SafeConfig'16 – Testing and Evaluation for Active and Resilient Cyber Systems

Nicholas J. Multari[1], Anoop Singhal[2], David Manz[1]
[1]Pacific Northwest National Lab [2]National Institute for Standards and Technology
nick.multari@pnnl.gov, anoop.singhal@nist.gov, david.manz@pnnl.gov

ABSTRACT

The premise of this year's SafeConfig 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.

Keywords

SafeConfig; Testing; Validation; Security; Resilience; cyber; testbeds; metrics; cyber experimentation; science of cybersecurity

1. SCOPE AND OBJECTIVES

The premise of this year's SafeConfig Workshop is that existing tools and methods for security assessments are necessary but insufficient for scientifically rigorous testing and evaluation of resilient and active cyber systems. For example, we contend that existing penetration testing tools, red team processes, and security testing are not able to cope with inherent nature of continuous and resilient systems. Using existing tactics, techniques and procedures (TTP) by adversarial groups and penetration teams are often adequate to accomplish the job needed for cybersecurity testing. However, to increase the scientific validity, the validation of resilient systems must not be a static test or one consisting only of breach of perimeter or exfiltration of data. Rather the objectives for this workshop are 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 at the most, wholesale new developments to ensure that resilient and agile aware security testing is available to the research community. These impediments will also include natural faults such as flooding, fire, or hardware failure, or even staff member negligence. They must also be repeatable, reproducible, subject to scientific scrutiny, measurable and meaningful to both researchers and practitioners. The following topics are of interest of this workshop:

- Configuration testing, forensics, debugging and evaluation.
- Continuous monitoring and response.
- Cyber agility and moving target defense.
- Cyber resiliency.
- Cost effectiveness.
- Resilience/ agility effectiveness.
- Risk measurement.
- Testbeds.
- Research Infrastructure.
- Verification techniques.
- Validation techniques.
- Testing & evaluation methods.
- Cyber-physical systems security.
- Security configuration verification and economics.
- Security metrics - Adversarial and user Measures
- Mission metrics - Mission assurance, Mission measures, Conflicting mission management
- Security policy management
- Theory of defense-of-depth

2. PROGRAM COMMITTEE

Steering Committee

Ehab Al-Shaer, UNC Charlotte, USA
Chris Oehmen, Pacific Northwest National Lab, USA
Krishna Kant, Temple University, USA

Technical Program Committee

Gail-Joon Ahn, Arizona State University, USA
Steve Borbash, US Department of Defense, USA
Richard Colbaugh, Periander, UK
Seraphin Calo, IBM Research, USA
Tom Carroll, Pacific Northwest National Laboratory, USA
Andrea Ceccarelli, Universita degli Studi di Firenze, IT Yung Ryn Choe, Sandia National Lab, USA
Nora Cuppens, Telecom Bretagne, FR
Herve Debar, Telecom SudParis, FR
Sabrina De Capitani di Vimercati, Universita degli Studi di Milano, IT
Qi Duan, University of North Carolina, USA
Thomas Edgar, Pacific Northwest National Lab, USA
Errin Fulp, Wake Forrest University, USA

CCS'16, October 24–28, 2016, Vienna, Austria.
ACM ISBN 978-1-4503-4139-4/16/10.
DOI: http://dx.doi.org/10.1145/2976749.2990485

Yong Guan, Iowa State University, USA
Arlette Hart, FBI, USA
Michael Huth, Imperial College London,UK
Doug Jacobson, Iowa State University, USA
Dong-Seong Kim, University of Canterbury, New Zealand
Rick Kuhn, NIST, USA
Peng Liu, Pennsylvania State University, USA
Luigi Mancini, Universita di Roma La Sapienza, IT
Nuno Neves, University of Lisbon, PT
Hamed Okhravi, MIT Lincoln Labs, USA
Mohammed Rahman, Tennessee Tech, USA
Harigovind Ramasamy, IBM Research, USA
Indrajit Ray, Colorado State University, USA
Walid Saad, University of Miami, USA
Mohamed Shehab, Univ of North Carolina Charlotte, USA
Neeraj Suri, Technishe Universitat Darmstadt, GE
Paulo Verissimo, University of Luxembourg, LU
Carlos Becker Westphall, Federal University of Santa Catarina, Brazil
Geoffrey Xie, Naval Postgraduate School, USA
Quanyan Zhu, New York University

3. WORKSHOP CO-CHAIRS

Nicholas J. Multari provides programmatic and technical guidance to cybersecurity research programs at the Pacific Northwest National Lab (PNNL). Prior to joining PNNL, he led the trusted cyber technology research at Boeing Research and Technology in Seattle, Washington. In 2008, he served as a consultant to the USAF Scientific Advisory Board (SAB) investigating the effects of the contested cyber environment on the USAF mission. Other positions held include five years as a Senior Security Engineer with Scitor Corporation in Northern Virginia, and 20 years as a computer scientist in the Air Force retiring as a Lt. Col. He is a member of external advisory boards at University of Washington and Iowa State University. He received his PhD in computer science from the University of Texas at Austin.

Anoop Singhal, is currently a Senior Computer Scientist in the Computer Security Division at the National Institute of Standards and Technology (NIST) in Gaithersburg, MD. He received his Ph.D. in Computer Science from Ohio State University, Columbus, Ohio. His research interests are in network security, network forensics, cloud computing security and data mining systems. He is a member of ACM, senior member of the IEEE and he has co-authored over 50 technical papers in leading conferences and journals. He has two patents in the area of attack graphs and he has also co-edited a book on Secure Cloud Computing.

David Manz is a Senior Cyber Security Scientist at the Pacific Northwest National Laboratory. He holds a B.S. in Computer and Information Science from the Robert D. Clark Honors College at the University of Oregon and a Ph.D. in Computer Science from the University of Idaho. David's work at PNNL includes enterprise resilience and cyber security, secure control system communication, and critical infrastructure security. Prior to his work at PNNL, David spent five years as a researcher on Group Key Management Protocols for the Center for Secure and Dependable Systems at the University of Idaho (U of I). David also has experience teaching undergraduate and graduate computer science courses at U of I, and as an adjunct faculty at Washington State University. David has co-authored numerous papers and presentations on cyber security, control system security, and cryptographic key management.