ACE — IETF 100 (Singapore)

Benjamin Kaduk, Jim Schaad

14 November 2017

NOTE WELL

Any submission to the IETF intended by the Contributor for publication as all or part of an IETF Internet-Draft or RFC and any statement made within the context of an IETF activity is considered an "IETF Contribution". Such statements include oral statements in IETF sessions, as well as written and electronic communications made at any time or place, which are addressed to:

- The IETF plenary session
- The IESG, or any member thereof on behalf of the IESG
- Any IETF mailing list, including the IETF list itself, any working group or design team list, or any other list functioning under IETF auspices
- Any IETF working group or portion thereof
- Any Birds of a Feather (BOF) session
- The IAB or any member thereof on behalf of the IAB
- The RFC Editor or the Internet-Drafts function

All IETF Contributions are subject to the rules of RFC 5378 and RFC 8179.
Statements made outside of an IETF session, mailing list or other function, that are clearly not intended to be input to an IETF activity, group or function, are not IETF Contributions in the context of this notice. Please consult RFC 5378 and RFC 8179 for details.
A participant in any IETF activity is deemed to accept all IETF rules of process, as documented in Best Current Practices RFCs and IESG Statements.
A participant in any IETF activity acknowledges that written, audio and video records of meetings may be made and may be available to the public.

Agenda

Agenda Bashing and Administrivia (Chairs, 5 mins)

Status Update (Chairs, 5 mins)

Current Working Group Documents:

- draft-ietf-ace-cbor-web-token (5 mins) — Mike Jones
- draft-ietf-ace-cwt-proof-of-possession (10 mins) — Mike Jones
- draft-ietf-ace-oauth-authz (15 mins) — Ludwig Seitz
- draft-seitz-ace-oscoap-profile (10 mins) — Francesca Palombini
- draft-ietf-ace-dtls-authorize (10 mins) — Göran Selander

Non-Working Group Documents:

- draft-aragon-ace-ipsec-profile (5 mins) — Marco Tiloa
- draft-tiloca-ace-oscoap-joining (15 mins) — Marco Tiloa
- draft-vanderstok-ace-coap-est (15 mins) — Peter van der Stok
- draft-tschofenig-ace-group-communication-security (30 mins) — Chairs

Wrap up — (Chairs, 15 mins)

Status Update

- New chairs
- CWT — in WG last call (ends 29 November)
- Adoption call for draft-seitz-ace-oscoap-profile

Presentations

[Change slide decks now]

Group Communication Security

How do low cost/low latency constraints translate into concrete security requirements?

- restrict set of people that can issue commands
- confidentiality not necessarily important
- assume low-security environment — breach of system security is not considered a drastic problem
- intend to operate in relatively homogeneous systems
    - minimal number of distinct types of participants
- multicast is needed for efficiency
- unicast traffic can use existing mechanisms
- do not need receipt/execution confirmation

Group Communication Security

Are we comfortable creating a document that targets this level of security?

Does “low-security” have a corresponding bit strength for brute-force resistance?

Are there faster/less secure signature algorithms that would provide sufficient strength for this situation? (128-bit ECDSA? Lattice cryptosystems? . . . ?)

Group Communication Security

Hums:

Are low-security systems a case that should be solved in the IETF?

Is unique source authentication/compromise detection a strong desirable?

Is a solution that has authentication and describes the drawbacks of not using it an acceptable solution?

Wrap Up

Goals for before London:

- Send CWT (and PoP?) to IESG
- Get core framework document to WGLC
- Adoption call for group communication
- Adoption call for EST work
- Adoption call for multicast work
- Do we need another interim?
  - EDHOC?
  - Core framework?
- Hackathon work on core framework