January 4-7, 2011, The Grand Hyatt Kauai Resort & Spa, Koloa, Kauai, Hawaii.

Track: Software Technology

Minitrack: Dynamic Analysis of Software Systems

According to public reports by anti-virus vendors, more malware is now produced each year than legitimate software. Much of it is customized to target particular organizations and objectives, rendering traditional after-the fact statistical and historical analysis increasingly ineffective, and transforming more intrusions into “zero-day” attacks. The problem is amplified by the explosive growth of distributed computing and ubiquitous downloading of executable content. The security research community has struggled to keep pace with the dynamic nature of Web 2.0, service-oriented computing, and distributed computation. Much research has focused on static analysis, trust establishment at load-time only, and individual OS security in isolation from the broader context of distributed computation.

Dynamic analysis is emerging as an approach to evaluation of software, system state, and correlated distributed system and network activity, in real-time or near real-time, to determine functional and security properties. Dynamic analysis applies knowledge of desired behavior to provide confidence that ever-changing streams of software executing in distributed systems are legitimate and do not contain malicious content, an approach that helps shift security analysis from a reactive to a proactive process. This minitrack brings together researchers and practitioners in dynamic analysis from academia, industry, and government to promote sharing of promising methods and technologies for more secure computing in a world increasingly awash with threats to critical systems.

Minitrack Co-chairs

Richard Linger (primary contact)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA
Email: rlinger@sei.cmu.edu

Luanne Burns
Johns Hopkins University
Applied Physics Laboratory
Email: luanne.burns@jhuapl.edu

Stacy Prowell
Cyber Sciences & Information Infrastructure Research
Oak Ridge National Laboratory

Oak Ridge, TN
Email: prowellsj@ornl.gov

Richard Linger is the manager of the CERT Survivable Systems Engineering group where he directs the Function Extraction project for computing software behavior. He is an expert in function-theoretic methods for software engineering. Linger also directs research in Flow-Service-Quality (FSQ) engineering for network-centric system survivability, and next-generation software engineering for dependable system development. He serves as a member of the faculty at the CMU Heinz School of Public Policy and Management. At IBM, Linger partnered with Dr. Harlan Mills, IBM Fellow, to create Cleanroom Software Engineering technology for development of ultra-reliable software systems, including box-structure specification, function-theoretic design and correctness verification, and statistical usage-based testing for software certification. He pioneered use of Cleanroom technology for product development, achieving zero-defect performance with improved productivity. He has extensive experience in project management; system specification, architecture, design, verification, and certification; software re-engineering and reverse engineering; and process improvement, technology transfer, and education. He has published three software engineering textbooks, twelve book chapters, and over 60 papers and journal articles. He holds a BSEE from Duke University, and is a senior member of IEEE and a member of ACM and AIAA.

Luanne Burns is an expert on human-computer interaction. She is currently the test and integration and demonstration lead on the CMAC (Cyber Measurement and Analysis Center) at Johns Hopkins Applied Physics Lab. She was also instrumental in organizing the C3E (Computational Cyberdefense in Compromised Environments) Workshop. Her prior work in the CERT organization of the Software Engineering Institute, Carnegie Mellon University, on the Function Extraction project for computing software behavior focused on design and development of the user interface and the system repository for storing behavior databases. She also produced a video on FX technology concepts to better communicate the concepts to non-specialists. Dr. Burns received her M.S. in Computer Science and her Ph.D. in Cognitive Science from Columbia University. Dr. Burns was a Research Staff Member at IBM's Thomas J. Watson Research Center for 18 years. The focus of her work has been on user interface design and implementation in the database, education, and internet domains. She participated in research efforts at IBM that eventually became commercial products, including Visualizer Ultimedia Query, Websphere Web Analyzer Viewer, the IBM SchoolVista Assessment Suite, and a web application for reporting Olympic scores. Dr. Burns has worked extensively in website design, programming, Flash development, database design, e-commerce, and graphics, and teaches courses in programming, logic, and web development.

Stacy Prowell is a senior research scientist in the Cyberspace Sciences & Information Infrastructure Research group of the Oak Ridge National Laboratory. He is an expert in the function-theoretic analysis of program behavior, rigorous software specification methods, and automated statistical testing. Dr. Prowell has managed both commercial and academic software development projects and consulted on design, development, and testing of applications ranging from consumer electronics to medical scanners, from small embedded real-time systems to very large distributed applications. Prior to joining the ORNL, Dr. Prowell worked as the chief scientist for the Function Extraction (FX) project at the Software Engineering Institute's CERT program. As a professor at the University of Tennessee, Dr. Prowell started the Experimentation, Simulation, and Prototyping (ESP) project, which develops software libraries and tools to support application and adoption of model-based

testing and sequence-based specification. Software developed by this program is in use by over 30 organizations. Dr. Prowell has also worked as a private consultant in the software industry, and holds a PhD in Computer Science from the University of Tennessee. Dr. Prowell is a senior member of the IEEE, and a member of the ACM and Sigma Xi.

2.3.10