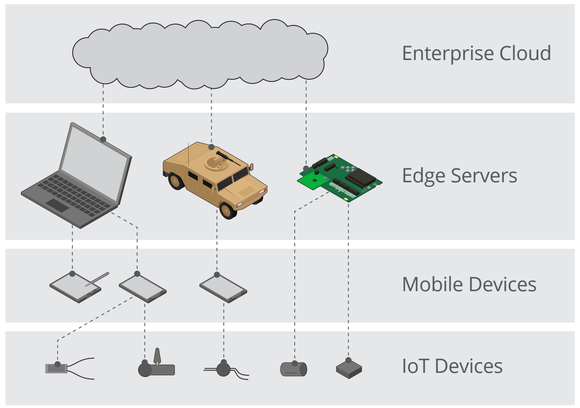
Two Perspectives on IoT Security

"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



Tactical Edge System

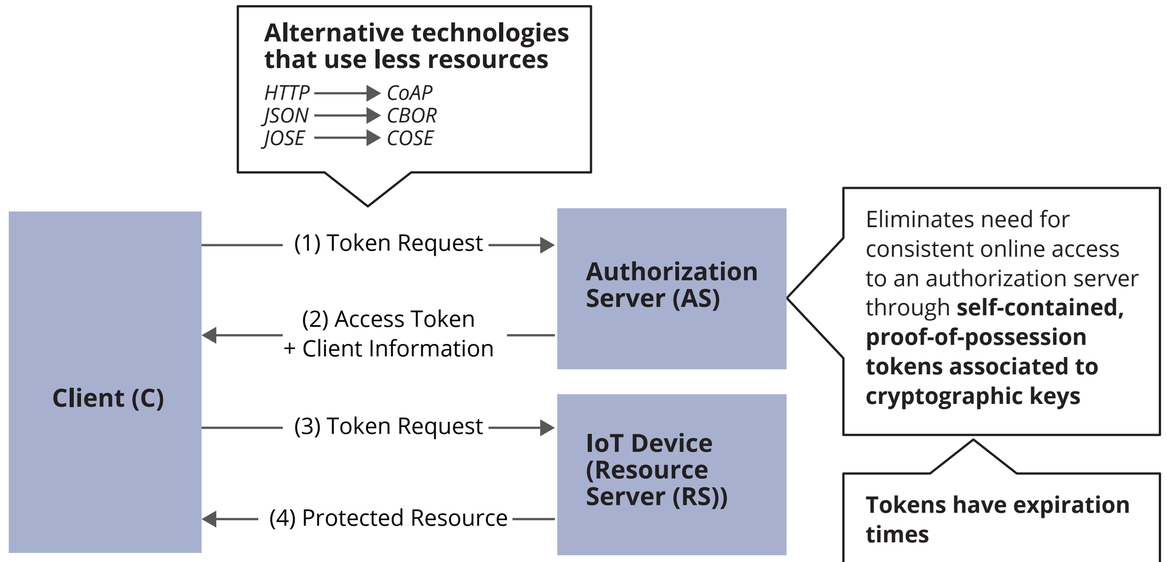
Goal:

Develop a solution for authorization and authentication of IoT devices that

- addresses high-priority threats of tactical edge environments,
- operates in DIL environments, and
- considers resource constraints of IoT devices

ACE (Authentication and Authorization in Constrained Environments)

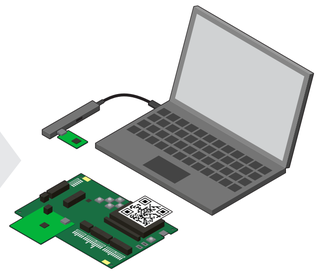
- IETF proposal in Working Group Status—next step is Proposed Standard
- Extends OAuth 2.0 to IoT devices
- Addresses some of the challenges of tactical environments

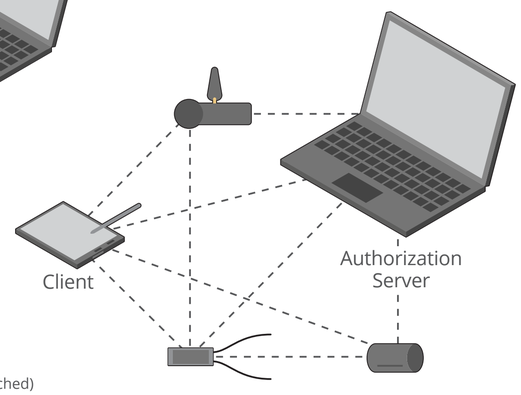


ACE Extensions to OAuth 2.0

Threat modeling identified the following gaps in ACE.

Gaps	Solution
Bootstrapping of credentials is considered out-of-scope	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)
Assumption of short periods of disconnection	Integration with delay-tolerant mechanisms and opportunistic routing for clients and IoT devices to reach AS
On-demand token revocation	Periodic introspection between IoT devices and the AS, and clients and the AS

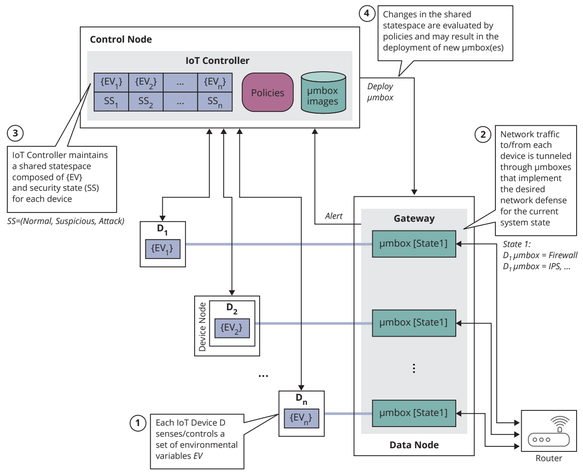




Periodic Introspection

```
if (introspection interval reached)
  for each token t in token list
      r = send_introspection_message(t)
      if (r == "Invalid")
        delete_token(t)
  end for
  reset introspection interval
end if
```

FY18: High-Assurance Software-Defined IoT Security



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

Grace Lewis | glewis@sei.cmu.edu

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.

DM17-0735
Two Perspectives on IoT Security