Transforming the Resilience of Critical Infrastructure Systems and Communities

Resilience Week Objective: A Symposium dedicated to advancing the interdisciplinary dialog on policy and technologies that accelerate critical infrastructure and community resilience to unexpected and malicious threats.

Session 02: *Firmware Code Analysis*

Session Chair

- Rita Foster, Idaho National Laboratory, rita.foster@inl.gov
- Brad Whipple, Idaho National Laboratory, bradley.whipple@inl.gov
- Christian Hunt, New Context
- Eric Byres, Adolus

Session Abstract

Wouldn't it be nice to see inside the secretive world of firmware to design better defenses? A myriad of devices, from Internet of things to specialized safety systems, rely on the firmware (software tightly coupled with hardware) to operator properly. The embedded systems are installed with blind trust to operate an array of functions with no insight into the quality of code in the firmware. Poorly written or obsolete code, supply chain or vendor support hacks creating back doors, known firmware vulnerabilities (i.e. Meltdown), and past malware (i.e. Trisis) focused on the firmware in these embedded systems and are potential pitfalls unseen to the installer or operator. Updates to the firmware are applied on a trust basis without knowledge of betterment of the firmware. The most critical systems go through expensive 'black-box' type of testing. Embedded systems have limited visibility into the firmware and code quality. Multiple binary analysis techniques, reverse engineering, visualization, scoring of goodness and machine learning of firmware provides additional insights into this critical code that will aid the designing appropriate defenses and risk management.

Topics

- Elements of Resilience: Control and Cyber Systems