Security Issues for Intelligence Information System based on Service-Oriented Architecture

Jugoslav Achkoski [1], Vladimir Trajkovik [2] and Danco Davcev [3]

[1] Military Academy „General Mihailo Apostolski“,
Str. Vasko Karangelevski bb, 1000 Skopje, Macedonia
jugoslav_ackoski@yahoo.com
[2, 3] Faculty of Electrical Engineering and Information Technologies,
Str. Rugjer Boshkovik bb, PO Box 574 1000 Skopje, Macedonia
trvlado@feit.ukim.edu.mk, etfdav@feit.ukim.edu.mk

Abstract. Security is important requirement for service-oriented architecture (SOA), because SOA considers widespread services on different location and diverse operational platforms. Main challenge for SOA Security still drifts around “clouds” and that is insufficient frameworks for security models based on consistent and convenient methods. Contemporary security architectures and security protocols are in the phase of developing. SOA based systems are characterized with differences in security implementation as an encryption, access control, security monitoring, security management through dissimilar domains etc. Domains have services as endpoints in the information systems, which usually form composite services. The workflow which is established through composite services is extending on different endpoints in different domains.
This paper main aim is to give contribution in developing suitable security solution to Intelligence Information System using web service security standards in order to reach appropriate level of information security as an authentication, authorization, privacy, integrity, trust, federated identities, confidentiality and more.
Our paper uses approach in which useful information provided by the services is send out directly from the creators of information to the consumers of information. We introduce security and logging system that can be used as verification and validation middleware.

Keywords. SOA, Intelligence Information Systems, security.

1 Introduction

Intelligence as a service has a great significance for any country. An information system for supporting intelligence activities should be used on daily basis and has a great influence in senior decision making process. Usage of the modern information technology in big way contributes for improvement of the process (activities) which are supporting intelligence cycles (planning, collecting, analyzing and dissemination). Although there is constant improvement as a result of the progress in the area of information technology, significant difference in the quality of work in the field of intelligence has not taken place in the last ten years.

Implementation of Service Oriented Architecture – SOA, i.e. the usage of SOA provides possibilities for making new opportunities in the form of expanded solutions for designing intelligence information systems, regarding the more efficient management of information, as well as their use by the end users for whom hum they are intended. In order to keep up with the pace with contemporary development, planning on short, medium and long term is needed for development of information systems for supporting intelligence, in relation to IT development.

Security systems should afford business application to fulfill necessary users' requirements in order to reach security goals: authentication, authorization, federative identity, privacy, integrity, accessibility, non-repudiation in terms of sending and receiving messages to users.

In this paper, we propose security solution for Intelligence Information System completely based on SOA. Our paper uses approach in which useful information provided by the services is send out directly from the creators of information to the consumers of information. We introduce security and logging system that can be used as verification and validation middleware.

This contribution is organized by following. Section 2 presents contemporary approaches for SOA based systems. Section 3 gives description for frequently used security protocols for web services such as XML, XML encryption, XML signature, SAML, SOAP and other standards within WS-Security family. Model of Security Solution for Intelligence Information System-Based on SOA and its implementation is presented in Section 4. Concluding remarks are given in a last section, Section 5.

2 Related work

In [1] authors projected that 90% from external attacks on applications refers to security vulnerabilities and mis-configured systems. Because it is not possible to develop 100% secure applications, it is convenient to analyze threats, vulnerabilities, risks and implementing secure mechanisms will be solution for SOA based systems. This security solution will improve security through entire system, and it will give contribution in decreasing incident response costs, application outage costs, cost of fixing, reputation damage costs, etc. Also, the paper gives directions for implementing security integration and access control in SOA and WSOA initiatives. In the paper following subjects are presented: The different Access control models, A meta-model for WSOA (Web service-oriented architecture), Goals of SOA Security, SOA Security implementation models, Industry standards for SOA Security and SOII (Service-Oriented Information Integration), standards for SOII.

The [2] explains that securing service-oriented systems is challenge, because security services are equally distributed as a workflow services in SOA based systems. Establishing security only on endpoints is not adequate security solution for SOA systems. On the other hand, implementing security services on each endpoint is expensive solution. Currently, there is little work done to separate security from endpoints of services. As a solution is given model of *Security As A Service* (SAAS), which exceeds security burden on the endpoints using shared security services within security domain. Security services are composed of integrated components based on

Service Component Architecture (SCA) models. In the paper SAAS paradigm is used and it is implemented in securing SECTISSIMO platform. Referent security architecture for protecting critical SOA systems based on paradigm *Security As A Service* (SAAS) is presented in the paper.

In [3], authors have introduced the SAAS approach and proposed a Security Decision Service (SDS), which provides service-based PDP to multiple enforcement points.

A more comprehensive discussion is given in [4] for implementing authentication, trust and secure conversation as separate services to solve security manageability and interoperability problems.

Considering big picture for SOA Security, it is important to understand different aspects for security, role of AAA (Authentication, Authorization and Auditing) in SOA Security and their implementation as industry standards. Special attention need to be given to web service security because web services are widespread in implementing SOA paradigm [1].

Since usage of SOA increasing, the limitations of using services are decreasing and it becomes comprehensive approach for using bottomless applications. In order to reach real reusability of services, organization should give access to the services on third parties, partners and end-users through unsecure network as Internet. Services are organizational property and without proper security measurements and level of threat for organization [5] increases in form of unauthorized access, misuse of services, overuse of services and hacker vulnerability.

To achieve above SOA based systems should consider security requirements and goals in the certain level due to process of their creation and planning.

3 Security Standards and Specification for Web Services

Web Services and Web Services Security are basis on several standards that should be presented in order to be selected appropriate solution for security in information systems which are based on service-oriented architecture.

XML Signature. XML Signature provides integrity and authentication for XML data using digital signature and it can be used in any digital content. Basic usage of XML Signature within Web Service Security is to provide integrity for digital signature on XML message and to prove signer identity.

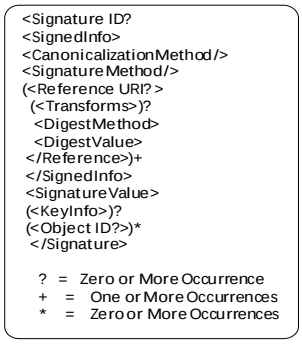

Figure 4 Informal XML signature syntax[6]

XML Signature is presenting itself as a XML. XML Signature consists following elements:

- Signature consists element that identifies digital signature;
- SignedInfo consists references for data and it determines whether are data digitally signed;
- CanonicalizationMethod refers to manner which element SignedInfo is prepared before signature is calculated. Reason about it is that different platforms can interpreted data in a different way (e.g., carriage returns <CR> versus carriage return/line feeds <CRLF>) so that can cause signature to be coded differently in different platform;
- SignatureMethod refers to algorithms which are used for creating or validating signature as a *dsa-sha1* and it is used for DSA algorithm and SHA-1 function for hashing;
- Reference element is complex but the most important is that it refers to data which should be signed and it is embedded in XML data or uniform resource identifier (URI) which refers to external data as document, web site or other digital content. In addition, Reference element determines transformation which will have influence to the content of hash function (via DigestMethod). As a result, there is hash value stored as DigestValue;
- SignatureValue is genuine computed value of signature. Rather than digitally signing content, signature is computed with element SignedInfo, so that all references, algorithms and resultant values are digitaly shared signed which provide integrity of signed data;
- KeyInfo allow consumer to receive key to approve signature if it is necessary. Structure of this function is very complex;
- Object element consists illogical XML data which can be referenced within method SignedInfo. It can include Manifest element which provides varied list of references, where integrity of list is validated itself and integrity of the actual items will not validate the signature. The purposes of this list is to include list of the items which should be in relation to Manifest element. Also it defines SignatureProperties element where other properties of signature are stored e.g. time and date when signature is created;

```
<Signature Id-"MySignature"
xmlns="http://www.w3.org/2000/0 9/xmldsig#">
<SignedInfo>
<CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/REC-xml-d4n-
20010315"/>
 <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#dsa-shal"/>
<Reference URI="http://www.company.ccm/file.doc">
<Transforms>
<Transform
 Algorithm="http://www.w3.org/TR/2001/REC-xml-cl4n-20
010315"/;
 </Transforms>
<DigestMethod
Algorithm="http://www.w3.org/2  0 0 0/0 9/xmldsig#shal"/>
<DigestValue>j90j2fnkfew3...</DigestValue>
</Reference>
</SignedInfo>
<SignatureValue>GFh8fw3greU...</SignatureValue>
 <KeyInfo>
 <KeyValue>
<DSAKeyValue>
<P>. . .</PXQ>. . .</QXG>. . .</GXY>. . .</Y>
</DSAKeyValue>
</KeyValue>
</KeyInfo>
 </Signature>
```

Figure 5 XML signature example [6]

Standard XML Signature defines three types of digital signatures: *enveloped*, *enveloping*, and *detached. Enveloped* signature refers to signature of XML data whether Signature element is in XML body. *Enveloping* signature consists XML content which is signed where Object element is used for signing data. Detached signature signs content that is external for XML signature defined by the URI.

XML Signature allows each type of digital content to be signed and used together with Web Services Security standards.

XML Encryption. According to design, XML has simple text format without embedded security. XML Encryption provides confidentiality of data through mechanisms for encrypting XML content where is used symmetric encryption key. Techniques for exchanging keys are based on cryptography for exchanging public keys which is provided secrecy for the key. Typically symmetric key is embedded within XML message in cryptographic form, URI or it is considered through key exchanged data. Because public key is very slow, symmetric is used to encrypt data for performance reasons.

```
<EncryptedData Id? Type? MimeType? Encoding?>
<EncryptionMethod/>?
<ds:KeyInfo>
<EncryptedKey>?
<AgreementMethod>?
<ds:KeyName>?
<ds:RetrievalMethod>?
<ds:*>?
</ds:KeyInfo>?
<CipherData>
<CipherValue>?
 <CipherReference URI?>?
</CipherData>
<EncryptionProperties>?
</EncryptedData>

? = Zero or One Occurrence
+ = One or More Occurrences
* = Zero or More Occurrences
```

Figure 6 Informal XML encryption syntax [6]

Also, XML encryption is presented as a XML. The structure of XML encryption conseiders following elements:

- EncryptedData is element which identifies that it is encrypted data;
- EncryptionMethod defines encryption algorithm which is used for encrypting data as a Triple-DES (3DES). This is optional element and if it is not present then the recipient must now which algorithm is used to decrypt data;
- ds:KeyInfo has information for encrypted key which was use for message encryption, so that actual key is embedded in encrytped form or there is information which affords key to be derived or located;
- EncryptedKey has encrypted form of key which should be shared with others. As previous mentioned, this type of key will be encrypted using public-key cryptography. There is possible to be more recipients for key, but for each of them have encrypted key element;
- AgreementMethod is alternative way for sharing key using Diffie-Hellman method. This method allows key does not to be embedded or shared in EncryptedKey element.
- ds:KeyName provides additional way for sharing encryption keys according to their name;
- ds:RetrievalMethod is method for retrieving encryption key form fromURI reference, whether it is in XML or external to it;
- ds:* refers refers to other information for keys which are emerging as a X.509v3 keys, PGP keys, and SPKI keys;
- CipherData has encrypted data where CypherValue consists data encrypted with base64 text or it uses CypherReference that refers to location of encrypted data in XML;
- EncryptionProperties consists additional properties as date and time for encryption;

```
<EncryptedData
xmlns='http://www.w3.org/2001/04/xmlenc#'
Type='http://www.w3.org/2001/04/xmlenc#Element'/>
<EncryptionMethod
Algorithm='http://www.w3.org/2001/04/xmlenc#tripledes-
cbc'/>
<ds:KeyInfo
xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
<ds:KeyName>John Doe</ds:KeyName>
 </ds:KeyInfo>
<CipherData><CipherValue>F59E7F12</CipherValue></Cip
herData>
</EncryptedData>
```

Figure 7 Example of an XML-encrypted message [6]

Figure 7 presents example for XML encrypted message. Encrypted data are located in CipherValue element. Together, XML Signature and XML Encryption standards form basis on which WS-S standards rely.

Security Assertion Markup Language [7] Together, SAML, XML Signature and XML Encryption are used to achieve integrity, confidentiality, authentication and SAML assertion in SOA based information systems. SAML uses XML for establishing communications between organization or entities in separated security domains within user's identity, user's properties and user's attributes.

SAML allows entity or organization to guarantee for user identity through SAML assertion. SAML assertion can be presented as a proof for identity of another entity to establish relations of trust. This is very important for SOA, because services are located in different companies and security domains. Previous mentioned Concept presents basis for federative identity, which protects organization and improves security management in order to accomplish authentication and identity to other organizations.

SAML make possible to be solved several problems:

- Web single Sign-on – user can access on certain web site and to continue on following web site using same SAML assertion from previous web site;
- Delegated identity – user's security clearance can be used in end-point service or web site from initial service or web site;
- Brokered Sign-on - mediating security service controls user's authentication. An attributes gained from mediating security services can be used in accessing on different web sites;
- Authentication - based authorization – user attributes are embedded in SAML assertion.

Within SAML assertion can be embedded information for user identity as a e-mail, X.509, name of subject, employer's ID or other attributes. For privacy purpose, SAML 2.0 introduces concept of pseudonyms or identification by pseudonyms which can be used instead of another identification type in order to hide personal information. SAML provides two methods for confirming subject identity. First method is "holder key" where message sender (subject) holds key which was used for digitally signing message. Another method for confirming subject identity is "sender-vouches", which means that digital signature was created by third party security service.

Description of SAML has intention to describe its usage in SOA. Increasing confidentiality between service providers, SAML provides loose coupling and service independents with respect to user identity. As a security token, SAML is connected to WS-S standards.

Web Services Security Standards.[8] In order to be presented more comprehensible approach for Web Services Security protocols and how they are shaped it is needed to see following illustration (Figure 8). Diagram shows that XML Signature, XML Encryption and SOAP are basis for Web services Security standards.

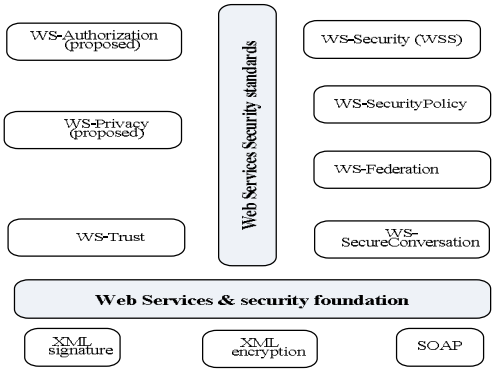

Figure 8 WS-S standards

Figure 8 shows that WS-Security protocol is complex, so that establishing SOA Security for information system designers is not simple task. WS-S [9],[10] standards are placed in SSL and security firewall policies in order to provide point-to-point security for SOA messages. Fortunately, tools are available to simplify integration of security into Web services and SOA.

4 Model of Security Solution for Intelligence Information System-Based on SOA

In Figure 9 are presented two flows by following order: control flow (blue direction) and data flow (red direction). XML Signature standard is used in control flow to validate security policies. XML Encryption is used in data flow to validate security policies.

Our solution for service security enables application of standards described in section 3 . In order to simplify the description, in the proposed model we do not explain how policy for digital certificate is incorporated, because it is possible to conclude that they are placed in Intelligence Information System (IIS) Center.

Furthermore, in Figure 9 are described two flows which are significant for IIS by following:

- control flow;
- data flow.

In both cases information flow through three phases:

1. Request phase – identifying information requester and registering request with the purpose of establishing security mechanism described in Section 3;

2. Verification phase – identifying requester and its security mechanisms are appropriate for gaining response according to security policies related to information;
3. Notification phase – according to security mechanisms and policies, requester for information is notified for access to use information form services or requester is notified that access is denied sending forward cause in terms of security policy.

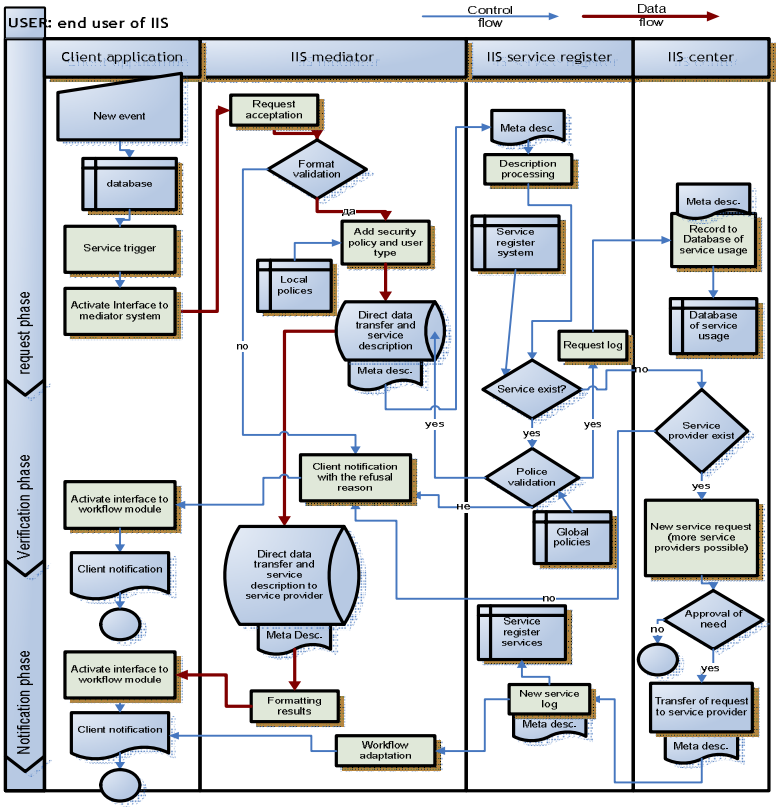

Figure 9 Model of Security Solution for Intelligence Information System

Requested information flows form source to the information requesters, going to mediation component which serves for connecting and formatting security systems in institutions. Mediation component is important for IIS, because it can be connected to more information systems which are embedded in heterogonous environment. Requested information is encrypted and it has unique security policy. Although IIS Center and System registry are not involved, they play important roles in control flow.

Control flow establishes three functions:

1. Recording information requester in terms of date and time, location and type of user who requests for information;
2. Validation to security policy of user type called requester of information and security policies attached to the information;

3. Recording each request which is not followed with information at moment of request. This third function is interested for information system designers on future services.

Highly structured suggested model of Security Solution for Intelligence Information System not only interpolates security a mechanism also provides by following:

- Effective data transmission endorsing data encryption and data formatting on appropriate level;
- Recording each request whether it is inserted in database or not, furthermore it has appropriate security policy or not. This supports recording possible disruption of security policy.
- Flexible scalable mechanisms and mechanisms for extending services which are located in IIS Registries.

CONCLUSION

In this paper, we presented Model of Security Solution for Intelligence Information System based on SOA paradigm, which provides secure data flow through information system, without any consequences to the security policies in terms of authentication, integrity, authorization, confidentiality and non-repudiation.

Proposed model affords recording all request and disruption of security policies on appropriate manner. In this paper we present structured solution that is easy adoptable but considers all contemporary security policies and protocols.

References

1. Torry Harris Business Solutions Inc. US, White Paper "Migration and Security in SOA", Distributed Systems & Services Group, University of Leeds, 03.03.2009 http://www.thbs.com/pdfs/Migration_and_Security_in_SOA.pdf, Consulted of April 19 2011
2. Mukhtiar Memon, Michael Hafner, Ruth Breu. "Security as a Service - A Reference Architecture for SOA Security", Security in Information Systems, Proceedings of the 7th International Workshop on Security in Information Systems, WOSIS 2009, In conjunction with ICEIS 2009, Milan, Italy, May 2009. INSTICC Press 2009, ISBN 978-989-8111-91-3
3. M. Hondo H. Hinton and B. Hutchison. Security Patterns within a Service-Oriented Architecture, 2005.
4. R. Kanneganti and P. Chodavarapu. *SOA Security in Action*. Manning Publications Co., Greenwich, CT, USA, 2007.
5. R. Breu, M. Hafner, F. Innerhofer-Oberperfler, and F. Wozak. Model-Driven Security Engineering of Service Oriented Systems. *Lecture Notes in Business Information Processing*, 5(5):59–71, 2008.
6. Harold F. Tipton, . Micki Krause, "Information Security Management Handbook", Sixth Edition, - Hardback 456 pages, Auerbach 2008
7. OASIS. Security Assertion Markup Language (SAML), 2005. http://www.oasis-open.org .
8. Oracle. Service-Oriented Security: An Application-Centric Look at Identity Management, 2008. http://www.oracle.com/
9. OASIS. WS-Trust Sepcifications, 2005. http://docs.oasis-open.org/.
10. OASIS. WS-SecurityPolicy, 2007. http://docs.oasis-open.org/