Secure Document Circulation Using Web Services Technologies

Shane Bracher

IBM PhD Student Symposium
3rd International Conference on Service-Oriented Computing (ICSOC 2005)

12 December 2005
Amsterdam, The Netherlands
Problem Statement

- **Security for Service-Oriented Computing:**
  - The “crossing organizational boundaries” issue – services can spread across multiple domains.
  - No single, central administration authority for enforcing security.
  - Complicating issue – how can security be enforced in an inter-domain, decentralized environment? (in other words, multiple, separately controlled domains)

- **Web Services Security**
  - Much activity into establishing security standards for Web Services.
    - For example: WS-* security stack, SAML, XACML
  - But this is all implementational based.
  - What about security at the design stage?
Objectives

1. **How can security be specified during the design phase of Web Services?**
   - Must consider the change in context to an inter-organizational (multiple domain) environment.
   - The aim is to investigate using model driven security techniques.

2. **Applying the first objective.**
   - Scenario – providing security support for electronic document circulation within inter-organizational processes.
   - The security issues of this scenario are comparable to those of Service-Oriented Computing.

3. **How to implement this scenario using Web Services technologies?**
Project Description

- **Security at the design phase:**
  - Investigate how to represent security goals and security measures within UML models.
  - Start off with augmenting UML use case diagrams with security features (and consider propagating these features to other UML diagrams later).
  - Forms of security specification:
    - Security at the level of systems.
    - Security at the level of use cases.
    - Security handled externally.
    - Security requirements on messages.
Project Description

- **Securing electronic document circulation within inter-organizational processes:**
  - Consider the following issues –
    - How is the document managed?
      - For example: structure, content, status, dates, contributors, etc.
    - How is document security handled?
      - For example: encryption, integrity, authentication, authorization, etc.
    - How is document flow controlled?
      - For example: specifying the workflow, specifying state descriptions, etc.
  - The challenge – achieving this in a distributed, heterogeneous, decentralized environment.
  - The proposal – the realization of a “smart” document which contains embedded security mechanisms and possesses knowledge on its flow.
Achieving Secure Document Circulation

• Enforcing security is complicated due to the absence of a single enforcement point.

• To provide access control in this case, this must now be done using encryption.
  • Shift required in policy specifications
    • Previously – “what actions is a user allowed to perform”
    • Now – “who has access to the decryption key”
  • Introduces the need for finer granularity for confidentiality and data integrity.
  • Introduces the need for key protection strategies.
High-Level Document Design

Document Description → Document → Document Metadata

Workflow Description → Flow States → Policies → Attributes
Future Steps

- Formulating a detailed document design.
- Investigating how Web Services technologies can be applied to implement the design.
- Conducting a case study to demonstrate the applicability of this concept in real world scenarios.
Conclusion

• **Two main directions of this research –**
  
  • To address the need for specifying security requirements during the early stages of Web Services development.
  
  • To investigate the use of Web Services technologies for implementing secure document circulation in inter-domain, decentralized environments.
Thank you for your attention.

• Shane Bracher
  sbracher@student.bond.edu.au

• Centre for Software Assurance
  School of Information Technology, Bond University
  Gold Coast, Queensland, 4229, AUSTRALIA

  www.sand.bond.edu.au

• Acknowledgements
  Special thanks to Siemens AG (Corporate Technology) for their support towards this research.