# INFORMATION SYSTEMS SECURITY BASED ON BUSINESS PROCESS MODELING

Joseph Barjis
*Delft University of Technology, Jaffalaan 5, 2628 BX Delft, The Netherlands*

Keywords: Secure business process modeling, Secure information system design, Information system security, Organizational semiotics, DEMO methodology.

Abstract: In this paper, we propose a conceptual model and develop a method for secure business process modeling towards information systems (IS) security. The emphasis of the proposed method is on social characteristics of systems, which is furnished through association of each social actor to their authorities, responsibilities and obligations. In turn, such an approach leads to secure information systems. The resulting modeling approach is a multi-method for developing secure business process models (secure BPM), where the DEMO transaction concept are used for business process modeling, and the Norm Analysis Method (organizational semiotics) for incorporating security safeguards into the model.

## 1 INTRODUCTION

Traditionally, security measures have been considered a technical issue to be dealt with when the system architecture, hardware performance, databases and software design are tackled (Backhouse & Dhillon, 1996), and mainly addressed in the implementation (coding, programming) phase of the life cycle. But the fact is that security is more of organizational issues and should be developed as early in the IT application life cycle as in the business modeling phase (Backes et al., 2003; Mana et al., 2003; Herrman & Herrman, 2006). The motivation for this is obvious. Information systems are developed to enable certain business processes within an enterprise context. Thus, security measures should be applied while IS design is in its early stages in the life cycle such as the process modeling phase, where business analysts and security experts have to identify security safeguards and implement them in the business process models.

Business processes are the starting point for any system development process (e.g., IS projects, IT applications, software design). Practitioners of software development project refer to a business process as a software system blueprint (Nagaratnam et al., 2005). As such, business processes are a natural phase in the application development life cycle, where security safeguards should conceive.

## 2 RELATED WORK

Information security and secure business process modeling attracted many researchers. There have been some research works done in this regard, where authors address the need for sliding security aspects down the system design ladder to business process modeling phase (Mana et al., 2003; Backes et al., 2003; Herrmann & Herrmann, 2006; Rodríguez et al., 2007). This paper further advances the study of security driven business process modeling by introducing an innovative method and approach, and proposes a conceptual model for secure BPM.

Incorporation of security safeguards in business process modeling greatly increases the likelihood of an adequate and secure system development. Research and practical findings at IBM, reported in (Nagaratnam et al., 2005), argue that business process modeling is an ideal time in the life cycle of software system development to begin capturing the business security requirements that address any security concerns that relate to the business.

The existing approaches to secure business process modeling are predominantly based on the extension of existing modeling notations and methodologies with security tags and properties. One of the earliest works tackling security issues of information system using existing methodologies is (Backhouse & Dhillon, 1996). In this work the authors propose a concept for using the notions of

Barjis J. (2009).
INFORMATION SYSTEMS SECURITY BASED ON BUSINESS PROCESS MODELING.
In *Proceedings of the 11th International Conference on Enterprise Information Systems - Information Systems Analysis and Specification*, pages 213-218
DOI: 10.5220/0002006502130218

authorities and responsibility in order to ensure that activities are carried out by the authorized actors.

The approach and method used in (Firesmith, 2003) is based on the extension of UML. In particular, the author proposes a method to derive security use cases in order to model a problem domain for secure application development. Actually, due to its popularity as a requirements elicitation method, the security use case approach has been researched and developed by many researchers.

Another popular and widely used modeling language and method extended with security properties is BPMN (business process modeling notation). In (Rodríguez et al., 2007), the authors integrate security requirements through business process modeling. In particular, they propose a BPMN extension to business process diagrams.

One of the dominant reasons that the role of business process modeling in IS security is undermined is because often the methods restrict themselves to merely the conceptual and semantic levels and, therefore, present little pragmatic value for information system designers and developers. By using the existing methods, it is difficult to automatically analyze the models and, therefore, it is not possible to test and simulate the embedded security measures. To elevate the importance and pragmatic value of security-driven business process modeling, it is required that the models possess certain qualities. First of all, the resultant model should be amenable to test and simulation in order to capture how and when security safeguards will be triggered and enacted. Secondly, the models should capture social roles, authorities and responsibilities pertaining to each action. Thirdly, it is imperative that the models capture interactions between different entities (human actors, business units, applications) to identify the level of security sensitivity (e.g., access and modification of sensitive data or inter-organizational transactions may be of special security scrutiny). These qualities are the research motivations and drivers for this paper. In this paper, it is attempted to show that the proposed method and approach for developing secure business processes yield the mentioned qualities to a certain extent and advances the existing experience from both a theoretical and an application perspective.

The contribution of this paper is the proposal of a conceptual model for developing secure business processes, an approach to implement the conceptual model, and a secure business process modeling method. The advantage of the proposed method is its underlying formal semantics, which allows models to be automatically analyzed and simulated. In the proposed approach, emphasis is made on the social characteristics of the system by associating each social actor to their authorities, responsibilities and obligations. In this paper we use the DEMO methodology transaction concept (Dietz, 2006) for business process modeling, and the Norm Analysis Method (Stamper, 1994) for incorporating security safeguards into the model.

# 3 CONCEPTUAL MODEL

The proposed conceptual model for secure BPM, illustrated in Figure 1, has two main components that need to be developed and combined to create a secure business process model. The first component consists of the 'business transactions' that needs to be identified based on a 'business processes description'. The second component is 'security safeguards' that are mainly defined based on security determiners (see below for definition) and represents a set of security safeguards that are defined in conjunction with each business transaction. These two components are developed in a collaborative manner (see Figure 2) and in correlation with each other. Together, the two components create a secure BPM, as depicted in Figure 1 and enclosed into the dashed-line rectangle.

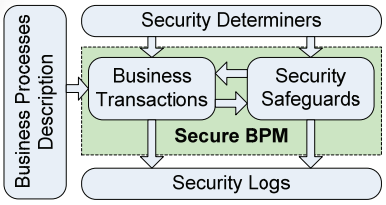


Figure 1: Conceptual model of security embedded BPM.

*Security determiners* – these are rules, procedures, laws, and other measures that an organization wants to be implemented with regard to certain activities, processes, and roles.

For example: The 'security determiners' define if a transaction execution involves any action on sensitive personal records (read, delete, modify), or whether a transaction is executed in the boundary of two organizations requiring more security (transmitting credit card information, health care records), and so on. For each such transaction, security rules, security precautions, and security alerts are formulated at the concept level.

Once security safeguards are defined, business transactions are coupled with their corresponding

security safeguards and every time a transaction is initiated it will trigger the security rules to be satisfied. Actually, security safeguards need not be implemented for each business transaction. In fact, analysts and designers are required to consider a trade-off between the level of security robustness and business processes performance.

There are two other components in the proposed conceptual model. The 'security logs' component contains records of all business transactions that carry security-sensitivity and trigger security safeguards. This component will allow monitoring and managing access and execution of sensitive transactions as well. The 'business processes description' can be found in the existing documentation or be prepared by the analysts where the underlying business processes are described. An example of such description will be presented later when the FHCC case is discussed.

The approach we propose to implement the above conceptual model is based on the collaboration of different expertise that allows developing a secure BPM in correlation with the components specified in Figure 1. The proposition is that for secure BPM, close collaboration of the three types of expertise should be considered crucial. This approach is illustrated through a secure BPM collaboration triangle in Figure 2. As depicted, in the collaboration triangle for secure BPM, the 'business analyst' role is emphasized as prominent and central. Essentially, for a successful secure BPM, it is important that although the business modeling phase is led by business analysts, it is carried out in collaboration with security experts and domain users. Each of these groups plays an essential role in developing secure models: the 'business analyst' leads the work; the 'domain users' provide domain knowledge to the analysts and security experts; 'security experts' support the business analysts identifying and incorporating security safeguards into the models. The outcome of these collaborative efforts is identification of the security safeguards at a high abstraction level. It is rather flagging security areas for more detailed and robust analysis and implementation as the analysis and design activities unfold.

For example: In developing secure BPM for a hospital, the business analyst (maybe also in collaboration with a security expert) determines which policies apply to a given activity in the context of the business process. The business analyst might model the requirement to control authorized access to a business activity such as medical records and to ensure that the medical information flow is protected from unauthorized access and ensures confidentiality. The medical security requirements can be defined within the secure BPM. These models rather provide a reference that may be used by the hospital compliance officers, such as security auditors, to verify and monitor adherence to the hospital security and confidentiality policies.

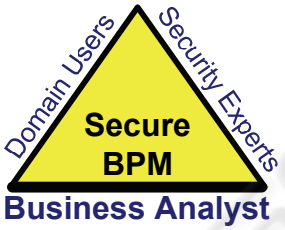


Figure 2: A secure BPM collaboration triangle.

Although the proposed conceptual model and approach is fairly specific and detailed security aspects are covered, this approach is still abstract enough not to limit the developers and security experts' freedom of implementation.

To summarize this section, it should be stated that in our approach, business processes are described in terms of business transactions, where each transaction entails interaction of actors (human actors), business units, and artifacts (IT applications). Depending on the sensitivity of the carried activities, transactions are complemented with security safeguards. Since interaction of components (actors, artifacts, agents) is the center-point of our approach, the DEMO business transaction concept (Dietz 2006) is used as a theoretical basis for identifying business activities. Next to the DEMO methodology, Petri nets are adopted for constructing the model diagrams. In fact, due to its formal semantics, models based on Petri net notations are formal and lend themselves to automatic analysis. Security safeguards are defined using the Norm Analysis Method of Organizational Semiotics (Stamper, 1994). The Norm Analysis Method is adapted to define rules, norms, authorities, responsibilities, and exceptions for the execution of each transaction. Both the DEMO Methodology and the Norm Analysis Method are discussed in the following sections.

## 4 BUSINESS TRANSACTION

According to the DEMO Methodology (Dietz, 2006), a business transaction is a generic pattern of action and interaction. An *action* is a *productive act*

and represents an activity that brings about a new result. An *interaction* is a *communicative act* involving two actor roles to coordinate and negotiate an action.

As depicted in Figure 3, the process in which a transaction is completely carried out consists of three phases:

- *Order phase (O)*, during which an actor makes a 'request' for a service or goods towards another actor. According to DEMO, this phase represents a number of communicative acts or interactions. This phase ends with a commitment ('promise') made by the second actor, who will deliver the requested service or good.

- *Execution phase (E)*, during which the second actor fulfills its commitment, i.e., 'produce' the service or goods. According to DEMO, this phase represents a productive act.

- *Result phase (R)*, during which the second actor does 'present' the first actor with the service or goods prepared. According to DEMO, this phase also represents a number of communicative acts or interactions. This phase ends with the 'accept' of the service or goods by the first actor.

In Figure 3, by arrows and circles, it is also illustrated that all 'request', 'promise', 'present', 'accept' acts can be logged in the model.

As it becomes obvious from the three phases, each business transaction is carried out by two actor roles. The actor role that initiates a transaction is called the 'initiator' (e.g., customer) and the actor role that executes the transaction is referred to as the 'executor' (e.g., supplier) of the transaction.

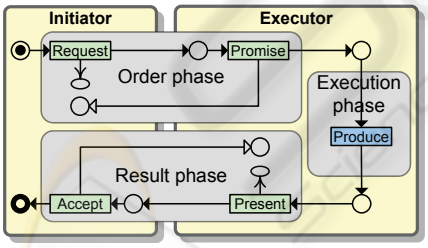


Figure 3: Business transaction pattern.

## 4.1 Illustrative Example

It should be noted that the case study discussed here is a simplified description of the processes in which some details are omitted and skipped. This description is based on a family health care center (FHCC), taken from (Barjis & Hall, 2007).

*In order to be examined by a doctor, a patient needs to make an appointment beforehand. On the appointment day, a nurse first conducts preliminary general checkup (blood pressure, EKG, basic lab work) and 'records' chief complaints, and reason for the visit. After completing this preliminary exam, the nurse escorts the patient to an available examination room. The doctor examines the patient and 'updates' the patients chart if any prescription is issued, diagnosis is made, referral is given, or if any other notes are taken. After completing the examination, the patient goes to the side-desk to check out, to make the (co-)payment relevant to the service delivered. In rare cases, patients may need further examination by external healthcare providers (sub-specialist) or advanced diagnostic equipment such as a CAT scan, available elsewhere.*

*In this case, the FHCC schedules an appointment with the external healthcare provider based on the availability of the network provider. Some procedures such as a CAT scan may require the insurance company's pre-approval.*

## 4.2 FHCC Business Transactions

Making an appointment is the first activity in the series of processes taking place in the "patient examination." By making an appointment, a new fact is created, being that a new appointment is made and recorded into the system. In this activity, the patient is the initiator and the receptionist is the executor. This activity comprises the first business transaction (T1) in the process of "patient examination." Thus, this and the other main activities are described as follows:

| | |
|---|---|
| **T1:** | making an appointment |
| **Initiator:** | patient |
| **Executor:** | FHCC (receptionist) |
| **Fact:** | a new appointment is made |

| | |
|---|---|
| **T2:** | requesting health care |
| **Initiator:** | patient |
| **Executor:** | FHCC (physician) |
| **Fact:** | patient is given health care |

Transaction 2 requires that the patient records will be accessed and modified by a physician. Therefore this transaction requires explicit access authorization to secure the patient's electronic records.

| | |
|---|---|
| **T3:** | conducting general physical test |
| **Initiator:** | FHCC (physician) |
| **Executor:** | FHCC (nurse) |
| **Fact:** | general physical test is conducted |

Similarly, Transaction 3 requires that the patient records will be accessed and new records will be added by a nurse. Therefore this transaction requires explicit access authorization to secure the patients electronic records.

| | |
|---|---|
| **T4:** | arranging an external appointment t |
| **Initiator:** | FHCC |
| **Executor:** | Specialist (external provider) |
| **Fact:** | an external appointment is made |

| | |
|---|---|
| **T5:** | requesting a pre-approval |
| **Initiator:** | Specialist |
| **Executor:** | Insurance |
| **Fact:** | a pre-approval is granted |

| | |
|---|---|
| **T6:** | paying the bill |
| **Initiator:** | FHCC |
| **Executor:** | patient |
| **Fact:** | the service is paid |

These business transactions constitute a network of actions and interactions through which the FHCC business processes emerge. Due to limited space, we skip the FHCC patient examination process. Instead, we would like to discuss a few points that relate this model to the research questions and objectives we identified in the beginning of the paper.

The resulting model using the transaction schema presented earlier can be automatically analyzed and simulated. However, the model would not include any security safeguards. Therefore, the DEMO transaction concept, as we discussed in the conceptual model, needs to be complemented by security safeguards, for which purpose we use the NAM of the organizational semiotics. To do so, we first introduce the NAM in the next section and then revisit the DEMO transaction diagram for security improvement.

# 5 NORM ANALYSIS METHOD

Organizational Semiotics is a framework and a set of methods based on the understanding of organizations as systems of social norms. It emphasizes the central role of the people, their responsibility and the organization in the analysis and design of information systems (IS) (Stamper, 1994). Organizational semiotics consists of a set of methods including the Norm Analysis Method discussed in this section.

In the previous section, we illustrated how business transactions can be identified and the relevant actors defined. The Norm Analysis Method is used as a suitable complement to deal with behavioral norms specification. According to the organizational semiotics framework, there are five types of norm that influence certain aspects of human behavior. They are 'perceptual norms', 'cognitive norms', 'evaluative norms', 'behavioral norms' and 'denotative norms' (Stamper, 1994).

In business, most rules and regulations fall into the category of behavioral norms. These norms prescribe what people must, may, and must not do, which are equivalent to three deontic operators "is obliged," "is permitted," and "is prohibited." Therefore, particular attention is given to the behavioral norms since they are expressed as business rules, and have direct impacts on business operations. Behavioral norms govern human behavior within regular patterns. The following format is considered suitable for specifying of behavioral norms – a generic structure for all norms:

| | |
|---|---|
| **whenever** | <condition> |
| **if** | <state> |
| **then** | <actor> |
| **is** | <deontic operator> |
| **to** | <action> |

In this structure, the condition describes the situation where the norm is to be applied, and sometimes further specified with a state-clause (this clause is optional). The actor-clause specifies the actor responsible for the action. The actor can be a staff member, a customer, or a computer system if the right of decision-making was delegated to it. As for the next clause, it is a deontic state and is usually expressed by one of the three operators - permitted, forbidden and obliged. For the next clause, it defines the consequence of the norm. The consequence possibly leads to an action or to the generation of information for others to act.

Now using the above format along with identified business transactions, we develop a secure model of business processes. We will use capital "S" for each security safeguard, where the number following it indicates the number of the corresponding transaction (e.g., S2 is definition of security safeguards associated with Transaction 2).

Here, using the norms, we will discuss security safeguards for only two business transactions: one for the physician role that requires 'update' of the patient medical records; one for the nurse role that requires 'record' of new data for each visit by the patient. Actually, in the same manner we can define security safeguards for all roles and transactions, but we will limit ourselves to only two transactions, in part due to space limitations.

| | |
|---|---|
| **S2:** | |
| **whenever** | <a physician examines a patient > |
| **if** | <the physician is the patient family doctor> |
| **then** | <the physician> |
| **is** | <permitted> |
| **to** | <update the patient medical records> |

| | |
|---|---|
| **S3a:** | |
| **whenever** | <a nurse records into the patient files> |
| **if** | <the nurse is authorized so> |
| **then** | <the nurse> |
| **is** | <obliged> |
| **to** | <sign the records with her e-signature> |

| | |
|---|---|
| **S3b:** | |
| **whenever** | <a nurse updates existing records> |
| **if** | <the record is created in the past > |
| **then** | <the nurse> |
| **is** | <is prohibited> |
| **to** | <make changes to existing records> |

All the safeguards can be diagrammatically incorporated into the complete model of the FHCC patient examination process. However, let us revisit the business transaction diagram (Figure 3) and show incorporation of security safeguards in more generic terms and how and where these security safeguards will be executed in a business transaction.

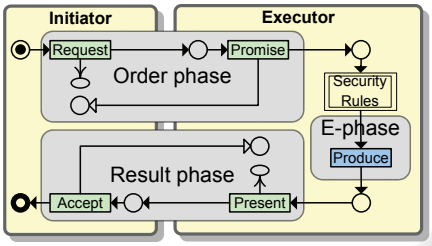


Figure 4: Business transaction with embedded security.

Figure 4 represents a generic form of business transaction with an added feature modeled as 'secure'. The secure box is basically implementation of the security safeguards (i.e., the aforementioned rules) defined for each transaction. As seen from the diagram, it will be triggered before an actor is allowed to perform or execute any action. In the FHCC case, such a box will be implementation of S2 before Transaction 2 is executed or implementation of S3a and S3b before Transaction 3 is executed.

# 6 CONCLUSIONS

In this paper we have discussed security driven business process modeling method that allows constructing models based on the DEMO transaction concept using formal graphical notations of Petri nets. The security safeguards embedded in the model are developed using the Norm Analysis Method of organizational semiotics. Although due to space constraints, the complete business process model of FHCC and simulation are skipped in this paper, the resultant models can be simulated in order to observe how the security safeguards are called and executed to ensure authorized access before security sensitive actions are executed. For example, if a nurse wants to modify existing medical records, this action will trigger a security measure that the nurse should be able to comply with. This security measure can be another level of access. An advantage of the proposed method is that the models can be simulated and dynamically tested in regard to security safeguards. As each secure transaction is executed, the corresponding security safeguard is deployed generating security logs for future analysis.

# REFERENCES

Backes, M., Pfitzmann, B., & Waidner, M. (2003). Security in Business Process Engineering. In Proceedings of 2003 International Conference on Business Process Management. Lecture Notes in Computer Science vol. 2678, Springer.

Backhouse, J., & Dhillon, G. (1996). Structures of responsibility and security of information systems. European Journal of Information Systems, 5, 2–9.

Barjis, J., & Hall, M. (2007). A Healthcare Center Simulation Using Arena. In the proceedings of MSVVEIS'07", June 12-13, Funchal, Madeira – Portugal.

Dietz, J.L.G. (2006). Enterprise Ontology –Theory and Methodology. Springer.

Firesmith, D. (2003). Security Use Case. Journal of Object Technology, Vol. 2 (3), pp. 53-64.

Herrmann, P., & Herrmann, G. (2006). Security requirement analysis of business processes. Electronic Commerce Research, Vol. 6 (3-4), pp. 305-335.

Mana, A., Montenegro, J.A., Rudolph, C., & Vivas, J.L. (2003). A business process-driven approach to security engineering. Proceedings of the 14th International Workshop on Database and Expert Systems Applications, pp. 477-481, Prague.

Nagaratnam, N., Nadalin, A., Hondo, M., McIntosh, M., & Austel, P. (2005). Business-driven application security: From modeling to managing secure applications. IBM Systems Journal, Vol. 44, No 4.

Rodríguez, A., Fernández-Medina, E., Piattini, M. (2007). A BPMN Extension for the Modeling of Security Requirements in Business Processes. IEICE - Transactions on Information and Systems, Volume E90-D, Issue 4, Pages: 745-752.

Stamper, R. K. (1994). Social Norms in Requirement Analysis – an outline of MEASUR. In Jirotka, M., & Gorguen, J. (Eds.) Requirements Engineering: Social and Technical Issues.