Resource Directory: What are we trying to protect?

Carsten Bormann 2018-07-16
IETF 102 Montreal, CA

Protect the objectives right ✔

vs.

Protect the right objectives 

Previous slides were about protecting the “endpoint name”

- RD requires authorization for the registration under an endpoint-name
- RD does not care what is registered under that name
- (Assumption seems to be: RD does not allow modifications to registration under an endpoint-name that the registrant is not authorized for.)

Threats?

- Could register a resource under my endpoint name but on another node's IP address with wrong attributes ("The temp sensor for room 405 is over there")

- Could register a resource under my endpoint name and under my own IP address with fake attributes ("I'm the temp sensor for room 405")

What’s so special about “endpoint names”?

- Server might not at all care about its endpoint name
    - It’s not visible in a resource lookup anyway
- Do we hinge all the protection on the endpoint name?

Can we protect <u>semantics</u>?

- E.g., authorize registration as a temperature sensor
- E.g., authorize registration “for room 405”
- How do we represent authorized semantics in authorization data structures?
  - CWT scope somewhat unwieldy