Application of DPU Accelerators to Process Layer Security
David M. Nicol, Deming Chen, University of Illinois at Urbana Champaign

Executive Summary

The classic Purdue model for OT systems defines vertical system layers, with protection between layers conceptualized as "North-South"; a layer is often treated as a single security zone, and devices in the same zone trust each other. The problem is that better trust management is required within a layer, e.g., between RTUs, IEDs, and controllers within the Process layer. There is a need to check the integrity of delivered traffic, possibly including the provenance and route taken between source and destination. There is a need to provide availability in the face of potential denial of service attacks on the network. There is a need to rapidly recover from installation of malware that corrupts data and behavior. There is a need to support detection of unusual traffic patterns that may indicate the presence of an adversary or malware left behind by an adversary.

One challenge is that the kind of computation and trust protocols one might use to address these problems can be computationally expensive, consume more network resources, and may tax the capability of the OT system to support them and fully provide its functional services. Another challenge is that the system providing the computational backbone for trust management may be itself attacked. These limitations may be offset by hardware-based acceleration, e.g., using NVidia's Bluefield DPU.

The key thing is that a DPU provides separation and performance. The code which provides the services offered by a DPU are inaccessible to the software on the same host which uses those services. A DPU can be used to provide a root of trust upon which logic can be built to enable certain security functions.

This project will consider how RTUs, IEDs, and controllers equipped with hardware-based accelerators (such as DPUs from NVidia) might be utilized to increase the integrity and resilience of the process layer of energy systems. It also considers how separate "Trust Servers" based on such accelerators might be used without changing the hardware of OT-specific devices. The project will explore applications and recommend solutions with promise of deeper exploration through implementation and testing.

The project team has received assurances of technical support from NVidia, and the provisioning of a DPU-endowed server from Dell. Both companies have an interest in OT security and seeing this kind of support for our team as being beneficial. Independent of CITES funding, the PIs plan to purchase one or two additional DPU-endowed computers to be used in other research, but which can be leveraged by a CITES project.

The proposal is for one year at a scale that supports on graduate, during which time the most fruitful directions will be established, possibly leading to a separately proposed second year. The project would actively seek REU funding for undergraduates as well.