I2RS security

Susan Hares (editor)
And Discussion Team

Discussion Team

- Editor: Sue Hares
- Co-authors on Architecture: Joel Halpern, Alia Atlas
- Chairs: Ed Crabbe
- Security folks: Ahmed Abro, Scott Brim, Nancy Cam-Winget, Eric Yu; Dacheng Zhang, Salman Asadullah, Wes George
- Information model people: Qin Wu, Sue Hares

Status

- Architecture draft has initial security issues covered, but misses confidentiality and mutual authentication
- Discussion Team
  - A discussion team is trying to see if there are other security items needed in this doc.
  - **Preliminary outline**: draft-hares-i2rs-security-arch-00.txt
  - **Joint outline** based on work from co-authors and past drafts:draft-abroasadullah-i2rs-security-00.txt
- Meeting on Friday's at 5pm ET/ 2pm PT/ 6am Sat (China)

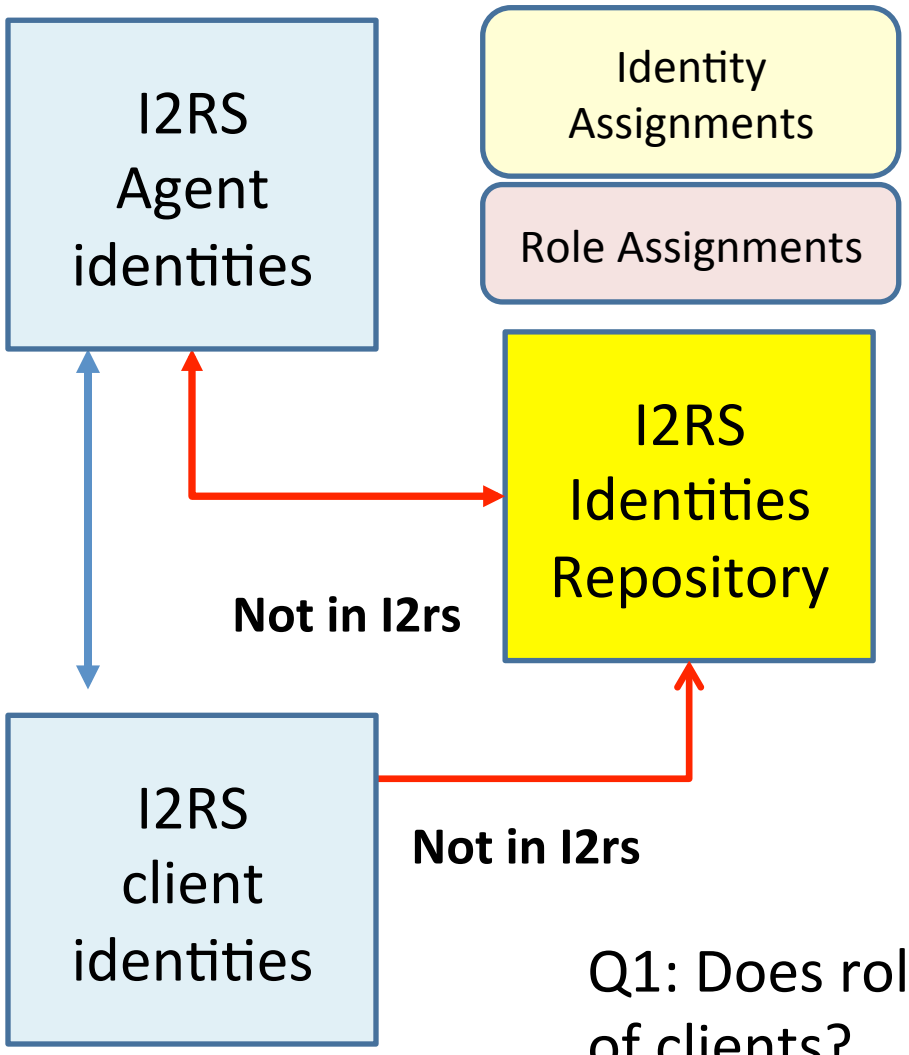
Current status

- Leveraging security definitions from RFC4949
- Investigating
  - Mutual authentication
  - Confidentiality
  - Role Based Security for I2RS Agent-Client interaction
    - **Not:** Application-I2RS Client
    - **Not:** I2RSAgent-Routing System
- Considering
  - Security requirements I2RS agent-client protocol
  - Impact of Security: Zero to full security – when/ where/how/why

RFC4949

- Access control (AC): (read, write, read + write)
  - Authorized use of resources by authorized entities (users, programs, processes)
  - Includes: Security policy + prevent unauthorized access, Identify who is authorized
- Role based AC: (RBAC) limits by role + identity
- Confidentiality –
  - data is not disclosed to system entities unless they have been authorized to know, and
  - data is not disclosed to unauthorized individuals, entities or processes.
- Mutual Authentication
  - Moving from mutually suspicious state to mutually authenticated by identify and verifying identity and role

Role-Based Access Control (RBAC)



Mutual Authentication
I2RS Agent Identity = OK ID
I2RS Client Identity = OK ID

Role =
Potential Read scope +
Potential Write Scope

Q1: Does role by client lead to proliferation of clients?

Q2: Grouping Tradeoff - # Functions/Role?

Environmental Issues

- Transport requirements
  - Implication on multi-stream model of I2RS
  - Impact on publishing broker or subscription to events
- Auditable Data Streams
  - Optional
  - Full stream or partial (Filtered audit/on Filtered events)
  - Use case draft: draft-clarke-i2rs-traceability-01
- Privacy
  - Encryption: optional or mandatory
- Stacked I2RS agents

  i2rs client --- i2rs-agent/i2rs-client ---- i2rs agent

Next steps

- Discussion on list?
- Small group target to complete draft quickly
  - Goal: Quick feedback to Architecture document
  - Goal: 1st Draft completed by 05/15/2015
  - Discussion and adoption afterward
  - Send mail to shares@ndzh.com if you want to join security discussions