15-NROI-019

Jury report Dutch Cyber Security Research paper Award 2015

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.

IIP-VV

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 (2014/2013) scientific cybersecurity research paper. The ICT.OPEN 2015 conference is an excellent place with the right audience to announce the first winner! An organization committee of IIP-VV board members designed the nomination and assessment process and came up with a long list of possible (foreign) jury members. Based on this NWO Physical Sciences composed a jury with the task to assess acceptable papers received as a result of the nomination process. The Jury consists of three well-respected scientists in the cybersecurity field, under technical chairmanship of NWO. Out of 16 papers received, the Jury selected the Top Five.

Track 'Highlights of Cyber Security Research' during ICT.OPEN 2015

The cybersecurity track within the ICT.OPEN program is scheduled in the afternoon of March 24th 2015. The objective of this track is to demonstrate the progress and achievements in the execution of recent Dutch cybersecurity research. During the track primary authors of selected papers will present their publications. On behalf of the Jury they receive a certificate from the chair: the "Dutch Cyber Security Research paper Award", signed by jury members. The jury not only selected the Top Five, but also unanimously determined which paper ranks as the very best out of this set of five. The ultimate winner receives a special Best Paper Award from Dr René Penning De Vries, recently appointed by the Dutch minister of Economic Affairs as Dutch ICT-Figurehead, and a special bonus donated by IBM. This bonus, a € 500 cheque, for the team of authors responsible for the best cybersecurity paper, is personally presented to the primary author and speaker by the IBM Director Security Europe, Johan Arts.

ICT.OPEN 2015 is a conference organized by NWO, STW and IPN.
The Dutch Cyber Security Research paper Award 2015 is sponsored by IBM.

Top 5 Paper Reports

1. On the Practical Exploitability of Dual EC in TLS Implementations
Stephen Checkoway, Matthew Fredrikson, Ruben Niederhagen, Adam Everspaugh, Matthew Green, Tanja Lange, Thomas Ristenpart, Daniel J. Bernstein, Jake Maskiewics and Hovav Shacham

Jury's assessment:

The Dual EC (pseudorandom number generator) paper from the Coding Theory and Cryptology group of the Eindhoven Technical University, presented by Ruben Niederhagen, was published at the 23rd USENIX Security Symposium in 2014. This symposium is known as one of the most prestigious venues in security research.

The paper shows the practicality of an attack against several implementations of the important Transport Layer Security protocol. Despite claims from NSA that it would be impossible to exploit alleged backdoors in TLS implementations, the paper shows that with moderate computer power the backdoor can be easily exploited. The result is very important, because it has shed light on a very controversial issue, such as the manipulation of algorithms by specific attackers.

The Jury concluded that this is a very influential paper with a clear demonstration of practical problems!

2. Out of Control: Overcoming Control-Flow Integrity
Enes Göktas, Elias Athanasopoulos, Herbert Bos and Georgios Protokalidis

Jury's assessment:

The "Out of Control" paper from the System Security group of the VU in Amsterdam, and presented by its primary author Enes Göktas, was published in May 2014 at the IEEE Symposium on Security & Privacy, one of the most important and prestigious venues in security research. The title nicely summarizes what the paper is about: the hijacking of the control flow. It demonstrates bypasses of several Control-Flow Integrity (CFI) implementations. In fact it was the first paper proving the limitations of state-of-the-art CFI implementations. In other words, it underlined the inefficacy of some countermeasures on very sophisticated forms of attack.

The paper triggered many researchers around the world to search for better solutions, which are able to stop increasingly sophisticated attacks.

The Jury concluded this is a very timely topic, with very high impact, resulting in further debate, follow-up research and follow up papers. This debate under researchers is still going on.

3. Quantum-secure authentication of a physical unclonable key
Sebastianus A. Goorden, Marcel Horstmann, Allard P. Mosk, Boris Skoríc and Pepijn W.H. Pinkse

Jury's assessment:

This authentication paper from the technical universities of Twente and Eindhoven, published December 2014 in Optica, and presented by Boris Skoríc, describes an interesting topic, not at the heart of computer science, but a nice application of quantum optics for a cybersecurity challenge. This work experimentally demonstrates the "quantum readout" authentication technique, which provides unconditional security against a whole class of spoofing attacks. The attacker cannot emulate the expected optical response, even if all information of the key is known.

The Jury calls quantum secure authentication a surprising new idea and a strong result of a fundamental problem, although it becomes not fully clear how practical this is and what the scientific impact will be. It is recognized that the paper has generated tremendous international media interest. It is rare that fundamental research in security reaches such a broad audience.

4. Framing Signals - A Return to Portable Shell code
Erik Bosman and Herbert Bos

Jury's assessment:

The "Framing Signals" paper from the System Security group of the VU in Amsterdam, and presented by its primary author Erik Bosman, was originally written for the IEEE Symposium on Security and Privacy conference held in May 2014. As already mentioned in another report, this conference is one of the most important and prestigious venues in security research. The paper explains that the traditional signal handling of UNIX-based systems can be misused by attackers using a (reusable) Sigreturn Oriented Programming approach. The security issue discovered and analysed is about as old as the C-programming language itself.

The paper describes an interesting construction of a "weird machine" for executing attack payloads, in other words a machine programmed in such a way that it manipulates or behaves far beyond its intended use.

The Jury considered this nice technical work, which however does not elaborate on computer attacks techniques themselves. The Best Student Paper award at IEEE S&P is very well deserved. The results triggered an interesting scientific debate.

5. Verifying Curve25519 Software

Yu-Fang Chen, Chang-Hong Hsu, Hsin-Hung Lin, Peter Schwabe, Ming-Hsien Tsai, Bow-Yaw Wang, Bo-Yin Yang and Shang-Yi Yang

Bart Jacobs (RUN) Digital Security group

Jury's assessment:

The Curve25519 Software verification paper from the Digital Security group of the Radboud University of Nijmegen, and presented by Peter Schwabe, was published for the Conference on Computer and Communications Security in 2014. The paper is about the formal verification of high speed Curve25519 elliptic curve cryptographic key exchange protocol software. Cryptographic software forms the backbone of information security. The article spans two fields of cybersecurity research: cryptography and formal verification.

The verification approach presented in this paper established with strong assurance that the optimized code implements the correct mathematical formulas, and hence ensures that the code does not suffer from implementation-level bugs.

The Jury considers this interesting write-up an impressive application of state of the art formal verification techniques to a hand-optimized implementation of a crypto primitive. It is challenging technical work and a nice example of international collaboration, with important practical impact.

The Winner *(text to be used by René Penning de Vries):*

Jury members, who individually ranked and collectively decided on the quality of the papers received, were highly impressed by the Dutch research as described in all 16 nominations. Primary authors of the Top Five papers each receive a signed certificate for their paper presentation. Out of these Top Five, one paper deserves the predicate best Dutch cybersecurity research paper.

René: *"I have the honor to present a special certificate to primary author Enes Göktas, because the Jury unanimously chose his paper "**Out of Control: Overcoming Control-Flow Integrity**", co-authored by Elias Athanasopoulos, Herbert Bos and Georgios Protokalidis, as the best Dutch cybersecurity research paper."*

After this Johan Arts, IBM Director Security Software Europe, offers a bonus cheque to the winner.

Jury members

- Professor Thorsten Holz (Germany)
- Professor Frank Piessens (Belgium)
- Professor Danilo Bruschi (Italy)
- Jan Piet Barthel (NWO NL) – chair

The Dutch Cyber Security Research paper Award 2015 is an initiative of the ICT Innovation Platform "Security and Privacy".

Veilig Verbonden