Co-Located with ACSAC-2014
Website: http://www.pprew.org

CALL FOR PAPERS

December 9th, 2014
Hyatt French Quarter
New Orleans, LA

Program protection and reverse engineering are dualisms of good and evil. Beneficial uses of reverse engineering abound: malicious software needs to be analyzed and understood in order to prevent their spread and to assess their functional footprint; owners of intellectual property (IP) at times need to recover lost or unmaintained designs. Conversely, malicious reverse engineering allows illegal copying and subversion and designers can employ obfuscation and tamper-proofing on IP to target various attack vectors. In this sense, protecting IP and protecting malware from detection and analysis is a double-edged sword: depending on the context, the same techniques are either beneficial or harmful. Likewise, tools that deobfuscate malware in good contexts become analysis methods that support reverse engineering for illegal activity.

PPREW invites papers on practical and theoretical approaches for program protection and reverse engineering used in beneficial contexts, focusing on analysis/deobfuscation of malicious code and methods/tools that hinder reverse engineering. Ongoing work with preliminary results, theoretical approaches, tool-based methods, and empirical studies on various methods are all appropriate. Studies on either hardware/circuit based methods or software/assembly based mechanisms are within scope of the workshop. We expect the workshop to provide exchange of ideas and support for cooperative relationships among researchers in industry, academia, and government.

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

- Obfuscation / Deobfuscation (Polymorphism)
- Tamper-proofing
- Watermarking / Digital fingerprinting
- Reverse engineering tools and techniques
- Program / circuit slicing
- Information hiding and discovery
- Hardware-based protection
- Source code analysis
- Forensic analysis and protections
- Virtualization for protection and/or analysis
- Theoretical Analysis Frameworks:
  - Abstract Interpretation
  - Term Rewriting Systems
  - Machine Learning
  - Large Scale Boolean Matching
  - Homomorphic Encryption
- Component/Functional Identification
- Program understanding
- Static/dynamic analysis techniques
- Moving target and active cyber defense

Submission Guidelines: Original, unpublished manuscripts of up to 12-pages including figures and references must follow the ACM SIG proceedings format.

Submission is through EasyChair: https://easychair.org/conferences/?conf=pprew4.

See conference website (http://www.pprew.org) for more details.

Program Co-Chairs:
J. Todd McDonald, Univ of South Alabama, USA
Milla Dalla Preda, Univ of Verona, Italy

Important Deadlines:

- Submission: *Oct. 10, 2014*
- Notification of Acceptance: *Nov. 10, 2014*
- Camera-ready: *Nov. 28, 2014*
- Workshop: *Dec. 9, 2014*