Authentication and Authorization for Constrained Environments (ACE)

BOF

Wed 09:00-11:30, Balmoral

BOF Chairs: Kepeng Li, Hannes Tschofenig

Responsible AD: Barry Leiba

Mailing List: ace@ietf.org

Note Well

This summary is only meant to point you in the right direction, and doesn't have all the nuances. The IETF's IPR Policy is set forth in BCP 79; please read it carefully.

The brief summary:

- **By participating with the IETF, you agree to follow IETF processes.**
- **If you are aware that a contribution of yours (something you write, say, or discuss in any IETF context) is covered by patents or patent applications, you need to disclose that fact.**
- **You understand that meetings might be recorded, broadcast, and publicly archived.**

For further information, talk to a chair, ask an Area Director, or review the following:
BCP 9 (on the Internet Standards Process)
BCP 25 (on the Working Group processes)
BCP 78 (on the IETF Trust)
BCP 79 (on Intellectual Property Rights in the IETF)

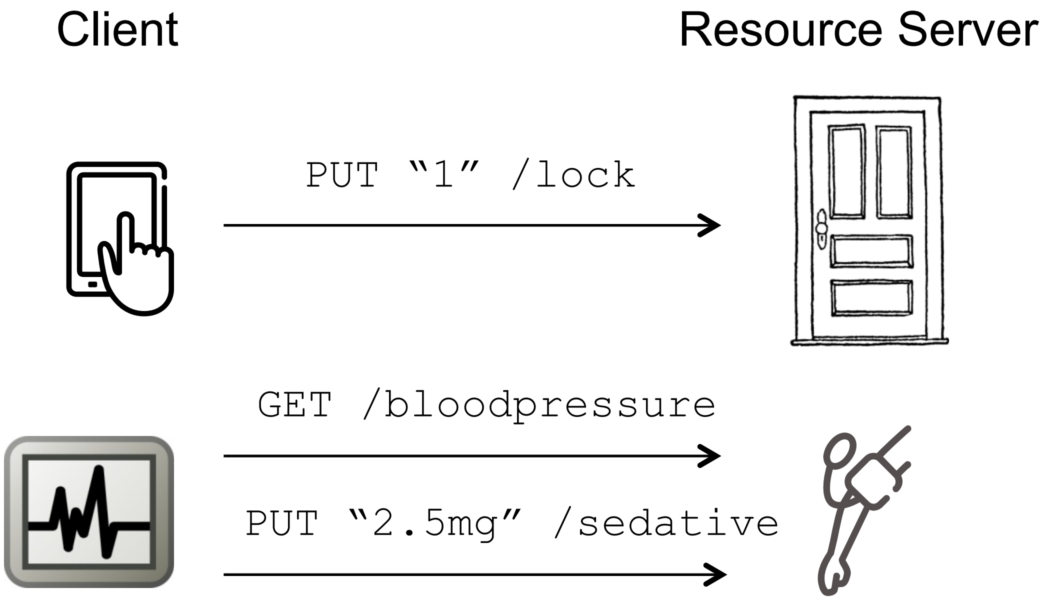
Agenda

- **Introduction** (Chairs) – 5 min
- **Constrained Node Network** (Carsten Bormann) -15 min
- **Use Cases and Requirements** (Ludwig Seitz) - 30 min
- **Architectural Design Choices** (Goran Selander) - 30 min
- **Gap Analysis** (Hannes Tschofenig) - 30 min
- **Charter Discussion** (Chairs) - 40 min

Prior Activities leading to this BOF

- Smart Object Workshop (March 2011)
- Smart Object Security Workshop (March 2012)
- Many relevant IETF working group activities this work builds on, including CORE, 6lowpan/6low, lwig, dice, etc.
- Various interoperability events

Problem Statement



Client

Resource Server

PUT “1” /lock

GET /bloodpressure

PUT “2.5mg” /sedative

Resource server, client and network may be constrained.

→ How to support explicit and dynamic authorization?

Related Work

- Use Cases:
  - http://tools.ietf.org/id/draft-garcia-core-security
  - http://tools.ietf.org/id/draft-greevenbosch-core-authreq
  - http://tools.ietf.org/id/draft-seitz-ace-usecases
- Solutions:
  - http://tools.ietf.org/id/draft-gerdes-core-dcaf-authorize
  - http://tools.ietf.org/id/draft-kang-core-secure-reconfiguration
  - http://tools.ietf.org/id/draft-selander-core-access-control
  - http://tools.ietf.org/id/draft-zhu-ace-groupauth
  - http://tools.ietf.org/id/draft-pporamba-dtls-certkey
  - http://tools.ietf.org/id/draft-schmitt-two-way-authentication-for-iot
  - http://tools.ietf.org/id/draft-seitz-core-security-modes
  - http://tools.ietf.org/id/draft-sarikaya-ace-secure-bootstrapping
  - http://tools.ietf.org/id/draft-bormann-core-ace-aif
  - http://tools.ietf.org/id/draft-porambage-core-ace-x509
  - http://tools.ietf.org/id/draft-tschofenig-ace-overview
  - http://tools.ietf.org/id/draft-seitz-ace-design-considerations
  - https://tools.ietf.org/id/draft-mehrtens-core-ace-concert

Constrained Node Network

Carsten Bormann

ACE BOF, IETF-89 London

Use Case and Requirements

Ludwig Seitz

http://datatracker.ietf.org/doc/draft-seitz-ace-usecases/

ACE BOF, IETF-89 London

Architectural Design Choices

Göran Selander

http://tools.ietf.org/id/draft-seitz-ace-design-considerations
http://tools.ietf.org/id/draft-gerdes-core-dcaf-authorize
http://datatracker.ietf.org/doc/draft-selander-core-access-control/

ACE BOF, IETF-89 London

Gap Analysis

Hannes Tschofenig

http://tools.ietf.org/id/draft-tschofenig-ace-overview/

ACE BOF, IETF-89 London

Charter Discussion

Kepeng Li, Hannes Tschofenig

http://trac.tools.ietf.org/wg/core/trac/wiki/ACE_charter

ACE BOF, IETF-89 London

An Important Question

a) Is this a topic the IETF **should** try to address?

b) Is this a topic the IETF **should not** try to address?

Charter: Narrative

- (**Constrained Environments**)
- standardized solution for authentication and authorization
- **authorized access to resources**
- **use CoAP and leverage DTLS** security where possible
- employ **additional less-constrained devices** in order to relieve the constrained nodes
- **existing** authentication and authorization protocols are used and re-applied ... **restricting** the options within each of the specifications
- operate across **multiple domains**

Charter: Tasks

- Document the **use cases and high-level requirements** for secured communication between constrained devices.
- Define profiles for encoding **authentication and authorization data**.
- Document **design criteria** for the required security protocols with respect to resource usage (RAM, message round trips, power consumption etc.).
- Define a mechanism for **authenticated and protected transfer of authorization information** suitable for constrained environments, and taking into account expiry/revocation.
- Define formats for **access tokens** and for **authorization information** that are suitable for constrained devices.
- Define bootstrapping for authorization information using the **Resource Directory** (see draft-ietf-core-resource-directory).

Charter Question

- The draft charter:
  - http://trac.tools.ietf.org/wg/core/trac/wiki/ACE_charter

a) Is the scope of the charter **clear** enough?

b) Is the scope of the charter **not clear** enough?

Engagement

a) How many are willing to review?

b) How many are interested to work on documents?