6tisch secure join process: the show so far

- When 6tisch started in 2013, the RPL and general 6lowpan security fields were too large to solve.
- But, as 6tisch partially grew out of the industrial requirements for RPL, there was a belief that in the far more **restrictive** industrial environment a solution could be found.

6tisch security scope

- The network has **professional management.**
- The scale of the network is large, from a diversity of vendors, with a diversity of installers
  - While installers are not outright hostile, they are not skilled in the arts of network configuration.
  - Rekeying the network after installation is important.

Simplying assumption 1: 6tisch like has a PCE

- Once one assumes external help, make the most of it.
- The PCE<->node protocol (now called 6top) will be present anyway: leverage that!

Simplying assumption 2: leverage 802.1AR work

- The “MIC” – Manufacturer Installed Certificate! – provides a way to authenticate the nodes
  - The network just needs to get the right list of valid nodes.

Challenge 1: how does the network authenticate?

- In a zero-touch system, the node needs a way to know if it has found the correct network!
- Systems are resold: not just controllers, but sometimes entire plants.
  - Situation described in which one tower in a large refinery might be sold to a competitor! Network adjancies with old network would still be possible!

Work done to date

- 2014 January to August
  - Security design team worked through many assumptions and design options.
  - A number of drafts produced outlining options:
    - draft-richardson-6tisch-idevid-cert-01
    - draft-richardson-6tisch-security-6top-05
    - draft-richardson-6tisch-security-architecture-02
    - 6tisch-security-architecture-elements-01.txt

Work done to date

- 2014 January to August
  - Security design team worked through many assumptions and design options.
  - A number of drafts produced outlining options:
    - draft-richardson-6tisch-idevid-cert-01
    - draft-richardson-6tisch-security-6top-05
    - draft-richardson-6tisch-security-architecture-02
    - 6tisch-security-architecture-elements-01.txt

Work done to date

- Drafts that were reviewed include:
  - draft-pritikin-bootstrapping-keyinfrastructures-00
  - draft-kelsey-intarea-mesh-link-establishment-05
  - draft-piro-6tisch-security-issues-02

Results so far

- Input to the terminology draft:
  - JCE, JA
- 6top objects to manage security
- There was a **lengthy** and *repetitive* discussion about K1, K2 in the minimal work.
  - Much dispute whether K1 is necessary, sufficient.
  - Concern that 802.15.4 (pre-2015) can not actually specify reception of encrypted and cleartext (joining packet) at the same time.

Future Work

From point of view of mcr:

- IETF ANIMA WG will take lead (MCR hasn't time/resources to work on both)
- Zigbee IP specification has EAP-TLS + PANA
  - Seems there is little enthusiam for this solution.
    - (why didn't Thread Group use it?)
- Thread Group specification uses DTLS with some extensions for proxying between JCE and JA.
  - This is very close to some proposed design team proposal
  - Still unclear to (mcr, yet) how Thread Group handles authorization (“is this the right network”) in a scalable way.

Suggestions

- Determine why/if Thread Group solution won't work.
  - Propose changes if necessary.
- Maybe it just works: adopt it.