5th SASTech
Iran |Mashhad
May 12 - 17 | 2011
5th Symposium on Advances in Science & Technology

Security Model for Service-Oriented Architecture(SOA)

Photograph of Presenter

Soheila Nasimi; Dr. Amir-Masoud Bidgoli
nasimi.soheila@gmail.com
0902-1006

Abstract

The security threats of SOA include threats to services in general. Services can provid functionalities to users that were not available before the service was in place. In addition, services can exist beyond the organization's security perimeter. Since services use standards, a possible adversary can use flaws in these standards to attack the service. These threats prevented by introducing security principles into the SOA model. These principles include secure interaction, distributed identities and distributed policies. Secure interaction provides confidentiality and integrity of messages between service providers, service registry and the service client. Distributed identities are used as the basis to provide authentication, authorization, integrity and non-repudiation. Distributed policies are used for authorization and availability. A service client can be authorized to access a service provider, or can be authorized access the service registry.
In summary, the proposed model promotes security of SOA as we have eliminated principles that do not belong to SOA. Instead, we have added principles of security to the foundational principles of SOA. The proposed model is based on the existing concepts and principles of SOA as well as CIA. The reusability principle has to be excluded from the concept of SOA because this principle creates contradictory results and unnecessary interdependencies. Lastly, the environment we refer to is an attractive and collaborative service environment aiming to response to all requisites of enterprise Agility.

Key words: Service-oriented Architecture (SOA), Confidentiality Integrity Availability (CIA), security principles,policies.

1. Introduction

Service Oriented Architecture is an architectural paradigm that has gained significant attention within the information technology (IT) and business communities. This section provides an introductory understanding of Service-Oriented Architecture (SOA) and its relation to the CIA security triad (Confidentiality, Integrity and Availability). It also provides the reader an insight of the security issues that must be satisfied by SOA.

CIA triad

The traditional view of security is based on the principles8 of confidentiality, and integrity and availability .These three principles combined are referred to as the CIA triad. One of the most important references, which also use the CIA triad, is the ISO 17799 Standard . This standard consists of recommended information security practices for information security management. Because this article is used in a business setting, I will adhere to the ISO

standard, since this provides companies with a framework by which (information) security can be managed. As said before, security used in this thesis concerns information security. Therefore, in this thesis security is the preservation of confidentiality, integrity and availability of information (also see Fig 1 adapted from).

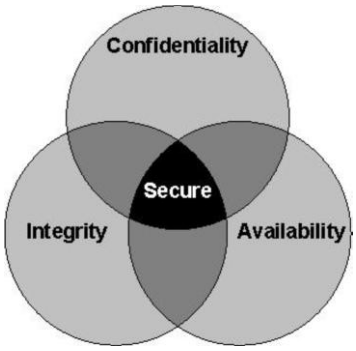

Fig 1: contains the three basic security elements

1. NASA: Security Enhanced Model for SOA

According to Pajevski (2004), SOA security issues can be resolved by mitigating risks caused by the increased exposure of services by using a two-fold approach. Firstly, to use a proxy service to insulate services from consumers and to split the service registry into public and private areas. By using this technique we can debilitate and also to an extent eliminate direct attacks. Secondly, by using access control techniques which limits what the users can do, whilst also limits the harm they can cause.
From the figure below, we can see that that the classic SOA Model (as shown in fig 2) has been upgraded with a set of proxy services;

 A public service registry for consumers which provides the location of all services.

 A private registry service for proxy and other trusted entities which lists the actual location of each provider.

We can see that all requests go through the proxy service and the proxy gets authorization before forwarding any requests. Also, the messages will be checked for its format and any malicious content.
Also, note that the system could have only one service registry, which reports different service locations depending on whether the requestor is a trusted proxy or not.

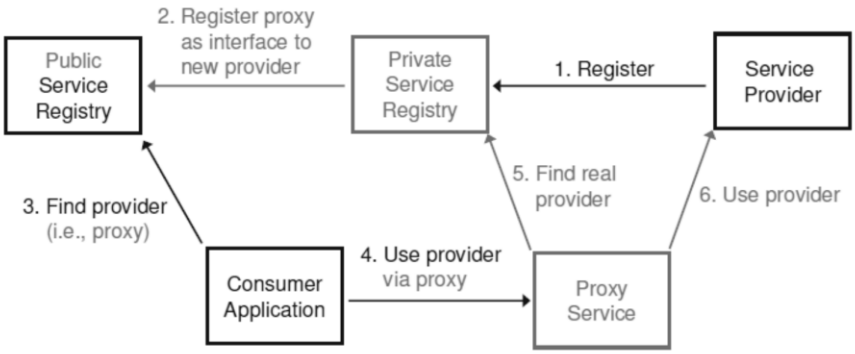

Fig 2: A "Security Enhanced" SOA Interaction Model (Pajevski, 2004)

2. IBM: SOA Security Reference Model

Nagaratnam et al (2007), define a SOA security model (see Fig 3) as a list of enabling capabilities. Here, the capabilities refer to the IT and business security services, enablers and supporting infrastructure. They suggest that a reference model helps to address requirements and lead to a logical architecture and then to a physical architecture, with products and technologies mapped to solve the problem. The reference model can be classified under three layers of abstraction described below (Nagaratnam et al, 2007);

 IT security services; These are the foundational building blocks for a SOA infrastructure, providing the ability to secure the services and meet the needs of applications and infrastructure. These include services like identity service, authentication service, authorization service etc.

 Security policy infrastructure; This infrastructure entails articulating, managing, enforcing and monitoring security policies. This includes the ability to authenticate and authorize.

 Business security services; These services involve managing the needs and requirements of the business, such as identity and access management, data protection, governance and compliance. They help to effectively manage the relevant policies applicable to meet the business needs.

 Security enablers; These include technologies like cryptography, directories etc. that would be utilized by the security services to perform their task.

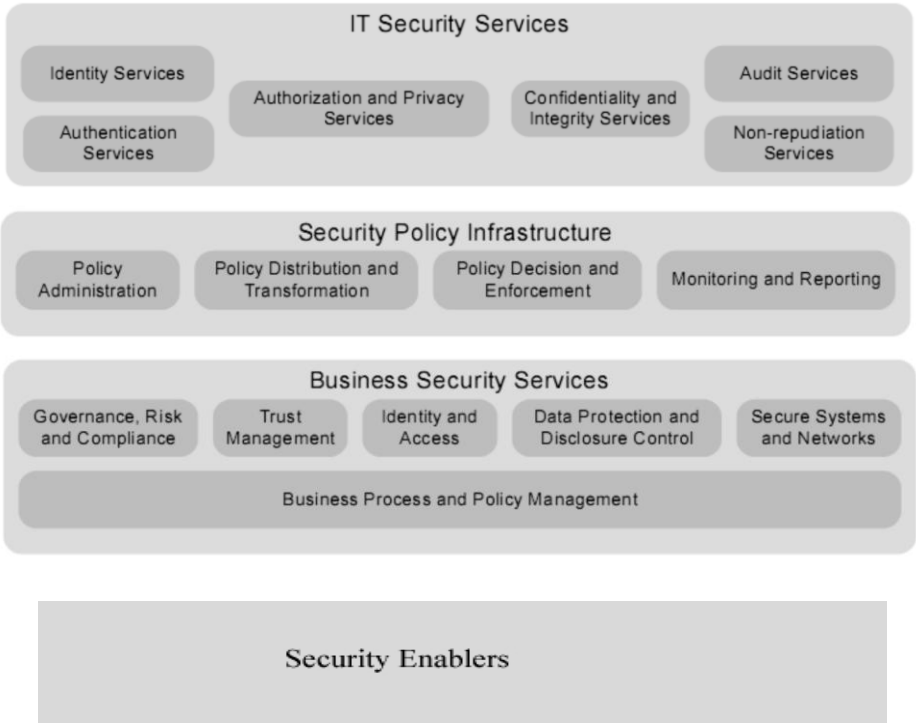

Fig 3 : SOA Security Reference Model (Nagaratnam et al, 2007)

4. NSTISS: Comprehensive model for securing Information Systems

The NSTISS20 committee defines “a comprehensive model for the security of information systems which also functions as an assessment, system development and evaluation tool” (NSTISS, 1994). This three-dimensional model illustrated below (see fig 4) attempts to address all security issues in an information system. The three

layers of security measures can be utilized to minimize vulnerabilities based on the threats to an information asset. There are several applications of this model which are listed in the sections below.
A user can make use of the model to identify vulnerabilities pertaining to the critical information characteristics (Confidentiality, Integrity and Availability). If a specific technology is available to fulfill one of these characteristics, the next logical step for the user is to determine the policy and practice, education, training and awareness etc. If a suitable technology cannot be identified, then the policy or practice must be adopted as the next likely solution. If none of these two layers can counter the vulnerabilities then as a minimum the awareness of this deficiency becomes important.
The model can also be used as an evaluation tool, where the evaluator identifies the different information states with the information system. After identifying all the states the evaluator can perform a review as discussed above. It must be noted that a specific vulnerability may be left unsecured if the evaluator determines that no threat to that vulnerability exists.

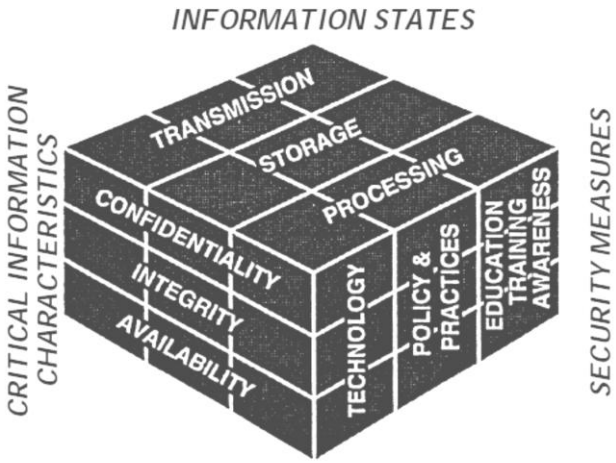

Fig4: Comprehensive Model for securing Information Systems (NSTISS, 2004)

The twenty-seven individual cubes created by the model can be extracted and examined individually (NSTISS, 2004). This can be useful for categorizing and analyzing countermeasures for security. It also serves as a tool for defining organizational responsibility for information security. The NSTISS security model acknowledges information and not technology, as the basis for our securing information systems.
Create security model for soa

5. Creating propositional model for SOA security

This section describes the SOA security model.the SOA security model consisting of four dimensions i.e. security measures and concepts, informational tasks and capabilities are described below (see Fig 5). This model attempts to address all security issues in a SOA business environment as follows;

- The first dimension of the SOA security model consists of explicit security measures and concepts such as: Confidentiality, Integrity, Availability, Authentication, Authorization, Identity, Auditing and Compliance, etc.

- The second dimension of the SOA security model consists of informational tasks such as: Transport security, Message security, Application security, Data security, Knowledge security, Control security etc.

- The third dimension of the SOA Security model deals with the requisites of capabilities such as: Education, Training, Awareness, Mutual understanding, Practices etc.

- The fourth dimension of the soa security model consists of security policies such as:discretionary access control(DAC),mandatory access control(MAC),role based access control(RBAC),$UCON_{ABC}$.

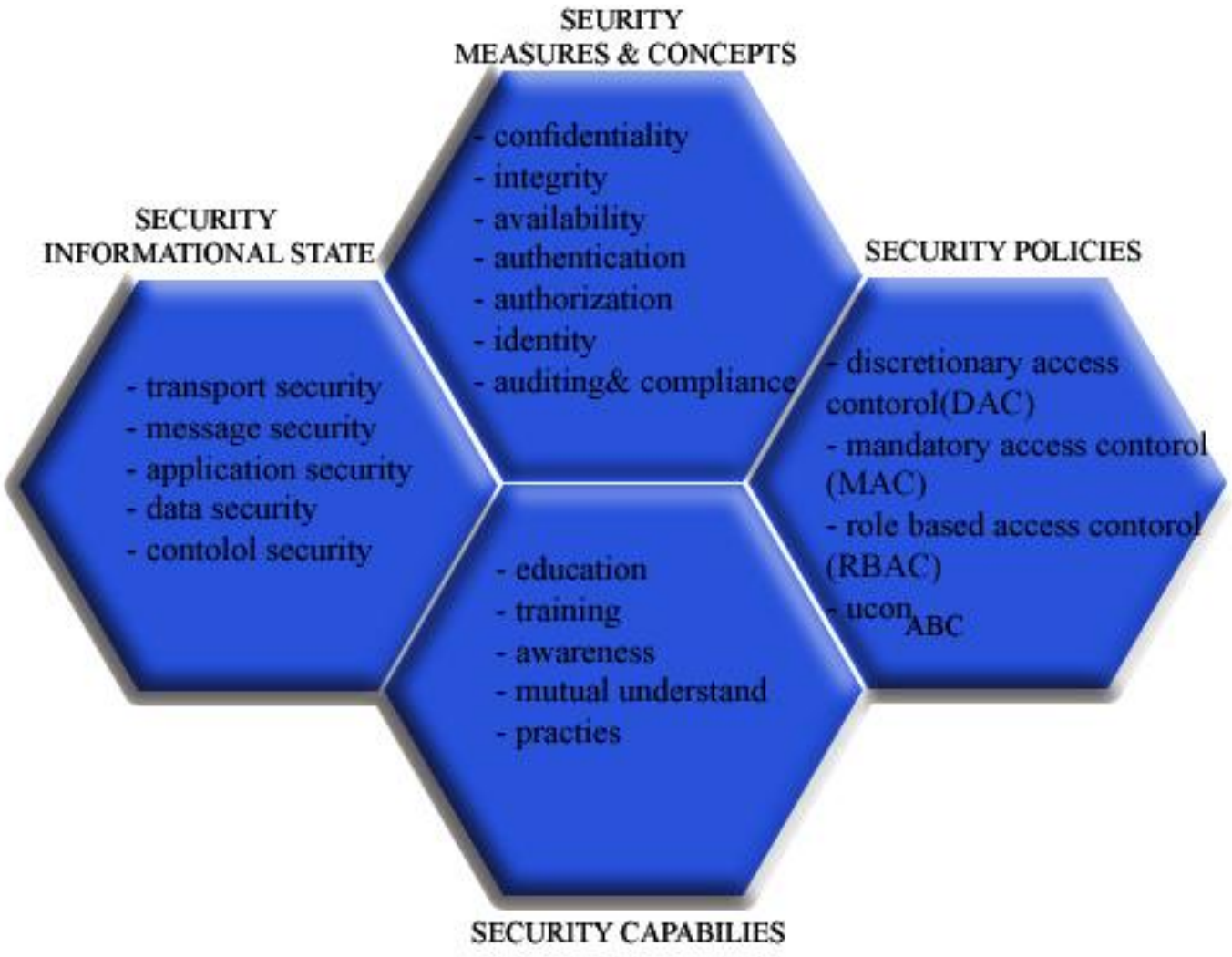

Fig4: propositional model for SOA security

In the model We add four of the most important Policy Models with respect to their ability to cope with complex Authorization Policies. Authorization restricts access to authenticated entities
holding the privileges to perform an action on a resource. AuthorizationPolicies define the rules of what is allowed and what is not. They are enforcedat the various service providers' endpoints through a security infrastructureacting as a single point of entry – a so-called Policy enforcement Point– into the security domains. Prior to granting access to a resource the requester is authenticated and then assigned privileges according to the underlying Security Model. The infrastructure decides by checking upon assigned privileges captured in executable XML policies whether to grant access or not. In SOA, the administration of these endpoints is a crucial issue. Endpoints not only need to be aware of the technology used to enforce security at the interaction partner's end .but they also need an efficient concept to dynamically manage these privileges.The efficient administration of Authorization Policies in distributed environments is a pivotal criteria for the choice of an appropriate Security Model.

- discretionary access control(DAC)

In DAC based systems, users in possession of an object are considered to be the owners of the resources. They have full control over the resource. This enables them to use objects they own as they wish, and, for example, to delegate access rights deliberately to any further user.

- mandatory access control(MAC)

In MAC based systems, users and their rights are enforced by a central mechanism (e.g., the operating system) and administered by a central authority(e.g., the system adminsitrator). Users do not have the ability to override thepolicy.
MAC is traditionally associated with multi-level secure systems. The concept of MAC is realized by assigning security labels to data elements at veryfine-granular levels, thereby expressing their security sensitivity and assigning clearance levels to subjects. In MLS, less-sensitive information can be accessed by higher-cleared individuals, and higher-cleared individuals can share"sanitized" documents – where sensitive information that the less-cleared individual is not allowed to see is removed– with less-cleared individuals.

- Role Based Access Control (RBAC)

RBAC enforces access control according to access policies, which define a number of roles and assign permissions to roles. Subjects are assigned one or more roles. A role hierarchy defines inheritance relations between roles.The principal motivation of RBAC – this is to provide administrative convenience – can be further strengthened by using RBAC to manage RBAC. Many approaches analyse the application of RBAC to workflow management even taking distributed scenarios into account The limitations .

- $UCON_{ABC}$

$UCON_{ABC}$ is a comprehensive policy model for usage control. It extends
traditional access control models in two respects:
1. continuity of access decision, and
2. mutability of attributes.

2.Conclusions

The main purpose of this article is to create a model of security which can define a secure, attractive and collaborative SOA-environment. Also, in order to create and verify this model the managerial and governance aspects of SOA also needs to be considered as it plays a cardinal role in shaping the SOA business environment. This study demonstrates that there are several aspects of security not covered by the foundational principles of security. These security requirements of SOA include Authentication, Authorization, Identity, Auditing, Compliance and Security Policies along with the primary security requisites Confidentiality, Integrity and Availability. it is important to satisfy all these requirements in order to secure a SOA environment comprehensively.

3.References:

1-Maclinovsky, A. (2007, November 15). A Formal SOA Security Model. Message posted to http://blogs.sun.com/RealSOA/entry/soa_security_model

2-Maclinovsky, A. (2007, November 15). Security Model Details. Message posted to http://blogs.sun.com/RealSOA/entry/security_model_details

3- Kingkarn K. (2008). An Integrated Model for SOA Governance. Unpublished master's thesis, IT University of Göteborg. Retrieved January 10, 2009, from http://gupea.ub.gu.se/dspace/handle/2077/10495

4- Pajevski, M. (2004). A Security Model For Service-Oriented Architectures [Data file]. Retrieved March 10, 2009, from NASA Web site: http://www.oasis-open.org/committees/download.php/17573/06-04-00008.000.pdf

5- IBM. (2007, November). Understanding SOA Security - Design and Implementation. Retrieved from http://www.redbooks.ibm.com/abstracts/sg247310.html

6- Peterson, G. (2008, February 9). Security in SOA - It's the Car, Not the Garage. Message posted to http://www.soamag.com/I15/0208-2.pdf

7- [Haf09] Hafner, M. Breu, R. Security Engineering for Service-Oriented Architecture. Springer. 2009.

8- Mitra, T. (n.d.). Layered architecture view. In Documenting software architecture, Part 3: Develop the architecture overview. Retrieved June 27, 2008, from IBM Web site: http://www.ibm.com/developerworks/library/ar-archdoc3/index.html