A BPMN BASED SECURE WORKFLOW MODEL

Li Peng
Software School, Hunan University, Changsha, Hunan, China

Keywords: Secure Workflow, Authorization, BPMN, Secure Workflow Model.

Abstract: Secure workflow has become an important topic in both academia and industry. A secure workflow model can be used to analyze workflow systems according to specific security policies. This model is needed to allow controlled access of data objects, secure execution of tasks, and efficient management and administration of security. In this paper, I propose a BPMN-based secure workflow model to manage specific processes such as authorizations in executing tasks and accessing documents. The secure workflow model is constructed using BPMN-elements. The model is hierarchical and describes a secure workflow system at workflow layer, task layer and data layer. This model ensures the security properties of workflows: integrity, authorization and availability. Moreover, the model is easily readable and understandable.

1 INTRODUCTION

Secure workflow has become an important topic in both academia and industry. A secure workflow model can be used to analyze workflow systems according to specific security policies. Since workflows are managed and executed in a secure way, the secure workflow model is needed to allow controlled access of data objects, secure execution of tasks, and efficient management and administration of security (Joshi et al. 2001, Kang et al. 2001, Thuraisingham et al., 2001).

The main security objectives of workflows involve integrity, authorization and availability. Integrity prevents the unauthorized modification of information. In a workflow, authorization means that no data or resource is accessed by unauthorized agents at anytime. Moreover, availability implies that a resource should be available when it is needed.

In order to ensure these three security properties of workflows, the secure workflow model should be able to monitor the assignment of task(s) and data to the agent(s). Thus, the model should describe when and what task to be granted to the agent(s) and to be revoked from the agent(s), as well as when and what data and privilege(s) to be granted to the agent(s) and also to be revoked from the agent(s) for executing a task.

Most of the work done in the workflow research area is concentrated on the infrastructure of WFMSs (Workflow Management Systems) and transaction management in workflow execution. The formal models for secure workflows were developed based on Petri nets or state machine, such as the Workflow Authorization Model (WAM) (Atluri & Huang 1996, Atluri et al. 1997) and the multi-layered state machine (Hung & Karlapalem, 2003). They are either too complicated or not sufficient to describe all aspects of a secure workflow. Since the BPMN (Business Process Modelling Notation) is a standard for modelling business process flows and workflows from the aspects of event, task, agent and data, in addition, the BPMN is a graphic notation and is easily readable and understandable for all business users, I choose BPMN as the basic model for the secure workflows.

In this paper, I propose a BPMN based secure workflow model to manage specific processes such as authorizations in executing tasks and accessing documents. In the rest of the paper, section 2 describes the related work, section 3 presents the secure workflow model and section 4 concludes the paper with a summary of the contributions of this research.

2 RELATED WORK

There has been much research on secure workflows. The Workflow Management Coalition (WfMC) summarizes a number of security services (WfMC,

Peng L. (2009).
A BPMN BASED SECURE WORKFLOW MODEL.
In *Proceedings of the 11th International Conference on Enterprise Information Systems - Information Systems Analysis and Specification*, pages 268-272
DOI: 10.5220/0002015702680272

2001) for a conceptual workflow model including authentication, authorization, access control, data integrity, security management and administration. Further, WfMC proposes an inter-operability protocol to support workflow services. However, WfMC does not consider the flow of authorizations among parties, tasks and resources during the workflow execution.

Discretionary Access Control (DAC) (Pernul, 1992) is used to control the access privileges from subjects to objects. DAC defines what kind of access a subject has to an object, and a set of predicates to represent access rules such as read, write, delete, create and copy. DAC only applies to control of system-oriented resources like database, file system, etc. Moreover, DAC cannot handle *when* to grant/revoke the access rights of the object to/from the subjects in this case.

The Workflow Authorization Model (WAM) (Atluri & Huang, 1996, Atluri et al., 1997) presents a conceptual, logical and execution model which concentrates on the enforcement of authorization flow in task dependency and transaction processing by using Petri Nets (PN). WAM defines the static parameters of the authorization using an Authorization Template (AT) during the build-time of the workflow. Further, WAM extends the PN model by proposing a multilevel secure workflow transaction model which is based on colored and timed PNs. The resulting PN is complex and special algorithms are needed for its construction. Though WAM discusses the synchronization of authorization flow with the workflow and specification of temporal constraints in a static approach, it is not sufficient to support workflow security. WAM grants all the authorizations to an agent once the task starts execution and it revokes all the authorizations from an agent once the task is completed, but it does not monitor the event(s) during the execution of task. WAM handles the security property of *Authorization* and MLS handles the security property of *Integrity* in the task dependencies, but they do not handle the security property of *Availability*(Hung & Karlapalem, 2003).

Hung & Karlapalem (Hung & Karlapalem, 2003) developed a secure workflow model using a multi-layered state machine to manage and monitor the flow of authorizations at different layers for a secure workflow execution. There are three layers in a secure workflow: *workflow*, *control* and *data*. A multi-layered state machine describes a system in different layers and each layer is an abstract mathematical state machine with a set of transition functions. The interaction between two mathematical state machines at different layers is triggered by an event. Further, they described a set of authorization functions to support the state machine. In this model, sets of state variables, functions and algorithms are defined. The model is complicated.

A secure workflow model should ensure the security properties of integrity, authorization and availability. Moreover, it should be easily readable and understandable. In this paper, I propose a secure workflow model, which describes a secure workflow from the aspects of task, agent, event and data.

3 SECURE WORKFLOW MODEL

Security is an essential and integral part of workflows. A secure workflow model should not only be able to manage and execute workflows effectively, but also satisfy the security requirements.

3.1 Basic Concepts in Secure Workflow Model

Workflow systems are software applications which automate and streamline business processes. The main elements of a workflow specification are: tasks, control flow, subject, data items and data flow. Formally, a workflow (W) is represented as a partially ordered set of tasks (T) that is coordinated by a set of events (E). The order of task execution is orchestrated by matching the input and output event(s) of each task. An event can be either a data event or control event. Each task represents a piece of work that needs to be done by an agent (A). Further, a set of documents (D) need to be processed by an agent during the task execution.

A secure workflow is a computer supported business process that is capable to against security threats and further satisfies the security requirements defined by the workflow modeller (Hung & Karlapalem, 2003).

In a secure workflow, a set of authorizations is needed for executing tasks and accessing documents. A secure workflow model needs to grant the agent the authorization(s) to execute a task(s) or to revoke the task from the assigned agent based on the occurrence of a certain event(s). Furthermore, an agent needs to get certain access privileges (PR) (e.g., “read”, “write” and “read-write”) to a set of documents (D) during the task execution. In other words, the secure workflow model needs to grant the document access privilege to the agent or to revoke the document access privilege from the agent.

Therefore, the following entities are included in a secure workflow: sets of tasks (T), events (E), agents (A), documents (D) and privileges (PR), where

- T = {t_1, t_2, …, t_m},
- E = {e_1, e_2, …, e_t},
- A = {a_1, a_2, …, a_n},
- D = {d_1, d_2, …, d_p},
- PR = {pr_1, pr_2, …, pr_q}.

In addition, a set of timestamps (TIME) are used to give the current discrete time, where

- TIME = {$time_1$, $time_2$, …, $time_s$}.

A secure workflow model can assign tasks (T) to agents (A) and give agents (A) certain document access privileges (PR). The authorization events for task assignment and for document access privileges are the following:

- grant(t, a, time), $t \in T$, $a \in A$, $time \in TIME$.
- revoke(t, a, time), $t \in T$, $a \in A$, $time \in TIME$.
- grant(d, pr, time), $d \in D$, $pr \in PR$, $time \in TIME$.
- revoke(d, pr, time), $d \in D$, $pr \in PR$, $time \in TIME$.

In a secure workflow, an agent can only execute the assigned task if and only if the privilege "execute" is granted. The secure workflow has to revoke the privilege from an agent if the task has completed execution or the time limit is exceeded. Further, an agent can only access a document with a specific privilege if and only if the document access privilege is granted to the agent and also it is needed to access the document with the privilege during the task execution. The secure workflow has to revoke the document access privilege from an agent if the document access privilege is no longer needed.

3.2 Overview of the BPMN

The Business Process Modelling Notation (BPMN) (BPMI.org & OMG, 2006) is a graph-oriented language for executable business processes. The BPMN model consists of four basic categories of elements: Flow Objects, Connecting Objects, Swimlanes and Artefacts. Events, Activities and Gateways are three Flow Objects and also the main graphical elements to define the behavior of a business process. Sequence Flow, Message Flow and Association are Connecting Objects which connect the Flow Objects to each other or other information. In the BPMN, there are two ways of grouping the primary modeling elements through "Swimlanes": Pools and Lanes. Moreover, Artefacts, such as Data Object, Group and Annotation are used to provide additional information about the process.

An event is something that "happens" during the course of a business process. There are three types of events, based on when they affect the flow: Start, Intermediate, and End. A Timer event indicates a specific time-date being reached.

An activity is a generic term for work that company performs. An activity can be atomic or compound. The types of activities that are a part of a process model are: Process, Sub-Process, and Task.

A Gateway is used to control the divergence and convergence of sequence flow. Thus, it will determine branching, forking, merging, and joining of paths. A Pool represents a participant in a process.

3.3 The Hierarchical Secure Workflow Model

The secure workflow model can be constructed by using BPMN elements. In a workflow system, tasks, events, agents and documents are represented by BPMN-elements Tasks, Events, Pools and Data Objects, respectively. The authorization events are represented by Timer Events.

In particular, the secure workflow model is hierarchical and constructed by using "Expand Sub-Process". An "Expand Sub-Process" means that the boundary of the sub-process is expanded and the details of the process are visible within its boundary. In this model, an authorization process is described at different layers: workflow layer, task layer and data layer. The details of a process at workflow layer are described at task layer by using an "Expand Sub-Process". Similarly, the details of a process at task layer are described at data layer.

3.3.1 Workflow Layer

At workflow layer, a workflow consists of a set of sub-processes that is interconnected by events. These sub-processes are executed by a set of agents. In this model, a sub-process can be an authorization process for executing a task. Figure 1 shows a secure workflow model at workflow layer, AP1 and AP2 are two authorization processes for executing task1 and task2, respectively, w represents workflow.

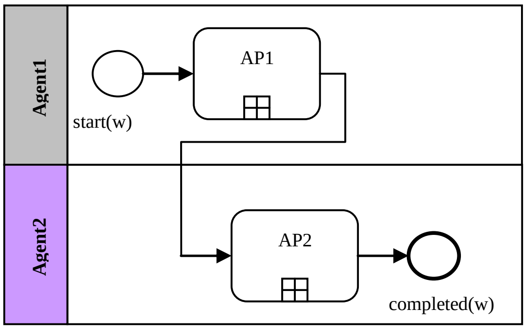

Figure 1: Workflow layer.

3.3.2 Task Layer

At task layer, the authorization process for executing a task is described in detail by using an Expand Sub-Process. Timer events trigger to grant or revoke the execution. The authorization process for executing task1 is as an example in Figure illustrated.

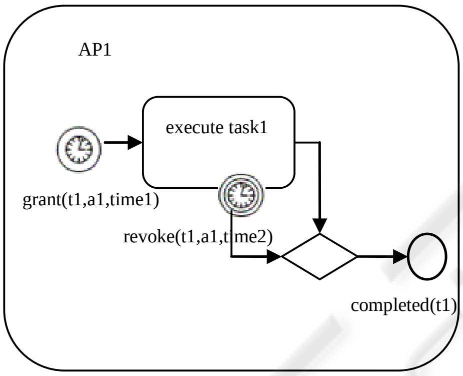

Figure 2: Task layer.

3.3.3 Data Layer

At data layer, the process for document processing during executing a task is described. Timer events trigger to grant the document access privilege to the agent or to revoke the document access privilege from the agent. Figure 3 depicts the process of processing the document during executing task1.

In Figure 2 and Figure 3, authorization events are represented by Timer events. An event “grant” is represented by a Start Timer Event, while an event “revoke” is represented by an Intermediate Timer event. The relationship among the Timer Events is: time1<time3<time4<time2,

Since the secure workflow model is a BPMN model, separating tasks, as well as concurrency and synchronization of executing tasks and processing documents can be described by using gateways.

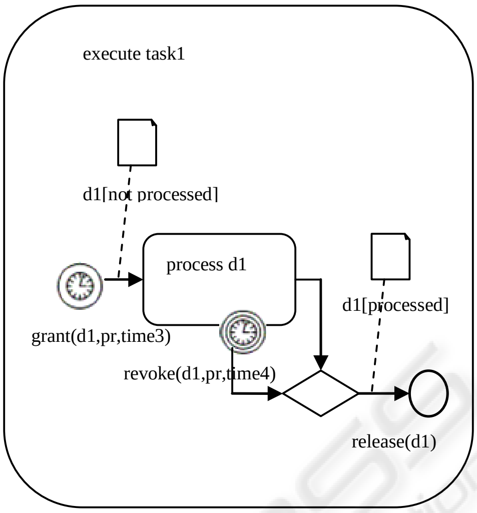

Figure 3: Data layer.

3.3.4 Evaluation

The BPMN-based secure workflow model assigns the task to an agent if and only if the agent can execute the task. It grants the task to the assigned agent for execution if and only if the set of input events is generated, the task is not started and all the dependent tasks are completed. Similarly, it revokes the task from the assigned agent if and only if the set of output events is generated and all the granted privileges for documents are revoked. Further, the model grants the document access privilege to the agent for execution if and only if it is authorized, and revokes the document access privilege from the agent if and only if the document access privilege or task is completed. Therefore, the secure workflow model ensures the security properties of integrity, authorization and availability.

This hierarchical model describes an authorization process at different layers: workflow layer, task layer and data layer. The details of a process are described at its lower layer. The model is easily readable and understandable.

Moreover, the secure workflow model is constructed by using BPMN-elements. It can be translated into BPEL and implemented.

4 CONCLUSIONS

In this paper, I proposed a BPMN-based secure workflow model to manage and monitor the specific processes in a secure workflow, such as authorizations for executing tasks and accessing documents. This model describes a workflow system from aspects of task, agent, event and data, and is constructed by using BPMN-elements. Using authorization events, the model ensures the security properties of integrity, authorization and availability.

Further, the secure workflow model is hierarchical and describes a process at different layers: workflow layer, task layer and data layer. The details of a process are described at its lower layer. The model is easily readable and understandable.

Moreover, since the secure workflow model is constructed by using BPMN-elements, it can be translated into BPEL and implemented.

REFERENCES

Atluri, V., Huang, W.-K, 1996. An Authorization Model for Workflows. In *Proceedings of the Forth European Symposium on Research in Computer Security*. pp.44-64.

Atluri, V., Huang, W.-K, 1996. An Extended Petri Net Model for Supporting Workflows in a Multilevel Secure Environment. In *Proceedings of the 10th IFIP WG 11.3 Working conference on Database Security*'. pp. 240-258.

Atluri, V., Huang, W.-K, Bertino, E., 1997. An Execution Model for Multilevel Secure Workflows. In *Proceedings of the 11th IFIP Working Conference on Database Security*. pp. 151-165.

Atluri, V., Huang, W.-K, 1997. Enforcing Manadatory and Discretionary Security in Workflow Management Systems. In *Journal of Computer Security, 5*. pp. 303–339.

BPMI.org and OMG, 2006. Business Process Modeling Notation Specification. Final Adopted Specification. Retrieved February 20, 2006. From *http://www.bpmn.org*.

Huang, W.-K, Atluri, V., 1999. SecureFlow: A Secure Web-enabled Workflow Management System. In *Proceedings of the 4th ACM Workshop on Role-Based Access Control*. pp. 83-94.

Hung, P. C. K., 2002. Specifying Conflict of Interest in Web Services Endpoint Language (WSEL). In *The ACM SIGecom Exchanges 3(3)*. pp.1-8.

Hung, P. C. K., Karlapalem, K., 2003. A secure workflow model. In *ACSW Frontiers '03: Proceedings of the Australasian information security workshop conference on ACSW frontiers*. pp. 33–41. Australian Computer Society, Inc.

Joshi, J. B. D., Aref, W. G., Ghafoor, A., Spafford, E. H., 2001. Security Models for Web-based Applications. In *Communications of the ACM 44(2)*. pp.38-44.

Kang, M. H., Froscher, J. N., Eppinger, B. J., Moskowitz, I. S., 1999. A Strategy for an MLS Workflow Management System. In *Proceedings of the 18th IFIP Working Conference on Database Security*. Seatle, WA, 1999.

Knorr, K., 2000. Dynamic Access Control through Petri Net Workflows. In *Proceedings of the 16th Annual Computer Security Applications Conference*. pp. 159–167. New Orleans, LA, December 2000.

Knorr, K., 2001. Multilevel Security and Information Flow in Petri Net Workflows. In *Proceedings of the 9th International Conference on Telecommunication Systems - Modeling and Analysis, Special Session on Security Aspects of Telecommunication Systems*. pp. 9-20.

Olivier, M. S., van de Riet, R. P., Gudes, E., 1998. Specifying application-level security in workflow systems. In *DEXA '98: Proceedings of the 9th International Workshop on Database and Expert Systems Applications*. pp. 346–351. Washington, DC, USA, 1998. IEEE Computer Society.

Pernul, G., 1992. Security Constraint Processing During Multilevel Secure Database Design. In *Proceedings of Eighth Annual IEEE Computer Security Applications Conference*. pp. 229-247.

Thuraisingham, B., Clifton, C., Gupta, A., Bertino, E., Ferrari, E., 2001. Directions for Web and E-commerce Applications Security. In *Proceedings of Tenth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises*. pp. 200-204.

Workflow Management Coalition (WfMC), 2001. Workflow Security Considerations. *White Paper, Document Number WFMC-TC-1019*. Document Status - Issue 1.0.