A dozen years of standardizing the Internet of Things

IIESOC Connections, Bengaluru, IN, 2017-11-08

http://slides.cabo.space

Carsten Bormann

Universität Bremen TZI
IETF CoRE WG
IRTF T2T RG

http://slides.cabo.space

RFC 2429	RFC 2509	RFC 2686	RFC 2687	RFC 2689	RFC 3095
RFC 3189	RFC 3190	RFC 3241	RFC 3320	RFC 3485	RFC 3544
RFC 3819	RFC 3940	RFC 3941	RFC 4629	RFC 5049	RFC 5401
RFC 5740	RFC 5856	RFC 5857	RFC 5858	RFC 6469	RFC 6606
RFC 6775	RFC 7049	RFC 7228	RFC 7252	RFC 7400	RFC 7959
RFC 8132	RFC 8138				

Bringing the Internet to new applications

- “Application X will **never** run on the Internet”
- …
- …
- “How do we turn off the remaining parts of X that **still** aren’t on the Internet”?

Internet of Things

Scale up:

Number of nodes

(xx billion by 2020)

Internet of Things

Scale down:

node

Internet of Things

Scale down:

cost

complexity

cent

kilobyte

megahertz

Constrained nodes: orders of magnitude

10/100 vs. 50/250

There is not just a single class of “constrained node”

RFC 7228

Class 0: too small to securely run on the Internet

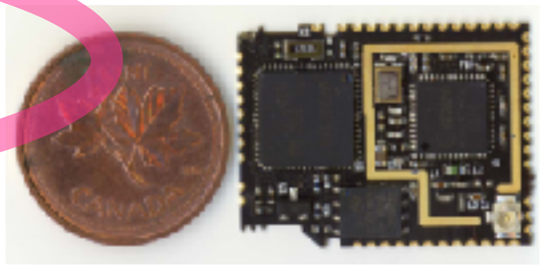
- ✘ “too constrained”

Class 1: ~10 KiB data, ~100 KiB code

- ✔ “quite constrained”, “10/100”

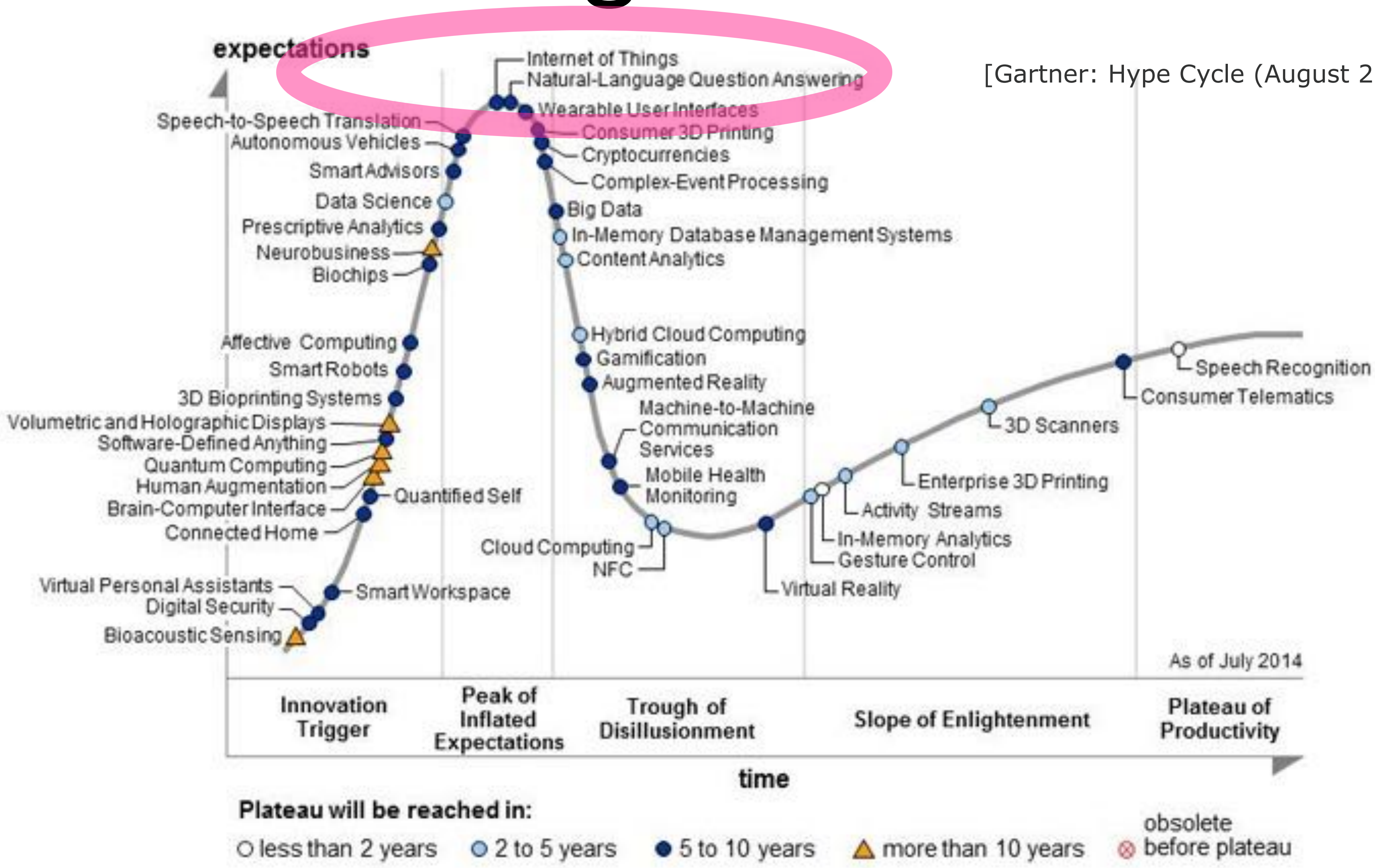
Class 2: ~50 KiB data, ~250 KiB code

- ✔ “not so constrained”, “50/250”



These classes are not clear-cut, but may structure the discussion and help avoid talking at cross-purposes

Danger ahead



[Gartner: Hype Cycle (August 2014)]

Internet of Things?

IP = *Internet* Protocol

“IP is important”

IP = *Integration* Protocol

IP: drastically reducing barriers

- **IP telephony** (1990s to 2018): replaced much of the special telephony hardware by routers and servers
  - several orders of magnitude in cost reduction
  - available programmer pool increases massively
  - What started as convergence, turned into **conversion**
- Everything is **not** the special snowflake it is said to be
- Now: **Internet of Things**

Hype-IoT	Real IoT
IPv4, NATs	IPv6
Device-to-Cloud	Internet
Gateways, Silos	Small Things Loosely Joined
Questionable Security	Real Security
$40+	< $5
W	mW, µW

IoT: Current Deployment Models

- **Device to cloud**
  - Add isolated nodes to existing LANs (e.g., WiFi)
  - Lots of “ants” (v4: You might see this in your CGNs)
  - v4: Reachability from outside requires keepalive (often UDP!)
- **Device to “gateway”**/hub (…to cloud)
  - Closer to other traffic we have today
  - Adds more periodic microflows to the mix
- **Device to device** (“thing-to-thing”, general Internet connectivity)
  - (v4: Behind the NAT, or lots of hole punching needed)

[RFC 7452]

> … a properly networked world … could be safer, greener, more efficient and more productive … But in order for that to emerge, the system has to be designed in the way that the internet was designed in the 1970s – by **engineers who know what they’re doing**, setting the protocols and technical standards that will bring some kind of order and security into the chaos of a technological stampede.

John Naughton, “The internet of things needs better-made things”
(The Guardian, 2016-07-10)

IETF®

IETF: Constrained Node Network WG Cluster

INT	LWIG	Guidance
INT	6LoWPAN ✓	IP over 802.15.4
INT	6Lo	IP-over-foo
INT	6TiSCH	IP over TSCH
INT	♨ LPWAN	Low-Power WAN Networks
RTG	ROLL	Routing (RPL)
APP	CoRE	REST (CoAP) + Ops
APP	♨ CBOR	CBOR & CDDL
SEC	DICE ✓	Improving DTLS
SEC	ACE	Constrained AA
SEC	COSE ✓	Object Security

2005-03-03: 6LoWPAN

- “IPv6 over Low-Power WPANs”: IP over X for 802.15.4
  - Encapsulation ➔ RFC 4944 (2007)
  - **Header Compression** redone ➔ RFC 6282 (2011)
  - **Network Architecture** and ND ➔ RFC 6775 (2012)
  - (Informationals: RFC 4919, RFC 6568, RFC 6606)

6LoWPAN breakthroughs

- RFC 4944: make IPv6 possible (fragmentation)
- RFC 6282: **area text state** for header compression
- RFC 6775: rethink IPv6
  - addressing: embrace **multi-link subnet** (RFC 5889)
  - get rid of subnet multicast (**link multicast only**)
  - adapt IPv6 ND to this (➔ “**efficient ND**”)

Technology	Traits	
IEEE 802.15.4 (“ZigBee”)	Many SoCs, 0.9 or 2.4 GHz, 6TiSCH upcoming	2.4 GHz
BlueTooth Smart	On **every Phone**	
DECT ULE	**Dedicated Spectrum,** In every home gateway	1.8 GHz
ITU-T G.9959 (“Z-Wave”)	Popular @home	0.9 GHz
802.11ah (“HaLow”)	Low power “WiFi”	
NFC	**Proximity**	13.56 MHz
6lobac	**Wired** (RS485)	
IEEE 1901.2 (LF PLC)	Reuses mains **power** lines	
Ethernet + PoE	**Wired**, supplies 12–60 W	
WiFi, LTE, …	**Power?**	

2008-02-11: ROLL

- “Routing Over Low power and Lossy networks”
    - Tree-based routing “RPL” ➔ RFC 6550–2 (2012)
        - with Trickle ➔ RFC 6206 (2011)
        - with MRHOF ➔ RFC 6719
    - Experimentals: P2P-RPL (RFC 6997), Measuring (RFC 6998)
    - MPL (Semi-Reliable Multicast Flooding) ➔ RFC 7731..7733
    - (Lots of Informationals: RFC 5548 5673 5826 5867 7102 7416)

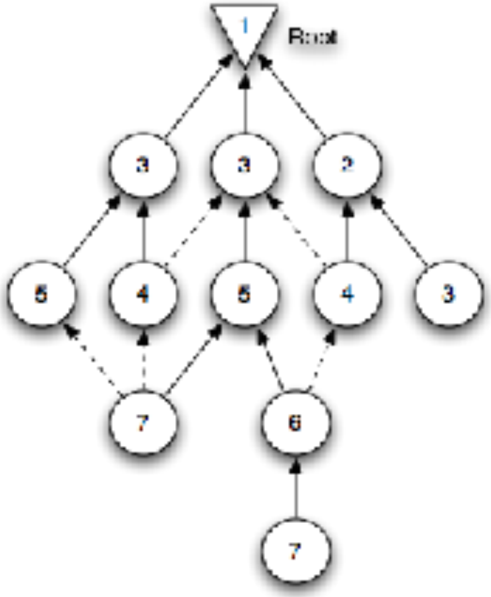
RPL: Routing for CN/N

2012

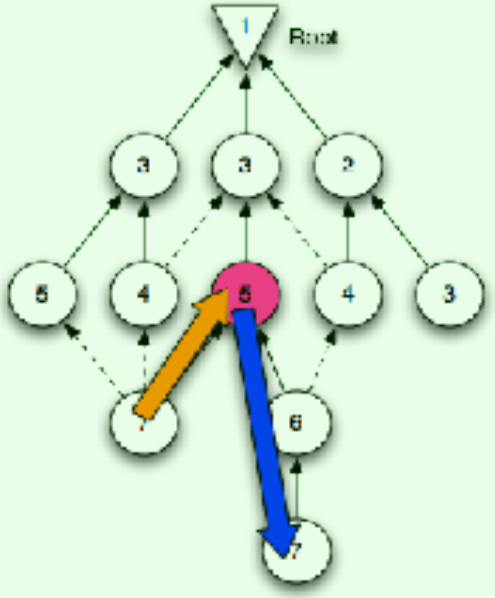
Metrics: e.g., ETX

- **RFC 6550**: Specialized routing protocol **RPL** – Rooted DAGs (directed acyclic graphs)

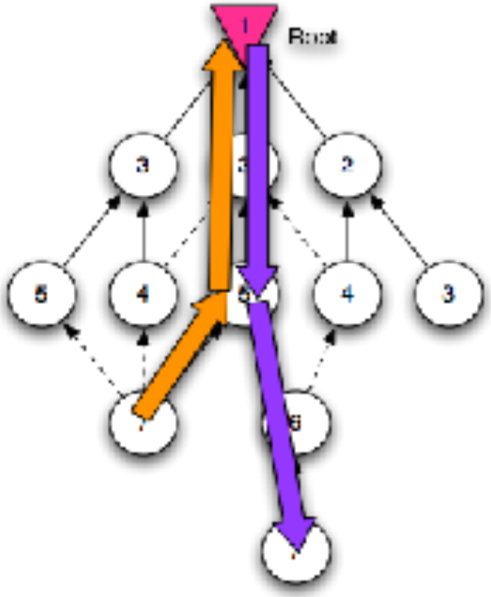
- **redundancies** in the tree help cope with churn
- "**rank**": loop avoidance



- **Storing** Mode: Every router has map of **subtree**



- **Non-Storing** Mode: Only **root** has map of tree



Application Layer Protocols

- CoRE: Constrained **REST**ful Environments:
  Replace HTTP by a less expensive equivalent (**CoAP**)
  - From special-purpose/siloed to **general purpose**
- ACE: Define Security less dependent on humans in the loop and on very fast upgrade cycles
  - Embrace the **multi-stakeholder** IoT

Application Layer Data Formats

- Industry move to **JSON** for data interchange
- Add **CBOR** where JSON is too expensive
- Use **JOSE** and **COSE** as the security formats
- Work on semantic interoperability (IRTF **T2TRG**), with W3C, OCF, OMA/IPSO (LWM2M), iot.schema.org, …
  ➔ self-description

Reducing TCO: Self-Description and Discovery

- Manually setting up 10^{11} nodes is a non-starter
- **Self-Description**:
  IoT nodes support automatic integration
  - RFC 6690 /.well-known/core “**link-format**”
  - W3C WoT work on “Thing Description” ongoing
  - **Semantic Interoperability**!
- **Discovery**:
  IoT nodes and their peers can find others
  - /.well-known/core exposes resources of a node
  - **Resource Directories** (with a bridge to DNS-SD)

2010-03-09: CoRE

- “Constrained Restful Environments”
  - CoAP ➔ RFC 7252 (~~2013~~2014)
    - Observe: RFC 7641, Block: RFC 7959
    - HTTP mapping: RFC 8075
  - Experimentals: RFC 7390 group communications
  - Discovery (»Link-Format«) ➔ RFC 6690

The **Co**nstrained **A**pplication **P**rotocol

CoAP

- implements HTTP’s **REST** model
  - GET, PUT, DELETE, POST; media type model
- while avoiding most of the complexities of HTTP

- **Simple** protocol, datagram only (UDP, DTLS)
- 4-byte header, compact yet simple options encoding

- adds “observe”, a lean notification architecture

IoT Devices as a secure application

Protect the objectives right ✔

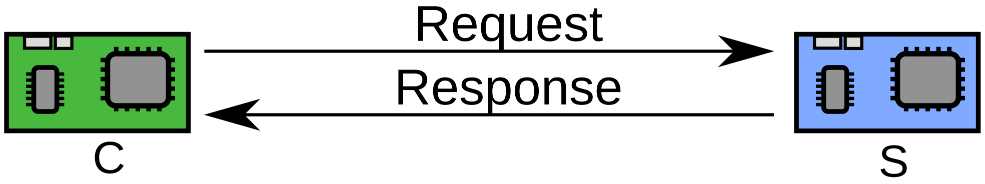
vs.

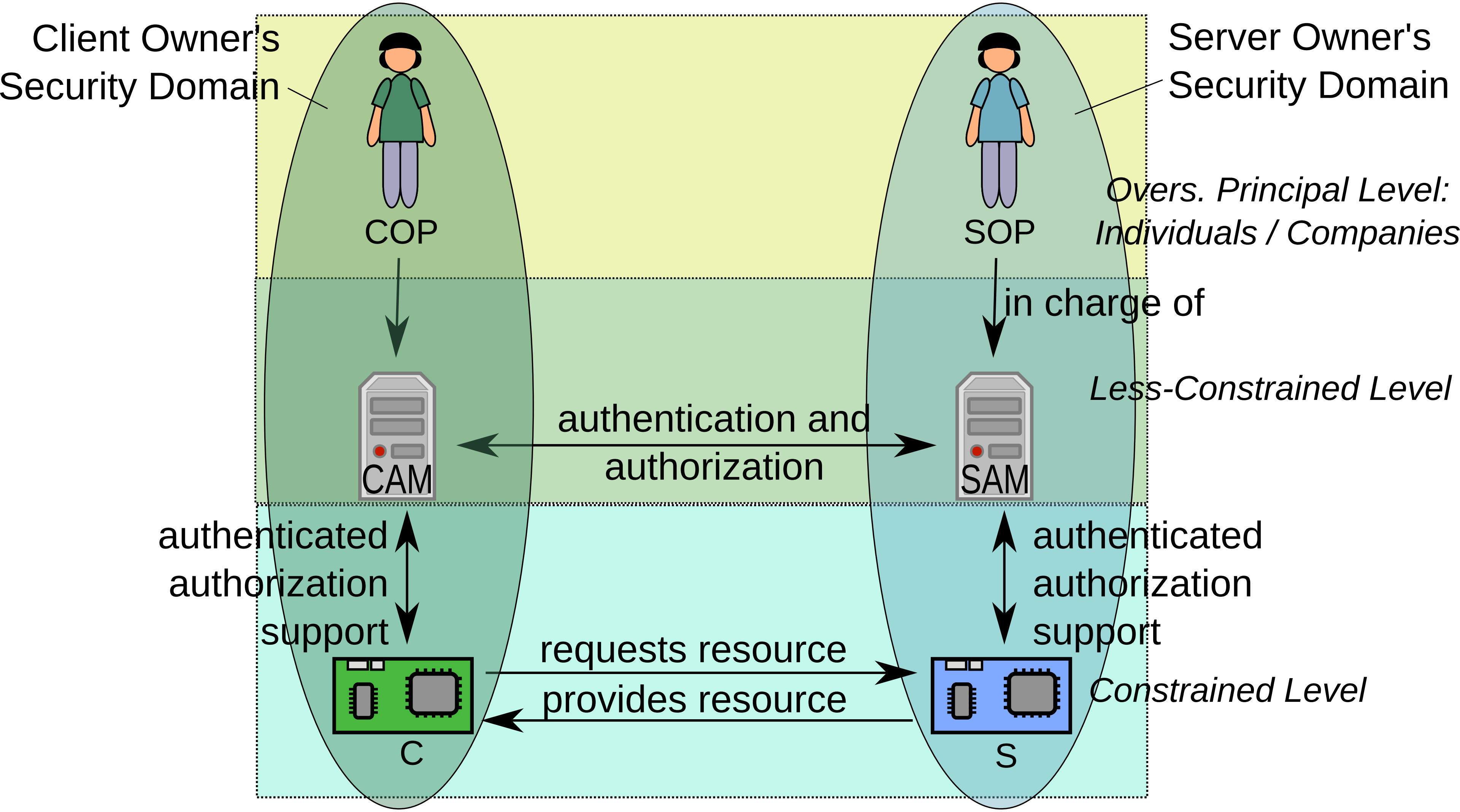
Protect the right objectives ♨

2014-05-05: ACE

- “Authentication and Authorization for Constrained Environments”
    - currently applying OAuth framework to IoT

Now let's apply all this to constrained devices




Client Owner's
Security Domain
Server Owner's
Security Domain
COP
SOP
Overs. Principal Level:
Individuals / Companies
in charge of
Less-Constrained Level
CAM
SAM
authentication and
authorization
authenticated
authorization
support
authenticated
authorization
support
requests resource
provides resource
Constrained Level
C
S

Shaping the Security Workflows

- Stakeholders, Principals
- Less-constrained nodes
- Constrained nodes

- Device Lifecycle
- Authorized, authenticated delegation

2013-09-13: CBOR

- "Concise Binary Object Representation":
  JSON equivalent for constrained nodes
    - start from JSON data model (no schema needed)
    - add binary data, extensibility ("tags")
    - concise binary encoding (byte-oriented, counting objects)
    - add diagnostic notation
- Started AD-sponsored, turned into a WG on 2017-01-09
- CDDL: Description language for CBOR (and JSON)

Data Formats

	Character-based	Concise Binary
Document-Oriented	XML	EXI
Data-Oriented	JSON	???

Data Formats

	Character-based	Concise Binary
Document-Oriented	XML	EXI
Data-Oriented	JSON	CBOR

2015-06-03: COSE

- CBOR Object Signing and Encryption:
  Object Security for the IoT

- Based on **JOSE**: JSON Web Token, JWS, JWE, …
  - Data structures for signatures, integrity, encryption…
  - Derived from on OAuth JWT
  - Encoded in JSON, can encrypt/sign other data

- **COSE: use CBOR instead of JSON**
  - Can directly use binary encoding (no base64)
  - Optimized for constrained devices

IRTF: Internet Research Task Force (sister of IETF)

- IRTF complements IETF with longer-term **Research Groups**
- New: Thing-to-Thing Research Group (T2TRG)
- Investigate open research issues in:
  - turning a true “Internet of Things” into reality,
  - an Internet where low-resource nodes (“Things”, “Constrained Nodes”) can communicate among themselves and with the wider Internet, in order to partake in permissionless innovation.

IoT Devices as an attack platform

user duty

garage?

vendor duty

CE • *regulation?* • UL

jails

Manufacturer’s Usage Description (MUD)

- Protect the network and other **unrelated** users against an IoT Device that may be insecure
- Idea: Document **expected behavior**
  in an actionable way
- MUD as standardized today:
  Can be used for **firewall** configuration
  - Poke firewall holes for desirable traffic
  - **Detect** when the IoT Device has been compromised
- Where can we take this idea?

Software Updates are needed

- Bugs are being found
- Environments change

→ Update or discard!

- Traditional: manual upgrade by connecting a special upgrader device (e.g., PC with upgrader app)
    - Too expensive; device might be hard to reach
- Needed: **Secure** Over-the-air Upgrade
- IETF100: SUIT BOF — manifest format for updates

If it is not **usably secure**,
it's not
the **Internet of Things**

IETF®