization of the DoS ecosystem**

Presenter: *Presenter:* Mattijs Jonker (on video)

Authors: Mattijs Jonker, University of Twente, Alistair King, CAIDA, UC San Diego, Johannes Krupp, CISPA, Saarland University, Christian Rossow, CISPA, Saarland University, Anna Sperotto, University of Twente, Alberto Dainotti, CAIDA, UC San Diego

Published at: Proceedings of the Proceedings of the 2017 ACM Internet Measurement Conference (IMC) November 1-3, 2017 London, UK ACM ISBN 978-1-4503-5118-8/17/11

Jury Report Dutch Cyber Security best Research Paper Award (DCSRP Award) 2018

Motivation by Aiko Pras:

The paper has been published at the ACM-IMC conference, which is among most prestigious conferences in its kind worldwide. The research has been performed by Mattijs Jonker (University of Twente) during his 6 months stay at the Center for Applied Internet Data Analysis (CAIDA), San Diego, USA. For the first time, a large-scale analysis of victims of internet denial-of-service (DoS) attacks worldwide has been carried out. And what is found is, in a phrase from the paper, “an eye-opening statistic”. Spanning two years, from March 2015 to February 2017, about one-third of all /24 networks were subject to some kind of DoS attacks, where a perpetrator maliciously disrupts services of a host connected to the internet. The study showed that 2.2 million /24 networks (one third of the address space) experienced 20 million attacks during the study, either as direct DoS attacks or some kind of reflection attack, and 137,000 targets were hit by both kinds of attack. To perform this research, data from multiple sources had to be analysed, including active DNS measurement data from the OpenINTEL project (University of Twente), UCSD Network Telescope (CAIDA), the AmpPot network of DDoS honeypots (CISPA) and data gathered from DDoS prevention companies like Cloudflare. The paper attracted quite some attention from various media, including The Register and the dcypher website.

Jury’s assessment:

Relevant and interesting measurement paper, based on a large study, with a wide impact and presented at the prestigious ACM-IMC conference. The research combines different types of measurement to give an overall picture, some of the results are presented a bit sensationalistic, but nonetheless a very useful snapshot.

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 fifteen paper nominations. Out of the Top Five as presented today, one paper deserves the predicate **best** Dutch Cyber Security Research Paper.

Final conclusion of the Jury

*Because of the high quality of the presented Top Five papers, the Jury had a very difficult choice to make. In the opinion of the Jury especially the work of Luca Allodi and the VUsecurity team sticks out, all world class research! Ultimately they decided to proclaim ”ASLR on the Line: Practical Cache Attacks on the MMU” as the winning paper. This means the author duo **Ben Gras and Kaveh Razavi** from the VU University Amsterdam are the winners of the 2018 Dutch Cyber Security Research Paper Award.*

Jury Report Dutch Cyber Security best Research Paper Award (DCSRP Award) 2018

Drs. Jan Piet Barthel,

Chairman Jury Dutch Cyber Security Research Paper Award 2018, Director dcypher

Jan Piet Barthel is Director of the Dutch platform for cybersecurity higher education and research and also is 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.dcypher.nl/en/content/drs-jp-jan-piet-barthel

Prof. Dr. Konrad Rieck

Professor (W3) Computer Science TU Braunschweig

Konrad Rieck is a Professor of Computer Science at TU Braunschweig and heads the Institute of System Security. His research interests revolve around Computer Security and Machine Learning. His group is developing novel methods for the detection of computer attacks, the analysis of malicious software and the discovery of vulnerabilities.

more at https://www.tu-braunschweig.de/sec/team/rieck

Prof. Evangelos Markatos

Professor Computer Science University of Crete

Evangelos Markatos is a Professor in the Department of Computer Science, University of Crete and the head of the Distributed Computing Systems Laboratory of the Institute of Computer Science, FORTH. His research interests are in the broader area of Systems: Internet Systems and Monitoring, Systems and Network Security, World Wide Web, Internet Systems and Technologies and Operating Systems.

more at http://www.ics.forth.gr/dcs/index_main.php?l=e&c=513

Dr. Richard Clayton

Doctor Computer Laboratory University of Cambridge, Director Cambridge Cloud Cybercrime Center

Richard Clayton works in the field of "security economics". When there is security failure a technical investigation will tell you what failed and how it did so -- but looking at the economic forces in play will often tell you why it was built that way and why it was allowed to fail. His research interest are many types of online crime like phishing and developing innovative ways of detecting and mitigating email spam.

more at https://www.cl.cam.ac.uk/~rnc1/