# Session 3: Security

Hard Problems in SOA Workshop  
January 30, 2008  
Pittsburgh, PA

## Participants

<table>
<thead>
<tr>
<th>John McLaughlin, IBM Co-facilitator</th>
<th>Anthony Gargaro, Computer Sciences Corporation</th>
<th>Michael McCarthy, CMU</th>
<th>John Goodenough, CMU</th>
</tr>
</thead>
<tbody>
<tr>
<td>David White, CMU, Co-facilitator</td>
<td>Sue Halterman, MITRE-GCSS-AF</td>
<td>Brandon McKenzie, UPMC Cancer Centers</td>
<td></td>
</tr>
<tr>
<td>Jessica Ascough, Harris Corporation</td>
<td>Dan Carr, FedEx Ground</td>
<td>Norman Sadegh-Koniecpol, CMU</td>
<td></td>
</tr>
<tr>
<td>Jeff Barnes, CMU</td>
<td>Joe T. Lee, Treasury Department</td>
<td>Mark Yanalitis, Highmark Inc.</td>
<td></td>
</tr>
<tr>
<td>Archie Andrews, CMU</td>
<td>James Lindley, IRS</td>
<td>Peter Hagemeyer, Future Skies</td>
<td></td>
</tr>
<tr>
<td>Parviz Dousti, CMU</td>
<td>Hal Lockhart, BEA Systems</td>
<td>Indrajit Poddar (IP), IBM</td>
<td></td>
</tr>
</tbody>
</table>
Taxonomy Consensus

- Security is conspicuous in its absence from the SOA Research Taxonomy
- Security should be added as a Cross-Cutting issue
Main Issues Discussed

- Composite Applications Complications
- User Identity
- Managing Security Across Diverse Applications

Composite Applications Complications
-description

- Composite applications are defined as choreographed services
- These are issues that arise in SOA, but not in monolithic applications, including
  - Security policy combination/alignment/conflict
  - Appropriate delegation
  - Architecture complexity and implementation challenges
  - Compliance at run-time
Composite Applications Complications
—rationale

- Goal is to guarantee security results even when we don’t know how the system will be assembled
- Non-deterministic nature of security policy choreography
- Agility and security can be opposing forces
- Heterogeneity makes security difficult

Composite Applications Complications
—current efforts

- Threat modeling and attack surfaces in SOA are in active study (Lindley)
- IBM Research engaged on composite business services (Poddar)
- Decentralized trust management (Sadeh)

Note: names in parentheses are participants who offered to provide specific references to current efforts
Composite Applications Complications – Challenges and Gaps 1

- We don’t know how to build context sensitive policies for SOA
- Effective de-conflicting of security policy remains hard to do (Lockhart)
- Policy specification in complex choreographies remains a challenge (Sadeh)
- Policy advertising and matching needs research and experience (Lockhart)
- How do we give adequate and useful security and privacy controls to the user (Sadeh)

Note: names in parentheses indicate the participant who mentioned the challenge (in case follow-up is needed)

Composite Applications Complications – Challenges and Gaps 2

- Integration of multiple policy administration points, decision points, and languages is difficult (Security Enforcement Points) (Poddar)
- Current infrastructures lack sufficient security ‘hooks’ (this is about more than API) (Hagemeyer)
- Resource allocation currently focuses on monitoring compliance at the expense of engineering; paradigm shift is needed (Lindley)
Composite Applications Complications
—ideas to address challenges and gaps 1

- Conduct user studies on prototype security tools (Sadeh)
- Collect data on SOA security problems that have occurred (Goodenough)
- Standards development such as XACML extensions (Poddar)
- Understand full implications of security problems in SOA from the top down, such as Model Driven Development (Lockhart)

Note: names in parentheses indicate the participant who mentioned the idea (in case follow-up is needed)

---

Composite Applications Complications
—ideas to address challenges and gaps 2

- Discover or predict ways that current technology can be used to resolve anticipated problems—bottom up (Lockhart)
- Challenge problems would be useful to motivate research (Goodenough)
- Study large-scale SOA implementations. Attempt to correlate success to resource allocation during development (Lindley)

Note: names in parentheses indicate the participant who mentioned the idea (in case follow-up is needed)
User Identity
—description

- User
  - Active entity/system entity
  - Requester of service
  - The cumulative user in a chain of entities

- Identity
  - Properties of user including aspects of trust and rights

User Identity
—rationale

- Cumbersome legacy issues – differing trust and authentication models
- Chaining of identities as service providers can sometimes be service consumers
- Generalized delegation is a hard problem
- Unbridled PII propagation is a large problem
- Systems controlled by different organizations; identities controlled by different organizations—Federation schemes are needed
  - Business and legal issues may be harder than technical issues here
- Non-unique user identification is sufficient for security, but audit/compliance motivates unique user identification, creating a potential PII conflict

[PII is personally identifiable information]
User Identity
—current efforts

- SAML, shibboleth, open-SAML
- Liberty Alliance (includes some work on legal and business aspects)
- OASIS Open ID
- MSFT Card Space
- Higgins project
- Federated Identity
  - Proof carrying authentication
  - Symantec (or Semantic?) web extensions (In the workshop, we captured this reference as Symantec, www.symantec.com; comments after the workshop suggest that the appropriate reference is to the Semantic Web as described at www.w3.org/2001/sw/)
- IBM Research initiatives

User Identity
—challenges and gaps

- Differing trust and authentication models
- Chaining of identities
- Generalized delegation
- Unbridled PII propagation
- Federation schemes for multi-organizational enterprises
- Must [uniquely] identify user for privileges, creating a PII conflict
  - Auditors wish for very granular identification
User Identity
—ideas to address challenges and gaps

- Many existing projects could be studied – in particular government efforts to build very-large citizen databases
- Legal and business requirements can drive development of technology
- Case law needed to sort out legal issues
- Better methods to de-identify PII to that it can studied more openly
- Improved data obfuscation techniques (PII) are needed to aid SOA development and testing (good test data sets are difficult to assemble because of PII)
- Case law and regulation reform – PII is nearly indefinable, especially due to dynamic and heterogeneous regulations

Managing Security Across Diverse Apps
—description

- Management issues are key here in distinguishing this from the first issue
- Technology, legal, and business issues are relevant
- This applies to the post-implementation/operation phase of the lifecycle
Managing Security Across Diverse Apps — rationale

- Management of a distributed SOA environment over the lifecycle remains hard
- Choosing what to worry about and what to ignore is important
- Your concerns may differ from third party (consumers and providers) in SOA
- Actual requirements for security management systems are very difficult

Managing Security Across Diverse Apps — current efforts

- IBM Global Grid Forum (Lockhart)
- Auditing tool development (Sadeh)
- IRS rebuild of its auditing architecture and approach (Lindley) (Lindley offered to provide paper on philosophy of auditing)
- Defense Department Net Centric Warfare work; Naval Post Graduate School
- IBM Tivoli product research on auditing (Mclaughlin)
- Jericho Forum – deperimeterization (Lockhart)
- NIST standards efforts
- CERT Resiliency Engineering work
  (http://www.cert.org/resiliency_engineering)
Managing Security Across Diverse Apps
—challenges and gaps

- Conflict between loose coupling and tight security policy management
- Outsourcing – managing security in outsourcing is a similar problem. Particularly acute for call centers
- Lack of large scale security tooling
- Lack of consistent security metrics
  - Management doesn’t understand what to measure
- Laws and regulations complicate data movement across borders; particularly problematic for PII

Managing Security Across Diverse Apps
—ideas to address challenges and gaps

- Codification of standards
  - Many management standards efforts for web services are currently stalled
- Proprietary standards are part of the problem
- Need for a family of tools to help people manage security in SOA
  - Human interface issues are important here
- Standards with extensions are pervasive
- Determine which SOA security demands cannot be addressed by current risk assessment methods (such as OCTAVE) and develop new methods to fill the gap