http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 7 (1): 228-230, 2008
ISSN 1812-5638

Modeling Non-Repudiation in Distributed Systems

[1]Hong Zheng, [2,3]YuYue Du and [2,3]ShuXia Yu
[1]Department of Computer Science and Engineering,
East China University of Science and Technology, Shanghai, 200237, China
[2]College of Information Science and Engineering,
Shandong University of Science and Technology, Qingdao 266510, China
[3]The State Key Laboratory of Computer Science, Institute of Software,
Chinese Academy of Sciences, Beijing 100080, China

Abstract: As an important security service in distributed systems, non-repudiation is required to implement evidence generating or validating in the application layer. Formal methods are powerful tools to provide security services. The study applies labeled colored Petri nets to modeling and analysis of the non-repudiation in distributed environment.

Key words: Distributed system, security service, non-repudiation, Petri nets

INTRODUCTION

In distributed systems, communication between the parties is notoriously insecure, transferred data could be eavesdropped or worse still tampered with by an attacker. The limited trust between the partners leads to the need for a system that provides non-repudiation to compensate for the lack of trust between different companies across trust boundaries (Anonymous, 2002). This study focuses on the provision of a formal model of non-repudiation service.

NON-REPUDIATION MODEL OF AN ELECTRONIC BUSINESS APPLICATION

The non-repudiation service is required to provide the evidence generation, evidence collection, evidence verification, evidence storage and evidence retrieval.

A non-repudiation model for electronic business systems is provided as shown in Fig. 1. We assume client Amy (a buyer) is communicating with an online store server (a seller) and wishes to make a purchase. The seller authenticates to ensure the buyer is not an impostor.

FORMAL ANALYSIS OF NON-REPUDIATION SERVICES

Over the past few years, formal methods have been successfully applied to the analysis of system security.

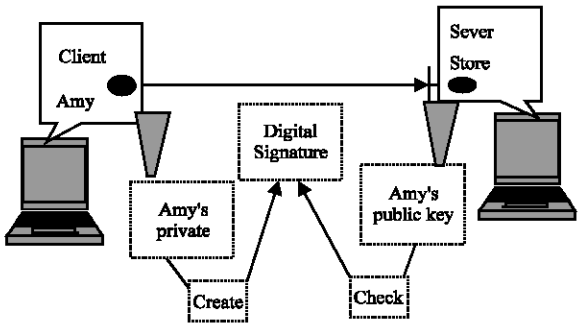

Fig. 1: A non-repudiation service model

Since the bulk of the effort has been concerned with authentication and confidentiality properties, there are now a range of maturing techniques and approaches for such analysis, as exemplified by Boleslaw and Sachin (2004) and Hong and Li (2002). By contrast, non-repudiation has not been addressed to the same degree by these techniques. Petri nets are widely used in various application domains because of its simplicity and strong expressive and analytic power of system behavior (Wiebke, 2005; Boleslaw and Sachin, 2005). The study discusses how Petri nets extend or adapt to the analysis of non-repudiation.

Labeled Colored Petri Net (LCPN): Formally, a Petri net (PN) is a 3-triple PN = (P,T;F), where P is a finite set of places represented by circles, T a finite set of transitions represented by bars or rectangles and $P \cap T = \varnothing$,

Corresponding Author: YuYue Du, College of Information Science and Engineering,
Shandong University of Science and Technology, Qingdao, 266510, China

$F \subseteq (P \times T) \cup (T \times P)$ a set of arcs. In this sub-section, a labeled colored Petri net is defined to model and analyze the non-repudiation service based on Fig. 1.

Definition 1: A Labeled Colored Petri Net (LCPN) is a 4-tuple LCPN = (CPN, M_0, Ω, l), where

- The CPN is a colored Petri net (Du and Jiang, 2004), CPN = (Σ, P, T, A, N, C, G, E, I), where $P = P_C \cup P_D \cup P_I$, P_C is a finite set of control places, P_D is a finite set of data places and P_I is a finite set of interface places. Let $I_p = P_C \cup P_D$
- T is a finite set of transitions, $P \cap T = \varnothing$. $T = T_{in} \cup T_{out} \cup T_{int}$, $T_{in} \cap T_{out} = \varnothing$, $T_{in} \cap T_{int} = \varnothing$, $T_{in} \cap T_{out} = \varnothing$. Where T_{in} is a finite set of receiving message transitions, which are represented to receive other participant messages from interface places, T_{out} is a finite set of sending message transitions, which are represented to send message to other participants from interface places. T_{int} is a finite set of internal transitions that represent internal actions of a participant regardless of other participants.
- $M = (M_C, M_D, M_I)$: $P \rightarrow \{0, 1\}$ is a marking function. M_C, M_D and M_I represent respectively the marking at the set of P_C, P_D and P_I. $M_0 = (M_{C0}, M_{D0}, M_{I0})$ is an initial marking. Let $I_M = (M_C, M_D)$
- l: $T \rightarrow \Omega$ is a labeled function. The labeled function is used to map transitions related the same task to a symbol or map internal transitions to an invisible action represented by τ.

Definition 2: Enabling and firing rules:

Let (CPN, M_0, Ω, l) be an LCPN, LCPN = (CPN, M_0, Ω, l), $M = (M_C, M_D, M_I) \in (M_0)$, such that step Y in the LCPN is said to be enabled at IM if only and if $\forall p \in IP$, $\sum_{(t,p) \in Y} E(p,t)<b> \leq M(p)$. If step Y is enabled at IM, step Y is firable. After Y is fired, a new marking is generated, namely, IM[Y>IM′=(M_C', M_D'), where

$$\forall p \in IP,\ IM'(p) = IM(p) - \sum_{(t,b) \in Y} E(p,t)<b> + \sum_{(t,b) \in Y} E(t,p)<b>.$$

Non-repudiation service models: In Fig. 2, p_{c11} and p_{c12} are two control places, Pc = {p_{c11}, p_{c12}, p_{c21}, p_{c22}}. Similarly, p_{d11}, p_{d12}, p_{d21}, p_{d22} and p_{d13} are data places. pri_key place is named for readablity. A set of interface places is P_I, P_I = {p_{i1}, p_{i2}, p_{i3}}. The place pri_key is used to deposit Amy's private key. Amy's public key is deposited in pub_key place. The token color is order which represents Amy's order form, k is Amy's private key, k(order) represents Amy's encrypted (by her private key signature) order form, c is a color set of control tokens.

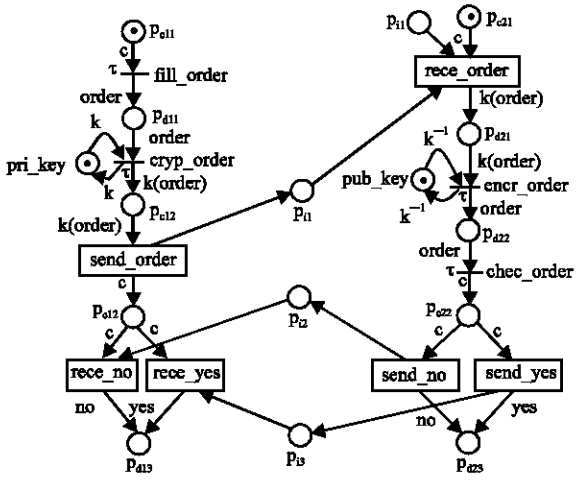

Fig. 2: Non-repudiation service model of a whole B-S business

M_0 is initial a marking, $M_0(p_{c11}) = 1$, M_0 (pri_key) = 1, M_0 (p_{c21}) = 1, M_0 (pub_key) = 1. Transition fill_order is an internal transition that represents Amy fills her order form, transition cryp_order is also an internal transition that represents Amy makes a digital signature by her private key and these two transitions can be mapped to a symbol τ. Transition send_order is a sending messsage transition used to send the order data to the seller, rece_no is a receiving messege transition used to receive the refused message by this seller, the seller uses rece_yes to receive the affirmed message. Tokeas no and yes describe respectively the refused and the affirmed message. Transition send_no denotes the seller sends invalid message to buyer Amy and send_yes is used to represent valid message to the buyer. encr_order and chec_order are two internal transitions mapped to a symbol τ. According to the net structure in Fig. 2, the liveness of the whole B-S business LCPN model is easily proved.

NON-REPUDIATION EVIDENCE

In this study we use LCPNs to analyze evidence generation and collection of non-repudiation service. In contrast to authentication, security auditing and other services, the non-repudiation service is not concerned with communication issues between participants. By using the identity and/or other privilege attributes of the distributed object, the security authorization and access control are provided. The distributed system basic security services can be implemented by security technologies and mechanisms. So we focus on evidence issues of non-repudiation by LCPNs.

With respect to this business system, we only provide formal models with a buyer and a seller. Actually, this system should contain bank or other corresponding entities. For the sake of simplification, we do not consider these details. If each participant strictly performs his own obligation and task in the trading, both the buyer and the seller will reach their respective aims, that is, the buyer can get her shopping goods and the seller get payments for goods. According to the two models of Fig. 2, the following propositions can put forward in terms of their firing steps.

Proposition 1: If there exists a firing step σ from an initial marking M_0 and $M_0(p_{c11}) = 1$, M_0(pri_key) = 1, such that σ = τ∘send_order. Therefore, any third party can prove the buyer has sent his order in terms of the step σ and the message transferred to place p_{i1}, that is, non-repudiation sending order of the buyer can be provided.

Proposition 2: If there exists a firing step σ from an initial marking M_0 and $M_0(p_{c21}) = 1$, M_0(pub_key) = 1, $M_0(p_{i1} = 1)$, such that σ = τ∘send_order∘rece_order. Therefore, one trusted third party could judge the seller has received the buyer's order in terms of σ and the message deposited in place p_{i1}, that is, the non-repudiation of receiving order of the seller can be provided.

Proposition 3: If there exists a firing step σ, σ = τ∘send-order∘rece_order, the seller is responsible to firing his internal transitions and other sending transitions, otherwise, both the buyer and the seller cannot reach their own aims.

Proposition 4: The firing step σ, σ = τ∘send-order∘rece_order∘τ∘ send_yes∘rece_yes, means that the business affair has been performed successfully. If there exists a firing step σ, σ = τ∘send-order∘rece_order τ∘send_no∘ rece_no, one trusted third party can use the firing step σ and message data deposited in place p_{i2} to prove no goods is provides to the buyer.

The non-repudiation service describes the functionality of the service, but implement details of such a service have not been addressed. Formally modeling and analyzing non-repudiation evidence by the LCPN method in the study helps to implement the non-repudiation service in distributed applications.

ACKNOWLEDGMENTS

This research is supported by the National High Technology Research and Development Program of P.R.China (No. 2002AA412610); the National Natural Science Foundation of China under Grants 60773034 and 60573018; Taishan Scholar Construction Project of Shandong Province, China; the National Basic Research Program of China (973 Program) under Grants 2003CB316902 and 2004CB318001-03; the Open Project of the State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences under Grant SYSKF0604 and the Research foundation of East China University of Science and Technology. The authors are also grateful to the anonymous referees for their insightful and valuable comments and suggestions.

REFERENCES

Anonymous, 2002. Deployment and Configuration of Component-based Distributed Applications. OMG Document: orbos/2002-01-19.

Boleslaw, M. and J. Sachin, 2004. Modeling of information systems security features with colored Petri nets. IEEE International Conference on Systems, Man and Cybernetics, SMC 2004, 5: 4879-4884.

Boleslaw, M. and J. Sachin, 2005. Specifying selected security features of interorganizational workflows. Proceedings International Conference on Computational Intelligence for Modelling, Control and Automation, CIMCA 2005 and International Conference on Intelligent Agents, Web Technologies and Interne, pp: 958-963.

Du, Y.Y. and C.J. Jiang, 2004. Verifying functions in online stock trading systems. J. Comput. Sci. Technol., 19: 203-212.

Wiebke, D., 2005. Security Analysis of the Secure Authentication Protocol by Means of Coloured Petri Nets. 9th IFIP TC-6 TC-11 International Conference on Communications and Multimedia Security, CMS 2005, LNCS3677 Springer Verlag, pp: 230-239.

Zheng, H. and S.X. Li, 2002. The Description of CORBA Objects Based on Petri nets. Proceedings of 4th International Conference on Formal Engineering Methods, Lecture Notes in Computer Science, LNCS2495, Springer-Verlag, Shanghai China, pp: 48-57.