9th
Software Security, Protection, and Reverse Engineering Workshop (SSPREW)
SSPREW-9

Co-Located with ACSAC-2019
Venue: https://www.acsac.org/
Workshop: http://www.ssprew.org/

CALL FOR PAPERS

December 9—10, 2019
Condado Plaza Hilton
San Juan, Puerto Rico, USA

The **9th Software Security, Protection, and Reverse Engineering Workshop** brings together communities that focus on program protection and software security. Software security is a discipline that lies at the crossroads of security, cryptography, networks, software engineering, computer architecture, operating systems, and compiler design. Program protection and reverse engineering techniques both find their practical use in malware research and analysis as well as legitimate protection schemes for intellectual property and commercial software. The workshop focuses primarily on how to protect software from tampering, reverse engineering, and piracy. The workshop will also provide opportunity for proposals of new, speculative ideas; evaluations of new or known techniques in practical settings; and discussions of emerging threats and problems in metrics, tools, and procedures for evaluating tamperproofing, watermarking, obfuscation, birthmarking, and protection algorithms in general.

SSPREW will provide a discussion forum for researchers that are exploring theoretical definitions and frameworks, implementing and using practical methods and empirical studies, and those developing new tools or techniques in this unique area of security. The workshop has historically provided exchange of ideas and support for cooperative relationships among researchers in industry, academia, and government. The workshop will feature peer-reviewed technical presentations on original work, a poster session, and talk sessions on potentially non-original research.

Topics of interest include, but are not limited to the following.

- Security modelling
- Protection metrics and measurements
- Obfuscation / Deobfuscation
- Tamper-proofing
- Watermarking / Digital fingerprinting
- Reverse engineering tools and techniques
- Program / circuit slicing
- Information hiding and discovery
- Hardware-based protections
- Source code analysis / program understanding
- Forensic analysis and protections
- Virtualization for protection and/or analysis
- New cutting-edge protection technologies
- Diversity metrics and measurements
- Man-at-the-end (MATE) attack technologies
- MATE characterization
- Theoretic Analysis Frameworks:
  - Abstract Interpretation
  - Term Rewriting Systems
  - Machine Learning
  - Large Scale Boolean Matching
  - Homomorphic Encryption
- User interface design for controlling protection
- Static/dynamic analysis techniques
- Moving target and active cyber defense
- Protection profiling, verification, and evaluation

Submission Guidelines: SSPREW offers three potential submissions.

- **Technical Paper:** Original, unpublished manuscripts of up to 12-pages including figures and references, presented at workshop and included in proceedings.
- **Poster:** One page abstract describing the topic and nature of the research, with poster presented at workshop.
- **Talk Proposal:** Two page abstract describing a talk and the related topics of interest to be presented at workshop.

Submission for all three types through EasyChair: https://easychair.org/conferences/?conf=ssprew9.

See workshop website (http://www.ssprew.org) for more details regarding submission format requirements.

Program Co-Chairs:
Sebastien Bardin, CEA LIST, France
Natalia Stakhanova, Univ of Saskatchewan, CA

General Workshop Chair:
J. Todd McDonald, Univ of South Alabama, USA

Important Deadlines:

Paper Submission:	*Sep 23, 2019*
Poster/Talk Proposal:	*Oct 10, 2019*
Notification of Acceptance:	*Oct 24, 2019*
Camera-ready:	*Nov 04, 2019*
Workshop:	*Dec 09-10, 2019*