UCF DEPARTMENT OF ELECTRICAL ENGINEERING AND COMPUTER SCEINCE

Spring 2015 Seminar Series

Presented by the CS Division

MINDING THE GAPS IN MEMORY FORENSICS

WEDNESDAY APRIL 15, 2015

1:30 PM – HEC 450

Over the last decade, memory forensics has transitioned from very rudimentary techniques to a powerful set of tools for preservation and analysis of volatile evidence. Memory forensics is now used both to support traditional forensics investigations as well as incident response and malware analysis. Now that mechanisms for providing basic memory forensics capabilities are well understood, the research community remains hard at work, developing techniques to close as many of the remaining gaps in which malware can hide and actionable volatile evidence be lost. The talk surveys the state-of-the-art in memory forensics and discusses research undertaken by the speaker and his collaborators to close some of these gaps. This work includes efforts to process compressed RAM and detect kernel-level rootkits in Mac OS X. The talk also touches on areas in memory forensics which still require substantial innovation. Only a basic background in operating systems and computer architecture is assumed.

DR. GOLDEN G. RICHARD III

University of New Orleans

Golden G. Richard III is a digital forensics and computer security expert and a Fellow of the American Academy of Forensic Sciences, with over 35 years of practical experience in computer systems and computer security. He is Professor of Computer Science, University Research Professor, and Director of the Greater New Orleans Center for Information Assurance (GNOCIA) at the University of New Orleans, where he has taught and conducted research for the past 20 years. His research interests mirror his teaching interests: digital forensics, reverse engineering, offensive computing, operating systems internals, and malware analysis. Dr. Richard is also a member of the United States Secret Service Electronic Crime Taskforce, the Editorial Board of the Journal of Digital Investigation, and the Editorial Board of the International Journal of Digital Crime and Forensics (IJDCF). He is a founding member and chairman of the non-profit that runs the Digital Forensics Research Workshop (DFRWS), the premiere venue for publishing digital forensics research. He earned his Ph.D. from The Ohio State University.

Hosted by: Dr. Cliff Zou