Cryptographically generated SIP-URIs to protect the integrity of content in P2P-SIP


Presented by Rashmi Padiadpu
19.06.2007
Contents

- Introduction
- Security for P2P-SIP
- Proposed scheme
- Evaluation
- Conclusion
Introduction

- SIP
  - Address of record - SIP-URI
  - Contact address - Location
- User registration & location lookup
  - Client server
  - Overlay networks
SIP User registration and Location Lookup - Using client server SIP

1. REGISTER IP-address & SIP-URI

2. Store location (binding between SIP-URI and IP-address)

3. Send SIP INVITE to establish session

4. Query for IP Address of the Destination Domain's SIP Proxy

5. Forward INVITE

6. Location Service checks that the destination IP address represents a valid registered device

7. Forwarded Request to the End-Device

8. Destination device returns its IP Address and a media connection is opened

SIP: alice@atlanta.com

SIP: bob@biloxy.com
SIP User registration and Location Lookup - Using structured overlay Networks

- DHT
- Possible attacks
Existing scheme

Options for authenticating contents in P2P-SIP & their limitations

- Trusted authority for certification
- Distributed reputation management system
Proposed scheme (1)

- Cryptographically generating a SIP-URI
  - Generate a public – private key pair:
  - Hash the public key using function hash:
  - Convert h1 to a string using function f:
  - Generate the SIP-URI u1 by:

- Registering a Location for a SIP-URI
  - User signs the current location to u1:
  - Then stores u1, kpub, s1 in the overlay:

- Verifying the authenticity of Location Data
  - Node requests a location for SIP-URI u2:
  - Node receives location binding, signature, and public key
  - Node verifies
  - If it is true, then
Properties of proposed scheme

- No central Authority
- Verification possible on all possible routing hopes
- Interdependency of overlay and routing strategy
- Backward compatibility
Evaluation of proposed scheme

- Readability of SIP-URIs
- Associating a SIP-URI with a user
- Attacks on hash function
- Performance / DoS attacks
Conclusion

- Cryptographically generated SIP-URI as self certifying data
- No central authority required
- It is independent of routing strategy used
- Enables integrity check in all routing hops

Thank you