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.

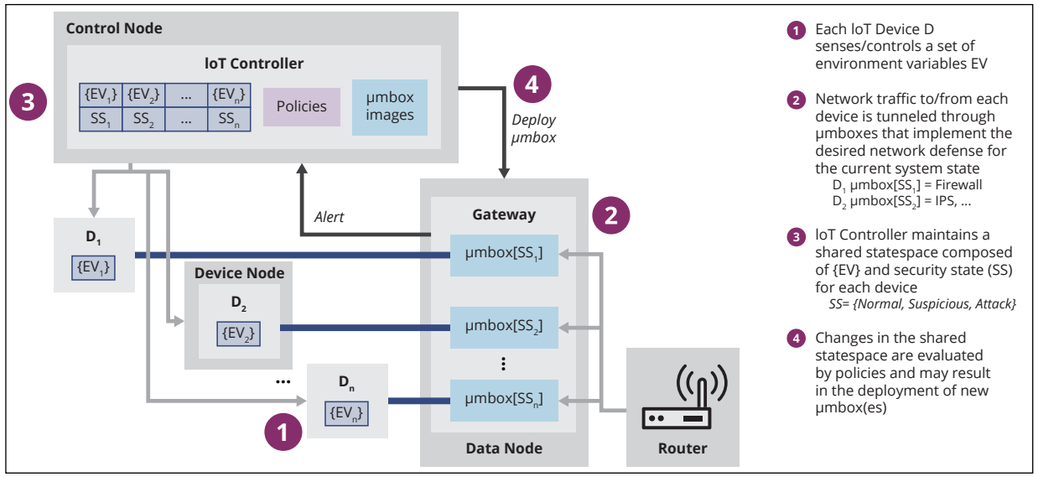
The "High Assurance" Aspect

Use the open-source uber eXtensible Micro-Hypervisor Framework (uberXMHF) to develop secure extensions that enforce security properties of critical elements of the software-defined IoT security platform at runtime, on commodity platforms.

KalKi IoT Security Platform Features

- Has flexible policies to define states, transitions and actions.
- Can protect from both cyber and kinetic attacks.
- Uses different network defenses for each device and state.
- Adapts to device-specific vulnerabilities or limitations.

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.

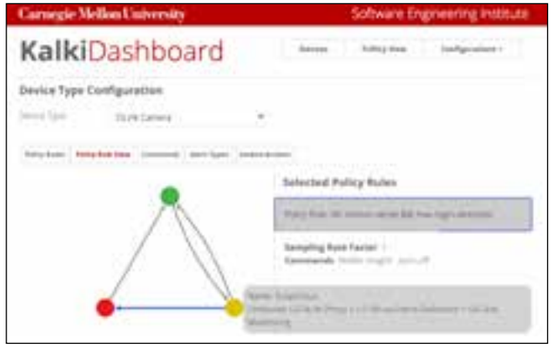


Security sensitive areas of the system are protected by the uberXMHF extensible and performant micro-hypervisor framework that provides three key runtime capabilities:
(a) isolation,
(b) mediation, and
(c) attestation.

- The micro-hypervisor verifies the integrity of the µmbox images when they are loaded, to ensure that each device has the correct network defenses.
- Signing network packets ensures that they are routed through the proper µmboxes for each specific device in the Data Node.

Year 3 Highlights

1. The new version of the platform prototype using docker containers showed significant performance and scalability improvements—threat reaction time is 3 seconds (90% improvement) with support for up to 125 connected devices (80% improvement).
2. User interface improvements to the Dashboard UI significantly reduce the time and complexity of adding new IoT devices, especially with respect to policy definition.



3. Architecture changes enable the system to adapt to different network layouts and to be deployed on low-cost hardware such as a Raspberry Pi.
4. We created a formal system model of our security architecture using the Alloy modeling language and successfully validated its designed-in resilience properties.
5. We demonstrated that the architecture provides intrinsic security against a broad spectrum of attacks, including nine published attacks against such software-defined architectures.
6. Kalki code is available as open-source on Github to invite the community to test or adapt the platform.
KalKi platform:
https://github.com/SEI-TAS/kalki-node-setup/wiki ;
uberXMHF micro-hypervisor: https://uberxmhf.org/

Sebastián Echeverría | info@sei.cmu.edu
Dr. Grace A. Lewis, Craig Mazzotta, Matthew McCormack, Marc Novakouski, Kyle O'Meara, Dr. Vyas Sekar, Dr. Amit Vasudevan

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.