An Approach to Extract RBAC Models from BPEL4WS Processes

Jan Mendling
Mark Strembeck
Gerald Stermsek
Gustaf Neumann

Department of Information Systems and New Media
Vienna University of Economics and Business Administration
Agenda

• Why RBAC and BPEL4WS Processes?

• How does BPEL4WS work?

• What is RBAC about?

• How can BPEL4WS be mapped to RBAC?

• How to automatically extract RBAC from BPEL4WS?

• Conclusion and future work
Why RBAC and BPEL4WS Processes?
Why RBAC and BPEL4WS Processes? (I)

- BPEL4WS
  - Business Process Execution Language for Web Services
  - Web Service Composition
  - Web Services work via Internet protocols
  - Different Security Issues

- Role-Based Access Control (RBAC)
  - Who is allowed to do what?
  - Subject-Operation-Object Triple
Why RBAC and BPEL4WS Processes? (II)

- BPEL
- RBAC
- WSDL, UDDI
- Transactions
- Coordination
- Reliable Messaging
- Cryptographic Security Services
- SOAP Messaging
Roles in RBAC and Workflow

• **Traditional Workflow:**
  - Local and secure Network or Information System
  - Coordinate obligation for tasks to responsible roles
  - Role represents a resource

• **BPEL:**
  - Internet accessible processes, unsecure network
  - Access control via roles
  - Role captures a permission
How does BPEL4WS work?
Example: Schedule Exam

BPEL

1 <process name="Schedule Exam" ...
2 <partnerLinks>
3 <partnerLink name="Exam"
4 partnerLinkType="uni:ExamLT"
5 myRole="Exam Service"
6 partnerRole="Teacher"/>
7 ...
8 <partners>
9 <partner name="Academic Staff">
10 <partnerLink name="Teacher"/>
11 <partnerLink name="Author"/>
12 ...
13 <partners>
14 <variables>
15 <variable name="Schedule"
16 messageType="uni:ScheduleM"/>
17 ...
18 <sequence>
19 <receive partnerLink="Exam"
20 portType="uni:ExamProcess"
21 operation="scheduleExam"
22 variable="Schedule"
23 createInstance="yes"/>
24 ...
25 <reply partnerLink="Exam"
26 portType="tch:Exam"
27 operation="sendResults"
28 variable="ResultList"/>
29 ...
30 <invoke partnerLink="Admin"
31 portType="adm:Results"
32 operation="bookResults"
33 inputVariable="ResultList"/>
34 ...
35 </sequence>
36 </process>
BPEL Metamodel
BPEL4WS and Security

- **Out of Scope for BPEL:**
  - Coordinated transaction semantics (ref. to WS-Transaction)
  - Cryptographic security services (ref. to WS-Security)
  - Access Control

- **All those issues left to implementations!**
What is RBAC about?
RBAC Vocabulary

• RBAC Concepts:
  • Permission (Object, Operation) assigned to Roles
  • Roles assigned to Subjects
  • Role Hierarchy
  • Senior-Role inherits permissions
  • Junior-Role
  • Context Constraints

• Advantages of RBAC:
  • Roles change less often than assignment to roles
  • Multiple subjects with similar permissions
RBAC Metamodel

context attribute

context constraint

context condition

consists of

consists of

constrains

1..*

*  

operation

object

permission

role

subject

hierarchy

used in

assigned to

assigned to
How can BPEL4WS be mapped to RBAC?
Metamodel Mapping

BPEL

- process
  - correlation set
    - message
      - operation
        - port type
          - partner link
            - partner
              - groups

RBAC

- context attribute
  - context constraint
    - context condition
      - operation
      - object
        - hierarchy
      - role
        - subject
      - permission
        - context constraint
          - attribute
            - constraint
              - condition
                - context
                  - operation
                  - object
                    - hierarchy
                  - role
                    - subject
                  - permission
                    - context constraint
                      - attribute
                        - constraint
                          - condition
                            - context
                              - operation
                              - object
                                - hierarchy
                              - role
                                - subject
                              - permission
                                - context constraint
                                  - attribute
                                    - constraint
                                      - condition
                                        - context
                                          - operation
                                          - object
                                            - hierarchy
                                          - role
                                            - subject
                                          - permission
                                            - context constraint
                                              - attribute
                                                - constraint
                                                  - condition
                                                    - context
                                                      - operation
                                                      - object
                                                        - hierarchy
                                                      - role
                                                        - subject
                                                      - permission
                                                        - context constraint
                                                          - attribute
                                                            - constraint
                                                              - condition
                                                                - context
                                                                  - operation
                                                                  - object
                                                                    - hierarchy
                                                                  - role
                                                                    - subject
                                                                  - permission
                                                                    - context constraint
                                                                      - attribute
                                                                        - constraint
                                                                          - condition
                                                                            - context
                                                                              - operation
                                                                              - object
                                                                                - hierarchy
                                                                              - role
                                                                                - subject
                                                                              - permission
                                                                                - context constraint
                                                                                  - attribute
                                                                                      - constraint
                                                                                         - condition
                                                                                           - context
                                                                                             - operation
                                                                                             - object
                                                                                               - hierarchy
                                                                                             - role
                                                                                               - subject
                                                                                             - permission
                                                                                               - context constraint
                                                                                                 - attribute
                                                                                                   - constraint
                                                                                                     - condition
                                                                                                       - context
                                                                                                         - operation
                                                                                                         - object
                                                                                                           - hierarchy
                                                                                                         - role
                                                                                                           - subject
                                                                                                         - permission
                                                                                                           - context constraint
                                                                                                             - attribute
                                                                                                                - constraint
                                                                                                                    - condition
                                                                                                                       - context
                                                                                                                          - operation
                                                                                                                          - object
                                                                                                                             - hierarchy
                                                                                                                          - role
                                                                                                                             - subject
                                                                                                                          - permission
                                                                                                                             - context constraint
                                                                                                                               - attribute
                                                                                                                                  - constraint
                                                                                                                                     - condition
                                                                                                                                        - context
                                                                                                                                             - operation
                                                                                                                                             - object
                                                                                                                                                - hierarchy
                                                                                                                                             - role
                                                                                                                                                - subject
                                                                                                                                             - permission
                                                                                                                                                - context constraint
                                                                                                                                                    - attribute
                                                                                                                                                       - constraint
                                                                                                                                                           - condition
                                                                                                                                                            - context
                                                                                                                                                                               - operation
                                                                                                                                                                               - object
                                                                                                                                                                                               - hierarchy
                                                                                                                                                                               - role
                                                                                                                                                                                               - subject
                                                                                                                                                                                - permission
                                                                                                                                                                                               - context constraint
                                                                                                                                                                                                 - attribute
                                                                                                                                                                                                                 - constraint
                                                                                                                                                                                                                       - condition
                                                                                                                                                                                                                           - context
                                                                                                                                                                                                                                               - operation
                                                                                                                                                                                                                                               - object
                                                                                                                                                                                                                                                               - hierarchy
                                                                                                                                                                                                                                               - role
                                                                                                                                                                                                                                                               - subject
                                                                                                                                                                                                                                                        - permission
                                                                                                                                                                                                                                                               - context constraint
Relation to Role Engineering

- **Scenario-Driven Role Engineering Process**
  - Define Scenarios
  - Define Roles that have permissions to execute scenarios
  - See Neumann/Stermbeck (SACMAT 2002)

- **Exploit mappings from BPEL to RBAC for automation**
How to automatically extract RBAC from BPEL4WS?
Automated Extraction of RBAC from BPEL

BPEL

<process>
  <partnerLinks>
    <partnerLink name="seller" partnerLinkType="as:sellerAuctionHouseLT" partnerRole="seller"/>
    <partnerLink name="buyer" partnerLinkType="as:buyerAuctionHouseLT" partnerRole="buyer"/>
  </partnerLinks>
  <partner name="SellerBuyer" xmlns="http://schemas.xmlsoap.org/ws/2003/05/partner-link">
    <partnerLink name="buyer"/>
    <partnerLink name="seller"/>
  </partner>

  <receive partnerLink="seller" portType="as:sellerPT" operation="provide" createInstance="yes"/>

</process>

<!-- PortType Operation Pairs to RBAC Permissions -->

<PERMISSION rdf:ID="#as:sellerPT_provide">
  <rm:permName xmlns:rm="http://www.xotcl.org/xorbac/rdf-schema#">as:sellerPT_provide</rm:permName>
</PERMISSION>

<!-- BPEL Partner to Senior Roles -->

<ROLE rdf:ID="#buyer">
  <rm:roleName xmlns:rm="http://www.xotcl.org/xorbac/rdf-schema#">buyer</rm:roleName>
  <rm:permission xmlns:rm="http://www.xotcl.org/xorbac/rdf-schema#" rdf:resource="#as:buyerPT_provide"/>
</ROLE>

<!-- BPEL Partner Roles to RBAC Roles -->

<ROLE rdf:ID="#SellerBuyer">
  <rm:roleName xmlns:rm="http://www.xotcl.org/xorbac/rdf-schema#">SellerBuyer</rm:roleName>
</ROLE>

<ROLE rdf:ID="#as:buyerPT_provide">
  <rm:permName xmlns:rm="http://www.xotcl.org/xorbac/rdf-schema#">as:buyerPT_provide</rm:permName>
</ROLE>

AUTO
XSLT Mappings from BPEL to RBAC

- PortType-Operation Pairs to RBAC Permissions
- BPEL Partner Roles to RBAC Roles
- BPEL Partner to RBAC Senior-Roles
Conclusion and future work
Conclusion and Future Work

• **Advantages:**
  - Security measures complementary to BPEL4WS
  - Partial Automation of Role Engineering Process
  - Consistency between RBAC Roles and Process

• **Future Work:**
  - Implementation of an RBAC-integrated Process Engine
  - Further Research into Interrelation of Process and Role Engineering
Thank you for your attention!

Jan Mendling, Mark Strembeck, Gerald Stermsek, Gustaf Neumann
Department of Information Systems and New Media
Vienna University of Economics and Business Administration