Thoughts on Authentication Issues of WEIRDS

Ning Kong, Linlin Zhou, Yan Wang, Sean Shen

WEIRDS-IETF 84-Vancouver
August 1st 2012
Backgrounds

• ... may use standard features of HTTP to support differential service levels to different classes of user. [Charter]

• How to define objects so you can restrict access to certain resources within the object. [A.2. Service Differentiation in a REST-pect-ful way.]
Discussions in the Mailing List

• Discussion on the mailing list [thread with subject "REST-pect-ful" and "Authentication Methods"]
  – One query or multiple queries?
  – One credential or multiple credentials?
  – One party or multiple parties authentication?
  – Can we work from the assumption that authentication is through features offered by HTTP?
  – What would we be closing the door on if we require that we only rely on features offered by HTTP?
  – Which authentication mechanism MUST, SHOULD or MAY be implemented?
Questions for Confirmation, Concensus or Discussion

1. What does authentication mean, what do we need:
   - Authentication of Client
   - Authentication of Server?
   - Authentication of Data (integrity, confidentiality, tls) ?

2. No difference for whois of names and numbers
3. Requirements, service differentiation

1. Authentication level:
   - Public: open to all
   - Group: open to a group of people, could be based on membership
   - Authorized: open to particular people with permit, could be based on token
   - Private: open to none
4. Data granularity in authentication: phone number or the whole contact info?
5. Does searching/redirect affect authentication? Are they orthogonal?

• if orthogonal, should go a head without worrying about searching.

• if not orthogonal, should the authentication for searching be left for another work till we know what the WHOIS searching/redirect will be?
6. Possible scenario (non-searchable)
   • Client-Server authentication
   • Third party authentication
Do we need one of them or both

7. Possible authentication method to use
   • Digest Authentication in RFC2617?
   • OAuth 2.0?
   • TLS?
   • Others?