November 19, 2021
Virtual Event, Republic of Korea

Association for
Computing Machinery

Advancing Computing as a Science & Profession

CYSARM '21

Proceedings of the 3rd Workshop on Cyber-Security Arms Race

Sponsored by:

ACM SIGSAC

General Chairs:

Liqun Chen, University of Surrey
Chris Mitchell, Royal Holloway, University of London

Program Chairs:

Thanassis Giannetsos, Ubitech Ltd
Daniele Sgandurra, Huawei Technologies

Co-located with:

CCS 2021

Association for
Computing Machinery

Advancing Computing as a Science & Profession

The Association for Computing Machinery
1601 Broadway, 10th Floor
New York, NY 10019-7434

ISBN: 978-1-4503-8661-6

Additional copies may be ordered prepaid from:

ACM Order Department
PO Box 30777
New York, NY 10087-0777, USA

Phone: 1-800-342-6626 (USA and Canada)
+1-212-626-0500 (Global)
Fax: +1-212-944-1318
E-mail: acmhelp@acm.org
Hours of Operation: 8:30 am – 4:30 pm ET

Printed in the USA

CYSARM'21 Chairs' Welcome

It is our great pleasure to welcome you to the 3^{rd} *Workshop on Cyber-Security Arms Race (CYSARM)*! This year we are thrilled to continue chairing this workshop at a prestigious venue as the ACM Conference on Computer and Communications Security (CCS). Although CYSARM is at the early phases (this year marks the third edition of this workshop), the workshop is already fostering collaboration among researchers and practitioners to discuss the various facets and trade-offs of cyber-security. Being the first workshop of its kind, CYSARM benefits the cyber-security community by addressing novel (and often controversial) topics in cyber-security, such as trade-offs and double-edged sword techniques. Beyond the study of cyber-security, privacy and trust as standalone components, it is also important to look at how to balance their trade-offs especially when it comes to several contradicting requirements, such as security vs privacy, security vs trust, and security vs usability. CYSARM considers all complex facets and double-edged sword aspects of the cyber-security ecosystem, in particular, how new technologies and algorithms might impact the cyber-security of existing or future models and systems.

The CYSARM'21 call for papers attracted ten valid submissions. Each submission was reviewed by at least three TPC members, using **a double-blind review process**, and in the end fours submissions were accepted for presentation at the workshop, of which three papers were selected as Full Papers and one paper was accepted as Short Paper, leading to a **full acceptance rate of 30%** and an overall acceptance rate of 40%. Submissions arrived from researchers in **fifteen countries**, from a wide variety of academic and corporate institutions. In addition to the papers' presentations, we also encourage attendees to attend the keynote **talk**:

- *"Hyperion, A Voter-Friendly, Verifiable and Coercion-Resistant Voting Scheme".* Peter Y A Ryan (University of Luxembourg).

We will also host a round of presentations from four EU projects consortia.

Putting together *CYSARM'21* was a team effort. We first thank all the authors for the quality of their submissions. We are grateful to the **Program Committee** who worked very hard in reviewing papers and providing valuable feedback to authors. In addition, we would like to thank the **General Chairs**, Professor Liqun Chen and Professor Chris Mitchell, for their help with the planning, design and organization of the workshop, as well as Margherita Facca and MARTEL for **Web Chair** and **Publicity Chair**. Finally, we thank the hosting organization, our sponsor, ACM SIGs, and our **supporters**, EU Projects ASSURED (GA: 952697), C4IIoT (GA: 833828), PUZZLE (GA: 883540) and RAINBOW (GA: 871403)

We hope that you will find CYSARM'21 program interesting and thought-provoking and that the workshop will provide you with a valuable opportunity to share ideas with other researchers and practitioners from institutions around the world.

Thanassis Giannetsos
CYSARM'21 Program Chair
Ubitech Ltd, GR

Daniele Sgandurra
CYSARM'21 Program Chair
Huawei Technologies, DE

Table of Contents

CYSARM 2021 Workshop Organization

General Chairs: Liqun Chen (University of Surrey)
Chris Mitchell (Royal Holloway, University of London)

Program Chairs: Thanassis Giannetsos (Ubitech Ltd)
Daniele Sgandurra (Huawei Technologies)

Web and Publicity Chair: Margherita Facca (MARTEL)

Program Committee: Manos Athanatos (Foundation for Research and Technology)
Colin Boyd (Norwegian University of Science and Technology)
Tassos Dimitriou (Department of Computer Engineering at Kuwait University)
Giannis Giakoumakis (Foundation for Research and Technology)
Sotiris Kousouris (Suite5 Intelligence, Cyprus)
Ioannis Krontiris (huawei Technologies, Germany)
Kaitai Liang (Technical University of Delft, Netherlands)
Weizhi Meng (Technical University of Denmark)
Antonis Michalas (University of Tampere, Finland)
Edgardo Montes de Oca (Montimage)
Meni Orenbach (Nvidia)
David Oswald (University of Birmingham)
Dimitris Papamartzivanos (Ubitech Ltd)
Thomas Poeppelmann (Infineon Technologies AG)
Elizabeth Quaglia (Royal Holloway, University of London)
Peter Y A Ryan (University of Luxembourg)
Fulvio Valenza (Politecnico di Torino, Italy)
Christos Xenakis (University of Piraeus, Greece)

Sponsor: acm SIGSAC

Supporters:

ASSURE

C4IIoT

PUZZLE

RAINBOW