MODEL-DRIVEN SECURITY ASSESSMENT AND VERIFICATION FOR BUSINESS SERVICES

Thirumaran.M[1] and Dhavachelvan.P[2] and Abarna.S[3]and Thanigaivel. K[4]

[1]Department of Computer science and Engineering, Pondicherry Engg College, India.
thirumaran@pec.edu

[2]Department of Computer science and Engineering, Pondicherry University, India.
dhavachelvan@gmail.com

[3]Department of Computer science and Engineering, Pondicherry Engg College, India.
abarna.pec@gmail.com

[4]Department of Computer science and Engineering, Pondicherry Engg College, India.
thanigaivel20@pec.edu

1. ABSTRACT

Information security covers many areas within an enterprise. Each area has security vulnerabilities and, hopefully, some corresponding countermeasures that raise the security level and provide better protection. The fundamental concepts in information security are the security model, which outlines how security is to be implemented. A security policy outlines how data is accessed, what level of security is required, and what actions should be taken when these requirements are not met. A security model is a statement that outlines the requirements necessary to properly support and implement a certain security policy. An important concept in the design and analysis of secure systems is the security model, because it incorporates the security policy that should be enforced in the system. A model is a symbolic representation of a policy. It maps the desires of the policy makers into a set of rules that are to be followed by a computer system. In the paper we propose a model driven security assessment and verification for business service. The Security Assessment and Verification verifies whether the Application and Services are secure based on the Service Level Agreement and generates the report on the level of security features. It is designed to help business owners, operators and staff to assess the security of their business. It covers potential areas of vulnerability, and provides suggestions for adapting your security to reduce the risk of crime against your business. A security policy states that no one from a lower security level should be able to view or modify information at a higher security level, the supporting security model will outline the necessary logic and rules that need to be implemented to ensure that under no circumstances can a lower-level subject access a higher-level object in an unauthorized manner. The security policy is an abstract term that represents the objectives and goals a system must meet and accomplish to be deemed secure and acceptable.

2. KEYWORDS: *Service Level Agreement (SLA), Security Policies, Security assessment and verification.*

3. INTRODUCTION

A security policy is a set of rules and practices dictating how sensitive information is managed, protected, and distributed. A security policy expresses exactly what the security level should be by setting the goals of what the security mechanisms are to accomplish. The security goals are based on legal compliance regulations and risk assessments, define how security configurations are determined, decide upon the ways in which a company's assets are

DOI : 10.5121/ijwsc.2010.1203

protected, and how the availability of resources is managed in the context of process-aware information systems [1].The security policy is an important element that has a major role in defining the design of the system, because it incorporates the security policy that should be enforced in the system [6]. A model is a symbolic representation of a policy. It maps the desires of the policy makers into a set of rules that are to be followed by a computer system. The security policy is a foundation for the specifications of a system and provides the baseline for evaluating a system. Many of these security issues must be thought through before and during the design and architectural phase for a product. Many processes are security critical in the sense that security requirements are a central part of process requirements and security mechanisms are required for their realization. Examples range from the authorization of a military engagement, to an enterprise purchase process, to even the coordination of the sequence of user interface masks displayed to a user .In such examples, the security policy can be quite complex and may be comprised of a collection of requirements, which are associated with different points of execution and checked and enforced at these points [11]. Hence Security is best if it is designed and built into the foundation of operating systems and applications and not added on as an afterthought. Once security is integrated as an important part of the design, it has to be engineered, implemented, tested, audited, evaluated, certified and accredited. The security that a product provides has to be rated on the availability, integrity, and confidentiality it claims [1]. Consumers then use these ratings to determine if specific products provide the level of security they require. This is a long road, with many entities involved with different responsibilities. So in a very general and simplistic example, if a security policy states that subjects need to be authorized to access objects, the security model would provide the mathematical relationships and formulas explaining how *x* can access *y* only through outlined specific methods. Specifications are then developed to provide a bridge to what this means in a computing environment and how it maps to components and mechanisms that need to be coded and developed. The developers then write the program code to produce the mechanisms that provide a way for a system to use access control lists and give administrators some degree of control. This mechanism presents the network administrator with a GUI representation, like check boxes, to choose which subjects can access what objects, to be able to set this configuration within the operating system. This is a rudimentary example because security models can be very complex, but it is used to demonstrate the relationship between the security policy and the security model. Hence the final step is to verify whether the Application and Services are secured based on the Service Level Agreement this is done using Security Assessment and Verification and generates the report on the level of security features.

4. RELATED WORKS

Christian Wolter present security policy and policy constraint models and discuss a translation of security annotated business processes into platform specific target languages, such as XACML or AXIS2 security configurations. To demonstrate the suitability of this approach an example transformation is presented based on an annotated process [1]. Nagaratnam et al discusses an approach to overcome this shortage by expressing security requirements in the context of business processes and how to monitor and manage them on the different enterprise architecture levels [2]. Similar concepts are addressed by Rodríguez et al. [3] and Sadiq et al. [4]. Both define a meta-model that links security requirement and compliance regulations stereotypes to sequence objects of a business process and proposed graphical annotation elements to visually enrich the process model with related security requirements, but both consider a model-driven scenario as future work. Michiaki Tatsubori proposed the domain of model-driven security in the context of business processes is an emerging research area. The need to support the application scenario and related security policies for web services on an abstract level is discussed in [5]. The authorization concepts are refined by Dong Huang in a semantic policy-based security framework for business processes identifying two levels of security for business processes. On the task or activity level, security

concerns, such as non-repudiation, confidentiality, and data integrity are considered. On the process level, general compliance rules, such as required by Sarbanes–Oxley are defined [6].Tom Goovaerts presented an open architecture for enforcing and composing complex policies that can depend on the available services in the environment. They have created a flexible run-time architecture that maximizes interoperability, adaptability, evolution and prototyped the architecture on an Enterprise Service Bus and illustrate how the solution supports realistic and complex policies [7].Carlos Gutiérrez proposed the application of the Process for Web Service Security (PWSSec), to a real web service-based case study. The manner in which security in inter-organizational information systems can be analyzed, designed and implemented by applying PWSSec, which combines a risk analysis and management, along with a security architecture and a standard-based approach. They additionally present a tool built to provide support to the PWSSec process [8]. Xinwen Zhang proposed group-based RBAC model (GB-RBAC) and applied it for authorization management in collaborations by introducing the concept of virtual group. A virtual group is built for collaboration between multi-groups, where all members build trust relation within the group and are authorized to join and perform operations for the collaborative work [9]. Jian Cao proposed an organizational model and an authorization model for supporting dynamic business processes. More specifically, authorization policies are expressed in an SQL-like language which can be easily rewritten into query sentences for execution. In addition, the framework supports dynamic integration and execution of multiple access control polices from disparate enterprise resources [10].David Basin propose a modular approach to constructing modelling languages supporting this process, which combines languages for modelling system design with languages for modelling security. They also present an application to constructing systems from process models, where we combine a UML-based process design language with a security modelling language for formalizing access control requirements. From models in the combined language, they automatically generate security architectures for distributed applications [11].

5. SECURITY ARCHITECTURE

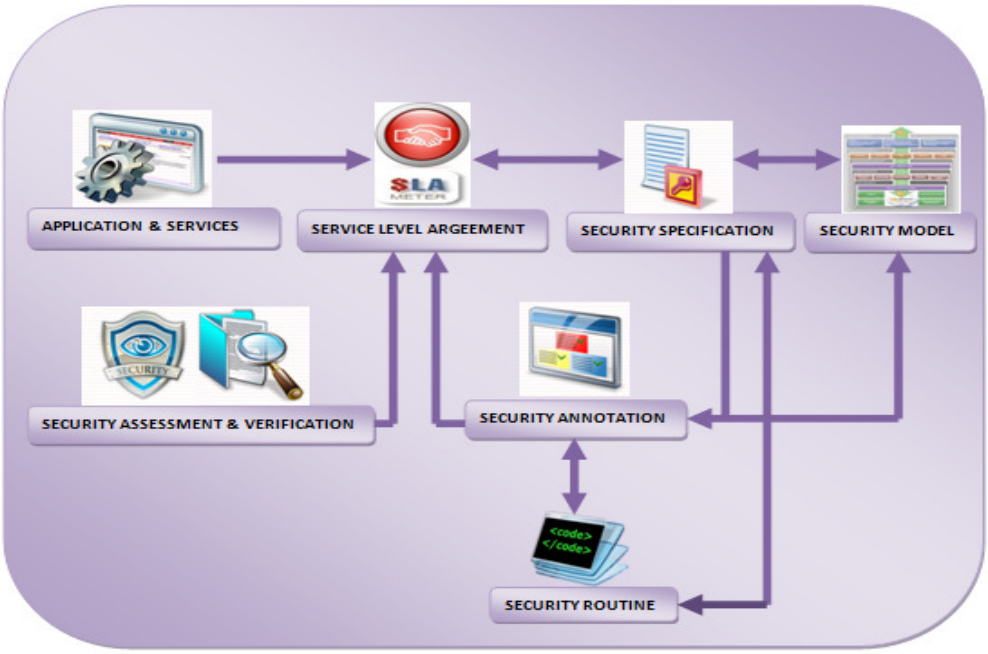

Figure 1. Security Architecture

The Security Specification is the requirements given by the customer and it's considered as input of the architecture. This Security Specification contains some implementation codes which are called as Security Routine. The Security Model contains many inbuilt existing models and these security models are compared with the Security Specification. Using the Security Routine, Security Annotation checks whether the customer requirements match with the existing models. If the security model satisfies all the requirements of the customer they provide the existing model or else the security analyst design a new model. The Service Level Agreement contains all the security agreements for the application and services. The Security Assessment and Verification verifies whether the Application and Services are secure based on the Service Level Agreement and generates the report on the level of security features. It is designed to help business owners, operators and staff to assess the security of their business. It covers potential areas of vulnerability, and provides suggestions for adapting your security to reduce the risk of crime against your business.

6. SECURITY POLICY MODEL

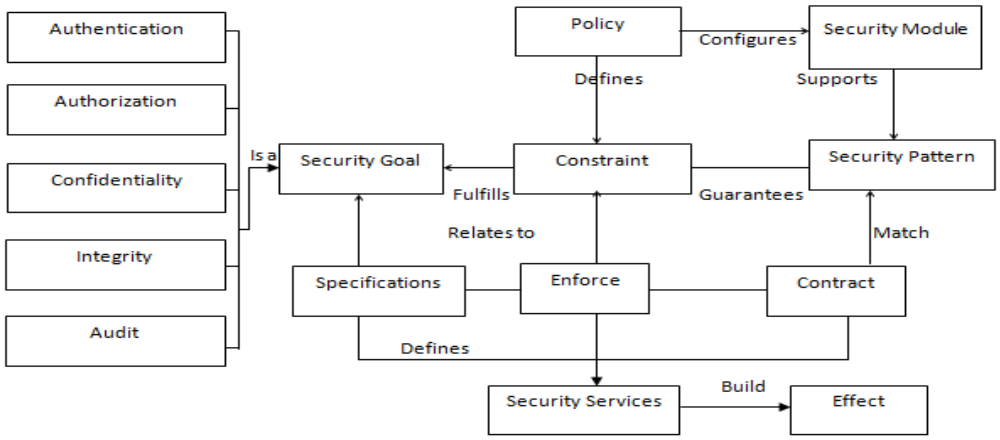

Figure 2. Security Policy Model

The security aspects can be defined by specifying a set of security goals, such as confidentiality, integrity, authentication, authorization and auditing. These security goals are defined in the context of a security policy. As indicated in above Fig.2 each goal is described by a constraint related to concerned entities .The basic entity in a security policy model is an Specification. The specification is defined as contract and it should match with the security pattern. Both the specification and contract enforces the security services to build the effect.

As shown in Fig.2 policies are interpreted and enforced by a security module that support specific security patterns to guarantee the defined constraints. Security patterns are used to map high level security requirements to concrete technical mechanisms that implement the enforcement of security constraints.

6.1 Authentication

The process of identifying an individual usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual. As shown in fig.3, The Administrator checks the User Credentials and it should match the predefined credentials using security algorithm and performs the Encryption and Decryption operation. Finally returns the Authentication Success or Failure.

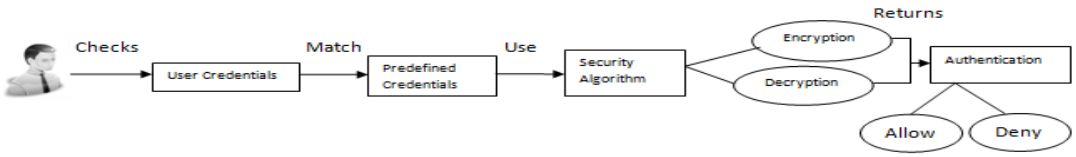

Figure 3. Authentication Model

6.2Authorization

Authorization is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth). Assuming that someone has logged in to a computer operating system or application, the system or application may want to identify what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is getting access. As shown in fig.4, The Administrator Identifies Roles & Access Permission of the User and matches with a Predefined Roles & Responsibility, if it matches allows the user to perform and make an entry in Audit log or else Deny.

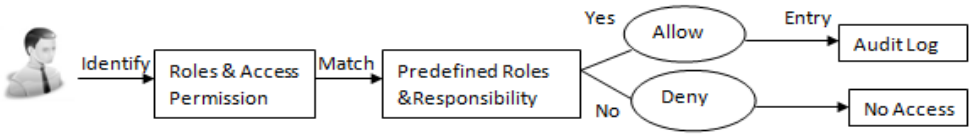

Figure 4. Authorization model

6.3 Confidentiality

Confidentiality is a set of rules or a promise that limits access or places restrictions on certain types of information. Confidentiality is the protection of transmitted data from passive attacks. With respect to the content of a data transmission, several levels of protection can be identified. The broadest service protects all user data transmitted between two users over a period of time. As shown in fig.5, The data should be protected from unauthorized disclosure and the resources should be classified based on the level of confidentiality.

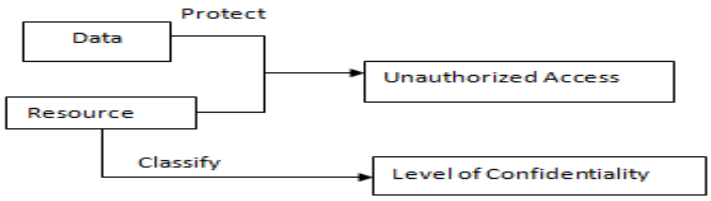

Figure 5. Confidentiality Model

6.4 Integrity

Integrity is the assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).As with confidentiality, integrity can apply to a stream of messages, a single message, or selected fields within a message. Again, the most useful and straightforward approach is total stream protection. As shown in fig.6, The Administrator monitors the Operation & Business Function and check the consistency of the operation. Finally the administrator ensures the Data and the Functional Integrity.

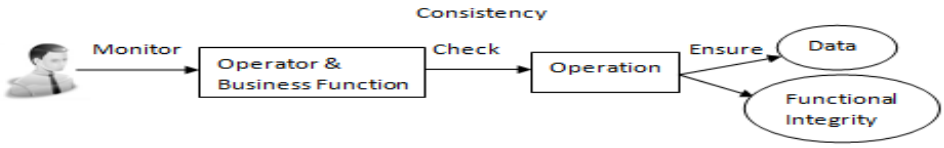

Figure 6. Integrity Model

6.5 Audit

The general definition of an audit is an evaluation of a person, organization, system, process, enterprise, project or product. The term most commonly refers to audits in accounting, but similar concepts also exist in project management, quality management, and for energy conservation. As shown in fig.7, The Administrator matches with the policy, constraint and rule

of the user and Audit every legal and illegal access on the resources as well as legal and illegal access by the user. If the access is legal then generate the report based on the audit result else diagnose the overall system security.

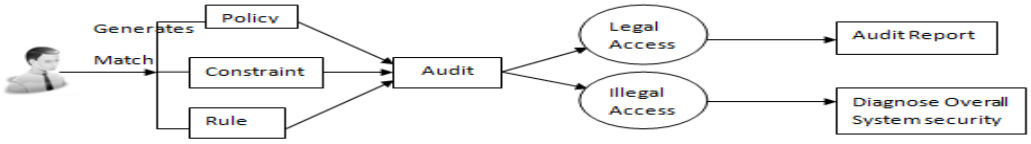

Figure 7. Audit Model

Authentication

<Authentication>

Algorithm =”RSA / SHA”

Operation = Encryption / Decryption

<Entity [Username, Password]>

</Authentication>

Authorization

<Authorization>

Algorithm =”RSA”

Operation = Permission Check

<Entity [User, Resource, Permission]>

</Authorization>

Confidentiality

<Confidentiality>

Algorithm =”SHA”

Operation = Protect, Maintain Level of Confidentiality

<Entity [Data, Resource]>

</Confidentiality>

Integrity

<Integrity>

Algorithm =”SHA”

Operation = Consistency check

<Entity [User, Business function]>

</Integrity>

Audit

<Audit>

Algorithm =”Matching”

Operation = Matching

<Entity [Policies, Constraints, Rule]>

</Audit>

7. FRAMEWORK FOR SECURITY ASSESSMENT AND VERIFICATION

Service Request can be of two types, new services with security model or existing services with Add-on security model. In our scenario we provide an Add-on security model which can be interoperable with new or existing business services acquired from our service provider. The Requirement Analyzer will analyze the Requirement of the Customer and the Service Request will intimate what service the customer needs. Security Requirements is the major component which will insets the security features for recommend business services. Service Request will give the requested service to the Service discovery Engine and it will insets what type of service suitable for the request made by the customer and the service selected will be managed by the Service Repository. The Service Description is for all the user using the service but Service profile is for the Service provider which content the business logic for the particular business service. Security requirements will then be analyzed in two steps the first one is the functional analyzer it will analyze the functionality of the security requirement for the recommend services. The second is security analyzer it will analyze the security features for the requested services. After analyzing the two steps for the requested services the main thing is to select the suitable security model, security policy and security requirement. From the security model we generate the schema which will intimate how the model will work and what operation the model performs. The schema generator also as the security template for the suitable security model and the schema will be added in the SLA planner in the form of contract and policy in order to reduce the overhead between the consumer and the service

provider. Once the schema is added in the SLA planner Security recommender will suggest the appropriate security service for requested business service based on the security specifications.

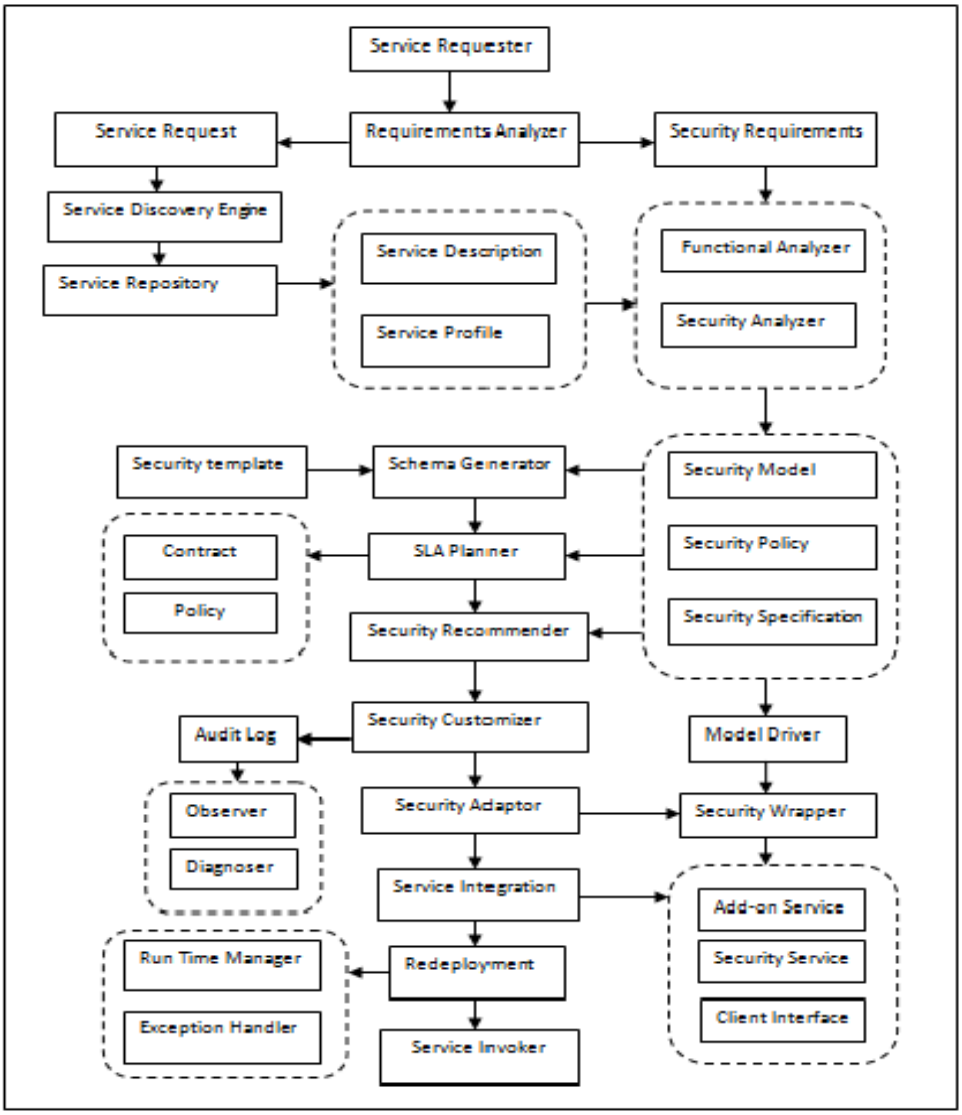

Figure 7. Framework for Security Assessment and verification

These security services can also be customize according to the need and requirements of the consumer using security customizer. The Audit log verifies whether the customized security services meet the consumer request and match with the security models using the Observer and Diagnoser. As the name insets Observer will observe the operations or mechanism take place while working where as Diagnoser will analysis overall security model. Security Adaptor is a special object that can be plugged to an existing class or function to change its behavior and control whether the Model is secured based on the specification and requirements. The Model Driver will drive a specific model for the consumer requirement and give the model as input to Security wrapper. Security Wrapper is an adapter program that converts plain XML exchanges to and from SOAP with WS-Security. It's designed to be used by applications which need access to secure Web services but do not have full SOAP

implementations available. The Wrapper serves as an intermediary for the application, adding SOAP and WS-Security to their input messages for submission to the service, then verifying the WS-Security on the response and sending the actual response message data back to the application. Service Integration is used to integrate the Add-on service, Security Services and Client Interface to the consumer dynamically in order not to take much effect. Redeployment does in two ways Run Time Manager and Exception Handler. Run time Manager will run the security model along with the business services dynamically where as the exception handler will look after the bugs and error in the service. The final step is the Service invocation is done based on the request of the consumer by the service invoker.

7.1 ALGORITHM

i. Get Service Request

$$R=(WS_{req},S_{req})$$

ii. Get Security Requirement

$$S_{req}=(S_{method},S_{policy},Context)$$

iii. Analyzer Security Requirement

$$Compare\ [S_{req}=(S_{method},S_{policy},Context),\ (S_{model},S_{policy},S_{spec})]$$

iv. Find Service & service Profile

$$ws_x=Lookup(Registry[ws_1,ws_2,ws_3,\ldots..ws_n])$$

$$ServiceDiscription(ws_x)=\ Match(ws\_profile,wsdl\_repository)$$

v. Extract Service Functional

$$Ws_x=Extract[ws_x(businesslogic,systemlogic,securitylogic)]$$

vi. Call Security Analyzer

$$Compare\ [S_{req}=(S_{method},S_{policy},Context),\ (S_{model},S_{policy},S_{spec})]$$

$$ServiceDiscription(ws_x)=\ Match(ws\_profile,wsdl\_repository)$$

$$Ws_x=Extract[ws_x(businesslogic,systemlogic,securitylogic)]$$

vii. Choose Security Model-ensure security Policy

$$Select(S_{models},S_{ploicy})$$

viii. Generate security specification

$$S_{spec}=ws_x[S_{model},S_{schema},context]$$

$S_{schema}=[S_{propery},S_{Alg}]$

ix. Import Schema to SLA

$SLA=\{BusinessAgreement,S_{spec}\}$

x. Call SLA Planner

$Get(S_{schema},S_{spec},S_{req})$

$Ws_x= Match(S_{spec},S_{req})$

xi. Recommend Security models

$Set(S_{spec},S_{models})$

Set $S_{service}$

xii. Customize Security service

$Ws_x=customize(S_{service},S_{spec},S_{models})$

xiii. Call Observer

$Validate(S_{service},S_{req},S_{spec})$

xiv. Audit & confirm the SLA

$Record(S_{service},S_{req},S_{spec})$

xv. Invoke Security Adaptor

Call $S_{service},ws_x$

Generate proxy[Sservice]

xvi. Call Service Integration

Add-on$[ws_x,S_{service}]$

xvii. Verify Integration Policy

Compose$[Ws_1,S_{req}]$ where S_{policy}=true

xviii. Call Add-on Service, Proxy & Wrapper and client Interface

xix. Evaluate Security Assessment & Verification

xx. Generate Audit Report

8. CONCLUSION

In this paper, we proposed a model driven security assessment and verification for business service. The Security Assessment and Verification verifies whether the Application and Services are secure based on the Service Level Agreement and generates the report on the level of security features. We also proposed a security model that verifies confidentiality, integrity, authentication, authorization and auditing. It is designed to help business owners, operators and staff to assess the security of their business. It covers potential areas of vulnerability, and provides suggestions for adapting your security to reduce the risk of crime against your business.

9. REFERENCES

[1]Christian Wolter, Michael Menzel, Andreas Schaad, Philip Miseldine and ChristophMeinel, "Model-driven business process security requirement specification", (ELSEVIER) Journal of Systems Architecture 55, (2009) 211-223.

[2] N. Nagaratnam, A. Nadalin, M. Hondo, M. McIntosh, P. Austel, "Business-driven application security: from modeling to managing secure applications", IBM Syst. J. 44 (4) (2005).

[3] Alfonso Rodríguez, Eduardo Fernández-Medina, Mario Piattini, "Towards a UML 2.0 extension for the modeling of security requirements in business processes", in: TrustBus, 2006, pp. 51–61

[4] ShaziaWasimSadiq, Guido Governatori, KioumarsNamiri," Modeling control objectives for business process compliance", in: BPM, 2007, pp. 149–164.

[5] Michiaki Tatsubori, Takeshi Imamura, Yuhichi Nakamura," Best-practice patterns and tool support for configuring secure web services messaging", in: ICWS, IEEE Computer Society, 2004. pp. 244–251

[6] Dong Huang, "Semantic Policy-based security framework for business processes", in: Proceedings of the Semantic Web and Policy Workshop, 2005.

[7]Tom Goovaerts, Bart De Win, and WouterJoosen, A Flexible Architecture for Enforcing andComposing Policies in a Service-OrientedEnvironment, IFIP International Federation for Information Processing 2007, pp. 253–266.

[8]Carlos Gutiérrez , David G. Rosado and Eduardo Fernández-Medina, "The practical application of a process for eliciting and designing securityin web service systems", Information and Software Technology 51 (2009) 1712–1738.

[9] Qi Li, Xinwen Zhang, MingweiXu and Jianping Wu,"Towards secure dynamic collaborations withgroup-based RBAC model", Computers & Security 28 (2009) 260-275.

[10] Jian Cao,JinjunChen, HaiyanZhao and MingluLi, "A policy-basedauthorizationmodelforworkflow-enabled dynamic processmanagement", Journal of Network and Computer Applications 32 (2009) 412– 422.

[11]David Basin, Jürgen Doser and TorstenLodderstedt, "Model Driven Security for ProcessOrientedSystems", SACMAT'03, June 2003, Italy.

Authors

Thirumaran.M, working as Asst.Professor in Pondicherry Engineering College, Pondicherry, India, one of India's premier institutions providing high quality education and a great platform for research. He pursued his B.Tech and M.Tech in Computer Science and Engineering from the Pondicherry University. The author is specialized in Web Services and Business Object Model and possesses a very profound knowledge in the same. He has worked on evaluating web services based on various QoS criterias, establishing the Business Object Model and Business Logic System with respect to Web Service Computation, Web Service Composition and Web Service Customization. His flair for research has made him explore deep in this domain and he has published more than 20 papers in various International Conferences, Journals and Magazines. Currently he is working on developing a model for Business Logic Systems for various E-Commerce systems.

Dr. P.Dhavachelvan is working as Professor, Department of Computer Science, Pondicherry University, India. He has obtained his M.E. and Ph.D. in the field of Computer Science and Engineering in Anna University, Chennai, India. He is having around a decade of experience as an academician and his research areas include Software Engineering and Standards, Software Agents and Distributed Systems. He has published around 50 research papers in National and International Journals and Conferences. He is heading two research groups working towards to develop the standards for Attributes Specific SDLC Models & Design of Business Object Model and Evaluation of Web Services.

S.Abarna is pursuing second year M.Tech in Information Security Department of Computer Science and Engineering in Pondicherry Engineeringllege, Puducherry, India. She received her B.Tech degree in Information Technology from Pondicherry university in the year 2008. She is currently working in the area of Web services.

The name of the author is Thanigaivel. K, studying in Pondicherry Engineering College, Pondicherry, India. He received his B.Tech degree in Computer Science and Engineering from the Pondicherry University in the year 2009. He currently pursuing M.Tech., degree in Computer Science and Engineering at Pondicherry University and he is currently working in the area of Web services.