Two Perspectives on IoT Security

“IoT Security Standards” and “Software-Defined Networking for IoT Security”

**FY17: Authentication and Authorization for IoT Devices in Edge Environments**

Evaluation, adaptation, and implementation of an IETF proposal for authentication and authorization in constrained environments (ACE) to enable future integration of ACE-compliant IoT devices into DoD systems.

**ACE (Authentication and Authorization in Constrained Environments)**
- IETF proposal in Working Group Status—next step is Proposed Standard
- Extends OAuth 2.0 to IoT devices
- Addresses some of the challenges of tactical environments

**Threat modeling identified the following gaps in ACE.**

- **Gaps**
  - Bootstrapping of credentials is considered out-of-scope
  - Assumption of short periods of disconnection
  - On-demand token revocation

- **Solution**
  - Pairing mechanism for IoT devices that involves the use of QR codes as an out-of-band channel for exchanging initial encryption keys between IoT devices and the Authorization Server (AS)
  - Integration with delay-tolerant mechanisms and opportunistic routing for clients and IoT devices to reach AS
  - Periodic introspection between IoT devices and the AS, and clients and the AS

**FY18: High-Assurance Software-Defined IoT Security**

Dynamic deployment of network defenses based on composite state analysis of all controlled IoT devices.

**Research Review 2017**
Two Perspectives on IoT Security