Authentication and Access Control to Resources in a RELOAD Overlay

AG-iNET Seminar

Gabriel Hege
hege@informatik.haw-hamburg.de

HAW Hamburg

October 19, 2010

Overview

The DisCo Conferencing Scenario

- Tightly coupled peer-to-peer conferences using SIP
- No central server for conference lookup, signaling and media distribution
- Focus functionality distributed transparently among participants
- Use RELOAD for registering conference URI

An Overview of RELOAD

- REsource LOcation And Discovery
- P2P-Overlay protocol
- Based on a distributed hash table (DHT), e.g. Chord
- Highly extensible by defining other usages,
  e.g. SIP- & XMPP-Usage
- In P2PSIP used to replace the proxy- and registrar-servers

The SIP-Usage for RELOAD

- Goal: Replacing the proxy and registar functionality in a P2P fashion
- Registration done by storing contact information using the SIP-Registration kind in the overlay
- Lookup of a SIP-URI done in normal DHT-Fashion: lookup hashed URI
- Proxy replaced by providing method to establish transport connection between any two peers (including NAT)

The DisCo-Usage for RELOAD

- Similar to SIP-Usage
- Register a conference URI to make it publicly accessible
- Focus peers register themselves as entry points to the conference
- Write permission to the conference registration kind needs to be delegated to focus peers

The RELOAD Security Model

- Security model based on certificates
- Certificates used to provide authentication among peers
- Usually certificates obtained from central enrollment server
- RELOAD provides security on three levels:
  1. Connection Level: (D)TLS for peer connections
  2. Message Level: all messages signed
  3. Object Level: all stored objects signed by creator
- Access control policies limit (write) access to resources based on certificates
- Policies indirectly prevent peers from storing arbitrary amounts of data

Resource Access Control Policies

- Access control policies limit who may write at a specific location
- All stored data must be signed
  $\rightarrow$ Storer presents certificate with fields matching policy rules
- Base RELOAD defines 4 policies:
  1. USER-MATCH
  2. NODE-MATCH
  3. USER-NODE-MATCH
  4. NODE-MULTIPLE
- Every resource kind specifies policy to use
  e.g. SIP-Registration: USER-NODE-MATCH
- **None of these fitting for DisCo-Registration**

Requirements for DisCo-Registration

- Shared resource (Needs to be written by multiple peers)
- Only (some) members of the conference allowed to write
- Anybody may retrieve stored data
- Group members need to verify stored data
- Must still fit into general RELOAD security model
  e.g. prevent resource exhaustion from storing lots of data (resource exhaustion)

Straightforward solution:

- Use one conference certificate for the whole group

Ask Enrollment Server

Simplest approach:

- Get new certificate from enrollment server for each conference
- Certificate User-Name contains conference URI
- Use USER-MATCH policy
- Distribute private key of the conference certificate among focus peers

Problem:

- Enrollment Server only supposed to be contacted when joining the DHT:

  Overlay should stay fully functional without server

→ **Need to get a certificate without enrollment server**

Self Signed Certificates Don't Work

- Malicious peer could take over a conference:
  - Generate certificate for existing conference URI (sybil attack)
  - Unable to tell if certificate is from conference initiator or not
  - Malicious peer registers itself as focus for the conference
- Peer could generate multiple certificates and store arbitrary amounts of data at multiple positions in the overlay

Generate Chained Certificates

- Conference initiator creates conf-certificate, signed with his private key
- Define new access control policy for use in DisCo-Registration: USER-CHAIN-MATCH
- Storing peer verifies certificate chain
- Distribute conference private key to all focus peers

Chained Certificates Need Restrictions

Remaining Problem:

- Malicious peers could still generate certificates for existing conferences

Solution:

- Restrict who can create a conference and certificate for a certain name

- Conference name must be correlated to initiator's name
- Restrict allowed conference URIs using pattern matching

Example:

URI pattern: *-conf-$USER@$DOMAIN
User Name: alice@example.com

Allowed:
XYZ-conf-alice@example.com
pretty-conf-alice@example.com
NOT allowed:
alice-conference@example.com

Remaining Problem: Revocation

- Chance of conference certificate being compromised enhanced, because multiple peers have the private key
- Still no solution for certificate revocation

Simple workaround:

- Short certificate lifetimes (e.g. a couple of minutes?)
- Renew certificate accordingly
- Certificate can only be used as long as creator is in the conference (+ lifetime)
  → probably makes sense because conference name is coupled to creator

Alternative:

- Publish Certificate Revocation List (CRL) in overlay
- Needs another kind definition...

Conclusion and Outlook

- Controlled access to shared resources not a trivial problem in P2P networks
- RELOAD is flexible enough to support fitting access control policies

  Are there better ideas than pattern matching?
- Certificate revocation can be done, but incurs more overhead

  Is it really needed for simple ad-hoc conferences?

Ich bedanke mich für die Aufmerksamkeit.

Fragen?