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
- System maintenance security requirements
- Physical protection requirements
- Survivability requirements
- Security auditing requirements
- Nonrepudiation requirements
- Privacy requirements
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]
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]
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
  - [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]
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
  - [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]
Information assurance and security

- Extensions based on the Reference model of Information Assurance Security

  - Security goals
    - Target (referent concept)
    - Security Goal
    - Low, Medium, High
    - Accountability (low criticality)
    - Non-repudiation (medium criticality)
    - Privacy (high criticality)
    - a) Security Goal Symbol Origin
    - b) Security Goal Criticality
    - c) Security Goal Type

  - Security countermeasures
    - Padlock (referent concept)
    - Security Countermeasure
    - Organisational
    - Technical
    - Human-Oriented
    - Legal
    - Non-disclosure Agreement
    - a) Security Countermeasure Symbol Origin
    - b) Security Countermeasure Types
    - c) Security Countermeasure Example

  - Application of sensitivity markers
    - Data Object classified as Confidential
    - Message classified as Proprietary
    - Data Storage classified as Restricted Sharing

(Cherdantseva, 2014)
Information assurance and security

(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
  - [Salnitri 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**
  - [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**
  - [Salnitrí 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

(Labda et al., 2014)
Privacy-enhanced business process modelling

- Privacy by design
- Privacy Enhancing Technology (PETS)

(Pullonen et al. 2017)
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

- 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></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Privacy</td>
<td></td>
<td>X</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

(Salnitri et al., 2014)
Modelling security policies

- **SecBPMN**

(Salnitri et al., 2014)
### Modelling security policies

**SecBPMN**

<table>
<thead>
<tr>
<th></th>
<th>Pool</th>
<th>Activity</th>
<th>Message flow</th>
<th>Data object</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accountability</strong></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Auditability</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Authenticity</strong></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Confidentiality</strong></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td><strong>Non-repudiation</strong></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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