KalKi: High Assurance Software-Defined IoT Security

The term “KalKi” is of Sanskrit origin and derived from the Sanskrit word “Kala,” which means destroyer of filth or malice and bringer of purity, truth, and trust.

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 infrastructure 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 framework.

1. Each IoT device, D, senses/controls a set of environment variables, EV
2. Network traffic to/from each device is tunneled through µmboxes that implement the desired network defense for the device’s current security state
   - µmbox[SS₁] = Firewall
   - µmbox[SS₂] = IPS, ...
3. IoT controller maintains a shared statespace composed of (EV) and security state (SS) for each device
   - SS = (Normal, Suspicious, Attack)
4. Changes in the shared statespace are evaluated by policies and may result in the deployment of new µmboxes

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 infrastructure.

Control Node Properties
- Policy data integrity
- µmbox image storage integrity

Data Node Properties
- Isolation between µmboxes of different trust levels: trusted, untrusted, and verified
- µmbox deploy-time integrity

Device Node Properties
- Attestation
- Authenticated channel of communication with the IoT controller

Security Policy Model

Initial architecture and prototype of the IoT security framework (focus on control node)