# SafeConfig'16: Testing and Evaluation for Active & Resilient Cyber Systems

It is our great pleasure to welcome you to the *SafeConfig'16 Workshop.* This workshop is in its 9th year, each one focusing on different aspect of cyber systems. The 2016 workshop focuses on the testing and validation of cyber systems, specifically those involving active security and resilient systems. The premise is existing tools and methods for security assessments are necessary but insufficient for scientifically rigorous testing and evaluation of resilient and active cyber systems. This workshop will explore and discuss scientifically sound testing regimen(s) that will continuously and dynamically probe, attack, and "test" the various resilient and active technologies. This concept necessitates 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 call for papers attracted submissions from Asia, Europe, and the United States. Of the 13 papers submitted, the program committee recommended acceptance of 6 for an overall acceptance rate of 46%. In addition to the six accepted papers, we are also excited to have one keynote and a panel to examine this topic from an academic, business, and government point of view.

The first keynote, *Configuring Software and Systems for Defense-in-Depth* will be given by Dr. Trent Jaeger from Penn State University. He will discuss how achieving defense in depth has a significant component in configuration. In particular, he advocates configuring security requirements for various layers of software defenses (e.g., privilege separation, authorization, and auditing) and generating software and systems defenses that implement such configurations (mostly) automatically. Dr. Jaeger will focus mainly on the challenge of retrofitting software with authorization code automatically to demonstrate the configuration problems faced by the community, and discuss how we may leverage these lessons to configuring software and systems for defense in depth.

The second keynote, *From Cyber Security to Collaborative Cyber Resilience,* will be given by Dr. George Sharkov, the Cybersecurity Coordinator for the Bulgarian Government. Dr. Sharkov will discuss his view of a holistic approach to cyber resilience as a means of preparing for the "unknown unknowns". He will also discuss the multi-stakeholder engagement needed and the complementarity of governance, law, and business/industry initiatives. He will end with an example of the collaborative model in the Bulgarian national strategy and its multi-national engagements.

Finally, we will have a panel of experts from diverse backgrounds to discuss their perspective of the subject of this workshop. The specific participants include:

1. Ehab Al-Shaer, University of North Carolina Charlotte
2. Bob Cowles, BrightLite Information Security
3. Jorge Cuellar, Siemens Corporation
4. Christopher Oehmen, Pacific Northwest National Lab
5. Gregory Shannon, White House Office of Science and Technology Policy

Putting together *SafeConfig'16* was a team effort. We first thank the keynote speakers, authors and panelist for providing the content of the program. We are also grateful to the program committee and the steering program committee, who worked very hard in reviewing papers and providing feedback for authors.

We hope that you will find this program interesting and thought-provoking and that the symposium will provide you with a valuable opportunity to share ideas with other researchers and practitioners from institutions around the world.

**Nicholas J. Multari**
*SafeConfig'16 Co-Chair*
*PNNL Lab, USA*

**Anoop Singhal**
*SafeConfig'16 Co-Chair*
*National Institute of Standards & Technology, USA*

**David O. Manz**
*SafeConfig'16 Co-Chair*
*PNNL Lab, USA*