Rochester Joint Chapter of the IEEE Computer and Computational Intelligence Societies

Rochester, New York

presents

Dramatically Reducing Attack Surface Using Integrity MAC Security Kernel for Programmable Logic Controllers

by

Ed Reed

1990 RIT MSCS graduate studying Artificial Intelligence and Databases

Date: Friday, February 26, 2021
Time: 12:30 p.m. to 1:30 p.m.
Location: Virtual meeting
Computer Society announcements and venue information:
https://ewh.ieee.org/r1/rochester/computer
Cost: Free. Open to IEEE members and non-members.
No registration required. IEEE event feed: https://events.vtools.ieee.org/m/258933
See this site for the Zoom meeting access link.

Abstract

We face an existential threat of permanent damage to critical physical components in our national infrastructure as a result of their poor resilience against cybersecurity attack. A Programmable Logic Controller (PLC) commonly provides the control system for such components, e.g., bulk power generators. Our proof-of-concept implementation dramatically mitigates threats to such cyber-physical systems (CPS) by specifically leveraging what NIST 800-160 calls "*highly assured, kernel-based operating systems in Programmable Logic Controllers*".

We dramatically reduce the attack surface visible to potential attackers to be ~1% of the total compared to competing approaches. Our demonstration refactors the common CPS architectural approach to data and cooperating processes into hierarchically ordered security domains using the widely available OpenPLC project code base. The GEMSOS security kernel verifiably enforces traditional integrity mandatory access control (MAC) policy on all cross-domain flows. GEMSOS is designed for wide-spread delivery as a Reusable Trusted Device, providing the reference monitor for secure single-board, multi-board, and System-on-a-Chip systems.

Only a processing component in the highest integrity domain can directly send/receive control signals, enforcing "safe region" operating constraints to prevent physical damage. This very small attack surface protects the critical physical components, making the overall CPS resilient to skilled adversaries' attacks, even though much larger lower integrity software running in other domains on the same Trusted Device hardware and network infrastructure may be thoroughly compromised. We make available our restructured OpenPLC source to encourage control system manufacturers to deliver verifiable PLC products to, as NIST puts it, "*achieve a high degree of system integrity and availability*" for control systems. UC Davis is using our demonstration on GEMSOS in their Computer Security Lab, today.

Speaker's Biography

Ed Reed is a 1990 RIT College of Applied Science and Technology MSCS graduate, studying Artificial Intelligence and Databases. Over the past 15 years he has led the development and upgrade of the Gemini Computers Distributed Trusted Computing Base (DTCB) run-time environment for the Gemini Secure Operating System (GEMSOS), a high assurance Multi-Level Secure (MLS) real-time operating system. In addition, he has integrated the DTCB with a commercial network protocol implementation and the Gemini Application Resource and NETwork Support (GARNETS) product to provide the MLS File System for a demonstration of the Network File Service (NFS) and a High Assurance Virtualized Guard Architecture running on GEMSOS under contract for a customer demonstration. He had direct technical responsibility for implementation and delivery of fully compliant, fully MLS Assured Sharing Platform Services/Sharing Architecture prototype, including hardware, software and C&A plan documentation. Prior to his work with Aesec and Gemini, Mr. Reed served as the Director of Product Management for Directory and Security products at Novell, Inc. and as their Security Tzar, overseeing Novell's incident response and security product strategies. He worked with Raytheon analyzing U.K. MoD IT software accreditation requirements for the airborne IS&R Sentinel R1 (ASTOR) project and writing proposals. At Harris-RF in Rochester, NY he filled a software testing role as a Software Engineer III on a distributed radio control system for NATO (CROSSFOX). He received his B.S. in General Management from Purdue University.