

# T2TRG: Thing-to-Thing Research Group

Joint Meeting with ICNRG  
November 13, 2016, Seoul, KR

Chairs: Carsten Bormann & Ari Keränen

# WiFi

- SSID: 63\_banquet-CYPRESS
- Pass: **a123456789**

# 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](mailto:t2trg@irtf.org)** — subscribe at:  
**<https://www.ietf.org/mailman/listinfo/t2trg>**
- Repo: **<https://github.com/t2trg/2016-11-icnrg>**

# Agenda

## **Morning**

Presentations 9:00-10:15

- Research and Development of the Hyper-connected IoE Network Technology — Taewan You
- Device and Network naming structures and ICN for IoT applications — Lopez Jairo
- A RESTful, Distributed and Enhanced ICN System for IoT — GQ Wang
- I3: some thoughts towards an Industrial Information-Centric Internet of Things — Thomas Schmidt

Break 10:15-10:40 [coffee, cookies -- thanks, ETRI]

- Discussion 10:40-12:00
- Introduction to discussion - Chairs
- Discussion

Next steps, Next meeting?, etc

**12:00 Lunch**

**Move to NMRG Workshop for the afternoon (Kensington Yoido)**

# 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

# Done so far

- Chartered in December 2015. Multiple meetings before official chartering co-located with IETF meetings and with W3C Web of Things (WoT) group
- 2016: RG meetings at Nice and Lisbon co-located with W3C WoT, at San Jose co-located with IAB IoT**SI** WS, at Buenos Aires and Berlin with the IETF meetings; participated in Dublin IAB IoT**SU** WS; RIOT summit in Berlin; Implementers' meeting in Ludwigsburg (Stuttgart)
- Three RG deliverable documents in progress on REST and security; multiple new documents on REST interaction
- Outreach (e.g., organizations like OCF and Bluetooth SIG)

# Where are we going

- Work on RG deliverables and outreach continues
- Future meetings co-located with good research venues (2017)
- Meetings co-located with open source activity
  - RIOT summit in Berlin (July)
  - Eclipse IoT meeting (October)
- Benchmark/reference scenarios
  - Initial discussion in various drafts and slides
  - More elaborate documentation by end of 2016



# Next meetings

- 2017 planning TBD

Thank you, ETRI!

# Agenda

## **Morning**

Presentations 9:00-10:15

- Research and Development of the Hyper-connected IoE Network Technology — Taewan You
- Device and Network naming structures and ICN for IoT applications — Lopez Jairo
- A RESTful, Distributed and Enhanced ICN System for IoT — GQ Wang
- I3: some thoughts towards an Industrial Information-Centric Internet of Things — Thomas Schmidt

Break 10:15-10:40 [coffee, cookies -- thanks, ETRI]

- Discussion 10:40-12:00
- Introduction to discussion - Chairs
- Discussion

Next steps, Next meeting?, etc

**12:00 Lunch**

**Move to NMRG Workshop for the afternoon (Kensington Yoido)**

Research and Development of the  
Hyper-connected IoE Network  
Technology  
*Taewan You*

Device and Network naming  
structures and ICN for IoT  
applications  
*Lopez Jairo*

A RESTful, Distributed and  
Enhanced ICN System for IoT  
*GQ Wang*

I3: some thoughts towards an  
Industrial Information-Centric  
Internet of Things  
*Thomas Schmidt*

# Discussion



# ICN & IoT

Dirk Kutscher

# ICN & IoT

IoT one of the use cases for ICN

Several claimed benefits

- Location-independent access to named data/actuators

- Data-oriented security model

- Data availability due to caching, in-network forward strategies

- Ad-Hoc communication features

- Stack implementation simplification

# Implementations

RIOT (CCNLite)

NDN-IoT

Cisco

Others?

# Research Questions

Naming in uncoordinated IoT networks

IoT interaction semantics in ICN (push, updates)

## Security

Security bootstrapping (onboarding, key distribution)

Feasibility of ICN PK crypto

Other security approaches: ABE

## Semantic interoperability

Discovery: how to know what to ask for etc.

Semantics and properties of named data and dynamic computation results

## Internet picture

Connecting ICN IoT networks to the Internet

Role of gateways, translators etc.

Possibility of avoiding silo networks

# Meeting Today

Leverage background and new ideas in T2T and ICN communities

Learn from current work in both groups

Chairs' suggestion: device/data naming & semantic interoperability

See mailing list discussion

Understand real-world problems and possible approaches

Identify relevant topics for follow-up work

# Endpoints

- Endpoint: you || the other party that you are talking to
- Initiator (Client):  
Server learns about it when the request hits
- Responder (Server):  
Client needs to “find” it (from URI data)

# Endpoints in HTTP

- Server endpoint: Scheme/Host/Port (**Origin**)
  - Translated to Address/Port by client (**DNS**)
  - HTTPS: Client verifies DNS name of Host (**PKI**)
- Client endpoint: anonymous
  - Can use Client Address/Port (usually considered ephemeral)
  - Client certs: rare
  - Put Client identity into **Cookie** (muddled up with application state)

# What's different in CoAP

- **DNS** deemphasized
- Certs (and thus **PKI**) deemphasized
  - PKI Certs need CRLs/OCSP, secure absolute time, ...
- We don't have **cookies**
- **Servients**: Servers often have client component — how to link server and client identities?



# Endpoints in CoAP/UDP

- Client uses **URI data** to look up server transport address
  - lookup mechanism intentionally not defined in RFC 7252
- Server uses **request transport address** to reply and send notifications

# CoAP/UDP: Issues

- Endpoint transport addresses might not be stable
  - IP addresses change due to renumbering
  - Transport addresses change due to NAT timeouts
- Transport address change loses endpoint identity

# CoAP/UDP: Issues

- Server address change:
  - New requests:  
Lookup mechanism likely to use cache → stale info
  - Observe, other long-running requests:  
Client cannot relate Notification from new address to the right server
- Client address change:
  - Observe, other long-running requests:  
Server cannot send Notification to the right client

# Endpoints in CoAP/DTLS

- Client uses **URI data** to look up server transport address
- Client states (**SNI**) and verifies server identity (and server possibly verifies client identity)
- Endpoint is the peer in the resulting **connection**
  - Ephemeral: endpoint dies with connection
  - (but long-term endpoint “identity” doesn’t)

# “Identity”

- Most misunderstood word in security
- Identity = set of claims
  - But that’s not how we use the term intuitively
- Need another word for the “real-world identity” of a Thing
  - But what is that? Owner change, role change, repairs (replace board/chip)...
- Where authorization is entirely identity-based: need “revocation”

# Endpoint claims in HTTPS

- server: DNS name  
(tied into Authority and thus Origin)
  - Cert can actually have other claims,  
but those are rarely visible to application
- client: (could have cert, but usually:)  
established in-band, then reified into cookies

# Endpoint claims in COAPS

- PSK mode: mutual verification
  - needs out of band channel; cf. DCAF
  - source, scope specified by those OOB mechanisms
- RPK mode: implicit server identity claim
  - OOB channel can be used (e.g., with directed identity)
- Cert mode: less well-defined (could use HTTPS model)

# Implicit vs. Explicit Claims

- PSK: Implicit claim of existing security association
- RPK: Implicit claim of server possession of private key
  - Both can be augmented by OOB information
- Cert: Explicit claim of SNI possession (time-bounded)
- With CWT, have more fine-grained, explicit claims:
  - Issuer, Audience, Scope, ...



# Identity confusion in APIs

- Very little of this makes it into APIs
- E.g., IoTivity uses the transport address as endpoint identity — even with DTLS
  - Application may send data via new, unrelated DTLS connection that happens to have the same transport address
- Issue: How to represent endpoints in APIs?

# CoAP/DTLS: Issues

- DTLS connection tied to transport address pair
  - dies when either pair changes
- Current request/response matching includes “epoch”
  - does not even extend Observe across session resumption

# Naming data

- (on an endpoint = server)
- resources, collections
- structured data: reach inside?
  - e.g., YANG data resource identifiers?  
COMI FETCH payloads?
- Names vs. semantics

# Schemas

- Describe the possible structures (descriptive)
- Augment structures with semantics (

# Securing data

- within a context (communication security)
- as a freestanding object (object security)
- Where are the trust anchors coming from?
- What is the relationship between resource discovery and setting up security associations?



# ABE for ICN IoT

Börje Ohlman

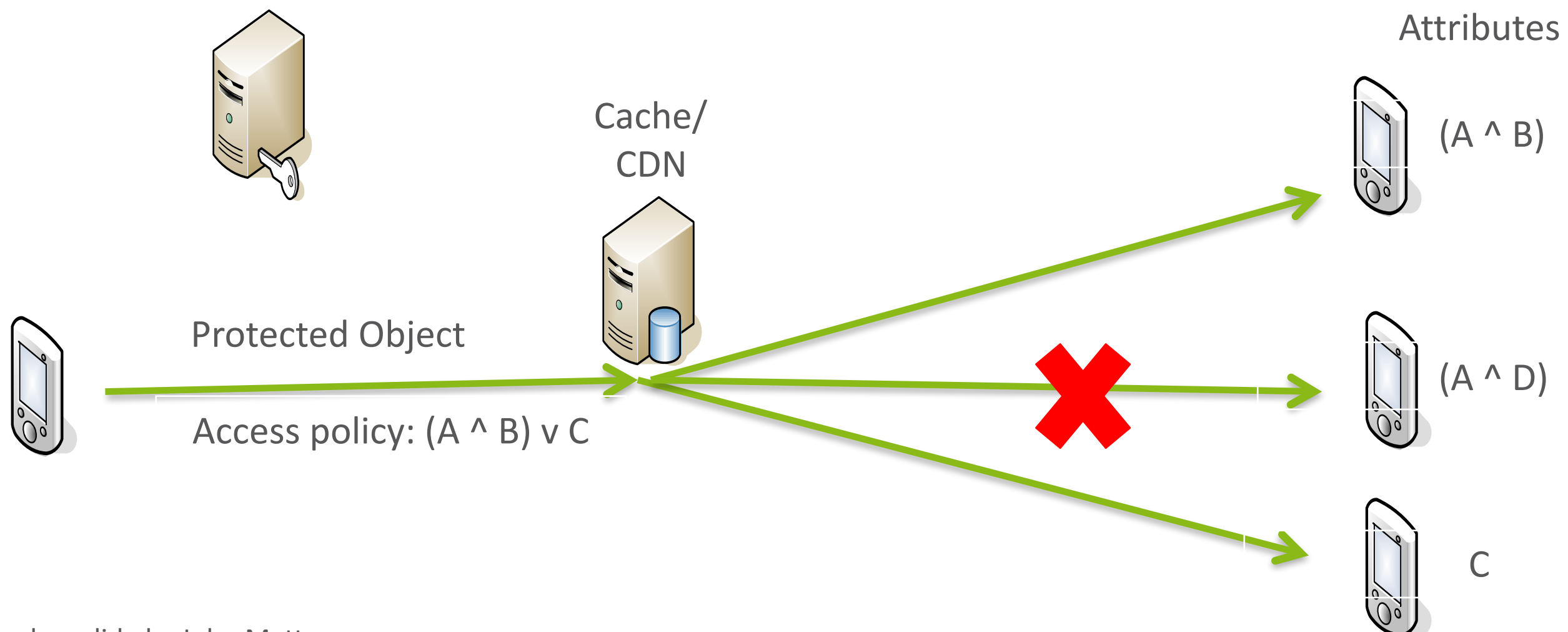
# Security requirements for IoT in an ICN context

---

- › An IoT security solution should ***not rely on e2e connectivity***, i.e. it should provide secure communication with disconnected or sleeping devices
- › After the information object leaves the sensor it should be ***secured without having to trust any intermediate device*** which it might be stored on.
- › ***Access control*** to information object ***should be done off-sensor*** to avoid DoS attacks through illegitimate requests that will drain the sensor battery

# ATTRIBUTE BASED ENCRYPTION (ABE)

**Main benefit:** Does not require communication with the key management server. Which would be a benefit for constrained devices (**how heavy are the ABE operations?**). Can encrypt to several selected recipients.





# ABE Key Characteristics

---

## Pros

- › Does not require communication with the key management server.
- › Very good match between ICN's need for secure objects and ABE's way of securing objects
- › Can provide fine grained access control for to objects while the objects still are cacheable (not different encryption for different sets of users)
- › Can provide good privacy by use of decentralized attribute authorities
- › Attribute authorities can be well integrated with the organizations responsible for related activities, e.g. health care authorities are issuing the health related attributes

## Cons

- › Computationally heavy, scalability issue
- › Expands data when encrypted



**ERICSSON**

# Beyond “data”

- Support for actions (actuators), events (push)
- Actions natural in IETF IoT stack
- But REST has no direct support for the state implied by publish/subscribe → Rucksack design?
  - HTTP world: reverse POSTs
  - CoAP: Observe (closer to REST)