T2TRG: Thing-to-Thing Research Group

IETF 99
July 18, 2017, Prague, Czech Republic

Chairs: Carsten Bormann & Ari Keränen

Note Well

- You may be recorded

- The IPR guidelines of the IETF apply:
  see **http://irtf.org/ipr** for details.

Administrivia (I)

- Pink Sheet
- Note-Takers
- Off-site (Jabber, Hangout?)
  - **xmpp:t2trg@jabber.ietf.org?join**
- Mailing List: **t2trg@irtf.org** — subscribe at: **https://www.ietf.org/mailman/listinfo/t2trg**
- Repo: **https://github.com/t2trg/2017-ietf99**

Agenda

13:30: RG status update (Chairs)

13:40: WISHI report and way forward (Chairs+)

14:20: Edge Computing: Summary of Chicago discussion and ideas for next steps (Dirk Kutscher)

14:50: Authorizing network access for IoT Devices (Mohit Sethi)

15:20: Future activities: Documents and Meetings (Chairs)

T2TRG scope & goals

- Open research issues in turning a true "Internet of Things" into reality
  - Internet where low-resource nodes ("things", "constrained nodes") can communicate among themselves and with the wider Internet
- Focus on issues with opportunities for IETF standardization
  - Start at the IP adaptation layer
  - End at the application layer with architectures and APIs for communicating and making data and management functions, including security

Next meetings

- 2017 meetings planned
  - September 23/24 work meeting (Berlin):
    Co-located with/before RIOT Summit and ACM ICN
  - November 10 (Singapore):
    Joint meeting with OCF co-located/before IETF
- 2018 planning started
  - Continue joint meetings with WoT, OCF, …
  - More academia?
  - Co-located with security conference (Feb/May maybe)?
  - Workshops @ IETF meeting(s). Montreal at least?

ACM ICN 2017 BERLIN

Venue :: FU Berlin

Topic for Berlin: Coexistence

- Many “IoT networks” will share
  - Spectrum (e.g., 2.4 GHz, but also sub-GHz)
  - IP networks
- So far, people have been trying to get the car going on the empty road
- How is the more crowded landscape going to look like?
- What can we do to avoid one network taking out the next?

Sat/Sun: WISHI

Workshop on IoT Semantic/Hypermedia Interoperability

- Follow-on to IoTSI March 2016: meeting of experts working with SDOs that standardize data formats for IoT interchange (IPSO, OMA [LwM2M], iot.schema.org, W3C WoT, OCF, OneM2M, Fairhair, Haystack)

- Materials in Git: https://github.com/t2trg/2017-07-wishi

- Meeting was great for getting a mutual understanding, now towards a sustainable mode of collaboration

Sustainable Collaboration: What to achieve? E.g:

- Collect:
  - Self-descriptions of participating organizations (don’t require “formal” participation for that)
  - Corpus of uses cases and examples
  - Glossary of relevant terms
  - References to relevant tools
  - Also what didn’t work for achieving semantic interop
- Better understand impact of licensing terms on collaboration
  - Machine-readable tagging of license terms for models
- Bi/tri-lateral collaboration (e.g., schema.org and W3C); expanding (e.g., relationship with LwM2M and IPSO Semantics work)

Sustainable Collaboration: What to achieve? E.g:

- Machine-readable interfaces for metadata
- Tools for applications to define the composition of resources without requiring standards action; fetching and observing the compositions / service objects
- Define kinds of “metadata”, common ways to express and deliver metadata
- Everything else needed to facilitate interop across data definitions (WoT, IPSO Semantics, …)

Sustainable Collaboration: How to get there

- Common infrastructure (repos and wikis on github for now; tools such as OneIoTa?; registries for identifiers?)
- Monthly calls for sync and followup
- Common plugfests

Interoperability

- **Semantic** Interoperability
  — understand what the data/actions mean

- **Structural** Interoperability
  — understand the structure of the data/actions

- **Syntactic** Interoperability
  — can parse/generate data/actions

Layering may be recursive

- E.g., within structural interoperability, there may be
  - Information models (more semantic)
  - Data models (more structural)
  - Generic data models/serialization frameworks (more syntactic)

Specific topics: Modeling Data for Security

1. Data for onboarding & provisioning, establishing trust relationships (interoperability needed now?)

2. Metadata about security (management of trust relationships over time), could live with translation for a while

3. Metadata about security of data (and systems)

4. Maintaining privacy of discovery (existence, type, level...) (e.g., medical devices); fingerprinting

5. Metadata about privacy of the data (see 3) (e.g., for GDPR)

6. Privacy of identifiers, secret handshake protocols

The IoT “secret handshake” problem

- ACME Inc. has a contract with COFFEE Inc.:
    - ACME employees can get free coffee on all vending machines run by COFFEE
- How does an ACME employee get free coffee from COFFEE vending machines
    - without the employee giving away that they are an ACME employee
    - or the vending machine giving away that it is run by COFFEE?

“Secret Handshakes from Pairing-Based Key Agreements” (SOSP 2003)

Abstract:

- Consider a CIA agent who wants to authenticate herself to a server, but does not want to reveal her CIA credentials unless the server is a genuine CIA outlet. Consider also that the CIA server does not want to reveal its CIA credentials to anyone but CIA agents – not even to other CIA servers.
- In this paper we first show how pairing-based cryptography can be used to implement such secret handshakes. We then propose a formal definition for secure secret handshakes , and prove that our pairing-based schemes are secure under the Bilinear Diffie-Hellman assumption. Our protocols support role-based group membership authentication, traceability, indistinguishability to eavesdroppers, unbounded collusion resistance, and forward repudiability.
- Our secret-handshake scheme **can be implemented as a TLS cipher suite**. We report on the performance of our preliminary Java implementation.

[Dave Thaler]

Subsequent Work on Auth Mechanisms

Security Patterns for Untraceable Secret Handshakes with optional Revocation (2011) surveys many other additions, e.g.

- Secret Handshakes from CA-Oblivious Encryption (2004) uses more standard algorithms
- RSA-Based Secret Handshakes (2005)
- Private Handshakes (2007) prevent group admin from tracing users
- Beyond Secret Handshakes: Affiliation-Hiding Authenticated Key Exchange (2008) also generates session key
- Affiliation-Hiding Authentication with Minimal Bandwidth Consumption (2011)

[Dave Thaler]

Agenda

13:30: RG status update (Chairs)

13:40: WISHI report and way forward (Chairs+)

14:20: Edge Computing: Summary of Chicago discussion and ideas for next steps (Dirk Kutscher)

14:50: Authorizing network access for IoT Devices (Mohit Sethi)

15:20: Future activities: Documents and Meetings (Chairs)