IICPS 2014 Workshop Keynote

Computing through Failures and Cyber Attacks: Case for Resilient Smart Power Grid

Zbigniew Kalbarczyk
Research Professor
Coordinated Science Laboratory
University of Illinois at Urbana-Champaign
Urbana, Illinois, USA

Abstract

Rapid proliferation of cyber physical systems (CPS) in our society makes them an attractive target for miscreants, in particular when CPS monitors and controls physical processes within a critical infrastructure such as power grid or water distribution. By integrating computation and physical processes in a tight control loop, CPS enables rapid response to changes in the controlled environment. However, regardless of how well a system is engineered, it is a matter of time for it to fail and hence, computing through failures and cyber-attacks becomes a norm rather than an exception. This talk first discusses challenges in achieving resilient smart cyber physical systems using examples from: (i) empirical studies on impact of failures/attacks on SCADA (Supervisory Control and Data Acquisition) systems used in power grid and (ii) data on real attacks on a commercial CPS. Then, we use an example of the SCADA deployed in the power grid, where a sophisticated attacker exploits system vulnerabilities and issues malicious control commands to drive remote facilities into an unsecure state without exhibiting any protocol-level anomalies. In order to detect such attacks, methods that combine system knowledge on both cyber and physical infrastructure in the power grid are needed to estimate execution consequences of control commands and thus, to reveal attacker's malicious intentions. We present an example method to address the challenge.

NatSec 2014 Workshop Keynote

Evolving Secure Computer Infrastructures

Errin Fulp
Professor
Wake Forest University

Abstract

Designs found in nature are increasingly used as a source of inspiration for securing complex-computing environments. Nature-inspired solutions add value because, like the living systems they are inspired by, they are robust, adaptive, and emergent, which are also important features for any cyber defense strategy. This talk will describe how evolutionary theory can be leveraged to secure computing infrastructures. Using the principles of replication, variation (mutation), and differential fitness (competition) observed in nature, the approach discovers more secure computer configurations from previous configurations. This project will demonstrate how nature can inspire practical and innovative solutions to the challenging problems associated with infrastructure cyber security.

Biography:

Errin W. Fulp is a professor of computer science at Wake Forest University. His research interests include computer security with emphasis bio-inspired solutions. This work has by funded by various agencies including US Pacific Northwest National Laboratory (PNNL), Department of Energy (DOE), and National Science Foundation (NFS). Errin Fulp is also the co-founder of Great Wall Systems, a network security start-up in Winston-Salem NC, and the head of the Network Security Group at Wake Forest University. Fulp received a PhD in computer engineering from North Carolina State University. He's a member of ACM and a senior member of IEEE.