Authentication and Authorization for IoT Devices in Edge Environments

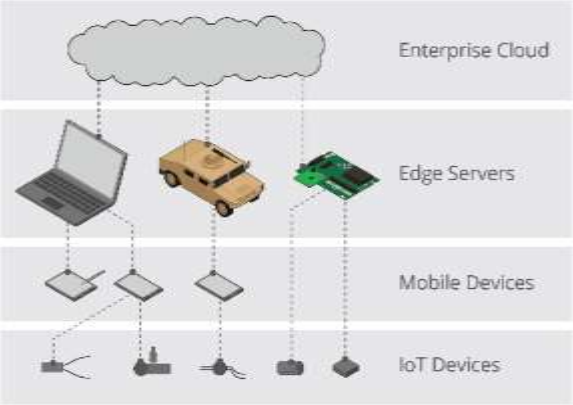
Grace A. Lewis

Principal Researcher

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.

DM17-0584

Overview



Tactical Edge System

Situational awareness in tactical edge systems can improve with integration of field-deployed IoT devices (e.g., sensors and actuators)

Problem

Integrating IoT devices into tactical edge systems expands the attack surface of the system

Most existing IoT security approaches are targeted at home and industrial environments with a very different threat model

Solution

Develop a mechanism for authentication and authorization of IoT devices that considers

- high-priority threats of tactical environments such as node impersonation and capture
- operations in disconnected, intermittent, limited (DIL) environments
- resource constraints of IoT devices

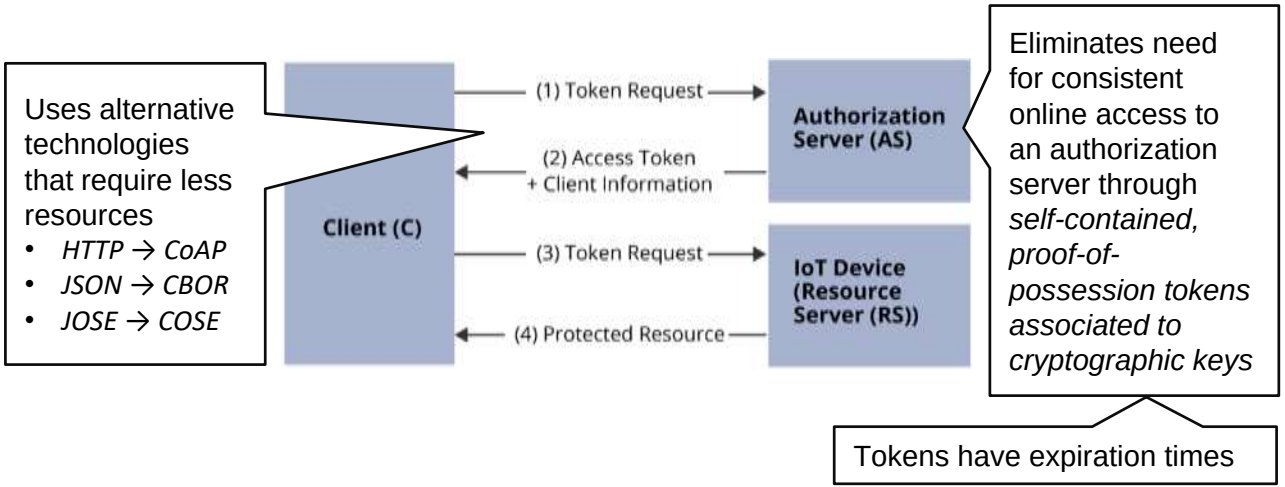
Approach

Approach

Evaluate, adapt, and implement an IETF proposal for authentication and authorization in constrained environments (ACE) such that it is resilient to high-priority threats and operation in DIL environments

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



Findings and Solutions

Threat modeling identified the following gaps in ACE

Gap	Threat/Problem	Solution
Bootstrapping of credentials is considered out-of-scope	Tactical environments cannot assume a secure network; encryption information to create tokens has to be protected	Developed a pairing mechanism for IoT devices that involves scanning QR codes as an out-of-band channel for exchanging initial encryption keys between IoT devices and the Authorization Server (AS)
On-demand token revocation	Compromised clients will have access to resources until expiration time; clients will have access to compromised resources until expiration time	Developed a mechanism for periodic introspection between IoT devices and the AS, and clients and the AS
Assumption of short periods of disconnection	Connectivity between nodes is less predictable in DIL environments — IoT devices and clients need to know of revoked tokens	Integration with delay-tolerant protocols and opportunistic routing for IoT devices and clients to reach the AS

Artifacts (In Progress)

Open source code

- ace-java: ACE library for non-constrained nodes (contributions to an existing project)
- ace-rc: ACE library for resources constrained nodes (new project)
- ace-sei (new project)
  - ace-client: ACE Client implementation
  - ace-as: ACE Authorization server implementation
  - ace-rs: ACE Resource Server implementation

Paper including

- Threat Modeling
- Solution (architecture and implementation)
- Evaluation via vulnerability analysis and ceremony analysis

Summary

Presented an analysis and potential solution for future integration of ACE-compliant IoT devices into DoD systems

Research results will drive and influence the development and final design of the ACE standard to ensure that DoD tactical edge use cases are well supported

Building knowledge for FY18 LSI on High-Assurance Software-Defined IoT Security

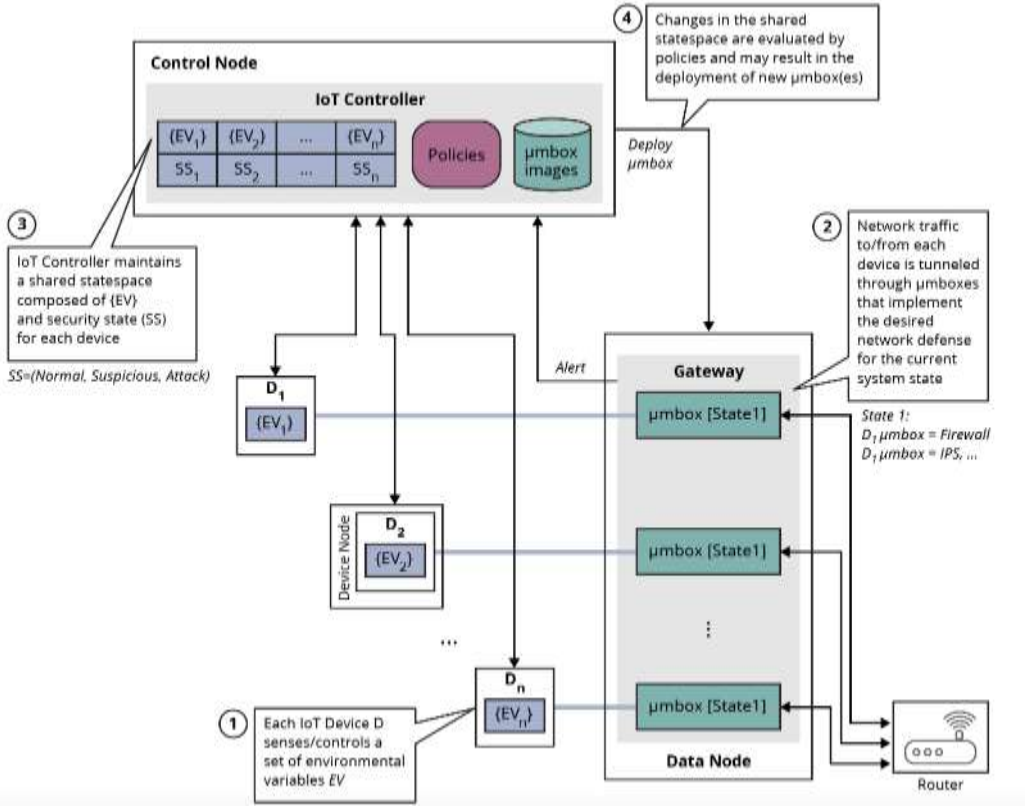
FY18 LSI: High-Assurance Software-Defined IoT Security

Problem

Despite the growing market and interest in IoT, many organizations are reluctant to use commodity IoT devices because of the growing number of reported vulnerabilities and untrusted supply chains

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



Contact Information

Presenter

Grace A. Lewis (SEI - SSD/TTG)
Principal Researcher
Email: glewis@sei.cmu.edu
Telephone: +1 412.268.5851

Team Members

Sebastián Echeverría (SEI - SSD/TTG)
Dan Klinedinst (SEI - CERT/VUL)
Ludwig Seitz (SICS)