Building Blocks for Trusted Coordination

Nick Cook
University of Newcastle
Trusted Coordination

♦ Two aspects:
  • Higher level mechanisms for policy specification and enforcement
    – Contract representation and monitoring
  • Lower level mechanisms for non-repudiable interaction - the scope of this presentation
Outline

♦ Building blocks for trusted coordination
  • Non-repudiable service invocation
  • Non-repudiable information sharing
♦ Infrastructure requirements
♦ Implementations
♦ References
Building blocks for trusted coordination

- Trusted coordination addresses VE requirement to regulate interactions (service access, update to shared information, etc.)
- Regulation implies an audit trail to monitor interaction and for dispute resolution
- Evidence generated is of little value unless irrefutably attributable to its source (non-repudiable)
- Implies two building blocks for trusted coordination:
  - Non-repudiable service invocation
  - Non-repudiable information sharing
Service invocation

- 2-party, client-server interaction
- Server needs evidence that:
  - The request originated at the client: non-repudiation of origin (NRO) of the request
  - The response was received by the client: non-repudiation of receipt (NRR) of the response
- Client needs evidence that:
  - The request was received by the server (NRR req.)
  - The response originated at the server (NRO resp.)
Non-repudiable service invocation

Client → server: reqId, req, NROreq

server → client: reqId, resp, NRRreq, NROresp

client → server: reqId, NRRresp

Where, for example:

\[ NROreq = \{ \text{sig}_c\left(\text{reqEv}\right), \text{sig}_T\left(t_r, \text{sig}_c\left(\text{reqEv}\right)\right) \} \]

\[ NROresp = \{ \text{sig}_s\left(\text{respEv}\right), \text{sig}_T\left(t_v, \text{sig}_s\left(\text{respEv}\right)\right) \} \]

\[ \text{reqEv} = h(\text{reqId}, \text{req}) \]

\[ \text{respEv} = h(\text{reqId}, \text{resp}) \]
Observations

♦ To guarantee protocol compliance, interceptors must be trusted
♦ Degenerate case is that the interceptors are a trusted third party (or parties)
  • protocol resembles fair exchange as discussed in the literature
♦ Interceptors can be configured to execute any non-repudiation protocol
  • For example: to meet different evidentiary requirements
Evidence for non-repudiable service invocation

- Request evidence includes the service invoked and any parameters to the invocation
- Response evidence is the result of the invocation
- 3 different types to consider:

1. **Values**: require the state of the value at invocation time (or at response time for result). Before evidence generation, must resolve references to local values to an agreed representation of their state.

2. **Service references**: require a globally resolvable name for the service, e.g. URL (not the state of the service)

3. **Shared information references**: require the state of the information at invocation time (or at response time for result) and a reference to the shared information that is resolvable by the remote party
Access and update to shared information

- Multi-party, peer-peer interaction
- For an update proposed by A:
  - B and C need evidence that update originated at A (NRO update)
  - A needs evidence that B and C received the update (NRR update)
  - A, B and C need evidence that, after update, the information will be in a consistent, agreed state (NRO agreement, NRR agreement)
Non-repudiable information sharing

Evidence required:
- State transition proposed by A (propose: step 2)
- Decisions on validity of transition from B and C (respond: step 3)
- Collective decision (resolve: step 4)

Shared information is only updated if the collective decision is that A’s proposal is valid

Incentives to good behaviour stronger than for one-off service invocation
Infrastructure Requirements

♦ Cryptographic primitives
  • Digital signatures, secure message digest (hash), secure random number generation
♦ Credential (certificate) management
♦ Access control services
  • Intra-organisation: map user to role
  • Inter-organisation: map credential to role
♦ Non-repudiation log
  • protocol-specific
  • include signed hash of state in evidence
♦ State store
  • map hash of state to persistent representation of state
Infrastructure contd.

- Coordination service to execute NR protocols (configurable to specific protocol)
- Membership service (for information sharing only)
  - Maintain group membership information (mapping members to credentials)
  - Membership is coordinated using NR protocols executed by coordination service
- Communication subsystem
- Trusted time-stamping service
  - To verify a signing key was not compromised at time of use (evidence generation)
  - Recent results from Zhou et al may make this unnecessary
- Trusted Third Parties for strong fairness guarantees
Implementations

♦ NR service invocation
  • Wichert et al’s CORBA service
    – Lacks protocol detail, (naturally) only addresses value types
  • Paul Robinson is working on J2EE implementation

♦ NR information sharing
  • B2BObjects
    – Realise shared information as object replicas at each member of coordinating group
    – Regulate access to and update of object state
    – Group membership and object state only change if all parties agree
    – Implemented in Java using RMI (also have initial version running on JBOSS)


Jianying Zhou’s **non-repudiation bibliography**: http://www.geocities.com/zhou_jianying/non-repudiation.html