2nd AMSec Workshop

Date and Time

Wednesday October 9, 2019.
The technical program starts as 13:00h (walk-in and coffee as of 12:30h).

Location

Euler Room
Amsterdam Science Park Congress Center
Science Park 125
1098 XG Amsterdam

Program

13:00 - 13:30 : Marc Stevens (CWI): *Real world cryptanalysis*

13:30 - 14:00 : Yuri Demchenko (UvA): *Cloud Security services and mechanisms: Can modern clouds provide secure and trusted environment for data and business applications?*

14:00 - 14:30 : BREAK

14:30 - 15:15 : Keynote - Ronald de Wolf (CWI, UvA, QuSoft): *The potential impact of quantum computers on society*

15:15 - 15:45 : Erik van der Kouwe (Leiden): *Benchmarking Crimes in Systems Security*

15:45 - 16:15 : BREAK

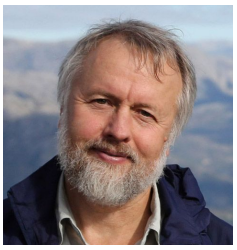
16:15 - 16:45 : Marleen Weulen Kranenbarg (VU, NSCR): *Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure*

16:45 - 17:15 : Joeri Toet (VU): *Move fast, but break (only) your own things?*

17:15 - 18:00 : DRINKS

Speakers

Yuri Demchenko



Senior researcher at the System and Network Engineering Research Group, University of Amsterdam

Erik van der Kouwe

Assistant professor in security at the Computer Systems Group of the LIACS, Leiden University.

Marc Stevens

Researcher in the Cryptology Group at CWI.

Joeri Toet

Lecturer at the Faculty of Law, Internet Law, VU Amsterdam.

Marleen Weulen Kranenbarg

Assistant professor at the Faculty of Law, Criminology, VU Amsterdam; author at NSCR, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving.

Ronald de Wolf

Researcher at the Algorithms and Complexity Group of CWI; part-time full professor at the ILLC, University of Amsterdam; member of QuSoft.

Presentations

Real world cryptanalysis

- Marc Stevens (CWI)

In this talk I will give an overview of cryptanalytic collision attacks on hash functions and how these impacted the real world. It will go from theory to practice to large scale computations to real world threat demonstrations, including supermalware and counter-cryptanalysis, and show the demise of one of industry's old de facto cryptographic standard to a cryptanalytic toy.

Cloud Security services and mechanisms: Can modern clouds provide secure and trusted environment for data and business applications?

- Yuri Demchenko (UvA)

The talk will provide a brief overview of the general cloud security model and security services and mechanisms, and next look at how they can be used to provide secure and trusted environment in few use cases of data centric applications. The talk will also introduce the proposed Virtual Infrastructure Trust Bootstrapping (VITBP) protocol that allows bootstrapping cloud virtual infrastructure and on-premises infrastructure.

The potential impact of quantum computers on society

- Ronald de Wolf (CWI, UvA, QuSoft)

This talk considers the potential impact that the nascent technology of quantum computing may have on society. It focuses on three areas: cryptography, optimization, and simulation of quantum systems. We will also discuss some ethical aspects of these developments, and ways to mitigate the risks.

Benchmarking Crimes in Systems Security

- Erik van der Kouwe (Leiden University)

Properly benchmarking a system is a difficult and intricate task. Even a seemingly innocuous mistake can compromise the guarantees provided by a systems security defense and threaten reproducibility and comparability. Moreover, as many modern defenses trade security for performance, the damage caused by benchmarking mistakes is increasingly worrying. To analyze the magnitude of the phenomenon, we identify 22 benchmarking crimes that threaten the validity of systems security evaluations, and survey 50 defense papers published in top venues. We show that benchmarking crimes are widespread even in papers published at tier-1 venues; tier-1 papers contain an average of five benchmarking crimes and we find only a single paper in our sample without any benchmarking crimes. Moreover, the scale of the problem appears constant over time, suggesting that the community is not yet taking sufficient countermeasures. This threatens the scientific process, which relies on reproducibility and comparability to ensure that published research advances the state of the art. We hope to raise awareness and provide recommendations for improving benchmarking quality and safeguard the scientific process in our community.

Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure

- Marleen Weulen Kranenbarg (VU, NSCR)

In the computer science field coordinated vulnerability disclosure is a well-known practice for finding flaws in IT-systems and patching them. In this practice, a white-hat hacker who finds a vulnerability in an IT-system reports that vulnerability to the system's owner. The owner will then resolve the problem, after which the vulnerability will be disclosed publicly. This practice generally does not focus on potential offenders or black-hat hackers who would likely exploit the vulnerability instead of reporting it. In this paper, we take an interdisciplinary approach and review the current coordinated vulnerability disclosure practice from both a computer science and criminological perspective. We discuss current issues in this practice that could influence the decision to use coordinated vulnerability disclosure versus exploiting a vulnerability. Based on different motives, a rational choice or cost–benefit analyses of the possible reactions after finding a vulnerability will be discussed. Subsequently, implications for practice and future research suggestions are included.

Move fast, but break (only) your own things?

- Joeri Toet (VU)

About the conditions under which the legal system would allow for an adequate level of security.