Call for Papers

https://aspire-fp7.eu/spro/

Important dates

Submission deadline:	31 January, 2015
Notification of acceptance:	18 February, 2015
Camera-ready papers:	27 February, 2015
Workshop date:	19 May, 2015

Scope

Software Protection techniques aim to defend the confidentiality and integrity of software applications that are exposed to an adversary that shares the execution host and access privileges of the application. This is often denoted as protection against MATE (Man-At-The-End) attacks. This is an area of growing importance. For industry, in many cases the deployment of such techniques is crucial for the survival of their business.

The aim of SPRO workshop is to bring together researchers and industrial practitioners both from software protection and the wider software engineering community to discuss software protection techniques, evaluation methodologies, and practical aspects such as tooling. The objective is to stimulate the community working in this growing area of security, and to increase the synergies between the research areas of software protection engineering and their practical deployment.

Questions that we aim to address include

- What protection techniques can be designed to protect given assets in software applications?
- Which threats need to be considered, and how can we evaluate the robustness of protected applications with respect thereto?
- How can different protection techniques be efficiently combined and what do we gain?
- What can we learn from existing use cases?
- How can protection techniques be efficiently tooled and integrated into a build process?

These are only a few of the many questions that practitioners face recurrently.

Desired articles should aim to address these questions. We seek articles that present new software protection techniques and novel insights into the evaluation thereof; and articles that aim to discuss industrial aspects.

Topics

Desired articles should cover one or several of the following topics:

1. Software Protection techniques
   - Code Obfuscation, Anti-reverse engineering
   - Data obfuscation, White-box Cryptography
   - Binary Rewriting, Binary Instrumentation
   - Anti-Debugging
   - Remote Attestation
   - Code Virtualization, Software Dynamic Translation
   - Software Tamper Resistance, Code Guards
   - Software Diversity
   - Software Renewability, Mobile Code
   - Software Licensing, Watermarking, Fingerprinting
   - Self-modifying Code
2. Software Evaluation
   - Evaluation Methodologies
   - Malware Analysis
   - Tools for static and dynamic software analysis
   - Threat modeling, Petri nets, attack graphs
   - Empirical studies
   - Metrics
3. Industry aspects
   - Protection technique tooling and tool chains

- Architectures and build process integration
- IDEs and tools for integration and deployment
- Validation
- Best practices from industrial use cases
- Software protection on heterogeneous devices

Submission Guidelines

Accepted papers will be published in the IEEE ICSE workshop proceedings. Submissions can be of two types: regular papers or short papers. Short papers can be initial works of PhD students or opinion pieces from recognized experts. Regular papers must follow the ICSE 2015 Format and Submission Guidelines and must have a maximum length of seven (7) pages; short papers must have a maximum length of four (4) pages. Submissions in excess of these limits may be rejected without refereeing. Articles must be novel: IEEE does not republish material published previously in other venues, including other periodicals and formal conference/workshop proceedings, whether previous publication was in print or in electronic form. For general author guidelines, see http://2015.icse-conferences.org/submission-guidelines. For submission, check the SPRO official webpage.

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
Brecht Wyseur, Nagra, Switzerland
brecht.wyseur@nagra.com

Keynote - "*Software Security: Squaring the Circle?*"

Bart Preneel – KU Leuven, Belgium

Programme Committee

Jerome d'Annoville – Gemalto, France
Jean Daniel Aussel – Gemalto, France
Cataldo Basile - Politecnico di Torino, Italy
Mariano Ceccato - Fondazione Bruno Kessler, Italy
Christian Collberg – University of Arizona, USA
Bart Coppens – Ghent University, Belgium
Mila Dalla Preda – University of Verona, Italy
Koen De Bosschere – Ghent University, Belgium
Saumya Debray – University of Arizona, USA
Bjorn De Sutter – Ghent University, Belgium
Werner Dondl – SafeNet Inc., USA/Germany
Michael Franz – Univ. of California, Irvine, USA
Roberto Giacobazzi – University of Verona, Italy
Yuan Gu – Irdeto
Wulf Harder – SIA QuBalt, Latvia
Pascal Junod – HEIG-VD, Switzerland
Johannes Kinder – Royal Holloway London, UK
Antonio Lioy – Politecnico di Torino, Italy
Isabella Mastroeni - University of Verona, Italy
Christian Mönch – Conax, Norway
Mattia Monga – University of Milan, Italy
Riccardo Scandariato – Chalmers Univ., Sweden
Christophe Tartary – University of East London, UK
Clark Thomborson – Univ.of Auckland, New Zealand
Paolo Tonella – Fondazione Bruno Kessler, Italy
Gaofeng Zhang – University of East London, UK
Michael Zunke – SafeNet Inc., USA/Germany