KalKi: High Assurance Software-Defined IoT Security

Problem
Despite the DoD’s current use of Internet of Things (IoT) devices in supervisory control and data acquisition (SCADA) systems, and its interest in using such devices in tactical systems, adoption of IoT has been slow mainly due to security concerns (e.g., reported vulnerabilities, untrusted supply chains).

At the same time, the DoD recognizes the rapid pace at which the IoT commercial marketplace is evolving, and its urgency to embrace commodity technologies to match its adversaries.

Solution
Move part of security enforcement to the network to enable the integration of IoT devices into DoD systems, even if the IoT devices are not fully trusted or configurable, by creating an IoT security platform that is provably resilient to a collection of prescribed threats.

The “Software-Defined” Aspect
Use software-defined networking (SDN) and network function virtualization (NFV) to create a highly dynamic IoT security platform.

The “High Assurance” Aspect
Use überSpark (a framework for building secure software stacks) to incrementally develop and verify security properties of elements of the software-defined IoT security platform.

The KalKi IoT Security Platform enables the integration of IoT devices into DoD systems, even if the IoT devices are not fully trusted or configurable.

Sensitive areas of the system are protected via FUNCy Views – a novel, performant, isolated execution environment extension to überXMHF/überSpark
- State machine that controls the security state transitions for each IoT device in the Control Node
- Routing tables and other sensitive data structures used by Open vSwitch (OVS) in the Data Node

Year 2 Highlights
End-to-end prototype of IoT Security Platform implemented and tested with different attack scenarios. Policies and μmboxes implemented for four representative devices.

Updated version of the KalKi Dashboard, which allows to fully configure and monitor the system.