# 2nd Workshop on Cyber-Security Arms Race (CYSARM 2020)

Thanassis Giannetsos
Technical University of Denmark
Copenhagen, Denmark
atgi@dtu.dk

Daniele Sgandurra
Royal Holloway, University of London
Egham, United Kingdom
daniele.sgandurra@rhul.ac.uk

## ABSTRACT

The goal of CYSARM workshop is to foster collaboration among researchers and practitioners to discuss the various facets and trade-offs of cyber-security. In particular, how new technologies and algorithms might impact the cyber-security of existing or future models and systems.

## CCS CONCEPTS

• **Security and privacy** → **Intrusion/anomaly detection and malware mitigation**; **Tamper-proof and tamper-resistant designs**; *Trusted computing*.

## KEYWORDS

Arms-Race, Attackers and Defenders

**ACM Reference Format:**
Thanassis Giannetsos and Daniele Sgandurra. 2020. 2nd Workshop on Cyber-Security Arms Race (CYSARM 2020). In *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20), November 9–13, 2020, Virtual Event, USA.* ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3372297.3416250

## 1 BACKGROUND

Cyber-security is a complex ecosystem that is based on several contradicting requirements. For this reason, it is often defined as an arms race between attackers and defenders: for example, when a new security model or algorithm is devised, it could act as a double-edged sword since it might both enhance the security posture of a system and introduce additional vulnerabilities. Similarly, many of the novel technological solutions that are used to improve the security of systems and networks are also being used by those who wish to threaten well-established algorithms and protocols. For example, it is already known that when large-scale quantum computers become available they will be able to break almost all the public-key cryptographic algorithms currently in use. Security is also about balancing several trade-offs, e.g. security vs privacy, security vs trust, security vs usability, security vs cost, research vs standardization, academic research vs real applications, just to name a few. For example, while artificial intelligence provides the ability to efficiently analyse massive data streams to detect patterns of anomalous behaviour, it also threatens user privacy by enabling the analysis of individual behaviours, and democratic government by subverting opinions via electronic media. Likewise, the use of trustworthy computing and trusted hardware: while it fortifies systems by providing stronger security and operational assurance guarantees, it also allows attackers to perform stealthy attacks and could be used to damage user privacy.

*CCS '20, November 9–13, 2020, Virtual Event, USA*


## 2 WORKSHOP ORGANIZATION

For the second edition of the workshop, we received nine valid submissions. Each submission was reviewed by at least four TPC members, using a double-blind review process, and in the end three submissions were accepted for presentation at the workshop, of which two papers were selected as Full Papers and one paper was accepted as Short Paper, leading to a full acceptance rate of 22.2% and an overall acceptance rate of 33%. Submissions arrived from researchers in fourteen countries, from a wide variety of academic and corporate institutions. This year, based on careful consideration of attendees' health and safety, CYSARM 2020 took place as a virtual event.

In addition to the presentations from the authors of the accepted regular and short papers, this year CYSARM hosted a panel discussion with representatives of four EU H2020 project consortia to discuss how new technologies and algorithms developed within these projects will impact the security of future security models, and the various trade-offs involved during their design.

### 2.1 Objective and Topics of Interest

Topics of interest for CYSARM included the following:

- Arms races and trade-offs in cyber-security (e.g., attackers vs defenders, security vs privacy, security vs trust, security vs usability, etc.)
- Double-edged sword techniques in cyber-security (e.g., artificial intelligence)
- Impact of quantum computing on cyber-security (not limited to cryptography)
- Intrusion detection and evasion, and counter-evasion (also applied to malware analysis)
- Next-generation trustworthy computing security solutions and attacks (e.g., TPMs, TEEs, SGX, SE), and their impact
- Novel attacks and protection solutions in mobile, IoT and Cloud
- Security analysis of protocols, including use of formal techniques
- Standardization of cyber security and trust techniques
- Validation of cyber-security technologies
- Post-quantum cryptography and advanced cryptographic techniques (e.g., homomorphic encryption, secure multi-party computation and differential privacy)

## 2.2 Program Committee

We would like to thank the Program Committee that has helped us reviewing the papers.

- Christoforos Dadoyan (Ionian University)
- Tassos Dimitriou (Department of Computer Engineering, Kuwait University)
- Andrea Höller (Infineon)
- Ghassan Karame (NEC Research Labs)
- Ioannis Krontiris (Huwaei Technologies)
- Antonios Michalas (Tampere University)
- Melek Önen (Eurecom)
- David Oswald (University of Birmingham)
- Dimitris Papamartzivanos (Ubitech)
- Thomas Pöppelmann (Infineon Technologies)
- Paul Pop (Technical University of Denmark)
- Eamonn Postlethwaite (Royal Holloway, University of London)
- Elizabeth Quaglia (Royal Holloway, University of London)
- Matteo Repetto (CNR-IMATI)
- Mark D. Ryan (University of Birmingham)
- Peter Y A Ryan (University of Luxembourg)
- Riccardo Sisto (Politecnico di Torino)
- Fernando Virdia (Royal Holloway, University of London)
- Christos Xenakis (University of Piraeus)

We would like to thank General Chairs, Professor Liqun Chen and Professor Chris Mitchell for their help with the planning, design and organization of the workshop, as well as Ursula Polessnig, Martina Truskaller and Technikon for the Web and Publicity Chairs.

## 2.3 About the Organizers

**Liqun Chen** (liqun.chen@surrey.ac.uk) is a Professor in Secure Systems at the University of Surrey. Prior to joining Surrey in 2016, she was a principal research scientist at Hewlett-Packard Laboratories, Bristol, UK. During her 19 years working for the company, she has obtained 64 granted US patents with 35 further applications pending. She designed a number of the cryptographic algorithms used in the Trusted Platform Module and also developed several cryptographic schemes adopted by ISO/IEC and IEEE. She has published 2 books and around 150 articles in refereed journals and conference proceedings and edited 13 conference proceedings. Her co-authored paper, describing direct anonymous attestation, was given a test of time award at ACM CCS 2014. She has served as general or program committee chairman at 16 international conferences and as associate editor or member of the editorial board for 4 international journals. She has also served as editor or co-editor for 7 international standards.

**Chris Mitchell** (me@chrismitchell.net) was appointed as Professor of Computer Science at Royal Holloway in 1990, having previously worked at Racal Comsec, Salisbury, UK (1979-85) and Hewlett-Packard Laboratories, Bristol, UK (1985-90). At Royal Holloway he co-founded the Information Security Group in 1990, and helped launch the world's first MSc in Information Security in 1992. Since then he has taught a wide range of courses at both undergraduate and masters level, as well as successfully supervising well over 30 PhD students to completion. His research interests lie within information security, focusing on applications of cryptography. He has published around 250 articles in refereed journals and conference proceedings, and edited 14 books. He is co-editor-in-chief of Designs, Codes and Cryptography (Springer), and section editor for Section D of The Computer Journal (Oxford University Press). He has been active in international security standardisation for over 30 years, has served as editor for over 20 international standards, and received the IEC 1906 award recognising his exceptional contributions to international standardisation.

**Thanassis Giannetsos** (atgi@dtu.dk) is an Associate Professor in Secure Systems at the Technical University of Denmark. Dr. Giannetsos received the BSc degree in Computer Science and Communication Engineering from University of Thessaly, Greece, in 2006 and the MSc degree in Information Networking from Carnegie Mellon University, Pittsburgh, Pennsylvania, and PhD degree in Computer Science and Engineering from University of Aalborg, Denmark in 2012. Prior to DTU, Dr. Giannetsos was an Assistant Professor at University of Surrey, UK where he was involved in a variety of national and international research and development projects on the design of trusted computing architectures in cyber-physical systems. His research interests span from applied cryptography to privacy and security in information technology; in particular, encryption, Internet of Things, privacy-enhancing technologies and implementation of efficient and lightweight secure communication protocols. He has co-authored 1 book chapter and over 40 peer-reviewed publications, served over 15 PCs and received a grant from ACCESS Linnaeus Center, Sweden for his research activities in privacy, trust and security in mobile sensing systems. Thanassis has been involved in EU projects for more than 8 years having participated in more than 8 EU funded projects.

**Daniele Sgandurra** (daniele.sgandurra@rhul.ac.uk) is a Senior Lecturer in Information Security at Royal Holloway in the Information Security Group (ISG), where he leads the Systems and Software Security Lab (S3Lab). Daniele received his PhD in Computer Science from the University of Pisa. Prior to joining RHUL, Daniele was a Research Associate at Imperial College London (2014-2016) working on Cloud security, a PostDoc researcher at the National Research Council of Italy (2010-2013) working on mobile security, and a visiting researcher at IBM Zurich Research Laboratory (2009) working on virtual machine introspection. His research interests are related to practical aspects of cyber-security, by focusing on attacks and defences at various architectural layers. His recent work investigates the arms-race between malware and anti-malware systems and the usage of AI/ML within cyber-security.

## ACKNOWLEDGMENTS

CYSARM'20 has been co-sponsored by the following EU projects: FutureTPM (GA: 779391), INCOGNITO (GA: 824015), ASTRID (GA: 786922) and GUARD (GA: 833456 ). All projects have received funding from the European Union's Horizon 2020 research and innovation programme under the above-mentioned grant agreement numbers.