SecBPMN2.0: extension of SecBPMN with BPMN 2.0

Mattia Salnitri

The following tables shows how SecBPMN is extended with BPMN 2.0 and with three, new, security annotations.

List of elements in SecBPMN2

Table 1 enlists the security annotations, the semantic for the security annotations introduced in SecBPMN2, and relevant BPMN 2.0 elements for SecBPMN2.

List of security concepts extended	BPMN 2.0 relevant elements
1. Accountability 2. Auditability 3. Authenticity 4. Availability 5. Confidentiality 6. Integrity 7. Non-repudiation 8. Privacy 9. Bind of duty Definition: It requires the same person to be responsible for the completion of a set of related tasks [2]. 10. Separation of duty Definition: it "is a security principle used to formulate multi-person control policies, requiring that two or more different people be responsible for the completion of a task or set of related tasks" [1] 11. Non-delegation Definition: all the actions performed in the scope of the security concept shall be executed only by the actor indicated	1. Task 1.1. Generic task 1.2. Send task 1.3. Receive task 1.4. Service task 1.5. User task 1.6. Manual task 1.7. Script task 1.8. Business rule task 2. Sub processes 2.1. Transactions 3. Call activity 4. Data object 4.1. Generic data object 4.2. Data object collection 4.3. Data store 4.4. Data input 4.5. Data output 5. Events 5.1. None 5.2. Message 5.3. Timer 5.4. Error 5.5. Escalation 5.6. Cancel 5.7. Compensation 5.8. Conditional 5.9. Link 5.10. Signal 5.11. Terminate 5.12. Multiple 5.13. Parallel 6. Gateways 7. Compensation 8. Pool 9. Lane 10. Message flow

	11. Data association

Table 1: list of security annotations and BPMN 2.0 elements

SecBPMN2 – collaboration/process

Table 2 shows the semantic of each security annotations. Depending on which SecBPMN2 elements are liked, the semantics of the security annotations change, therefore it is specified for each possible target. The numbers in the column "Target" refers to the number of BPMN 2.0 elements in Table 1. The dash between two numbers means all the elements included in the interval specified by the number. The round brackets are used to mark a pair of elements, while the vertical bar between two numbers represents a choice. For example (1|2,3) represents two pairs: 1,3 and 2,3.

Security concept	**Target**	**Semantic**
Accountability	1.1-1.7	A user involved in the execution of the task shall be held for his misbehaviour.
	8,9	The participant will be held for their misbehaviour.
Auditability	1.1-1.4, 1.7	The execution of the task is monitored.
	1.5, 1.6	The execution of human actions are monitored.
	4.3	The actions on the data store are monitored.
	8,9	All actions of participant will be monitored.
	10	All actions to send/receive a DO shall be monitored.
	11	All actions to write/read a DO shall be monitored.
Authenticity	1.1 - 1.7	User involved in the execution are identified.
	4.1, 4.2, 4.4, 4.5	Genuineness of information in data object shall be verified.
	4.3	Identity of data store users shall be verified.
	8,9	Identify of participant shall be verified before the execution of the business process.
Availability	1.1-1.7	The task shall be executed every time is requested by the BP.
	2	The sub process shall be executed (completed) every time is requested by the business process.
	4.1, 4.2, 4.4, 4.5	The data object shall be available to authorized users every time is requested by the business process.
	4.3	The data store shall be available every time is requested by the business process.
	10, 11	The communication channel shall be available as specified in the security properties of the security annotation.
Confidentiality	4.1, 4.2, 4.4, 4.5	Authorized users can read/write the data object.
	4.3	Authorized users can access the data storage.
	10	Only authorized users can send/receive data.
Integrity	1.1-1.3, 1.5, 4.3	The functionalities f the tasks shall be protected from intentional corruption.
	1.4,1.7	The functionalities f the tasks shall be protected from intentional corruption.
	1.6	The functionalities of the tasks shall be protected from intentional corruption.
	4.1, 4.2,	The data object shall be protected from intentional corruption.

	4.4, 4.5	
	10	The messages shall be protected from intentional corruption.
Non-repudiation	1.1-1.7	The (not) execution of the task shall be provable.
	3	The call to a global task shall be provable.
	5.2, 5.4, 5.6, 5.7, 5.10	The (not) throw/wait of an event shall be provable.
	10, 11	The (not) usage of a message flow shall be provable.
	11	The (not) usage of a data object shall be provable.
Privacy	1.1, 1.4-1.7, 4.3	Task shall be compliant with privacy legislation, data owners shall be able to control the data.
	1.2, 1.3, 5.2	Immediately before the sent (after the reception), the data shall be anonymized.
	4.1, 4.2, 4.4, 4.5	The data objects shall be handled according with privacy legislation.
Bind of duty	([8|9], [8|9])	Two participants shall be the same physical person.
Separation of duty	([8|9], [8|9])	Two participants shall be two different people.
Non-delegation	1.1-1.7, 2, 3	The participant specified in the swim lane shall execute all the actions required to execute a task.

Table 2: Semantic of security annotations in SecBPMN2 process and collaboration models

SecBPMN2 - Choreography

Table 3 shows the semantic of the security annotations in the SecBPMN2 choreography model. In this case the target contains the name of the BPMN 2.0 elements. The "X" symbol is used to mark security annotations that cannot be used in SecBPMN2 choreography models.

Security concept	**Target**	**Semantic**
Accountability	X	X
Auditability	Participant	The participant shall monitor the conversation.
Authenticity	Message	The message exchanged shall be genuine.
	MEP (Message exchange patterns)	All the messages exchanged shall be genuine, i.e., trust the information in the message.
Availability	Message	The message shall be send/received every time is requested by the business process.
	MEP	The conversation shall take place every time is requested by the business process.
Confidentiality	MEP	Only the users specified in the MEP shall send/receive messages.
Integrity	MEP	The messages exchanged shall be protected from intentional corruption.
Non-repudiation	MEP	Each user involved shall not repudiate the set of interactions.
Privacy	X	X

Bind of duty	Participant, Participant	The two participants (of different MEP) shall be the same person.
Separation of duty	Participant, Participant	The two participants shall not be the same person.
Non-delegation	MEP	The participants specified in the MEP shall execute all the actions required for the interactions.

Table 3: Semantic of security annotations in SecBPMN2 choreography models

SecBPMN2.0-Q

Table 4 shows the semantic of the relations used in SecBPMN2-Q. Source and targets columns specify the source and the destination allowed for the relations.

BPMN-Q relations	Source	Target	Semantic
Path	1.1-1.8, 2, 3, 5	1.1-1.8, 2, 3, 5	The target must be executed after the source.
Negative path	1.1-1.8, 2, 3, 5	1.1-1.8, 2, 3, 5	The target must never be executed after the source.
Negative flow	1.1-1.8, 2, 3, 5	1.1-1.8, 2, 3, 5	The target must not be executed immediately after the source.

Table 4: Semantic of SECPMN2-Q relations

Bibliography

1. Simon, Richard T., and Mary Ellen Zurko. "Separation of duty in role-based environments." Computer Security Foundations Workshop, 1997. Proceedings., 10th. IEEE, 1997.
2. Jacques Wainer, Paulo Barthelmess, and Akhil Kumar. W-rbac - a workflow security model incorporating controlled overriding of constraints. Int. J. Cooperative Inf. Syst., 12(4):455–485, 2003.