SafeConfig'16: Testing and Evaluation for Active & Resilient Cyber Systems Panel Verification of Active and Resilient Systems: Practical or Utopian?

Nicholas J. Multari
Pacific Northwest National Lab, USA
nick.multari@pnnl.gov

Anoop Singhal
National Institute of Standards and Technology, USA
anoop.singhal@nist.gov

David O. Manz
Pacific Northwest National Lab, USA
david.manz@pnnl.gov

Robert Cowles
BrightLite Information Security, USA
bob.cowles@gmail.com

Jorge Cuellar
Siemens Corporation, GE
jorge.cuellar@siemens.com

Christopher Oehmen
Pacific Northwest National Lab, USA
chris.oehmen@pnnl.gov

Gregory Shannon
Office of Science and Technology Policy
gregory_e_shannon@ostp.eop.gov

Introduction

The premise of the SafeConfig'16 Workshop is existing tools and methods for security assessments are necessary but insufficient for scientifically rigorous testing and evaluation of resilient and active cyber systems. The objective for this workshop is the exploration and discussion of scientifically sound testing regimen(s) that will continuously and dynamically probe, attack, and "test" the various resilient and active technologies. This adaptation and change in focus necessitates at the very least modification, and potentially, wholesale new developments to ensure that resilient- and agile-aware security testing is available to the research community. All testing, validation and experimentation must also be repeatable, reproducible, subject to scientific scrutiny, measurable and meaningful to both researchers and practitioners.

The workshop will convene a panel of experts to explore this concept. The topic will be discussed from three different perspectives. One perspective is that of the practitioner. We will explore whether active and resilient technologies are or are planned for deployment and whether the verification methodology affects that decision. The second perspective will be that of the research community. We will address the shortcomings of current approaches and the research directions needed to address the practitioner's concerns. The third perspective is that of the policy community. Specifically, we will explore the dynamics between technology, verification, and policy.

Keywords: Cyber Resilience, Testing, Validation, Active Systems, verification

SafeConfig'16, October 24, 2016, Vienna, Austria.
ACM 978-1-4503-4566-8/16/10.
http://dx.doi.org/10.1145/2994475.2994486

Bibliographies of Panelist

Robert (Bob) Cowles is principal in BrightLite Information Security performing cybersecurity assessments and consulting in research and education about information security and identity management. He served as CISO at SLAC National Accelerator Laboratory (1997-2012); participated in security policy development for LHC Computing Grid (2001-2008); and was an instructor at University of Hong Kong in information security (2000-2003). Recently, he has been working with the Center for Trustworthy Scientific Cyberinfrastructure (CTSC) by participating in development of cybersecurity guidance documents and in engagements to evaluate and advise the cybersecurity programs at NSF facilities.

Jorge Cuellar is a principal research scientist at Siemens AG. He was awarded the DI-ST Award for the best technical Achievement for his work on modelling of operating systems and transaction managers. He has worked in several topics, including performance analysis, on learning algorithms, hand-writing recognition, formal verification of distributed system design, and security and he has co-authored 50 publications. He has done technical standardization work on privacy and security protocols at the IETF, 3GPP, and the Open Mobile Alliance. He has worked in several EU funded research projects, mostly on security topics. He regularly serves in Program Committees for international conferences and he has held many short term visiting teaching positions, in different Universities around the world.

Christopher Oehmen is **l**ead and Chief Scientist of the Asymmetric Resilience Cybersecurity Initiative at the Pacific Northwest National Lab. **:** His research is built on a foundation of high performance computing applications in biology, with special emphasis on how these biological approaches can be used as a new paradigm for other fields such as cybersecurity. Beginning with ScalaBLAST, an open source high performance biosequence analysis application developed by his team at PNNL, Chris has led efforts exploring a variety of connections between sequence analysis and national security applications including analysis of software binaries and network traffic. He has developed applications in both of these areas which are being transitioned into operational use. More recently, he has led multiple efforts focused on adaptive, resilient cyber systems inspired in part by complex biological systems. His resilience and active defense work rely on a foundational application of biological principles for survivability and regeneration. Chris has over seven years of experience developing, leading, and executing research programs for a variety of sponsors. Chris received his B.A. in physics and mathematics from Saint Louis University in 1995. He earned M.S. and Ph.D. degrees in biomedical engineering from the University of Memphis/University of Tennessee, HSC Joint program in 1999 and 2003, respectively.

Gregory Shannon is the Chief Scientist for the CERT(r) Division at Carnegie Mellon University's Software Engineering Institute, expanding cybersecurity research, advancing national and international research agendas and promoting data-driven science for cybersecurity. He currently is on part-time detail to the White House Office of Science & Technology Policy as the Assistant Director for Cybersecurity Strategy. He has testified before Congress on cybersecurity, science for security, critical infrastructure, resilience, and cyber threats. Greg received a bachelor's in Computer Science from Iowa State University with minors in Mathematics, Economics and Statistics. He earned his master's and doctorate in Computer Sciences at Purdue University on a fellowship from the Packard Foundation. He is a member of the Association for Computing Machinery and a senior member of IEEE.

We expect thought provoking introductory thoughts from each of the panelist followed by a lively question and answer period. We hope that you will find this panel and its topic interesting and thought-provoking and that it will provide you with a valuable opportunity to share ideas with other researchers and practitioners from institutions around the world.