IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 6 (Mar. - Apr. 2013), PP 69-73
www.iosrjournals.org

Workflow Signature for Business Process Compliance: A Survey

Nasseena.N[#], Pretty Babu [*]
[#]Dept.Of Computer Science &Engg.*.,Sree Buddha College of Engineering *Sree Buddha College of Engineering,Pattoor Alappuzha(Dist),Kerala*

Abstract: *Inter organizational workflow management systems play a very important role in executing business processes among business partners in a dynamic and timely manner. An inter organizational workflow management engine is used to model and control the execution of business processes involving a combination of manual an automated activities between organizations. Before delivering their product and services to their customers each of them have to authenticate using workflow signature scheme. A workflow consists of number of tasks in the organizations. For providing more security, signing keys can be used to grant permission to perform the task and these keys are issued on the fly. Cryptographically secure scheme is not suitable because the workflow graph is arbitrary. Cryptographic scheme such as RSA provide only data authenticity and integrity. In addition to authenticity and integrity, workflow signature provides the logical relationships such as AND-join and AND-split of a workflow. In workflow signature scheme multi key hierarchical encryption scheme is used. This survey paper mainly examines the workflows and various encryption techniques are explained along the way of discussion.*

Keywords*-Workflows, Inter organization, Multikey hierarchy*

I. Introduction

In paper based workflow system signature are used for different purposes such as authorization, authentication, accountability, integrity, witness and timestamp. As the development of information technology it leads to the migration of workflow system from paper based to electronic workflow system. Here different procedures are required for handling signature for different purposes. A business process is a set of one or more interconnected activities which collectively realize a business objective or policy goal, normally within the context of an organizational structure defining functional roles and relationships. A workflow is the automation of a business process, in whole or part, during which documents, information, or tasks are passed from one participant to another, according to a set of predefined rules. A workflow management system defines, creates and manages the execution of workflow.

. The development of internet technology has gained popularity in online transaction. Web services are an important technology in this area. Its standards and specification have been studied and widely used, serving as a tool to perform multiple workflow activities such as service integration, interaction, coordination and interoperation through standard interface. The presence of workflow and their application is concentrated in decentralized collaborative environment such as peer to peer , grid and cloud computing[1].

In workflow system the workflow management engine is either centralized or decentralized. In most cases of workflow system the decentralized workflow engine is preferred due to scalability and heterogeneous and autonomous nature of organizations. In a centralized workflow system, the central workflow engine is responsible for distributing the related task to the appropriate task agent. In the case of decentralized workflow system, the central workflow engine send the entire task to the first execution agent in the workflow and received the final output from the last execution agent in the workflow system.

In workflow system consists of number of task and each task is authenticated by using the cryptographic techniques. The standard signature scheme such as the digital signature is not suitable in workflow system. The standard signature scheme provides only data authenticity and integrity of workflow data. So to provide the logical relationship of workflow data digital signature is used along with some other data protection mechanism. Digitally signed messages related to a task within the workflow can be used as a proof that the associated business process has taken place and it is authorized by relevant parties.

The standard signature is not used because such signature scheme cannot be used to represent a workflow graph with AND-split, AND-join, OR-split, and other relations. To achieve this multikey hierarchical encryption scheme is used. The main application of workflow system includes online banking, ATM, online shopping and E-commerce.

This paper is organized as follows. Section 2 discussed the example of workflow system. In section 3 discussed the different types of signature schemes used in cryptography. In section 4 gives a summary regarding the various aspect of the signature. In section 5 discussed the conclusion.

II. Example Of Workflow System

A business workflow consists of a set of tasks and the associated task dependencies that control the coordination among these tasks. Each task is performed by the associated task execution agent. Each task is represented by ti and task execution agent is represented by A(ti). In decentralized workflow system the execution agents are different and task evaluations are performed by the agent without knowing the central workflow engine.

Consider a business travel planning process that makes a flight booking, and a hotel room and car reservations. The workflow of this process is graphically represented by Fig. 1 and the corresponding tasks are described as follows:

t_1: Input travel information;
t_2: Request for a flight quotation from Key Travel;
t_3: Check and compare flight tickets of different airlines through Opodo;
t_4: Obtain manager's approval;
t_5: Purchase flight tickets from Opodo;
t_6: Purchase flight tickets from Key Travel;
t_7: Reserve a room from Hotel Booker; and
t_8: Rent a car at Euro Car.

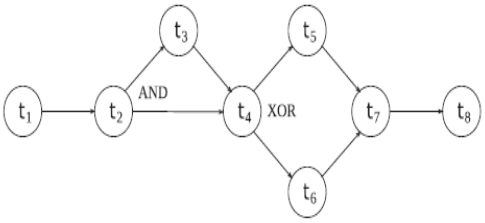

Fig 1.Example of Workflow System

In Fig. 1 the entire workflow is initiated by a CWE and is then forwarded to the first execution agent. In our example workflow, A(t1) is a travel requester who needs to perform task t1, that is entering travel information into the workflow system. Upon completion of task t1, agent A(t1) forwards the remaining workflow (t2. . . t8) to agent A(t2), a travel agency. Agent A(t2) is then expected to execute task t2 and send the remaining workflow (t4, . . . , t8) to agent A(t4). In addition, agent A(t2) triggers the execution of task t3 by agent A(t3), another independent travel agency in parallel, as part of the company travel policy, for example. Next, agent A(t4), who in this case is the manager of the requester, decides whether the requester should purchase the flight tickets from Key Travel or Opodo, perhaps based on the current company budget. In other words, agent A(t4) would either forward tasks t6, t7, t8 to agent A(t6) if the flight tickets are to be purchased from Key Travel, or tasks t5, t7, t8 to agent A(t5) if it decides to go for Opodo. Subsequently, agent A(t7), followed by agent A(t8), execute their respective tasks. At the end, agent A(t8) reports the results back to the central workflow engine.

III. Signature Schemes

The different types of signature schemes are,

a) Identity based Signature Scheme(IBS):

In IBC, a public key can be computed based on a publicly available identifier, for example, e-mail address or phone number, and used on-the-fly. The matching private key is obtained from a private key generator (PKG), a trusted authority. This is in contrast to most conventional public-key cryptosystems in which a public key is simply a fixed-size string that looks random and needs to be attested through the means of public key certification. In such systems, one needs to verify the authenticity of a public key by checking the validity of the corresponding certificate before using it.

b) Hierarchical Identity based Signature Scheme(HIBS):

The main motivation of hierarchical based signature scheme to avoid single point of failure in the IBC setting, where all system users rely on a single PKG. The natural way to introduce multiple levels of PKGs, analogous to the multiple levels of certificate authorities (CAs) in a hierarchical PKI setting. Hence in HIBC, it is assumed that entities can be arranged in a tree structure. There exists the root PKG at the top of the tree, at level 0. Each entity has an identifier. The identifier of an entity is the concatenation of the node identifiers in the path
from the root of the tree to the node associated with that entity. Each level produces a private key to the next level of the tree. For example, the root PKG, at level 0, produces private keys for entities at level 1, who in turn act as PKGs and issue private keys for entities at level 2, and so on.

c)Multilevel Hierarchical Identity based Signature(MHIBS)

In HIBS only one signing key is used for generating the private key. In MHIBS multiple signing keys are issued on the fly for producing a single signature. These identifiers may be located at arbitrary positions in the hierarchy. This type of scheme is suitable for workflow signature.

IV. Literature Survey

In [2] Workflow systems are gaining importance as an infrastructure for automating inter-organizational interactions. In inter organizational management system a decentralized workflow management system is used. Because the central system is not suitable for monitoring or controlling the entire task in an organization. In decentralized workflow management system the workflow is partitioned into self describing workflow and is controlled by workflow stub. Each workflow stub is responsible for receiving the Self describing workflow, updating and send to the next agent. Decentralized execution of inter-organizational workflows may raise a number of security issues including conflict-of-interest(COI) among competing organizations.

This paper proposes a Chinese wall security model for the decentralized workflow management system for solving the conflict of interest in the self describing workflow. In this model the company dataset are represented as disjoint conflict of interest(COI). For example, Banks, Oil Companies, Air Lines are the different conflict-of-interest classes. The Chinese wall policy states that information flows from one company to another that cause conflict of interest for individual consultants should be prevented. Thus, if a subject accesses Bank A information, it is not allowed to access any information within the same COI class, forexample, that of Bank B. However, it can access information of another COI class, for example, oil company.

This model implements partitioning and workflow management system stub algorithms to enforce security policy. The partition algorithm generates a non-restrictive self-describing partition if it does not contain sensitive objects, it generates restrictive self-describing partitions if it contains sensitive objects involving the same COI group. This approach allows to hide the sensitive information contained in dependencies so that the task agents cannot manipulate their output for their own advantage. It also describe the logical relationship of the workflow such as AND, OR relationship of workflow.

In [3] describe the different types of signature and its purposes in workflow management process. In traditional workflow system we use paper document. This process is time consuming and inefficient. In electronic workflow system digital signature is used for authenticating the participating entities. In electronic system the signature has different purpose. A signature within a document means that it provides authentication, integrity, confidentiality, accountability etc. But the document does not give the complete information about different signature purpose. So a Laison workflow architecture is used for capturing all the information related to the signature purposes. It consists of a workflow model and a workflow engine. It also contains different data structure for capturing the information. Using this information we can verify the different signature purpose. The purposes of signatures are closely associated with the two modes of decision making, namely single and group. This architecture includes signature purpose, modes of decision making, different data structure to handle the information and also include the signing and validation requirement for handling the signature purpose.

In [4] a computational grid is a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational facilities. A grid system uses public key infrastructure (PKI) to authenticate identities of grid members and to secure resource allocation to these members. Identity based cryptography techniques are used to the security of grid computing. As the grid security grown PKI is not suitable key generation, certification and verification purposes. To provide security for grid system, implement an identity-based key infrastructure for grid (IKIG). It support single sign on the use of identity based proxy credentials. Since the users' proxy public keys are based on some identifiers and the matching proxy private keys are stored locally at the user side, user authentication can be performed without any physical intervention from the users and without the need for certificates. Users in the IKIG setting do not need to obtain proxy private keys from their respective PKGs. This is because through HIBC, the users themselves can act as PKGs for their local proxy clients. Thus, proxy private key distribution is not an issue in IKIG.

IKIG includes attributes of a user, such as roles and group memberships, in his identifier. This offers a more clean and simple way of binding the user's identity with his entitled privilege attributes and also to provide access control to grid resources. It also supports an identity-based authenticated key agreement protocol based on the TLS handshake. IKIG replace the CA(certificate authority) in the current PKI-based GSI with a trusted authority (TA). The TA's roles include acting as the PKG and supporting other user-related administration and management. This may enable the expansion of grids to service users with bandwidth-limited or low memory platforms.

In [5] Identity-based cryptography is a type of public-key cryptography in which a publicly known string representing an individual or organization is used as a public key. The public string could include an email address, domain name, or a physical IP address. The is paper deals with identity based cryptosystem in which any user can communicate securely and to verify each other's signature without using key directories

and with a third party. Each user has a personalized smartcard in which the information of the user is embedded and helps the user to sign and encrypt the message when he sends and to decrypt and verify when he receive the message. When a user wants send message from A to B, A sign the message with his secret key in the care and encrypt the message using Bs name and address, add As name and address and send to B. When B receives the message, B decrypts the message using his secret key in the card and verify the message using address in the message. Secret key is generated by key generation centre.

The implementation of secret key in two ways. The choice of a good random seed is crucial in the field of computer security. When a secret encryption key is pseudo randomly generated, having the seed will allow one to obtain the key. If the same random seed is deliberately shared, it becomes a secret key. One way is that when the seed value is known secret key can be easily generated from possible public keys. The second way is, if we didn't know random seed generating this from key pair is a complex task.

In [6] Proposed an Id based signature based on Gap Diffie-hellman Group (GDH). This scheme proves the security against existential forgery on chosen message and ID attack under random oracle model. GDH is obtained from bilinear pairing. This scheme shares the same system parameters. Here the secret key is shared by more parties. So it provides stronger non repudiation property.This algorithm consists of four steps; set up, extract, sign and verify. The set up algorithm generate the system parameter and a secret key. The extract algorithm generates a private key based on given Id. The sign algorithm output a signature that contain the message, secret key and a random number .The verify algorithm verify that the signature is valid or not. The same algorithm is used for proving the security attack under the random oracle model.

In [7] is based on computational Diffie Hellman group and it provides the security of chosen ciphertext under random oracle model. It based on bilinear map between two group. A random oracle is a function H : X -> Y chosen uniformly at random from the set of all functions h : X ->Y . Random oracles are used to model cryptographic hash functions such as SHA-1. Note that security in the random oracle model does not imply security in the real world. The random oracle model is a useful tool for validating natural cryptographic constructions. ID based signature uses four algorithms to provide security such as set up, extract, sign and verify. This four algorithm is not suitable for providing security on ciphertext. We use a technique Fujisaki-Okamoto to convert the BasicIdent scheme of the previous section into a chosen ciphertext secure IBE(identity based encryption) system in the random oracle model. In this method two additional hash function is used in the set up algorithm. This algorithm prove the security under random oracle model.

In [8] Hierarchical identity-based encryption(HIBE) schemes and signature schemes that have total collusion resistance on an arbitrary number of levels and that have chosen ciphertext security in the random oracle model assuming the difficulty of the Bilinear Diffie-Hellman problem. In PKI based encryption the public is available from a certificate authority and a public key directory is maintained. To overcome this IBE scheme came. Here no key directory is used and public key is obtained from a known identifier of the receiver. One problem here is that a private key is obtained from a PKG .All users have a single PKG. To overcome this HIBE came and it is tree like structure. Each level has a PKG and each PKG produces private key for the next level and so on.

A HIBE scheme is specified by five randomized algorithms: Root Setup, Lower-level Setup, Extraction, Encryption, and Decryption: in root setup the root PKG takes a security parameter *K* and returns system parameters and a root secret. The system parameters include a description of the message space and the cipher text space . The system parameters will be publicly available, while only the root PKG will know the root secret. In Lower-level Setup users must obtain the system parameters of the root PKG. In Extraction PKG with ID-tuple may compute a private key for any of its children by using the system parameters and its private key. In Encryption sender inputs system parameter, and the ID-tuple of the intended message recipient, and computes a ciphertext . In Decryption user inputs system parameters, and its private key , and returns the message.

In [9] Present a new cryptographic primitive that we call multi-key hierarchical identity-based signatures (multi-key HIBS). Using this primitive, a user is able to prove possession of a set of identity-based private keys associated with nodes at arbitrary levels of a hierarchy when signing a message. It is similar to hierarchical identity based cryptography. But different signing keys are used for signing purposes. This is based on identity-based multi-signatures and aggregate signatures. In MHIBS multiple signing keys are issued on the fly for producing a single signature. These identifiers may be located at arbitrary positions in the hierarchy. This type of scheme is suitable for workflow signature. In hierarchical identity-based cryptography multiple levels of private key generators (PKGs) and users form a tree-like structure which similar to the existing hierarchical PKI model. A user at any level of the tree can encrypt or sign a message targeting any intended recipient at any level, using only a set of shared cryptographic system parameters published by the root PKG. Entities at one level can share the same set of system parametes and produces a private key for next level.

A multi-key HIBS scheme is specified by the following algorithms, root setup algorithm is performed by the root PKG. It generates the system parameters and a master secret on input a security parameter. The system parameters, which include a description of the message space and the signature space, will be made

publicly available to all entity. However, the master secret is known only to the root PKG. In lower-level setup algorithm all entities at lower levels must obtain the system parameters generated by the root PKG. This algorithm allows a lower-level PKG to establish a secret value to be used to issue private keys to its children. Extract algorithm is performed by a PKG with identifier ID to compute a private key for any of its children using the system parameters and its private key . Sign algorithm contains a set *of* signing (private) keys, a message, and the system parameters, this algorithm outputs a signature and this algorithm outputs valid or invalid.

V. Conclusion

The purpose of this survey is to describes workflows and their relevant contexts. While designing the web security in different organization to maintain the authenticity, integrity and logical relationship between the different organizations is a challenging task. This survey on effective signature purposes between the organizations give solutions to the problems associated with the web security. The signature scheme in cross organization provides not only the authentication and integrity of the task but also to provide the logical relationship between the organizations.

References

[1] G. Fox and D. Gannon, "Workflow in grid systems," Concurrency and Computation: Practice anExperience, pp. 1009–1019, 2006.
[2] V. Atluri, S. Chun, and P. Mazzoleni, "Chinese Wall Security for Decentralized Workflow Management Systems," J. ComputerSecurity, vol. 12, no. 6, pp. 799-840, Dec. 2004.
[3] Karl R.P.H. Leung Lucas C.K. Hui, "Handling Signature Purposes inWorkflow Systems".
[4] Hoon Wei Lim · Kenneth G. Paterson, "Identity-based cryptography for grid security".
[5] A. Shamir, "Identity-Based Cryptosystems and Signature Schemes," CRYPTO: Proc. Advances in Cryptology, G. Blakley and D. Chaum, eds., pp. 47-53, Aug. 1985.
[6] J.C. Cha and J.H. Cheon, "An Identity-Based Signature from Gap Diffie-Hellman Groups," Proc. Sixth Int'l Workshop Theory and Practice in Public Key Cryptography (PKC '03), Y.G. Desmedt, ed.,pp. 18-30, Aug. 2001.
[7] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," CRYPTO: Proc. Advances in Cryptology, J. Kilian, ed., pp. 213-229, Aug. 2001.
[8] C. Gentry and A. Silverberg, "Hierarchical ID-Based Cryptography," ASIACRYPT: Proc. Advances in Cryptology, Y. Zheng, ed., pp. 548-566, Dec. 2002.
[9] H.W. Lim and K. Paterson, "Multi-Key Hierarchical Identity- Based Signatures," Proc. 11th IMA Int'l Conf. Cryptography and Coding (IMA '07), S. Galbraith, ed., pp. 384-402, Dec. 2007.