OVERVIEW OF THE SECURITY ARCHITECTURE OF THE COMPREHENSIVE MARITIME AWARENESS SYSTEM

Myong H. Kang, Margery Li, Bruce Montrose, Amitabh Khashnobish

Naval Research Laboratory
Information Technology Division
4555 Overlook Ave. Washington DC 20375

Scott Elliott, Mike Bell, Steven Pieper

Naval Research Laboratory
Space Systems Division
4555 Overlook Ave. Washington DC 20375

ABSTRACT

The Comprehensive Maritime Awareness (CMA) system tries to identify anomalous behavior and potential threats associated with the global maritime domain that could impact the United States and coalition partners' security. It analyzes data from multiple sources that impose different data handling requirements, to discover potential threats.

Security architecture and mechanisms are essential enablers for data sharing. More data stewards will share their data when they feel secure with the data protection mechanism of the system that will host their data. Critical technologies for data protection and access mediation for CMA are Oracle label security (OLS) and attribute-based access control (ABAC) based on federated identity management. Federated identity providers use security assertion markup language (SAML) 2.0 as a protocol to exchange user identity and attributes. This paper provides a high-level overview of the CMA security architecture. It explains how different security mechanisms seamlessly work together to protect data and mediate access.

1. INTRODUCTION

The Comprehensive Maritime Awareness (CMA) Joint Capability Technology Demonstrations (JCTD) program tries to identify anomalous behavior and potential threats associated with the global maritime domain that could impact the United States and coalition partners’ security, safety, economy, or environment. Information from multiple agencies and nations is gathered and analyzed, and the users from multiple agencies and nations access the system to discover potential threats.

The data protection and access policies of the system become quite complex when the data comes from multiple data producing organizations and the system is accessed by the users from multiple data consuming organizations. The system should be able to codify all data access policies that reflect the agreements among participating organizations. One of the important enablers for such multi-agency and multi-nation cooperation is the security architecture and mechanisms of the information system that will hold the data from multiple sources. When participating organizations understand the security mechanisms of the system and realize that their data is in good hands, they are encouraged to share their data. CMA contains law enforcement sensitive data, US military data, data from coalition partners, commercial proprietary data, etc. Therefore, data has to be well protected and the access to the data has to be carefully mediated.

CMA can expose selective functionalities as services in service oriented architecture (SOA) paradigm. However, its main architecture is a web-based 3-tier architecture due to the requirements of handling large volume of data. Data is stored in an Oracle database with labels (e.g., Oracle label security, OLS), and its presentation and logic tiers are implemented in ASP.NET. CMA deployed attribute-based access control (ABAC) based on federated identity management (FIM) because CMA will be accessed by various users from remote organizations. FIM builds a secure, trusted environment from multiple organizations, giving users Single Sign On (SSO) and Single Log Out (SLO) capabilities within a circle of trust. Building upon this circle of trust, the CMA authorization system makes access decisions based on user attributes from the FIM system. Even
though this paper focuses on CMA security architecture, the architecture and techniques are generic enough to be adopted by other secure systems.

In this paper, the overview of CMA security architecture is presented in section 2. Section 3 describes an authentication method based on federated identity. The authorization scheme is explained in section 4. Section 5 explains the use of Oracle OLS in the context of CMA. Section 6 discusses accreditation issues. Section 7 concludes the paper.

2. OVERVIEW OF CMA SECURITY ARCHITECTURE

Although data comes from multiple classification levels (e.g., UNCLASSIFIED, SECRET, TOP SECRET), CMA is a SECRET system-high architecture. That means all data in the system is protected as single classification level (e.g., secret level) and all users of the system have the same level of background checks even though they may not have the same level of need-to-know. In a simplified view (see figure 1), CMA software can be divided into two parts: the user-access side (a.k.a. the frontend of CMA), and data-fusion side (a.k.a. the backend of CMA).

Figure 1: High-level view of CMA security architecture

The user-access side of CMA software consists of authentication, authorization and web frontend components. Users cannot access the database directly; they have to access data using web interfaces through Hypertext Transfer Protocol (HTTP) over Secure Socket Layer (SSL). The data presented through CMA web interfaces is dynamically populated from an Oracle database that holds pertinent information regarding vessel, cargo, people, companies, and others as requirements dictate. When a user tries to access a CMA system, user authentication is performed through the FIM. If the user is from a trusted partner organization, the system retrieves the user attributes from the identity provider of the user organization and passes the user attributes on to the CMA web application. Based on the user identity/attributes, web access is mediated. Data in the web pages comes from the CMA Oracle database. The data in the Oracle database is labeled, and it is protected by the CMA OLS policy and Oracle’s built-in OLS mechanism. Oracle OLS was chosen due to multiple previous certifications for similar applications requiring authorized access to data. The user can only access the data that s/he has privilege to access. Therefore, even if two users access the same web page, different data, views, and images may be presented based on different user privileges.

The data-fusion side of CMA software consists of the data provider (DP) that moves data from various data sources to the queue and the integration controller (IC) that fuses incoming data with the existing data in the CMA database. If the data from a source already has security labels, CMA either re-uses the labels or maps them to the equivalent CMA labels. If the data comes from data sources that do not provide security labels (e.g., Automatic Identification System (AIS) data), the DP adds security labels. The labeled data will be stored in the Oracle database where the data is protected by the OLS mechanism and the CMA OLS policy.

CMA systems have been deployed to many organizations to monitor the threats in their area of responsibility (AOR). The users of the organizations that do not have their own CMA system may reach out to nearby CMA systems to monitor maritime threats. In such cases, the user organization is referred to as a client organization and the organization that hosts a CMA system is referred to as a server organization (see Figure 1). Even users of organizations that have their own CMA system may sometimes want to access other CMA systems because their system may not have the information that their users are looking for (e.g.,
different AOR). To authenticate users from other organizations, CMA deploys a FIM system.

3. AUTHENTICATION BASED ON FEDERATED IDENTITY MANAGEMENT

Users from many organizations may require access to more than one CMA system. Centralized identity management that manages all user accounts by a single domain is slow, cumbersome and creates unnecessary security risks. For example, let’s assume that user A from organization X is granted a CMA user account in organization Y. If user A moves to other organization or a different assignment, the user’s CMA account should be suspended. However, the account suspension will occur only if someone from organization X notifies organization Y. To avoid such unnecessary administrative overhead and security risk, CMA uses a federated identity management.

The goals of federated identity management are enabling (1) each organization manages its own users and (2) users of one domain to access resources of another domain seamlessly, without redundant user management. To enable federated identity, a trust relationship between organizations has to be established. Let’s assume that organizations X and Y establish a trust relationship for federated authentication through exchanging a memorandum of understanding (MOU) between two organizations. User information from organization X will be honored by organization Y. However, organization Y is autonomous with respect to authorization decisions. Therefore, passing legitimate user information from organization X to organization Y may not guarantee the access of the resources in organization Y.

The Naval Research Laboratory (NRL) has developed a federated identity management (FIM) system based on a Security Assertion Markup Language (SAML) 2.0 [1]. It employs a peer-to-peer federation model that is based on a bilateral agreement between peers. Unlike the conventional federation model that typically requires a multilateral agreement and membership (e.g., InCommon [4]), a peer-to-peer federation model does not require membership to a federation, and is thus a little simpler and more flexible.

In the NRL implementation, a peer is the federation server (see Figure 2) of an organization that may provide many services. Since the NRL FIM is based on bilateral relationships, every relationship may have different flavors in terms of the attributes that need be passed and the resources that can be accessed. A detailed explanation about the NRL FIM appears in [2]. The following discussion summarizes its components and functionality briefly for the sake of completeness of this paper.

The NRL FIM consists of three components: federated authentication module (FAM), federation server (FS), and authentication & attribute gateway (AAG). The federation server is the main entity that participates in a bilateral agreement with a partner federation server. To become trusted partners, 1) the two FSs have to exchange certificates that will be used to validate SAML statements, and 2) they have to agree on the user attributes that they will exchange. FAM acts as the connector between FS and a web application. Any web server that takes advantage of FS should have FAM. FAM also acts as a gatekeeper to redirect unauthenticated web service requests to the identity provider of the client organization (via the FS). The identity provider will provide user information including necessary user attributes. The AAG acts as the connector between the FS and either a domain controller or an attribute store. Therefore, the server-side NRL FIM requires a FAM and FS, and the client-side requires an FS and AAG (see Figure 2). The interaction among the components of the NRL FIM is also depicted in figure 2. There may be an optional attribute store that may store additional user attributes.

If Active Directory (AD) is used as an identity provider (IdP) and a domain user logs on to the system, the user does not need any more authentications to access the resources of partner organizations. The authenticator validates the user from the AD using stored credentials and provides all necessary attributes to the FS. Therefore the users will experience a true single sign on (SSO).
An “accept or deny” authorization decision is made between the times when user attributes are retrieved from user’s IdP (step 10 in Figure 2) and when user access is granted (step 11 in Figure 2).

4. Attribute-Based Access Control

Since CMA authentication depends on the FIM, it does not have any preloaded user information. The user has to be validated by the user’s domain identity provider and user attributes have to be supplied by user’s domain attribute store. However, the validation of user identity from the trusted client domain does not guarantee the user’s access to the CMA application. The CMA access must be mediated by the authorization mechanism of the CMA application.

Authorization scheme has to be carefully designed and seamlessly integrated with application. Since CMA is based on 3-tier architecture, we have designed three access control policy enforcement points (Figure 3) that correspond to three layers of resources:

1. Federation Layer: Site or application access policy,
2. Web Layer: Web resource access policy, and
3. Data Layer: Data access policy that is Oracle label security and discretionary access control policies

FAM validates if the user comes from a trusted partner site (including its own local site). If the user is from a trusted organization (including its own organization), it retrieves user attributes and passes them to the CMA application. If the CMA web site wants to block specific users from a specific organization, FAM provides a simple access control mechanism to accept or deny access based on the value of an attribute (e.g., deny access to a user whose e-mail address is John.Doe@nrl.navy.mil).

The CMA web server (Internet Information Services, IIS) access policy determines if a user can access the requested CMA URLs. At this point, there are two types of users: CMAuser and CMAadmin. This decision is based on the values of user attributes. If the user does not have the appropriate attribute values, some web page URL accesses may be denied.

The CMA web frontend application is closely related to the CMA backend database that is protected by an OLS policy. In other words, data that is displayed on a CMA web page URL has to be retrieved from the backend database. Since Oracle does not allow dynamic user creation, CMA creates predefined Oracle accounts that have proper privileges. Specifically, CMA OLS policy has several predefined Oracle user accounts such as CG_LEA_user, CG_INTEL_user, and DoD_user, where CG is Coast Guard and LEA is Law Enforcement Agency. Each Oracle user has pre-assigned OLS user labels and database privileges. CMA maps each user to one of the predefined Oracle user accounts based on the values of user attributes (e.g., organization, role). Data access is mediated based on the OLS user label, data labels, and the OLS policy. For example, CG_LEA_user
may be able to see more data (e.g., US person data) than DoD_user due to Privacy Act restrictions. Also one type of user may see more vessel positions than other types of users because different users can access different set of data sources.

When a user logs in, the CMA system will map the end user to one of the predefined Oracle user accounts based upon the user attributes. Therefore, multiple end users can be mapped to the same predefined Oracle user account. Thus, database audit may not provide accurate audit information. Therefore, CMA provides application-level audit capability.

The CMA database provides one special privileged OLS account that is being used to fuse incoming data with existing data (see Figure 1). This privileged account can access all data in the database regardless of its security labels. As a result, CMA is fusing data in a "label-agnostic" fashion. The fused data will be labeled based upon its original label, the labels of previously fused data, and an OLS label policy based upon label combining rules.

CMA also defines many more CMA application-specific privileges such as delete position, merge fusion object, delete fusion object, etc. These are called the capabilities of users. CMA administrators can assign CMA-specific privileges (i.e., capabilities) to CMA users through CMA applications. CMA users exercise their capabilities through executing stored procedures of Oracle.

5. ORACLE LABEL SECURITY AND DATABASE TABLE LABELING STRATEGY

Even though there are many tables in CMA, only a few tables are important from the labeling perspective. The first important table is the DataSource table that captures information about the sources of data. This table is protected by the CMA OLS policy. The other important tables are FusionObject table, Fusion table, Metadata table, Relationship table, Position table, etc. The FusionObject table represents important concepts such as vessel, cargo, people, and company. It is a container of Fusion objects comprising concrete elements from specific data sources. For example, a vessel FusionObject may contain a Fusion from an Automated Identification System (AIS) data source and another fusion from some other data source. Since FusionObject is just a container, FusionObject table is not labeled. The Metadata table contains attributes of the physical concepts represented by FusionObjects. This is another table that has to be labeled because even two metadata from the same data source may have different sensitivities. All other important tables such as Fusion, Relationship, Position tables have to be also labeled.

CMA deploys the CMA OLS policy that specifies which user (e.g., each predefined Oracle user in section 4) can access what data (e.g., data with which labels). Since data is labeled and each user has user labels, Oracle can enforce the CMA OLS policy.

The sluggish performance of OLS was one of the reasons that OLS was not widely deployed. We have observed 50% overhead for some operations. Therefore, naïve, straightforward OLS implementation is not an option for CMA system that requires high performance, high ratio of database insert and update operations. CMA has optimized OLS performance by properly mixing OLS and Oracle discretionary access control (DAC) techniques. A detailed description of CMA performance optimization strategy is beyond the scope of this paper.

6. APPROVAL TO OPERATE AND ACCREDITATION ISSUES

Whenever a system contains data that has different handling requirements, the accreditation becomes an important issue. CMA contains data from a single classification level but still has different handling requirements. Typically, the reasons for different data handling requirements come from the proprietary nature of certain data, rules and regulations (e.g., protecting personal data), or the restriction based on a contract, memorandum of understanding, legal restriction, or international agreement. Typically, the users of this type of system have the same clearance level but have different need-to-know. Thus, it is sometimes called a need-to-know separation.

The key to the accreditation of systems and the utilization of data is support from data owners/stewards.
When data stewards feel comfortable about the security architecture and security mechanisms of the system, they are willing to share data and approve the system. Another key to the speedy accreditation of such systems is using proven technology. For example, Oracle OLS is a Common Criteria Evaluation Assurance Level (EAL) 4+ product that is being used for need-to-know separation. Thus, data stewards and system owners have more confidence about the technology.

Data provided to the CMA system loosely falls into four major categories: contributed data from international partners, law enforcement or data pertaining to the Privacy Act, proprietary data and other intelligence data. These categories all have specific handling restrictions, and are releasable to different groups of users based upon the need-to-know that is decided using a number of criteria. As previously stated the system itself operates at a system-high mode; meaning that all operators or users have been vetted and cleared for access to the classification of data that resides in the system. However, all users do not have the need-to-know all data in the system. In order for a system to correctly process information that some users may need to know, and other users may not, below are a few requirements captured in US policy.

**Separation of Duties and Need to Know**

US Policy dictates that DoD systems protect data according to need-to-know [5]. There are two identified states for need-to-know and separation of duties confidentiality: protection of data in transmission and protection of the Automated Information System (AIS) processing this data.

Policy for the transmission of data is:

---

1. **“E2.1.8. Confidentiality Level”**

Applicable to DoD information systems, the confidentiality level is primarily used to establish acceptable access factors, such as requirements for individual security clearances or background investigations, access approvals, and need-to-know determinations; …” [6]

---

**“E4A4: Enclave and Computing Environment ENCK-1 Encryption for Need-to-Know”**

Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at minimum, with NIST-certified cryptography.” [7]

The National Institute of Standards and Technology (NIST) certify technologies that have been evaluated against the Federal Information Processing Standards (FIPS) 140-2 criteria. Currently the strongest algorithm is AES-256, and NRL suggests that incorporation of AES-256 if possible. This cannot be considered a requirement as NIST currently certifies implementations of triple-DES (3DES), RSA, SHS, and many other cryptographic engines, algorithms, and implementations.

NIST provides minimum standards for security controls in automated information systems. Policy for the treatment of data for separations-of-duties within systems is:

“Control:

The information system enforces separation of duties through assigned access authorizations.

Supplemental Guidance:

[…] There is access control software on the information system that prevents users from having all the necessary authority or information access to perform fraudulent activity without collusion. […]” [8]

This security consideration is generally focused on the “insider threat.” For the purposes of this paper, this policy guidance is interpreted to be a requirement restricting users without need-to-know from being able to access this data inadvertently or maliciously without the aid of a user who does have need-to-know (system administrator, user, etc). These controls should apply to users or system components that will further ensure that information is not available to unauthorized users or organizations without the aid of authorized users.
Accreditation Issues

OLS is the mechanism that is enforcing this requirement (e.g., preventing data access from unauthorized users), and this is bolstered by the fact that no user directly interfaces with the database. Oracle database including OLS has been evaluated by the Common Criteria EAL 4+, and is viewed to be sufficient for protection of the Automated Information System (AIS) processing of the data.

The CMA is in the process of seeking Approval to Operate (ATO). The authors do not believe it is such a difficult task because ATO seeks the permission to put this system on a network. This system is not different from any other system from the perspective of seeking ATO. What is more important from an operational perspective is the approval from various data stewards. The data stewards need to be convinced that the system enforces a correct security policy that honors data handling requirements that have been approved through exchanging a memorandum of understanding (MOU) etc. between the system owner and a data steward. Authors believe that convincing data stewards is not such a difficult task because

- The fine-grained data separation and the access mediation in CMA are enforced through Oracle OLS which is a proven technology, and
- A pilot demonstration program shows the cooperation from data stewards is not that difficult as long as there are mutual benefits among system owners and data stewards.

7. CONCLUSION

CMA contains data from multiple sources that have different handling requirements. Therefore, data has to be carefully separated and the access to the data has to be guardedly mediated. Oftentimes, security is an afterthought for many application designers. The CMA design process was different. From the beginning, the designers of the CMA system realized that data sharing among stakeholders would be extremely difficult unless there were proper security mechanisms in place. The security architecture of the CMA system is the result of this effort.

Good security mechanisms and concepts may often exert too great a performance penalty, rendering the secure system less responsive, and consequently less useful. The CMA security team put a large effort into optimizing the system to make sure the secure CMA system is responsive.

The NRL implementation of attribute-based access control and federated identity management has many potential applications far beyond CMA. There are many problems within the DoD, IC, and internal military cooperation arenas that could easily benefit from similar approach. One area that has been of continuing interest to the team at NRL is coalition interoperability and military coordination. Many of the coalition networks and systems are multilateral and information provided to those systems needs to be sanitized for release to all participant countries. There could be a great deal of value to the implementation of systems that allow for Community of Interests (COI) to have need-to-know separations so that their communications could be confidential from the community at large.

REFERENCES