A lesson learned from the information assurance and delivery in the project “Multinational interagency situational awareness – extended maritime”¹

BARTOSZ JASIUL¹, PER OLOFSSON², JOANNA ŚLIWA¹, MARTIN SJOBLOM², ROBERT GONIACZ¹, RAFAL PIOTROWSKI¹

¹ Military Communication Institute, ul. Warszawska 22A, 05-130 Zegrze, Poland
² Swedish Defence Materiel Administration, Stockholmsgvagen 18, SE-749 40 Enköping, Sweden

Abstract: The main tenet of net-centricity is to achieve information superiority by sharing reliable information collected from various sources, creating situational awareness and distributing it among mission participants, across domains, contexts and organizational boundaries. In order to accomplish this goal the change of focus must take place: from the idea of standalone, stovepiped systems (i.e. platform-oriented) to the idea of shareable, universal information. This was experimentally verified during multinational exercises. The paper presents achievements and capabilities, how to accomplish a cross-domain interoperability in order to build situational awareness.

Keywords: Interdomain authentication, situational awareness, web services, Service Oriented Architecture

Introduction

The Multi-National Inter-Agency Situational Awareness of the Extended Maritime Environment Project abbreviated MISA-EM () is one of objectives of the 6th Multinational Experiment (MNE-6) lead by the United States Joint Forces Command. The aim of these experiments was to provide opportunities to explore new concepts and capabilities for multinational and interagency operations. MNE-6 is a multinational and interagency effort focused on improving coalition capabilities to counter irregular adversaries and to prevent uncooperative leaders from becoming adversaries through the application of a comprehensive approach. MISA-EM supports this goal in the maritime area.

¹ This work was partially supported by the Research Project PBZ – MNiSW – DBO-02/I/2007
The maritime environment common operational picture is crucial for the security, prosperity and stability of many nations, as well as for the support of most joint operational theatres. Maritime security becomes a key factor of any large operation. Maritime Situational Awareness (MSA) comes up as an enabling capability for achieving the required Information Superiority to support the decision-making process in order to guarantee the security and stability of this environment.

Technically MISA-EM focuses on sharing information between countries involved in order to build MSA within operators of these systems. This is especially to protect from irregular adversaries and non-compliant actors. As the maritime environment continues to evolve, a number of irregular threats to security come up, posed by new actors whose identities, capabilities and interest are not always clear. Maritime borders, confined sea lanes, littorals, deltas and rivers are challenging but inseparable parts of the common operational environment, and no freedom of action should be left there for the irregular adversaries. Maritime piracy is one of the most conspicuous examples [1].

**Proposed solution**

Creating multinational situational awareness requires information sharing among cooperating countries' systems. Service Oriented Architecture (SOA) provides possibilities to dynamically and flexibly distribute information based on commonly known, well described system interfaces. SOA is a distributed system architecture that succeeded lately in commercial applications and is recommended by NATO as a crucial Network Enabled Capability solution [6]. SOA can make information resources available in the form of services that can be discovered and used by all mission participants that do not need to be aware of these services in advance. The use of SOAs simplifies the application and data sharing and provides a flexible mechanism for reusing existing services and information sources to enable the development of new, value-added information services. Within this approach the inclusion of a service-based environment allows contributed systems to be independently managed and controlled by their stakeholders.

One of the SOA's advantages is the possibility to integrate systems (or software applications) regardless of the software platform they use, preserving their autonomic functionality, without central management and coordination. On the basis of SOA all of the participating countries which have their own MSA systems can cooperate with each other sharing crucial information that support them in taking decisions faster in case of detecting some unusual behavior at the sea. This distribution covers vulnerable information important in terms of discovering anomalies and alarms that may be the starting point for any dangerous actions. It is though important to provide security of this information sharing process, solving the problem of heterogeneity of systems connected both in terms of communication protocols and incorporated security mechanisms.
For the purpose of the MISA-EM there has been proposed architecture that provides mechanisms to efficiently exchange information based on Web Services technique, one of the most mature implementations of SOA. Web services were used to share data about vessels (the so called Query by Example service). Every country registered their services in the service registry (based on the mobile Domain Name System solution – mDNS). There has been also proposed the mechanism to distribute notifications using the Extensible Messaging and Presence Protocol (XMPP). XMPP was also used as a chat server and allowed operational and technical teams to discuss the progress of operation during exercises.

In order to realize MISA-EM objectives it was necessary to establish a common understanding and definition of notifications (anomalies and alarming situations) in the MSA environment, tailored to the needs of different users. Some anomalies that are regarded by the coastal guard are not interesting for the Navy. Some observed by the management of seaports are not anomalies for the coastal guard. Civilians may also have other needs in terms of alarms. These common definitions are very important for achieving systems’ interoperability also in terms of a semantic description of shared data. They allow using smart agents, automatically processing received information and capable of aggregating it with the data collected inside the system and possibly generating conclusions and proposing actions for the operators.

Services realized at the misa-em project

According to the SOA assumptions each service is considered as a reusable component, which can be invoked by various users or other services. This guarantees that the sides taking part in the mission can easily obtain needed information.

A primary service, based on which data was exchanged, was Query by Example, implemented as the SOAP web service, that provided the possibility to ask another system for the available data about a particular vessel (or a group of vessels) identified by any of information included in the vessel ontology (described in vessel.owl), e.g. name, MMSI number, IRCS, flag, etc. Using QbE together with the service registry enables to query all the systems currently connected and receive information from all of them. For the purposes of MISA-EM, information was exchanged in the RDF format (Resource Description Framework).

Information about anomalies was exchanged using the Notification services based on the XMPP protocol. Data was sent to all subscribed users in the form of notifications, compliant with the agreed semantic description proposed for the experiments (notification.owl with nation.owl, vessel.owl, location.owl).

Implemented services enabled to distribute information about the Vessel of Interest (VoI) approaching the Polish coast, the anomaly regarding two ships with the same MMSI numbers and then to notify all the actions related to locating and taking control over the ship. Moreover it was possible to send information
about the VoI existing in the cooperating systems that is gathered locally for the purposes of this system.

Sharing sensitive information in a multinational environment requires that the cooperating parties are convinced that the information is reliable and that its consumer and producer are credible. It means that each producer of information must be assured that only authenticated and authorized users can consume requested services.

Security provision in MISA-EM focused on the provision of a trust relation and on the facilitating of authentication of users and services in a multidomain multinational environment. Therefore, the Swedish and the Polish domains implemented secure token services that were able to provide local authentication of users on the basis of credentials conformation generated by a national authority. This enabled to send SOAP queries extended by the security header that was processed by a local authentication service.

Services enabling secure communication

First of all, in order for the users to share information and use the received data, they must be sure that the source and sink are reliable. Information can be though shared only among users/devices that have been identified and are approved for this kind of data. Only cross-domain authentication and authorization, based on a trust relation between security providers and an appropriate identity management are able to fulfill the initial security requirements for the FoS (see Fig. 1).

![Diagram](image-url)

Figure 1. Cross-domain authentication and authorization of users and services. Intradomain and interdomain security mechanisms
As shown in Fig. 1, in the national C4I system the access to information is controlled and granted only for authenticated and entitled users from this domain. Access control is an internal issue of the system and can be realized in different ways. An authorization decision is made locally and usually bases not only on the user’s rights and attributes, but also on the invoked web service attributes and a valid security policy. The set of user’s attributes required for making decision may differ depending on the system implementation. The mechanism usually secures all information flows inside the system.

The goal of an authentication mechanism is to confirm the identity of a user or a service. To perform access control, Web services need to identify and authenticate requesters. In the FoS it can be performed by different means. Authentication services in different domains must interoperate with each other and accept an identity confirmation issued in another domain (some kind of a token). It must be emphasized that the user must be appropriately identified across domain boundaries.

**Verification of SAML authentication**

An authentication mechanism aims at confirming the identity of a user or a service and an authorization is to provide an appropriate access or deny the use of services and data stored and processed in the system. Authentication and authorization mechanisms were developed in MISA-EM project as a set of loosely coupled security web services.

To perform a user authentication with SAML, the user had to be verified in his own domain (he needed to be authenticated in his own domain). In order to prove his identity in the other domain he obtained a security assertion (some kind of a passport), consisting of a user identity, a public key and attributes that proved his authentication in his domain and his rights to receive sensitive information from other partners. Authentication was a local process based on a public key infrastructure. This solution guaranteed the independence of policy rules in each autonomous domain. However this security assertion (sent between the domains of the service requester and provider) had to be understandable to the cooperating systems in order to take appropriate actions and to verify the status of local authentication based on a trust relation between security domains. Moreover, the user’s attributes included in the security assertion were used to provide appropriate access to invoked services. Authorization decision was made on the basis of the user’s attributes and an internal security policy.

In the presented solution X.509 certificates [12] were implemented for intra-domain user authentication. Certificates based on open industry standards are supported on many platforms and on top of that, X.509 certificates can be used to provide confidentiality and data origin authentication at the message and the transport layers. The identity of a particular participant in a message exchange was unique and was confirmed by the verification of signature made with X.509 certificates.
For cross-domain authentication Security Assertion Markup Language (SAML) [11] tokens were chosen. They carry X.509 credentials and additional values e.g. signatures and user's attributes. SAML is an XML-based standard introduced by the Security Services Technical Committee of the OASIS for exchanging authentication and authorization data between security domains. In the presented model SAML assertions were transferred from the identity provider (that can be e.g. Secure Token Service [STS] or Policy Enforcement Point [PEP]) to the service provider. It must be noted that signatures included in SAML tokens guaranteed message integrity and non-repudiation (signatures unable to fake identity of user and his attributes).

The advantage of utilizing SAML is its flexibility and adaptability to carrying variety of properties which can be used for securing communication. In fact only a few elements are mandatory in SAML assertion and the rest is optional. An assertion contains statements that the service provider uses to make access control decisions. SAML provides three statements:

- **authentication** – asserts to the service provider that the principal (e.g. STS, PEP) authenticated the requester at a particular time using a given method of authentication (e.g. user/password, biometric data, X.509 certificates, Kerberos, etc),
- **attribute** – provides the requester's attributes that could be used to make access control decision,
- **authorization decision statements** – provides permissions for particular actions.

SAML assertion is composed of obligatory and optional elements. This allowed incorporating information about a local authentication of the user based on X.509 certificates and send user's attributes for the purpose of authorization. SAML assertion used for the trial consisted of the following elements:

- **Issuer** – the unique identifier of the requesting service provider / the unique identifier of STS, PEP;
- **Subject** – SOAP message source unique identifier (a requester or a service provider);
  - Both the issuer and the subject data are extracted from X.509 certificates and consist of a common name, an organizational unit, an organization, a country (CN, OU, O, C).
- **Signature** – a value obtained from signing the whole request/response message; it provides message integrity and guarantees non-repudiation;
- **Conditions** – validity period; it consists of values: NotBefore and NotOnOrAfter;
- **Authentication statement** – a method used to authenticate the user;
- **Attribute statement** – attributes of the user used for authorization e.g. a military rank, a function in the organization, secrecy permissions.
It is important to emphasize that security mechanisms and functional services were implemented separately by all sites in order to present possibilities of interconnection of heterogeneous systems. Moreover, programmers internally involved in the realization of functional services were not used to implement security mechanisms. This was to prove that SOA enables a loose coupling of services by the orchestration of various systems and services.

**Securing communication with TLS**

Traffic Layer Security is a well defined standard used to prevent communication across the network from eavesdropping. It allows unilateral and bilateral authentication for client/server applications. Moreover it encrypts the data while it is distributed over the network. Despite a broad range of its possibilities, only unilateral authentication with data encryption was verified. In comparison with SAML assertions, it allowed also to secure XMPP notifications because security mechanisms were implemented in a transport layer. This – unlike in SAML – renders impossible a multilevel access control to resources, depending on the user's rights and the internal domain policy.

**Implementation and test cases**

For the experimentation purposes a set of security services was implemented. They provided cross-domain authorization and authentication based on trust relations. One of them is the Policy Enforcement Point (PEP) treated as a main SAML assertion processing engine. It analyses part of the SOAP message header i.e. SAML assertion and delegates tasks to particular auxiliary security modules: *CertVerify Service*, *AuthorizationWS Service* and *KeyNegotiate Service*. All these services and PEP make up the Core security services system (see Fig. 2).

PEP and auxiliary modules were implemented as Web services communicating with each other with SOAP messages. As mentioned before, PEP, with auxiliary services, was responsible for the validation of SAML assertions. i.e.: validation of X.509 certificate and a digital signature of SOAP message embedded in the assertion, extraction and validation of user's attributes. If all of these processing stages return valid and correct values, PEP module, in turn, allows Web Service to proceed further with proprietary operations. The only stated requirement from the service provider is to call PEP operations before processing any Web Service task, just after receiving SOAP message request.
Reverse processing workflow took place while sending each of the SOAP response messages, e.g., to authenticate the service to the requester. After the client was granted the access, the requested service communicated with PEP in order to have its response message appropriately prepared. Just before sending a Web Service response PEP is involved in the preparation of the SAML assertion i.e.: gains user’s attributes and a crypto key, prepares the whole SOAP message including the SOAP header. A general logical workflow of processing the request and the response via SOAP messages is presented in Fig. 3.
National implementations were prepared separately, without exchanging any line of code. A general concept of the cross-domain security solution for both realizations was based on the same assumptions and was agreed before experiments. However the software products and solutions of security WebServices are different – e.g. Swedish implementation did not include PEP, however its functionalities were adopted by a security proxy service adding/removing security assertions – Secure Token Service (STS).

Figure 4 presents the invoking of the Polish Blue Force Tracking (BFT) service by Swedish side.

![Sequence diagram]

Figure 4. Example test scenario sequence diagram

At the client side, the STS – provided exclusively by the Swedish side, was responsible for preparing appropriate SAML assertions embedded in the SOAP messages. After receiving by BFT service provider, SAML assertion was analyzed by PEP, provided exclusively by the Polish side. In the case of any errors (i.e. wrong or not valid X.509 certificates, inappropriate private keys, modifications injected into SOAP messages) PEP informed BFT provider about such situation and the processing chain was stopped (access denied). In the case of a successful SAML assertion validation, BFT access was granted and the service was called. Before sending BFT response to the Swedish client, PEP was responsible for preparing an appropriate SAML assertion embedded in the SOAP response message. After receiving BFT
response, STS analyzed SAML assertion prepared at the Polish side. Similar checking workflow was executed by STS module and in the case of any BFT incompatibilities, access was not granted and the client was informed about that.

Conclusions

In the interagency collaboration domain, a traditional way of collaboration was the department to department cooperation. In the MISA-EM project, one of the goals was to decrease this rigid way of cooperation by allowing access to other agencies. By the use of a Service Oriented Architecture and by pushing information into the information sink, the resistance against interagency collaboration was significantly decreased. This, in turn, has led to a faster rate of information exchange between both national and international stakeholders. A clear example have been the Swedish coastguard that can provide video and photos from their routine surveillance missions, provided that the interaction domain is limited to a collaboration group with a relevant classification level. This information is used by other parties nationally and internationally that can identify vessels according to their own needs.

The MISA-EM project was very useful in the assessment of current operational and technical capabilities, leading to the formation and utilization of the Common Operational Picture. Tests carried out during multinational experiments at workshops as well as demonstrations led to a conclusion that experimentally implemented information distribution mechanisms could be used in multinational operations in order to support building a comprehensive operational picture, integrating information from various domains. This was especially visible during operational exercises at the Baltic Sea, when decision makers were able take appropriate actions faster and more adequately to the situation. Thanks to valid procedure and techniques, the whole operational process lasted a few hours and not 24.

Technical verification of functional services such as a semantic search, the Vessel of Interest, XMPP alarm notifications, a chat proved that they significantly expand the situational awareness of potential users. Moreover information exchange can be realized in a secure and timely manner. Although verified solutions cover only some of security requirements such as authenticity, non-repudiation and access control, and to some extent confidentiality, they were suitable to propagate the trust among coalition partners and allowed them to exchange sensitive operation information with an appropriate degree of security.

The project shows technical and operational capabilities of forming the network centricity, however the lack of formal regulations and legally valid procedures renders impossible to use achievements produced by a multinational environment.

The next step in the MISA-EM project perspective will be the area of service availability. When the need of information is determined, where will the user find the appropriate information? In other words: how to bring order to the information sink? This problem will need a solution pretty soon, since the quantity of information
quickly increases. The availability is not limited to finding the correct location of the service provider, but also the timeframe in which the service will be available and will provide useful information. The concept of the metadata repository could provide the means of solving this issue. This problem will also underline the need of refined operational methods and doctrines since the finding, validation and qualification of information needs to be handled by the conceptual part of MISA-EM.

REFERENCES

[9] Protected Core Networking reports and presentations, Task Group on PCN.