Eliciting Security Requirements from the Business Processes Using Security Risk-oriented Patterns

Nutzung risk-basierter Muster zur Erhebung von Sicherheitsanforderungen in Geschäftsprozessen

Raimundas Matulevičius*, Naved Ahmed, Institute of Computer Science, Tartu, Estonia

* Correspondence author: rma@ut.ee

Summary Although importance of aligning modelling of business processes and security is growing, there is rather limited research performed on elicitation of security requirements from the business processes. In this paper we discuss how security risk-oriented patterns could help solving the above problem. Using the illustrative example, we present a two-step method for (i) pattern occurrence discovery in, and (ii) for security requirements definition from the business process model. We hope that our proposal could help elicit security requirements at the early system development stages, however, we still need to validate it empirically.

Keywords ACM CSS → Security and privacy → Formal methods and theory of security → Security requirements; ACM CCS → Applied computing → Enterprise computing → Business process management

1 Introduction Business process modelling (BPM) deals with presenting enterprise activities so that they would be analysed and improved. Security engineering is concerned with lowering the risk of intentional unauthorised harm to valuable assets to level that is acceptable to the system’s stakeholders by preventing and reacting to malicious harm, misuse, threats and security risks [8]. Assuming that business analysts concentrate on improving the business performance, early security analysis could discover and discard system design alternatives that do not offer sufficient security levels. Although the importance of aligning the business process modelling and security engineering is growing [1], there is rather limited attempt [9; 13] to understand how security requirements could be elicited from the business processes. To address this problem, in this paper we propose to use the security risk-oriented patterns (SRPs) [2]. The application of the patterns includes two subsequent steps as illustrated in Fig. 1 (the remaining of the paper is basically structured along the steps and artefacts of the SRP application). We discuss the illustrative example of the order management process to show (i) how the SRP occurrences are identified and, then, (ii) how the security requirements are elicited.
2 Security Risk-oriented Patterns

According to Schumacher et al. “a security pattern describes a particular recurring security problem that arises in a specific security context and presents a well-proven generic scheme for a security solution” [14]. Following this definition, in [2] we have developed a set of SRPs for the business process models. The patterns are based on understanding security risks (i.e., recurring security problems) that arise within business processes (i.e., specific security context). To mitigate the risks, the patterns recommend security requirements (i.e., security solution).

Following the domain model [5] for the information systems security risk management, each SRP includes concerns – on asset, risks, and risk treatment.

Example. In Fig. 2 we illustrate an asset model (expressed using BPMN) of SRP for securing confidential data using access control models. Here a client requests data, which are retrieved (and potentially provided back to him or her). Here the data are considered as the business asset which needs to be confidential (i.e., disclosed from the unauthorised individuals, entities or processes). The confidentiality concern (noted as C) is expressed using the lock visual symbol situated on the protected asset. The business assets (e.g., data) are supported by the IS assets – in this pattern corresponding to the retrieval interface and its tasks request data and retrieve data. The security risk threat arises if the retrieval of the confidential data is allowed to the user (independently whether s/he is malicious or not) without checking his or her access permissions to the data. The risk event would (i) negate confidentiality of the data, (ii) lead to the data discloser (and provoke the unintended data use), and (iii) harm the retrieval (and potentially storage) interface (by questioning its reliability).

To reduce the risk, the check for the data access rights should be implemented. In Sect. 5 we will illustrate how security requirements regarding the role-based access control (RBAC) model are elicited from the business model. One should also note that other access control models (e.g., guarded access [10]) could be an alternative solution to the RBAC model. A process of selecting between different security models potentially would result in the security requirements prioritisation based on the risk...
reduction level, security requirements cost or return on security investment.

3 Business Process Model

The current set of SRPs [2] is specifically developed for the business processes expressed in BPMN. To illustrate our approach in this section we present the extract of the order management process.

Example. In Fig. 3 we depict a situation where three different roles, i.e., (i) Order manager, (ii) Sales manager (both played by a human), and (iii) Tracking system (played by a software system) – monitor and control the information (i.e., Order) managed using the Order management system. Here Order is not explicitly stated in the example, however, it could be characterised by three different attributes – OrderID, Item list and Order status.

The order preparation is managed by the selection of the business process (see task Select business process). Order manager may have multiple request from the Order management system, thus, depending on the selected process, Order goes through three stages: (i) order is initialised (see event Order initiated); (ii) invoice is received (see event Invoice received); and validation report is prepared (see event Validation report received). The process finishes with linking it to the delivery service. Different stages of the order management require that the Order manager executes different business processes using the Order management system. For instance, after the Order manager requests for the orderID, which is pre-allocated by the sales manager (see task Pre-allocate orderID). The status of the new order is recorded by the Tracking system, which sets its value to “allocated”. The ID of newly initiated order is sent (see task Send OrderID) to both the Sales manager and Order manager.

Similarly, the Order manager could initiate the processes for the identification of the Order items (see task Extract item list) and for the validation of the order status (see Validate order status). In both situations, the Sales manager and Tracking system need to manipulate the Order attributes Order ID, Item list or Order status.

4 Pattern Occurrences

As discussed in [3], pattern occurrences could be found using methods of (i) model granularity matching, (ii) business perspective matching, (iii) structural similarity, and (iv) semantic similarity. In this paper we will not discuss the pattern identification, but will concentrate on the second step (see Sect. 5), which results in the security requirements model. But as the example, we will show...
the occurrences of the SRP for securing confidential data using access control (see Sect. 2), which are found in the business process model.

**Example.** There are three occurrences of the SRP for securing confidential data using access control in the order management process model (see Fig. 3). The first match is with respect to the OrderID, specifically:
1. The data object OrderID corresponds to the SRP data;
2. The task Pre-allocate orderID matches to the SRP task Request data; correspondingly, the task Send orderID aligns to the SRP task Retrieve data;
3. The swimlanes Sales manager and Order management system correspond accordingly to the SRP swimlanes Client and Retrieve interface.

The second SRP occurrence is regarding the data object Item list and task Extract item list (see Fig. 3). Finally, the third one is with respect to the data object Order status and task Validate order status.

After identifying the pattern occurrences one could define the early security requirement¹ as the necessity to check for the access permissions in the order management system. How this (early) requirement is refined to the late security requirement we discuss in Sect. 5.

5 Security Requirements Elicitation

The single aspect of the security requirements is, typically, not addressed in the “single place” of the developed system, but it rather cross-cuts through the overall system. In the following discussion we will illustrate how the early requirement for the necessity to check for the access permissions in the order management system is refined to the RBAC security model, presented in Fig. 4. But first we will present the major principles of the RBAC model [7].

**Role-based access control.** The main RBAC concepts are Users, Roles, Objects, Operations, and Permissions. A User is typically defined as a human being or a software agent. A Role is a job function within the context of an organisation. In Fig. 4, roles, like OrderManager, SalesManager, and TrackingSystem, are modelled using the secuml.role stereotype.

Permissions are approvals to perform one or more Operations on one or more protected Objects. An Object is
a protected system resource (or a set of resources). Figure 4 contains one protected object, namely Order, which carries the secuml:resource stereotype. An Operation is an executable sequence of actions that can be initiated by the system entities; thus the Order operations, like preAlocateOrderID, sendOrderID, extractItemList and others, are the one, on which the permissions are defined.

There are two major RBAC relationships – User assignment and Permission assignment. User assignment relationship describes how users are assigned to their roles. Permission assignment characterises the set of privileges assigned to a Role. For instance, in Fig. 4 there are three permission assignments (see classes with the secuml:permission stereotype) defined between the roles (i.e., OrderManager, SalesManager, and TrackingSystem) and the protected object (i.e., Order). OrderManagerPermissions, SalesManagerPermissions, and TrackingSystemPermissions specify the security actions – namely, create, read, and update – that the role can perform over the object state, characterised by the attribute values of this protected object.

Defining security model. In the case of our analysed SRP, the RBAC security model (i.e., Fig. 4) is defined from the business process model (Fig. 3). We have performed the following steps:

1. The secure resource is elicited from the context of the business process. In our example the considered problem is order management. Thus, we define Order as the protected resource.
2. Application of the SRP (see Sect. 4) has resulted in the need to secure Order using access control. Since the values of OrderID, Item list, and Order status (considered as business assets during the SRP application) describe the state of the Order, they are defined as the attributes of the protected object (i.e., Order).
3. Each BPMN swimlane linked to the one where the SRP is identified is considered as the (potential) role.
4. In our example the elicited roles are Order manager, Sales manager, and Tracking system.
5. All the tasks that have an in/out-going data flow with the data (object) identified as the SRP business assets, are considered as secured operations. Thus they are situated as operations within the protected object.
6. In our example, regarding the occurrence of the OrderID, three tasks are elicited: (i) Pre-allocate orderID (identifies security permission to Sales manager), (ii) Send orderID (introduces security permission to Sales manager and Order manager), and (iii) Search orderID (identifies security permission to the Tracking system).
7. In the final step, one need to define the security action types. This depends on the context given in the business process model and, more specifically, on the relationships between the identified role swimlanes and tasks where protected object attributes are used. We have observed that the direction of the data flow has no influence on the definition of the security action type, so each case needs to be considered by the developer separately. In our example, with respect to the permission on the OrderID, we define that Order manager should be able to read (see Fig. 4, orderInitialized: READ), Sales manager – create (see Fig. 4, requestOrderID: CREATE) and read (registerOrderID: READ), and Tracking system – read (see Fig. 4, getOrderID: READ) the OrderID.

To finalise, the following security requirements are defined regarding the Order access (see Fig. 4).

- SecReq: 1 OrderID should be checked for access permission.
  - SecReq.1.1: SalesManager should be able to create the OrderID;
  - SecReq.1.2: OrderManager and TrackingSystem should be able to read the OrderID.
- SecReq: 2 ItemList should be checked for access permission.
  - SecReq.2.1: SalesManager should be able to create the ItemList;
  - SecReq.2.2: OrderManager and SalesManager should be able to read the ItemList;
  - SecReq.2.3: SalesManager should be able to update the ItemList.
- SecReq: 3 OrderStatus should be checked for access permission.
  - SecReq.3.1: TrackingSystem should be able to update the OrderStatus;
  - SecReq.3.2: TrackingSystem and OrderManager should be able to read the OrderStatus.

6 Discussion

In [11] Hung and Karlapalam define a model using multi-level state machine to address workflow security at three levels: workflow, control and data. In the workflow each task is associated with the required data objects needed and their order in which the objects should be accessed. The data level enforces the rules associated with access to the data objects. The problem with their model is that it limits the task execution and data accessibility. Similarly, it lacks the role concept that makes it difficult to change the role and their association [6]. In [9], authors propose an extended access control model to support the assignment of task delegation. They define the workflow authorisation constraints that authorises users to perform tasks and present a formal security model to support the authorisation requirements in workflow. The focus is on the tasks requirements to analyse and specify security constraints while accessing the workflows data. In our approach we identify data as a business asset i.e., resource and can specify the actions that tasks can perform on the attributes of the data that allows defining the security constraint in more detail. Furthermore, several approaches (e.g., [4]) that use process mining to extract the access control policies from the process logs of information systems. These approaches are good candidate for
verifying the access controls after the information system is implemented but make it difficult to use in early and late requirement stages of information system development.

7 Conclusion

In this paper we discuss how security requirements could be elicited from the business process models using SRPs [2]. More specifically, we present the application of the SRP for securing confidential data using access control models in the illustrative example.

The main observation of the study is that the SRP application is rather a semi-automated process. For instance, as discussed in [3], although it is possible to automate the search for pattern occurrences regarding the model granularity, business perspective, and structural similarity analysis, the semantic similarity analysis requires the developers involvement. Similarly, when eliciting the security model, some security concepts (e.g., RBAC roles, operations) could be captured automatically, however, other (e.g., RBAC security actions) needs to be defined manually.

Here we have reported only on one application of one SRP. But we have observed that the same steps are performed when applying other SRPs (e.g. for securing the transmitted data between business entities [2]).

The SBP application could potentially help developers to capture security requirements earlier in the system development stages. Our next step is to conduct an empirical study in order to understand how the SRPs could scope with the large/industrial business process models.

We also expect that such a study will help us to enhance the SRP set with new patterns.

References


Received: 2013

Dr. Raimundas Matulevičius

Address: Institute of Computer Science, J. Liivi 2, 50409 Tartu, Estonia, e-mail: rma@ut.ee

Naved Ahmed

Address: Institute of Computer Science, J. Liivi 2, 50409 Tartu, Estonia, e-mail: naved@ut.ee
Please add a short curriculum vitae.