BPMN Extensions for Security Modelling

Edgars Gaidels and Andrejs Gaidukovs, 
*Riga Technical University, Latvia*

Raimundas Matulevičius
*University of Tartu, Estonia*

Security requirements

- A condition over the phenomena of the environment that we wish to make true by installing the system
  - Domain properties must be respected, so that security requirements could be fulfilled
  - Define the expected level of security

*(Dubois et al., 2010; Matulevičius, 2017)*
Taxonomy of Security requirements

[Firesmith, 2003]

- Identification requirements
- Authentication requirements
- Authorisation requirements
- Immunity requirements
- Integrity requirements
- Intrusion detection requirements
- Privacy requirements
- System maintenance security requirements
- Physical protection requirements
- Survivability requirements
- Security auditing requirements
- Nonrepudiation requirements

BPMN extensions to security

- Security requirements modelling
  - [Rodriguez et al., 2007]
- Trust modelling
  - [Menzel et al., 2009]
- Compliance for restricting modification behaviour
  - [Schleicher et al., 2010]
- Management of risk factors
  - [Marcinkowski and Kuciapski, 2012]
- Security risk management
  - [Altuhhova et al., 2013]
- Information assurance and security
  - [Cherdantseva et al., 2012]
- Modelling security policies
  - [Salnitri et al., 2014]
- Privacy-aware business process modelling
  - [Labda et al., 2014]
- Privacy-enhanced business process modelling
  - [Pullonen et al., 2017]
BPMN extensions to security

- Security requirements modelling
  - [Rodriguez et al., 2007]

- Trust modelling
  - [Menzel et al., 2009]

- Compliance for restricting modification behaviour
  - [Schleicher et al., 2010]

- Management of risk factors
  - [Marcinkowski and Kuciapski, 2012]

- Security risk management
  - [Altuhhova et al., 2013]

- Information assurance and security
  - [Cherdantseva et al., 2012]

- Modelling security policies
  - [Salniti et al., 2014]

- Privacy-aware business process modelling
  - [Labda et al., 2014]

- Privacy-enhanced business process modelling
  - [Pullonen et al., 2017]

Trust Modelling

- Annotations to capture and model trust
  - Trust relationship between two or more participants
  - Security intentions for the group of tasks, artefacts or pools

(Menzel et al., 2009)
Trust Modelling

- Annotations to capture and model trust
  - Trust relationship between two or more participants

(Menzel et al., 2009)

BPMN extensions to security

- Security requirements modelling
  - [Rodriguez et al., 2007]

- Trust modelling
  - [Menzel et al., 2009]

- Compliance for restricting modification behaviour
  - [Schleicher et al., 2010]

- Management of risk factors
  - [Marcinkowski and Kuciapski, 2012]

- Security risk management
  - [Altuhhova et al., 2013]

- Information assurance and security
  - [Cherdantseva et al., 2012]

- Modelling security policies
  - [Sallitri et al., 2014]

- Privacy-aware business process modelling
  - [Labda et al., 2014]

- Privacy-enhanced business process modelling
  - [Pullonen et al., 2017]
Compliance for restricting modification behaviour

- Compliance scopes – areas where certain compliance conditions must hold
  - Attached to the compliance scopes

(Schleicher et al, 2010)

BPMN extensions to security

- Security requirements modelling
  - [Rodriguez et al., 2007]

- Trust modelling
  - [Menzel et al., 2009]

- Compliance for restricting modification behaviour
  - [Schleicher et al., 2010]

- Management of risk factors
  - [Marcinkowski and Kuciapski, 2012]

- Security risk management
  - [Altuhhova et al., 2013]

- Information assurance and security
  - [Cherdantseva et al., 2012]

- Modelling security policies
  - [Salnitri et al., 2014]

- Privacy-aware business process modelling
  - [Labda et al., 2014]

- Privacy-enhanced business process modelling
  - [Pullonen et al., 2017]
Information assurance and security

- Extensions based on the Reference model of Information Assurance Security

  - Security goals
  - Security countermeasures
  - Application of sensitivity markers

(Cherdantseva, 2014)
BPMN extensions to security

- Security requirements modelling
  - [Rodríguez et al., 2007]
- Trust modelling
  - [Menzel et al., 2009]
- Compliance for restricting modification behaviour
  - [Schleicher et al., 2010]
- Management of risk factors
  - [Marcinkowski and Kuciapski, 2012]
- Security risk management
  - [Altuhhova et al., 2013]
- Information assurance and security
  - [Cherdantseva et al., 2012]
- Modelling security policies
  - [Salniti et al., 2014]
- Privacy-aware business process modelling
  - [Labda et al., 2014]
- Privacy-enhanced business process modelling
  - [Pullonen et al., 2017]

Management of Risk Factors

- Risk factor
  - Occurrence property
  - Impact
  - Risk factor types
    - Physical resource risk, human resource risk, time frame risk, financial risk, communicational risk
  - Risk mitigation
    - Reduce, retain, avoid, transfer, exploit, ignore

(Marcinkowski and Kuciapski, 2012)
BPMN extensions to security

- Security requirements modelling
  - [Rodriguez et al., 2007]
- Trust modelling
  - [Menzel et al., 2009]
- Compliance for restricting modification behaviour
  - [Schleicher et al., 2010]
- Management of risk factors
  - [Marcinkowski and Kuciapski, 2012]
- Security risk management
  - [Altuhhova et al., 2013]
- Information assurance and security
  - [Cherdantseva et al., 2012]
- Modelling security policies
  - [Salnitri et al., 2014]
- Privacy-aware business process modelling
  - [Labda et al., 2014]
- Privacy-enhanced business process modelling
  - [Pullonen et al., 2017]

Privacy aware BPMN

- Access control
  - Allow, prevent, limited
- Separation of tasks
- Binding of tasks
- User consent
- Necessity to know
  - High, medium, low

(Labda et al., 2014)
Privacy aware BPMN

Privacy-enhanced business process modelling

- Privacy by design
  - Privacy Enhancing Technology (PETS)
BPMN extensions to security

- **Security requirements modelling**
  - [Rodríguez et al., 2007]

- Trust modelling
  - [Menzel et al., 2009]

- Compliance for restricting modification behaviour
  - [Schleicher et al., 2010]

- Management of risk factors
  - [Marcinkowski and Kuciapski, 2012]

- Security risk management
  - [Altuhhova et al., 2013]

- Information assurance and security
  - [Cherdantseva et al., 2012]

- **Modelling security policies**
  - [Salnitri et al., 2014]

- Privacy-aware business process modelling
  - [Labda et al., 2014]

- Privacy-enhanced business process modelling
  - [Pullonen et al., 2017]

---

**Security Requirements Modelling**

(Rodríguez et al., 2007)
Security Requirements Modelling

- Nonrepudiation
- Attack Harm Detection
- Integrity
- Privacy
- Access Control

(Rodríguez et al., 2007)

Security Requirements Modelling

- Secure Business Process Diagram (SBPD)

(Rodríguez et al., 2007)
Secure Business Process

<table>
<thead>
<tr>
<th>Security Requirement</th>
<th>Pool</th>
<th>Activity</th>
<th>Message flow</th>
<th>Data object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-repudiation</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Attack harm detection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Integrity</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access control</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Rodríguez et al., 2007)

Modelling security policies

- Accountability
- Auditability
- Authenticity
- Availability
- Confidentiality
- Integrity
- Non-repudiation
- Privacy

(Salniti et al., 2014)
Modelling security policies

❖ SecBPMN

(Salnitri et al., 2014)
<table>
<thead>
<tr>
<th>Security requirements</th>
<th>SBPD</th>
<th>SecBPMN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td></td>
<td>Not supported</td>
</tr>
<tr>
<td>Authentication</td>
<td>Access control (Pool, Activity)</td>
<td>Authenticity (Message flow, Data object)</td>
</tr>
<tr>
<td>Authorisation</td>
<td></td>
<td>Confidentiality (Message flow, Data object)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Availability (Data object)</td>
</tr>
<tr>
<td>Immunity</td>
<td>Not supported</td>
<td>Availability (Activity)</td>
</tr>
<tr>
<td>Integrity</td>
<td>Integrity (Message flow, Data object)</td>
<td>Integrity (Actors, Activity, Message flow, Data object)</td>
</tr>
<tr>
<td>Intrusion detection</td>
<td>Attack harm detection (Pool, Activity, Message flow, Data object)</td>
<td>Not supported</td>
</tr>
<tr>
<td>Privacy</td>
<td>Privacy (Pool)</td>
<td>Privacy (Activity, Data object)</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>Non-repudiation (Message flow)</td>
<td>Non-repudiation (Activity, Message flow)</td>
</tr>
<tr>
<td>Security audit</td>
<td>As auditing values</td>
<td>Auditability (Activity, Message flow, Data object)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Accountability (Activity)</td>
</tr>
</tbody>
</table>

**Conclusion**

- Only fractions of security requirements
- Models become overloaded with too many details
- Focus on the software security
- Physical and security maintenance are not taken into account
Questions / Discussion

- What **security extensions** should be introduced to business process modelling?
  - Security risk management
  - Privacy
  - Trust
  - Compliance
  - Security requirements

- What **security analytics concerns** should business process modelling support?
  - GDPR
  - Security/privacy by design
  - Big data
  - Security / privacy in IoT