Formal Analysis of Workflow Systems with Security Considerations

(Progress Report)
Weiqiang Kong
Japan Advanced Institute of Science and Technology (JAIST)
weiqiang@jaist.ac.jp

Purpose

Workflow systems play an essential role in today's enterprises by providing automatic manipulation of business processes. As an integral part of workflow systems, workflow security has received extensive attentions, within which role-based access control (RBAC) mechanism and separation of duty (SoD) constraints are important topics. RBAC is a natural mechanism to lighten the complexity of security administration, with the basic notion that permissions are associated with roles and users are assigned to appropriate roles. However, to satisfy the complex security policies of workflow systems, SoD constraints are also necessary, which aim at reducing the risk of fraud by not allowing any individual to have sufficient authority within the system to perpetrate a fraud on his own [1].

Currently, most existing approaches to the specification of RBAC mechanism, and especially of SoD constraints are complicated and not suitable for the verification of desired security properties that workflow systems should possess; besides, the workflow process and authorization flow are separated during specification and verification in most approaches. Our goal is to propose appropriate and efficient methods to formally specify and verify workflow systems with such security considerations, and thus prove that execution of any workflow instance will be secure with respect to RBAC and SoD.

Approach and Progress

We proposed the use of an equation-based method - the OTS/CafeOBJ method to specify workflow systems with such security considerations, and verified some desired safety and liveness properties of workflow systems. Specifically, in our method, the workflow system, together with its security considerations, is modeled as an OTS (Observational Transition System) [2], a kind of transition system. Activities, such as grant/revoke privilege to/from roles, are triggered by events that are generated by transition rules; and SoD constraints are specified in effective conditions that are attached to each transition rule. The OTS is then written in CafeOBJ [3, 4], an algebraic specification language. We express safety and liveness properties of the workflow system in CafeOBJ, and verify that the OTS satisfies these properties by writing proof scores in CafeOBJ and executing the proof scores with CafeOBJ rewriting engine. The verification of safety properties ensures that the RBAC mechanism and SoD constraints are correctly realized by the given workflow specification; and the verification of liveness properties ensures that the existence of security considerations will not prevent completion of the execution of workflow. We have applied our method to analyze a sample workflow - travel expenses reimbursement workflow.

The advantages of our method include: (1) The workflow system, together with the RBAC mechanism and the SoD constraints, is described in terms of equations, which are easier to understand; and the verification is done by means of equational reasoning, which moderates the difficulties of proofs. (2) Different workflow instances are distinguished explicitly during specification and verification, which reflects the important feature of concurrent execution of workflow systems. (3) The analysis of workflow processes is combined with authorization flows. In other words, our method analyzes whether the workflow process is executable along with the authorization flow.

Future Work

In the OTS/CafeOBJ method, we used theorem proving technique to verify safety and liveness properties possessed by workflow systems which are modeled as OTSs. In the future work, we plan to use model checking technique to do some parts of the verification work, which would be a good complement of our currently used theorem proving technique. As a sibling language of CafeOBJ, Maude is a specification and programming language which has model-checking facilities [5]. Our current plan is to: develop a tool that can translate workflow specification written in CafeOBJ with the underlying OTS model to Maude specification with the underlying OTS model. Through this translation, the same CafeOBJ specification of workflow systems with the underlying OTS model can be used both to theorem proving and model checking. And therefore, some desired properties of

workflow systems, such as liveness property, can be proved easily by using model checking technique; and besides, counterexample will be provided if the property cannot be proved. After the development of this translation tool, we plan to use this tool to analyze inter-organizational workflow systems. Web services composition could be considered as an effective method to realize inter-organizational workflow.

Publications

[1] Weiqiang Kong, Kazuhiro Ogata, Jianwen Xiang, Kokichi Futatsugi: Formal Analysis of an Anonymous Fair Exchange E-Commerce Protocol, In: CIT 2004, IEEE CS Press, 2004, pp.1100-1107.
[2] Weiqiang Kong, Kazuhiro Ogata, Kokichi Futatsugi: Formal Analysis of Workflow Systems with Security Considerations. Submitted to SEKE 2005.

References:

[1] Bertino E., Ferrari E.: The specification and enforcement of authorization constraints in workflow management systems. ACM TISSEC, (1999), 65-104.
[2] Ogata K., Futatsugi K.: Proof scores in the OTS/CafeOBJ method. In: FMOODS 2003, LNCS Vol.2884, Springer (2003), 170-184.
[3] Diaconescu R., Futatsugi K.: CafeOBJ Report. AMAST Series in computing, 6. World Scientific, Singapore, 1998.
[4] CafeOBJ Homepage: www.ldl.jaist.ac.jp/cafeobj.
[5] Steven Eker, Jose Meseguer, and Ambarish Sridharanarayana: The Maude LTL model checker. In: WRLA 2002, ENTCS 71. Elsevier, 2002.