Call for Papers

https://spro.aspire-fp7.eu

Scope

Software Protection techniques aim to defend the confidentiality and integrity of software applications exposed to man-at-the-end (MATE) attacks, performed by a trusted user on a computer system.

MATE attacks can take many forms. In a tampering attack, the user violates the integrity of the code, by modifying it in ways the software vendor didn't intend. In a malicious reverse-engineering attack, he violates the vendor's confidentiality rights by extracting intellectual property from the code; in a cloning attack (software piracy), he violates copyright laws by distributing illegal copies.

Topics

1. Software Protection techniques

- Code Obfuscation, Anti-debugging, Software Diversity
- Data obfuscation, White-Box Cryptography
- Code Virtualization, Software Dynamic Translation
- Software Tampering Detection, Code Guards
- Software Renewability, Remote Attestation
- Software similarity, Plagiarism detection, Legal aspect
- Software Licensing, Watermarking, Fingerprinting, Anti-cloning
- Homomorphic Encryption, Hardware-Software co-design
- Open-Source tools for software protection

2. Software Protection Evaluation

- Insights on new reverse engineering techniques and their effectiveness against specific protection methods.
- Possible applications of Machine Learning for attacking and improving software protection.
- Evaluation Methodologies: security metrics, risk analysis, and empirical studies
- Resilience, De-obfuscation, Malware analysis
- Tools and their extensions for static and dynamic analysis
- Threat modelling, Petri nets, attack graphs, taxonomies and ontologies
- Decision support systems and security optimization
- Formal Methods for software protection

3. Software Protection in Industry

- Protection tool-chains and IDEs
- Software Architectures and build process integration
-Code and Data Protection in video-games, digital television, and streaming services
- Security Validation and best practices from industry
- Software protection on heterogeneous platforms (sensors, smartphones, cloud)

Important dates

Submission deadline:	30 June 2019
Notification of acceptance:	7 August 2019
Camera-ready papers:	30 August 2019
Workshop date:	15 November 2019

Submission Guidelines

ACM Proceedings of the workshops will be available to the workshop attendees. The submission of must occur through the workshop submission system on:
https://easychair.org/conferences/?conf=spro2019
Submissions must be at most 12 pages in double-column ACM format including the bibliography and well-marked appendices. Only PDF files will be accepted. Submissions not meeting these guidelines risk rejection without consideration of their merits. Each accepted paper must be presented by an author, who will have to be registered by the registration deadline. For informal queries about the submission contact the workshop chairs.

General Chair

Paolo Falcarin, University of East London, UK
falcarin@uel.ac.uk

Program Chair

Michael Zunke, Thales Group, Munich, Germany
michael.zunke@thalesgroup.com

Programme Committee

Sebastian Banescu – TU Munich, Germany
Cataldo Basile - Politecnico di Torino, Italy
Mariano Ceccato - Fondazione Bruno Kessler, Italy
Christian Collberg - University of Arizona, USA
Bart Coppens - Ghent University, Belgium
Béatrice Creusillet - QuarksLab, France
Mila Dalla Preda - University of Verona, Italy
Jerome d'Annoville - Thales Group, Paris, France
Jack Davidson - University of Virginia, USA
Saumya Debray - University of Arizona, USA
Bjorn De Sutter - Ghent University, Belgium
Michael Franz - University of California Irvine, USA
Roberto Giacobazzi - University of Verona, Italy
Yuan Gu - Irdeto, USA
Karine Heydemann - Sorbonne Université Paris, France
Pascal Junod - Snap, Switzerland
Clark Thomborson - University of Auckland, New Zealand
Dinghao Wu - Pennsylvania State University, USA
Brecht Wyseur - NAGRA, Switzerland
Babak Yadegari - Juniper Networks, USA