Protocol Requirements

draft-bryan-p2psip-requirements-00.txt

D. Bryan/SIPeerior-editor
S. Baset/Columbia University
M. Matuszewski/Nokia
H. Sinnreich/Adobe

69 IETF, Chicago, July 26, 2007

An orderly approach to requirements

- Deployment scenarios
- NAT traversal
- Bootstrap and other servers
- SIP-P2P overlay interface and API
- P2P Overlay requirements
- DHT selection criteria
- Client protocol requirements
- Security: SIP, DHT, client

This reflects the work of several authors, so there is still some inconsistency

P2P overlay requirements

- Data replication
- Load balancing
- Overlay performance
  - Routing performance: Tables and state
  - Routing styles
  - Join/leave (churn) handling
  - Enabling mobility: nodeID not based on IP
  - Fault tolerance to non-transitive connectivity

SIP-Overlay Interface

- No dependence on any particular overlay
  - SIP-P2P interface
  - APIs for DHT usage
    - API for the peer protocol
    - API for the client protocol

The client protocol

Benefit from, but not contribute to overlay

- Avoid battery consumption and charges from “always talking” in DHT mode
- Bandwidth limitations+churn make a poor peer
- Access to find/insert/modify data in overlay
- Flexible interface for non-SIP applications

Selecting a DHT

- Deployed and tested over the Internet with millions of users?
- Has the research been published?
- Running code available?
- Can the experience be extrapolated for P2PSIP?

Some people suggested that we should not select mandatory-to-implement DHT, instead leave the decision to developers.

Security Requirements

draft-matuszewski-p2psip-security-requirements-01.txt

M. Matuszewski -editor

J-E. Ekberg

P. Laitinen

69 IETF, Chicago, July 26, 2007

Attacks

- Storage
  - Attacker may discard, modify data it is responsible for
  - Attacker may fill up the network with data
  - Attacker may modify, delete resource (user) records of other users
- Routing
  - Attacker may discard or modify messages
  - Attacker may reply with wrong data
  - Attacker may misroute messages
- Privacy
  - Attacker may eavesdrop routed messages
- Other e.g. replay attacks
- Scope
  - Bootstrapping, joining, data insertion, modification and retrieval
  - SIP operations: proxy, registrar

P2PSIP security

Security must be an integral part of the overlay protocols design

Consider user requirements and first target “good enough security”

“Good enough security” at least should address:

- Enrolment: control identity and issue credentials
- Secure data stored in the overlay
- Limit the impact of badly behaving nodes

… while not re-defining the existing security mechanisms (or DHT itself) more than necessary

OPEN ISSUES

Who enrolls to the P2PSIP system: only a user or also a peer? Do we need separate credentials for peers and users?

Do we allow a distributed enrolment system?