

*The 7th IEEE International Conference on
Software Security and Reliability*

SERE 2013

Washington, D.C., USA, 18-20 June, 2013

<http://paris.utdallas.edu/sere13>

Half-Day Tutorial

Secure Android Programming: Best Practices for Data Safety & Reliability

Angelos Stavrou

Computer Science Department
George Mason University

&

2013 Engineer of the Year
IEEE Reliability Society

This tutorial will cover both basic and advanced Android Dalvik programming concepts and how they can be implemented efficiently and securely within the Android permission model. In addition, we will present examples of Android code that is not well designed both in terms of security and power consumption and the potential implications of such code in the reliability of an Android device. We will conclude by presenting what are currently considered the best coding practices. Our goal is to assist both experience and novice mobile developers steer away from security and reliability pitfalls in their code while delivering efficient and robust applications.

About the speaker

Dr. Angelos Stavrou is an Associate Professor at George Mason University and the Associate Director Center for Secure Information Systems. Stavrou has served as principal investigator on contracts from NSF, DARPA, IARPA, AFOSR, ARO, ONR, and he is an active member of NIST's Mobile Security team and has written more than 40 peer-reviewed conference and journal articles. Stavrou received his M.Sc. in Electrical Engineering, M.Phil. and Ph.D. (with distinction) in Computer Science all from Columbia University. He also holds an M.Sc. in theoretical Computer Science from University of Athens, and a B.Sc. in Physics with distinction from University of Patras, Greece. His current research interests include security and reliability for distributed systems, security principles for virtualization, and anonymity with a focus on building and deploying large-scale systems. Stavrou was awarded with the 2012 George Mason Emerging Researcher, Scholar, Creator Award, a university-wide award. In 2013, he

received the IEEE Reliability Society Engineer of the Year award. He is a NIST associate researcher and a member of the ACM, the IEEE, and USENIX.

Over the past few years, Dr. Stavrou's research has focused on two aspects of security: Systems' Security and Reliability. In the context of the first, he is working with NIST as part of the DARPA "*Transformative Applications*" effort that seeks to secure Android mobile phone devices against kernel-level attacks. Furthermore, Stavrou is the GMU PI participating along with Columbia, Stanford, and Symantec in the IARPA "*StoneSoup*" effort. In addition, the PI is funded by DARPA under the CyberGenome project to perform analysis on the phylogenetic origins of malware. Dr. Stavrou is currently supported by a NSF Trustworthy Computing (NSF-CNS- 0915291) grant on "*Scalable Malware Analysis using Lightweight Virtualization*". This effort seeks efficient methods to collect and analyze the nature of Internet malfeasance.