EDITORIAL MESSAGE
2020 Special Track on Computer Security

Giampaolo Bella, *Università di Catania, Italy*
Rosario Giustolisi, *IT University of Copenhagen, Denmark*

As chairs of the Computer Security track, we are pleased to welcome you to its nineteenth edition at the ACM Symposium on Applied Computing. The Program Committee for this track, as in past years, is composed of eminent representatives from both industry and academia. Here is the list of members of this year's committee, in alphabetical order:

Aslan Askarov (Aarhus University, Denmark)
Tom Chothia (University of Birmingham, UK)
Jannik Dreier (Université de Lorraine, France)
Paul Duplys (Robert Bosch GmbH, Germany)
Barbara Fila (INSA Rennes, IRISA, France)
Simone Fischer-Hübner (Karlstad University, Sweden)
Christian Gehrmann (Lund University, SE)
Christian Hammer (Potsdam University, DE)
Lucca Hirschi (Inria & LORIA, France)
Martin Johns (SAP Research, DE)
Erisa Karafili (Imperial College, UK)
Sokratis K Katsikas (Norwegian University of Science & Technology, NO)
Robert Künneman (CISPA Saarland University, DE)
Ilaria Matteucci (CNR, Italy)
Chris Novakovic (University of Birmingham, UK)
David Nowak (CNRS & Lille 1 University, FR)
Elizabeth Quaglia (Royal Holloway, UK)
Alejandro Russo (Chalmers, Sweden)
René Rydhof Hansen (Aalborg University, Denmark)
Sebastian Schinzel (Muenster University of Applied Sciences, DE)
Helen Treharne (University of Surrey, UK)
Melanie Volkamer (KIT, Germany)
Ruoyu Wang (Arizona State University, US)

This year we received 36 submissions, as usual from virtually everywhere in the world. The review process, which also involved a number of qualified delegates, was double-blind in the sense that the paper authors were kept anonymous from the reviewers. Each paper received at least 3 reviews, and all papers and reviews were ultimately discussed in depth by the entire Program Committee. As a result of this scientifically thrilling process, papers were marked either for acceptance or for rejection. In the end, only 10 papers were accepted. We are therefore confident of the high quality of the published material, and remain indebted to the reviewers for their thorough work.

Here is this edition's programme:

- Olivier and Han propose a new design of behavior-based malware signature, which are resistant against behavioral transformation and provide interpretable information about the decision of classification tasks.
- Kock et al. work concerns with testing web applications against race conditions that can have dramatic security implications. The underlying idea consists in combining race condition detection with dynamic testing, the former generating race condition candidates and the latter minimizing the number of false positives. The evaluation shows a reduction of candidates and some new race conditions with security implications.

- Xu et al. present novel attacks to evade Machine Learning-based classifiers that consider the whole call graph of an app. The authors craft adversarial apps based on two approaches and evaluate these approaches on a set of malware apps. The white-box approach achieves more than 70% evasion, where they know the exact configuration of the Machine Learning model.
- Bortolameotti et al. introduces HeadPrint, a tool that detects malicious applications in network traffic from header sequences. The authors evaluate HeadPrint using several databases of benign and malicious network traffic and compare HeadPrint's performance with DECANTeR. The results show that HeadPrint performs better at detecting malicious activity with fewer false alerts.
- Fuchs et al. analyse the security requirements for secure provisioning, storage and usage of credentials in an electric vehicle (EV), and proposes a security architecture for EV's charging and billing services, guaranteeing these requirements. The proposed solution is compliant with ISO 15118 and backward compatible for components that do not support the proposed architecture. They advance an implementation and evaluation of a proof of concept.
- Loch et al. address the problem of improving performance of taint analysis for Java programs written using the Java EE API. For this purpose, they present a tool called Juturna which performs taint analysis of string values in the program. Unlike prior taint analysis tools, Juturna utilizes program slicing to identify parts of the program where taint analysis is actually needed, and hence reduces performance overhead of taint tracking during execution of the program.
- Safarzadeh et al. present HAL-RD, a technique for synthesizing information contained within logs from disparate sources into a single, clear timeline describing an attack against a network. Their technique enables one to correlate entries across logs that would otherwise appear unrelated. The authors demonstrate the feasibility of HAL-RD using a running network intrusion example, and evaluate it using a further 11 similar attacks. Their technique is able to cross-correlate log entries with a high degree of precision, recall and accuracy.
- Abdelmawgood et al. present a method of protecting the kernel of a Virtual Machine. Attacks against the kernel are notoriously hard, however, the method presented by the authors works by marking parts of the kernel as read only, and building the machinery needed for a hypervisor to enforce this. This makes attacks based on malware chaining certain parts of the kernel code impossible.
- Demetrio et al. advance WAF-A-MoLE, a tool that defeats the ability of web application firewalls (WAFs) to detect SQL injection attacks. Leveraging the fact that semantically-equivalent SQL statements are often quite different syntactically, the authors propose a set of mutation operators that progressively transform a common malicious SQL injection string into an equally-malicious string that is undetected by state-of-the-art WAFs.
- McDonald et al. propose an approach for polymorphic circuit replacement based on random boolean logic expansion. The work addresses IP theft, which is a serious problem in the industrial context. The underlying idea is to derive an efficient method of expanding circuits to a given target size in order to make reverse engineering more difficult. This is done by converting it to a Boolean formula and applying a set of 28 expansion rules until a target size or a fixed number of expansion steps was reached.

About the track chairs

Giampaolo Bella is Associate Professor at the University of Catania, doing teaching and research in Computer Security and Formal Methods. He has chaired the Computer Security track at ACM SAC since its inception. After his Ph.D. from Cambridge University, he was a research associate at TU Munich, Cambridge University, and a senior researcher at SAP Research France. He has recently been developing formal approaches and methodologies to studying the security problem as a socio-technical, inter-disciplinary one.

Rosario Giustolisi is Assistant Professor at the IT University of Copenhagen. His research interests cover many aspects of computer security, including automated analysis of cryptographic protocols in the symbolic model, accountability notions in security protocols, and cybersocial security aspects of real-world systems. Before joining the security group at ITU, Rosario was a postdoc at SICS RISE and a member of the security lab in Lund, Sweden. He received his Ph.D. from the University of Luxembourg where he mainly worked in the design and analysis of secure exam protocols.