Breakout B

T2TRG 2015-07-19
Report from 2015-07-18

B1: Security & Privacy Features in Current IoT Projects

- Questions to the participants (Oliver Pfaff)

- Surprises:

  - More **capital goods** projects than consumer goods (in W3C WoT the impression is inverse)

  - Thing itself usually of **low value** —
    but might control (parts of) **high value** asset

  - Most now address **cross-domain** scenarios —
    not just same-domain any more

same-domain vs. cross-domain

- If same domain is/stays a valid proposition for IoT projects then a standard solution gives **reuse**. Things could be done without!

- If cross domain is aimed at (by a relevant subset of the projects) then a standard solution gives **interop** AND reuse. Things cannot be done without!

B1: Security & Privacy Features in Current IoT Projects

- Surprises (cont.):

  - Most implement **authorization**.
    In absence (as of now) of a standard **authorization** solution for things the current solutions are ad-hoc resp DIY.
    That's an apparent contradiction: DIY solutions are a valid for **same domain** (one vendor/provider controls all components) but not for **cross-domain**

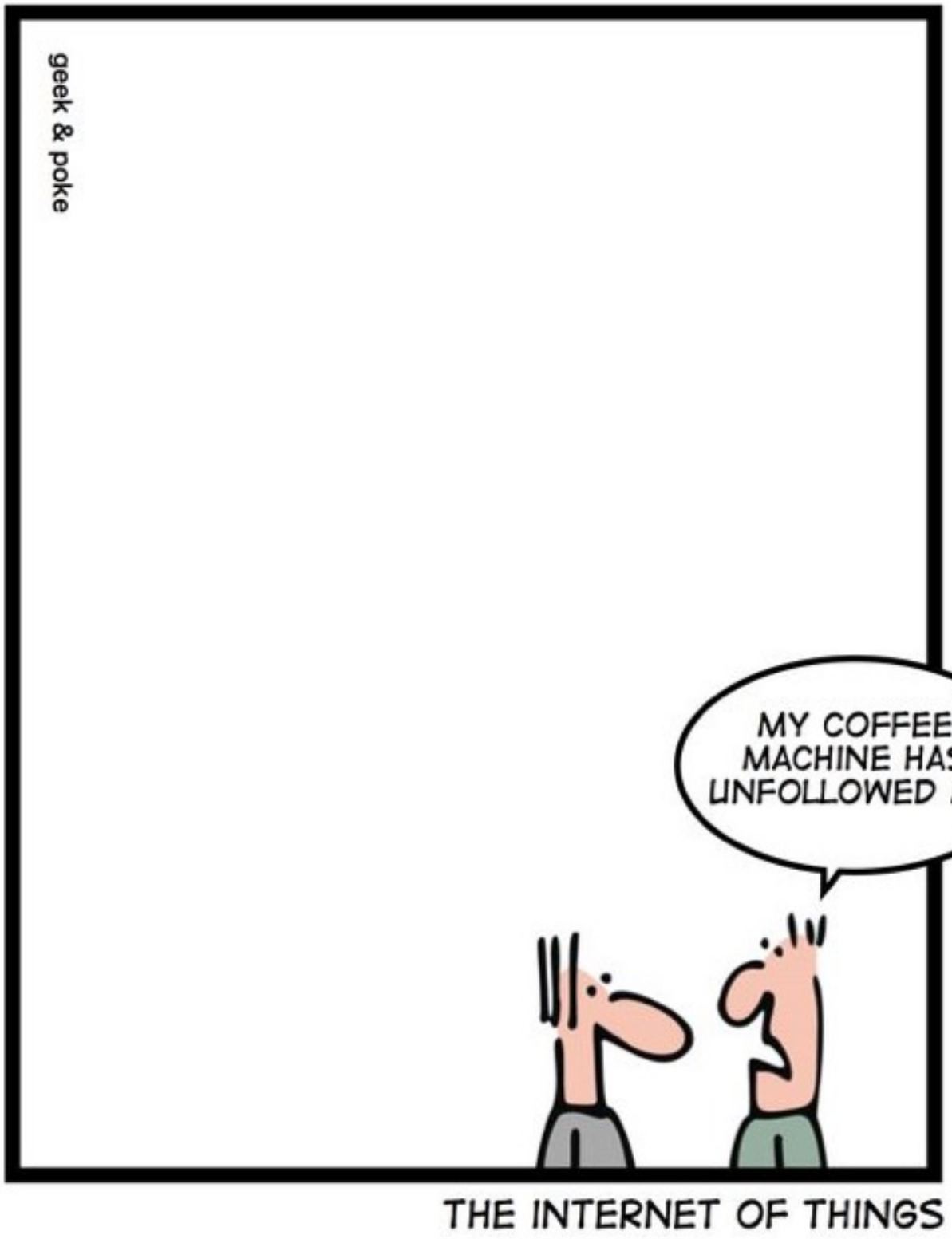
  - Preference is on **symmetric** cryptography (here: schemes that hit devices). If asymmetric schemes are used then in the '**raw**' form factor. Public key cryptography with public key certificates is avoided.

B2: Existing Infrastructure vs. New Challenges

- See slides [33]

- There really is a need for a **third wave** of innovation

- We need to understand how the cogs in our copious set of tools **work together**


geek & poke
MY COFFEE MACHINE HAS UNFOLLOWED ME
THE INTERNET OF THINGS

B3: RADIUS, WiFi

- (We noticed that we mostly are working on security, much less on privacy.)

- One possible takeaway:

  - Spewing around persistent, trackable identifiers (e.g., hashes of permanent public keys) will no longer be the method of choice.

B4: ACE Highlights

- We **REALLY** need to understand how the cogs in our copious set of tools **work together**