High-Level Language Microcontroller Implementation

Hardening microcontrollers against low-level cyber attacks

Background

As the nation's critical infrastructure expands, monitoring and control tasks such as fault reclosing and power system reliability analysis are being handled by general-purpose personal computers connected to special-purpose devices. These devices, which have direct control of critical infrastructure, may be compromised by standard low-level cyber attacks; the most prevalent being buffer overflows and memory corruption bugs, potentially circumventing higher level protections and compromising the associated critical infrastructure.

Barriers

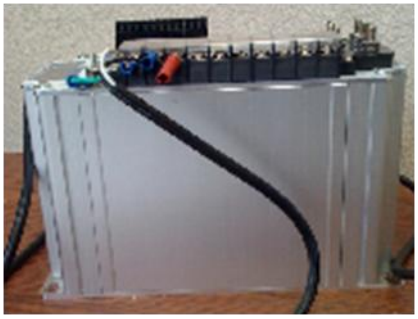
- Electric sector system architectures are complex and widely distributed
- Some control system devices can be compromised with standard low-level cyber attacks such as buffer overflows and insecure authentication
- Field devices have direct control over the physical energy delivery infrastructure
- Cyber attacks may circumvent high-level cybersecurity solutions on the communication network

Project Description

This project will implement a high-level fourth generation programming language for use with microcontrollers. This new language will limit users' direct access to the memory of the device, making more common, low-level cyber attack techniques infeasible. This will enhance the security of the critical infrastructure, provide a familiar development environment for programmers, and reduce development costs for industry.

The project will also develop standardized security libraries in the new programming language for use with embedded devices to perform functions such as secure authentication and data encryption down to the hardware point. Combined, these elements should encourage developers to produce more secure products as part of everyday embedded systems development.

Target Industrial Embedded Device



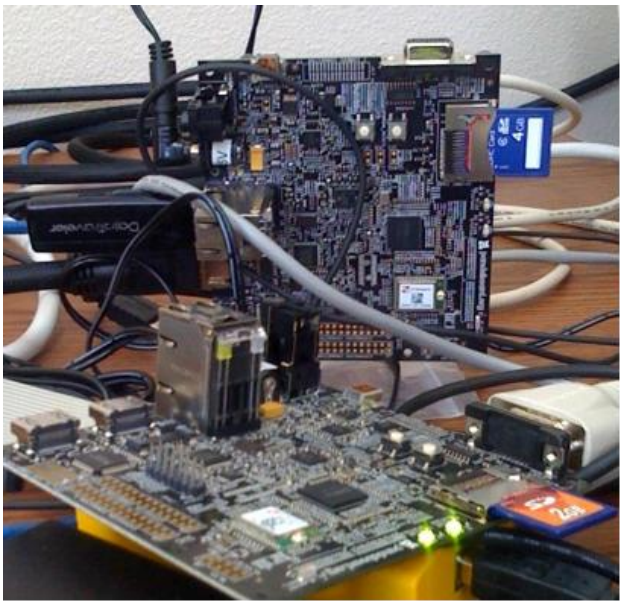
Benefits

- Limits direct access to microcontroller memory by control system users
- Decreases vulnerability to low-level cyber attacks
- Provides a familiar development environment for programmers
- Reduces development costs for industry

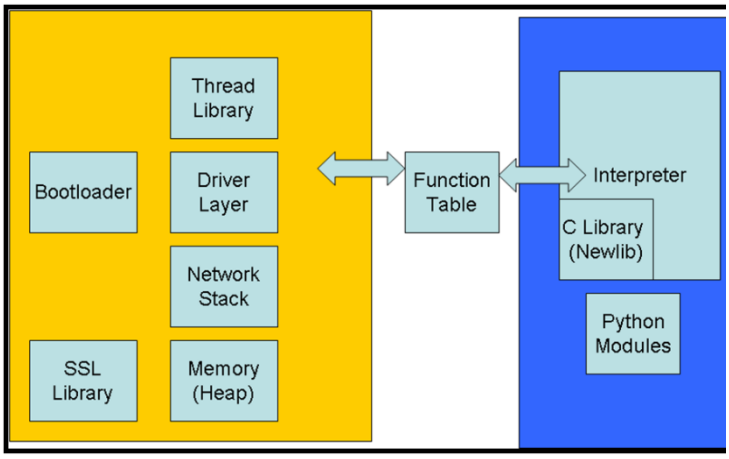
Partners

- Idaho National Laboratory
- Siemens Corporate Research

Communication Protocols on Test Devices



Block Diagram of Module Interaction



Technical Objectives

This project will help meet the challenge of securing critical infrastructure by implementing a fourth generation programming language for use with microcontrollers and by establishing standard security libraries in this language for use with embedded devices.

- Develop and test a high-level language for use in firmware implementation
- Establish standard security libraries in this language for use with embedded devices
- Implement and test the embedded system with the target language
- Conduct performance analysis

End Results

Project results will include:

- A high-level fourth generation programming language for use with microcontrollers
- Standardized security libraries for use with embedded devices
- A stronger barrier for protecting microcontrollers against low-level cyber attacks
- A development environment that encourages programmers to produce more secure products as part of embedded systems development

Content last updated: August 2012

Cybersecurity for Energy Delivery Systems (CEDS)

CEDS projects are funded through the Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) Research and Development (R&D) program, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of emergency disruptions due to cyberattacks.

For more information: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/cybersecurity-research-development-and

Initial Leads

Carol Hawk
Program Manager

Dave Kuipers
National SCADA Test Bed
Program Manager
Idaho National Laboratory
208-526-4038
david.kuipers@inl.gov

Current Contact as of Aug. 2020

Akhlesh Kaushiva
Program Manager
DOE CESER
202-287-6062
akhlesh.kaushiva@hq.doe.gov