SECCORE

Another topic series for T2TRG?

WISHI

Work on IoT Semantic/ Hypermedia Interoperability
Followup to 2017 Workshop of this name
~ monthly Web meetings

SECCORE

Security for Constrained RESTful Environments
RFC 8576:
IoT Security: State of the Art and Challenges

Why recognize this as a structure?

— Organize periodic meetings

— A space with regular attendees

— Can explain activity to outsides/noobs

— Can report at T2TRG summary meetings

How did we deal with Security so far

RG drafts, RG submissions:

— RFC 8576 took a long time

— "Initial Security Setup" (draft-irtf-t2trg-secure-bootstrapping) needs some attention

— as does draft-richardson-t2trg-idevid-considerations
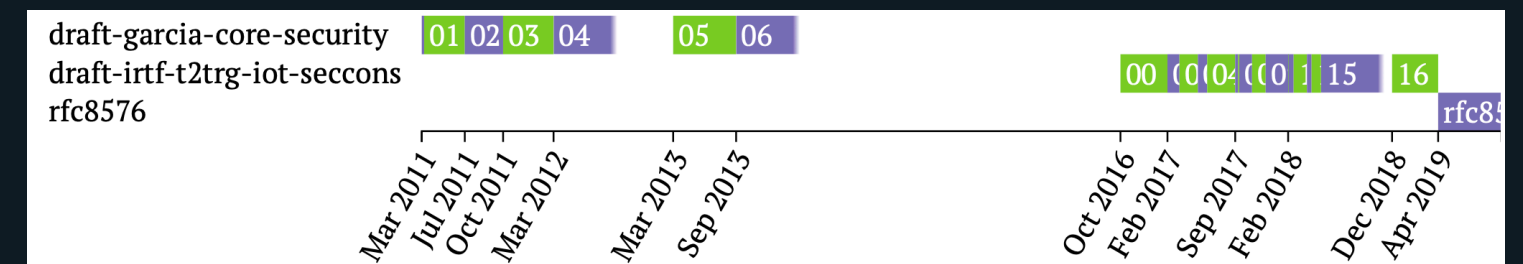
Little attention to what also was going on:

What IETF activities do we interact with

A large number of CoRE-related security documents are out there:
- EAP-NOOB (RFC 9140-to-be) in emu
- BRSKI etc. in anima, EST in core and
- Group communication in core, ace
* lake (EDHOC) and related core drafts
- suit, rats, teep
- iotops, …

Connected via shared people, but little structure
Need to analyze commonalities and emerging architecture

What could we look at?

(Göran's list:)

— Rekeying with PFS vs. stateless operations [KUDOS]

— Firmware updates using group communication

— Efficient and secure tunnelling of CoAP in CoAP

— Notifications surviving rekeying

— Progressing pub-sub with CoAP

Possible scope?

(Göran:)

To progress applications of CoAP in different security settings which "touch standardization in the IETF" [1] but are not necessarily in scope of a single working group like CoRE, ACE, SUIT, COSE, LAKE, etc.

(potential wider scope)

Include discussion about players, trust relationships, protocols dealing in these (anima, rats!)?
Interact with security researchers in this contact?

Boundaries?

— CFRG will do actual crypto, but interaction between lightweight crypto and IoT security protocols is of interest; lake will do AKE on top of that

— opsawg and rats will focus on security self-description and validation of self-assertions

— ___