Design and implementation of multilevel security subsystem based on XACML and WEB services

Jacek Jarmakiewicz  
Faculty of Electronics  
Military University of Technology  
Warsaw, Poland  
jarmakiewicz@wat.edu.pl

Tomasz Podlasek  
C4I Systems Department  
Military Communication Institute  
Zegrze, Poland  
t.podlase@wil.waw.pl

Abstract – Controlled sharing of confidential information in military environment, especially as a part of joint and coalition forces, is an important mean to achieve the network-centricity goals. During last few years a technology for building the Service-Oriented Architecture has been developed. The Service-Oriented Architecture maps the concept of distributed service-oriented processing. It is a good application framework for integration of heterogeneous military systems. However, these systems could process the confidential data divided onto hierarchical classification levels. We can rise up the question: can Service-Oriented Architecture serve as a middleware layer to integrate such systems?

The paper presents selected cases of information systems cooperation in systems federation. We developed the functional mechanisms according to XACML architecture and we proposed necessary attributes for users and data, what enabled to control information exchange and to authorize users to access sensitive information resources.

The developed MLS implementations were tested in terms of interoperability in the consortium and domestic test environment. In June 2012, both the implementations services were successfully tested in an international test environment during testing of interoperability with foreign partners (Germany) and NC3A agency in the NATO Secret network during CWIX 2012 exercises.

Keywords: Information sharing, Multi Level Security, XACML, SOA, WEB Services, Common Operating Picture, C4I Systems

I. INTRODUCTION

Design works relating to computer security (trusted computer) began already in the 1970s. They referred to development of requirements for open use, multi-user, resource shared computer systems which process various levels of classified and unclassified information simultaneously in both secure and non-secure areas.

Although, to some extent, part of the problems relating to multilevel computer security, operation systems and databases has been solved, the problem appears again when new technologies emerge.

Controlled sharing of confidential information in both the military environment and as part of joint and coalition forces is an important means for achievement of network-centricity goals. To this end, in the last few years a technology for building the Service-Oriented Architecture (SOA) has been developed. SOA maps the concept of distributed service-oriented processing.

Although this technique is supported primarily by civil standardization organizations such as OASIS, W3C, WS-I, it is also very promising for engineers involved in building modern military command support systems. Modern command systems can be quickly implemented through object-oriented computer tools that are supported by such companies as Oracle, IBM and Microsoft.

At present SOA is being implemented using Web Services (WS) technology. Applications supporting commanders through WS provide them with an intuitive graphical interface of own and enemy forces dislocation combined with a map and data required for performance of the command process and blue force tracking.

Systems built with the use of these tools could process information and exchange it in an effective manner.

As it turns out, not the lack of available tools for building systems is one of the greatest obstacles, but their excess, namely the implementation differences between the WS implementations that hinder cooperation of systems implemented using them. The style and habits of programmers as well as the use of different optional fields and facilities for rapid programming are the additional limitations. The form of data based on XML formatting determines the use of WS in creating various system solutions. XML ensures the possibility of syntactic analysis, i.e. data parsing of processed and exchanged data. Data format is the key element of the success of WS technologies, also in terms of their security. Differentiation of data can be obtained through its tagging which enables distinguishing them and, at the same time, using various protection mechanisms, depending on different permissions of the recipients.

This XML feature could be the basis for organization of Multilevel Security mechanism (MLS) in entire ICT systems, including computers, databases, visualization means and telecommunications equipment. Data in the form of XML can be exchanged through the interface described in WSDL using SOAP communication. In order to organize the MSL and to
distinguish data sources and destinations, it is necessary to organize a cryptographic system and cryptographic data exchange (electronic key exchange) which is not a trivial problem. The difficulty of organization of such a system increases with the distribution scale and heterogeneity of the system of systems.

II. CURRENT AUTOMATED COMMAND SYSTEMS IN POLAND

The structure of the Polish armed forces covers headquarters of Land Forces, Air Forces and Navy. The following automated command systems operate therein: Szafran and Jasmine (automated command systems for land forces), Dunaj (surveillance and command system for the airspace defense of the country) and Leba (automated command system for the Polish Navy) (Fig.1). The above command and display systems are based on data exchange interfaces that use the WS technology.

Szafran is a command and control system designed to support the land forces at the battalion, brigade, division and corps level. It supports the command staff by enabling command and control processes.

Jasmine - Battlefield Management system designed to support command processes at tactical level, was designed for building C4ISR system (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance). It is dedicated to vehicles, ships, vessels and flying objects in the armed forces, public services and the civilian organizations.

Dunaj is the system for detection and command of the state airspace defense. That is a stationary, multi-position system which connects command and guidance centers, the Mobile Command Unit of Air Operation with the Air Operations Headquarters Center.

Leba is an Automated Command System for the Polish Navy. It is dedicated for units of the tactical and operational level to support the process of collection of data on the maritime situation in the Polish area of responsibility, developing and distributing a unified maritime situation picture and command reports.

Data from the Szafran, Leba and Dunaj systems are delivered to the Common Operational Picture (COP) where they are aggregated, presented using the Geographic Information System (GIS) and presented on a map.

A. Common Operational Picture

The system was designed to collect data from armed forces C2 systems and enhance situational awareness in decision making process.

In order to achieve the required efficiency of command support in combined operations, the cooperation of forces command systems can be obtained as a result of implementation of joint interfaces and data exchange standards.

In this regard, STANAG 5525, the Joint C3 Information Exchange Data Model (JC3Iedm) and the Multilateral Interoperability Programme Data Exchange Mechanism (MIP DEM) are of significant importance. These standards provide for automated data exchange between the cooperating systems.

In order to organize the collaboration of the command systems of own forces types among them and with allied forces, mechanisms derived from SOA based on eXtensible Access Control Markup Language (XACML) and WS technologies can be used. Owing to dynamically configured cooperation policy sets, it will be possible to combine computer systems of command systems. The policy should include sets of requirements and limitations relating to cooperation of WEB services as regards management, security, quality of services, objects and subjects tagging as well as possible relations between them.

III. THE PROBLEM OF ORGANIZATION OF MULTI-LEVEL SECURITY SYSTEM

In computer systems, both data objects and subjects can be tagged. Metadata in the form of labels inextricably linked with data describe the level of data sensitivity, whereas in relation to users they describe their permissions. Relations between the sensitivity of data and user permissions are the essence of the multi-level security systems. The access to sensitive data is controlled by the user permissions. The first attempts of formal model description were made in [1]. In the report by Paul Anderson, the tamper proof reference monitor concept was proposed, which is always invoked and must be small enough to be subject to analysis and tests. The concept is predicated upon positive authentication of all users at all times. The costs of production of the system were evaluated in 1972 for USD 11 million. The work by Anderson were continued by David Bell and Len LaPadula [2]. They formulated the BLP mathematical model describing (1). The current state of the modeled system is described by:

\[(S, O, A)\]  

where:

\(S\) – is a set of users,
\(O\) - set of objects,
\(A\) - access matrix.
The authorization mechanism checks whether access "r" which user "s" is trying to use for object "o" belongs to the subset of access rights defined as "s" and "o" in matrix A, i.e. whether at the intersection of the column corresponding to "o" and the line corresponding to "s" there is such a RsO set, that r ∈ RsO.

Each user has a security level defined by a pair:

\[(C, G)\]  

(2)

where:

C - is the classification level (e.g. top secret, secret, confidential, classified, unclassified),

G - subset of classification categories.

The set of classification subsets is linearly ordered due to the majority relation ≥.

Multilevel security in IT systems is of broader nature than implementation in operation systems, although the rules of access to resources have remained identical and can be most simply described as "no read up" and "no write down" (Fig. 2). The user can write down and read up information on the sensitivity level corresponding to its permissions. However, it cannot read up information on the higher sensitivity level than its permissions allow and write down information with a sensitivity level lower than its permissions.

The BLP model of IT systems security policy changes describes a set of access control rules, defines the secure state term and checks whether the state change during transformation from one state to another is performed in a secure manner.

Multilevel security in federated IT systems is of broader nature than implementation in operation systems, although the rules of access to resources have remained identical and can be most simply described as "no read up" and "no write down". The user can write down and read up information on the sensitivity level corresponding to its permissions. However, it cannot read up information on the higher sensitivity level than its rights and write down information with a sensitivity level lower than its permissions. The access to information applies to the entire federation of IT systems and not just to a single domain. The permission control mechanism is mandatory and discretionary.

Military communications systems for commanding use dedicated ICT networks that are supervised by the state security services. In the public sphere the systems are organized in a different manner.

Nowadays, the majority, if not all public institutions are connected to the Internet along with their services. The same rule applies to private entities. Apart from the Internet, VPNs are used for business activity purposes, that are organized on the basis of public IP networks.

In order for military systems, public institutions, companies and organizations to interact effectively, mechanisms are necessary which ensure dynamic cooperation depending on the needs. The service-oriented architecture is the type of architecture providing effective cooperation for institutions and companies, whereas the XML is the most reliable data format owing to the possibility of its semantic interpretation by network machines.

Institutions connected to the Internet secure their internal network using firewalls, however remote cooperation of users and servers in the internal network is often needed. There are many ways to access internal services, e.g. the secure VPN channel can be used. In this case, the remote user must use the secrets previously agreed with the administrator (keys, certificates, entries in LDAP), therefore the cooperation is safe but not dynamic.

Another effective solution is to use a protocol which enables information flow above the firewalls - HTTP. With the use of HTTP it is possible to access services within networks operating in the application layer. Users are authorized using e.g. certificates and may be authorized to resources through functional elements of the eXtensible Access Control Markup Language (XACML).

For the purposes of management of users access to information resources in XACML (OASIS), functional elements were developed which enforce the use of security policy in relation to invoking utility services. Confidentiality and verification of users identity are provided as a result of the authentication process using WS-Security mechanisms, i.e. digital tokens and certificates (X.509 Certificate Token and SAML Token).

Multilevel security in the operation system was not implemented until the end of the 1990s as part of the SELinux project sponsored by NSA [3]. With regard to IT systems, there have been a lot of concept trials. The report for the Naval Research Laboratory [4] published in 2009 is one of them. It presents the concept of an infrastructure for multilevel secure service-oriented architecture using the multiple single level approach by Jim Luo and Myong Kang. Similar works were performed as part of the National Centre for Research and Development project in Poland, whose results have been included herein.

IV. FEDERATED SYSTEM ARCHITECTURE WITH MULTILEVEL SECURITY

Dynamic sharing of information sources is nowadays achieved by creating federated systems using global database applications of federated institutions. The dependence of institutions on network ICT systems means that they are prone to the risk of security loss, whereas security management for
access control grows more difficult. The XACML mechanisms [5] developed in OASIS are the answer to the complicated management of access to resources.

In the previous practice of ICT system management, the strategy of risk elimination has prevailed. Physical (galvanic) separation of the protection network from the remaining ICT resources of institutions is one of the fundamental protection methods (Fig.3). The isolated networks create domains accredited to specific level of protection in accordance with the adopted classification of protection levels (in accordance with the security policy). Domains are used according to the accepted ICT national security procedures [6-8]. The need for cooperation of domains entails sharing of information between isolated ICT networks. In this regard two approaches have been developed in practice [11]:

- MILS (Multiple Independent Level Security) - cooperation of independent domains with different protection levels [9-11];
- MLS - providing information on the various protection levels within a single network [4, 10-12].

In the mandatory access model (MAC), the administrator still has the highest permissions in the system. However, it does not specify the access rules enforced on all subjects. The MAC model introduces centralization of access control management on the part of the Internet. The users have rights limited by the applicable policy and do not have control over the properties of their files, folders, processes and devices. The access controlled policy applies also to administrators who loose part of their permissions to the benefit of the system. So, if an intruder gains access to the administrator account, it will not have access to data that are owned by other users.

There is also the need for the federated system with MLS mechanisms to enforce security policy independently of user activities (regardless of the functioning of programs run by the user). In this way, it is prevented that any process of the higher level is able to transfer anything to any object of the lower level.

As part of the design works of the consortium, the concept of MLS subsystem for information systems federation was developed, based on [4,12]:

- functional elements implemented according to XACML architecture within the realization of authorization of the Mandatory Access Control (MAC) [4];
- the basis of implementation in the web services technology (SOA) [13];
- the mechanisms of creating trust relationship between services in accordance with OASIS WS-trust specifications based on the Security Token Service (STS) [14];
- user authentication mechanisms, level of their permissions and web services, the implementation was based on certification using the ITU-T X.509 standard [12];
- ensuring confidentiality and integrity of the messages exchanged between the web services using the SAML assertion secured with asymmetric cryptography functions [15];
- labeling mechanisms of information sensitivity, users permissions and processes in accordance with the standards [16-18];
- registering traces of information resources published in the digital mail room logs.

The MLS physical architecture (Fig. 4) is realized based on the elements that can be divided into:

- Elements of authorization processes in the information domain: Policy Enforcement Point (PEP) and Proxy Server, Policy Decision Point (PDP), Policy Administration Point (PAP) and Policy Store (PS). Elements of management of access to the mechanism of issuing sensitive information based on the security attributes of the users and arrangements relating to security policy in the federation. In PS, the data of security policy are written down in the XML. PAP is an interface for configuration of rules of access to information resources. The rules are written in the XML. PPE, PDP, decisions are made that relate to approval/rejection of access to the service and issuance/refusal to issue sensitive information by the broker issuing sensitive information from the database. A
decision is made in PDP based on the rules written down in PS and relating to federated domain users. The decision on authorization is returned to PEP Server (that previously intercepted the user request for access to sensitive resources).

- Elements of authentication and management of identity in domains and between the federation domains were based on X.509 certificates and tokens (from Central Authority Public Key Infrastructure and from servers of STS - SAML and X.509 security tokens). Each user and service in the developed system has its certificate authenticating the identity and containing data for security function, trust relationships and permissions in the information system.

- User permissions server as part of the Directory Services in information systems.

- Trust relationships established using CA PKI/STS as part of information domains and between federation domains.

- Users and services defined in CA PKI of domains, that have X.509 certificates examined by authorization elements to enforce security policy. Within and between domains, a trust relationship is established to enable authorization of users as per the permissions.

- The database server/broker of secure exchange of labeled sensitive information with encryption and decryption functions within the BD and secure information exchange with the user/web service.

- The server of the log for access to sensitive information/storage of information on the use of information resources in a federation of systems.

- In foreign domains cooperating within the agreed security policies a system mapping the access of external users to sensitive information was implemented. The mapping of permissions is employed through agreements between the security services of information domains.

Fig. 5 shows functional architecture of the MLS WIŁ domain and network relationships between the elements. The domain includes the following functional elements:

- WSP (Web Service Provider) - secured information service with proxy server of access to labeled information;

- WSC (Web Service Client) - client application for performance of information and STS service, which is used by the user to retrieve sensitive information from the MLS;

- Truststore - a database with a set of the X.509 certificates, common for each domain. The database containing these certificates is common for the WSC, WSP and STS within a single domain;

- Keystore - a database containing a set of the X.509 certificates which is dedicated to each service: WSC, WSP and STS.

Authentication management components:

- Identity Provider - a component responsible for delivery of data on the service client.

- STS (X.509) - a component responsible for authentication of clients in the domain using the X.509 certificates. After successful authentication a security token SAML is issued.

- STS (SAML) - a component responsible for authentication of clients in a domain using security tokens issued by a trusted STS, e.g. from the domain of ACP. After successful authentication a security token SAML is issued.

Authorization management components (XACML):

- PEP - responsible for controlling access to the service, strong integration with the service;

- PDP - responsible for authorization based on user data to the policy of access to the service;

- PAP - responsible for creating and managing security policies in a domain.

An element of network directory, LDAP Server - a service that stores information on the users and enables management thereof. Server LDAP OpenDJ, version 2.4.4;

An element of labeled database, Data Broker - a component responsible for labeling information resources [18] and cooperation with PostgreSQL database.

Within one of the domains, the services of access to information cooperate with the labeled database resources. The download of information from the database server is preceded by a sequence of messages exchange between functional elements that authenticate the user or service in the system and...
authorize it for resources. Functional elements of the architecture can be embedded on various physical elements in different network locations. Fig. 6 shows a sequence of message exchange between functional elements in the case of authentication of a service within an information domain for the target service.

In the case of a positive verification in the authentication process, the user gains access to authorization service in the target service. As part of the target service, the user authorization process for the defined resource (of sensitive information) is implemented. The permission level is compared with the sensitivity label of the information resource. In a positive case, a permission for information access is granted. In this case Data Broker decrypts the information stored in a secured form in the database and then re-encrypts it using the public key in a relationship with the user (service), and directs it to the WSC user. The results of processes efficiency shown in Fig. 4 have been presented in the first test scenario later in this paper.

The case of cooperation of information system federations has been presented in the form of a diagram in Fig. 7 showing the cooperation of components and sequence of messages exchanged between elements of the implemented domains. The domains were implemented based on two different projects that in turn based on identical assumptions and requirements.

Due to the clarity of the figure, not all domain elements have been presented.

Communication scenario completed with a successful authorization is performed according to the following processes (Fig. 7):

- (1) the process on the user's computer performs authentication in the local STS server by sending a HTTP/SOAP request with the X.509 certificate;
- (2) the process of the STS service server retrieves directory information from the LDAP server;
- (3) the LDAP server returns a message on the authentication and confirmation of permissions;
- (4) in the case of successful authentication and authorization, the SAML assertion is issued back to the user process (version 2.0);
- (5) the user process sends to the STS service an authorized request for a token valid within the domain;
- (6, 7) the process of the STS server from the external domain verifies whether the SAML permission assertion included in the request is signed by a trusted STS from the parent domain;
- (8) in the case of a positive verification based on the SAML assertion, a new token is issued which is valid in the external domain;
- (9) the user process sends a request to the Web Service Provider (WSP) in which the received STS token is included. The request is intercepted and the authorization process of user permissions for sensitive resources (labeled by the level of information sensitivity) specified in its certificate (X.509) is started;
- (10, 11) PEP verifies whether the SAML assertion included in the request is signed by a trusted STS from the external domain;
- (12, 13) if the token verification is successful, service access policy is downloaded from the access policy set and authorization permissions are validated;
- (14, 15) in PDP, the compliance of access policy with the user permissions downloaded from SAML assertion is validated;
- (16, 17) the authorization result is stored in the log base for access to sensitive information for accountability and non-repudiation;
- (18) if the user process has the required permissions, it is granted access to the service to issue sensitive information for which it has the permissions. The information (data) is issued in the form encrypted by the user public key;
- (19) the user process receives a feedback to the request along with the included sensitive information which is then decrypted by the user private key.
V. ANALYSIS OF THE EFFECTIVENESS OF DATA EXCHANGE BETWEEN DOMAINS OF INFORMATION SYSTEM FEDERATIONS

As part of assessing the effectiveness of the system consisting of two domains, the effect of security mechanisms on the quality of authorization service in a federation of information systems was tested. To evaluate the effectiveness as a measure of web service quality [19], the delay time of authorization process was assumed. A detailed description of scenarios was included in the presentation of system architecture in section 4 herein (Fig. 6 and 7). The scenarios relate to the effects of the implemented MLS security mechanisms on the delay of the performance of services concerning access to sensitive information realized in a federation of systems.

The first scenario regards authorization to local information resources in the 1st domain. The user requests a token from the STS server. In the process the user profile in LDAP is verified. Then, the user requests the sensitive information database with the X.509 certificate and token through elements of the XACML architecture.

The second scenario relates to authorization of information resources in the 1st domain by the user (process) from the external network of the federated system from the external domain. The user requests issuance of the STS token from its own domain. Then, with the token and X.509 certificate, it requests the system of the 1st domain to grant access to the database with information on the different levels of sensitivity. The authorization is performed by the XACML elements and then DataBroker checks the permissions and organizes access to labeled services and information resources.

Fig. 8 shows time measurements of authorization process in the MLS WILO parent domain. 60 test measurements of the authorization process were performed. It follows from the analysis of authorization time results that the values of the measurements are similar and equal 120 - 300 [ms]. Minor differences between the individual results are due to current loads caused by processes run on computer systems participating in the test scenarios.

At the first authorization of an external user to sensitive resources of the 1st domain the process lasts approx. 1 [s]. It can be assumed that the results of the first authorization of a given user (for the validity period of a token equal to 5 [min.] or 60 [min.]) to resources of its own domain will take approx. 1 second.

The time of the first authorization is almost 3-fold longer than that of those that follow. This results from Java properties and the used frameworks in which the system was implemented. However, the total time of authorization in the parent domain is not significant and has little effect on the utility service (use of the sensitive information from the database).

In order to provide independence of the conditions of use of the ICT network elements and reproducibility of the results for easy interpretation, the test was performed on a single computer with all services of the MLS system installed on the application server, whereas the exchange was carried out using a stack of protocols and loopback interface.

In the case of a network test environment, an increase of delays in performance of the authorization service by the delays introduced by the ICT network should be taken into account.

Fig. 9 shows the results of measurements of the user authorization time in the remote domain. A series of 60 measurements was performed which indicate that the authorization delay in the case of allocation of sensitive resources to a user from the external domain in the 1st domain is equal to 150 [ms].

As in the previous test scenario, the performance of authorization process for the given user lasts, for the first time, significantly longer than the subsequent authorization requests. The test was performed repeatedly and the results obtained indicate that the authorization lasts approx. 1.5 [s]. The tests did not consider the effect of network conditions on the delay in realization of the authorization process.

Significant amount of time of token allocation for the first time is associated with the specific character of Java (framework JAX-WS 2.1/2.2 and Metro 2.0/2.1), where objects for the support of communication with WSP and STS services are generated. These services provide objects that are generated and initiated at the first request on the application server, which results in longer time of the first realization.

The above tests were performed during the international CWIX exercise. The tests in the military environment were carried out in a two-domain system which provided for authorization and confidentiality function between servers performing the service relating to displaying location of the own forces between the Szafran command system and POSO COP (Fig. 10). The messages were exchanged using the authentication, authorization and confidentiality mechanisms. They were dynamically delivered from the two above mentioned domains.

The Szafran visualization system was included in the first domain as the service user. A security policy for data generated by Szafran was developed.

![Figure 8. Time of user authorization in the parent domain](image)

![Figure 9. Authorization time of the user from the external domain in the 1st domain](image)
The POSO COP system was included in the second domain and the security policy was elaborated for this system as well. Two data streams from different web services were treated as users of the MLS system that were assigned specific permission and all necessary security attributes. Owing to the developed security policy and the asymmetric key infrastructure, the possibility of dynamic cooperation of systems for displaying operational situation was provided. Obviously, as it might be expected, regardless of the source and test system, the measurements obtained during the exercises confirmed the results generated in the previous tests. The time periods of performance of the security services were equal to the previously specified levels.

VI. CONCLUSIONS

Within the consortium, in the project, two independent implementations of the multilevel security subsystem were developed. The above results indicate that a safe realization of the process of authorization for sensitive resources between the domains of information system federations with the multilevel security mechanisms is possible and can be effective. Due to the no-native programming technologies used and the generally available open programming tools that do not allow for verification of security level of the compiled binary code, the solutions developed in the project should be used with additional external encryption mechanisms.

The developed MLS implementations were tested in terms of interoperability in the consortium and domestic (BUMAR Elektronika) test environment. In June 2012, both the implementations services were successfully tested in an international test environment during testing of interoperability with foreign IABG partners (Germany) and NC3A agency in the NATO Secret network during CWIX 2012 exercise [20].

The solutions described by the consortium can be extensively used in civil environments for cooperation of ICT systems that share and process sensitive data, e.g. in the case of public administration or big-scale companies.

Implementation of the project has led to the conclusion, important in view of the state defense, that the condition of development of the IT technology has probably surpassed the possibilities of ensuring complete ICT security. The complicated and non-certified tools and technologies such as Java or WS involve some threats and vulnerability that cannot be allowed in the case of military systems processing and exchanging confidential information without any additional encryption mechanisms. However, according to the authors, it is possible to dynamically share sensitive data in a business environment, after application of additional mechanisms such as IPsec, TLS and SSL.

REFERENCES