NCI AGENCY

Content-based Information Protection and Release in NATO Operations

NATO OTAN

April 2013

This work was previously published in A. Armando, M. Grasso, S. Oudkerk, S. Ranise, K. Wrona: Content-based Information Protection and Release in NATO Operations, SACMAT 2013, Amsterdam, Netherlands.

Abstract

The successful operation of NATO missions requires effective and secure sharing of information among coalition partners and external organizations, while avoiding the disclosure of sensitive information to untrusted users. To resolve the conflict between confidentiality and availability, NATO is developing a new information sharing infrastructure, called Content-based Protection and Release, in which decisions about accessing information are made based on user attributes, content metadata associated with resources, and terminal capabilities to process and transmit information.

We describe the architecture of access control in NATO operations, which is designed to be easily built on top of available (service-oriented) infrastructures for identity and access control management. We then present a use case scenario drawn from the NATO Passive Missile Defence system for simulating the consequences of intercepting missile attacks. In the system demonstration, we show how maps annotated with the findings of the system are filtered by the access control module to produce appropriate views for users with different clearances and terminals under given release and protection policies.

1. Introduction

The successful operation of NATO missions requires effective and secure sharing of information among not only partners of the coalition, but also with external organizations (e.g. the International Committee of the Red Cross). While making as much information as possible available to the various participants involved in a mission, it is crucial to avoid the disclosure of sensitive details to users with insufficient clearance. Of course, the conflict between confidentiality and availability of information greatly complicates the task of information sharing. On the one hand, some pieces of information must be disclosed to external partners in order to ensure their effective involvement in a NATO mission. On the other hand, the disclosure of certain other pieces of information may negatively affect the outcome of the mission and should clearly be avoided.

In current NATO operations, timely sharing of information is hampered as a result of a number of limitations that are inherent to the traditional use of security markings, the two most important of which are the following. First, a security marking reflects the protection requirements and release conditions of a resource at the time of creation. Only manual (time-consuming) intervention can be used to update the markings to accommodate changes in security constraints, following strict information management procedures that may involve consultation with the resource originator (when possible). Second, owing to subjective interpretations of the security policy, resource originators may derive different security markings for resources with similar content. This leads to a situation in which similar resources are protected in different ways, leading to under- or over-restricted information sharing. To overcome these limitations, NATO is developing a new information sharing infrastructure [5] that uses (XML-based) content metadata to enable decisions about the release of information according to *Content-based Protection and Release (CPR)* policies. Access control decisions are taken by considering the attributes (e.g. the clearance) of the user re-questing the resource, the content metadata associated with the various pieces of information in the requested resource (e.g. the paragraphs comprising a text), and the capabilities of the *terminal* (i.e. the device and connection used by the requester to access the resource) that are related to processing, storing, and transmitting data. CPR policies aim to overcome the limitations introduced by the use of security markings discussed above by separating the association of attributes with resources from the process of determining their protection requirements and release conditions. The attributes of a resource are content properties used to derive access decisions by taking into consideration also the attributes of users, those of terminals, the protection requirements and the release conditions specified in appropriate policies by NATO security experts. This greatly reduces errors due to subjective interpretations of security directives, ensures the homogeneous protection of resources with similar content, and permits timely changes in release or protection policies to reflect evolving security requirements.

In this paper, we focus on the access control component of the NATO information sharing infrastructure. We first review the access control model of CPR policies (Section 2). We then present the enforcement architecture for CPR policies, which are designed to be easily built on top of available (service-oriented) infrastructures for identity and access control management (Section 3). Finally (Section 4), we describe a demonstration of the enforcement of CPR policies for use case scenarios drawn from the NATO Passive Missile Defence (PMD) system (see e.g. [5]), which simulates the consequences of intercepting missile attacks. The demonstration shows how maps generated by the PMD system are filtered to produce appropriate views for users of both NATO and civilian organizations, and prevent the disclosure of sensitive information to untrusted users.

2. Overview of the CPR Access Control System

Modern joint military missions rely on network-centric operations. The NATO information sharing infrastructure [5] is built around an access control component that operates in an open and distributed environment. It has been observed that traditional access control models - such as discretionary (DAC), Mandatory (MAC), and role-based

(RBAC) models - are not always adequate in this environment [2]. The Attribute-Based Access Control (ABAC) model (see e.g. [3]) offers a powerful and unifying extension to these well-known models.

In ABAC, requesters are granted or denied access to a resource based on the properties, called attributes, that may be associated to users, resources, and the context. Examples of attributes are identity, role, and military rank of users; identity, precision, and sensitivity of resources; time of day and (some part of) the system state for the context. In ABAC, suitably defined attributes can represent security labels, clearances and classifications (for encoding MAC), identities and access control lists (for DAC), and roles (for RBAC). In this sense, ABAC supplements traditional access control models rather than supplanting them [3]. Policies in ABAC can be seen as conditions on the attribute values of the entities involved in an access decision or, in other words, they are Boolean functions that map the attribute values of the user *u*, the resource *r*, and the context *c* to true ("permit") when *u* is entitled to get access to *r* in the context *c*, and false ("deny") otherwise.

The model underlying CPR policies can be seen as a refinement of ABAC in three respects. First, in addition to the attributes of users, resources, and the context, those of terminals are considered, i.e. the capabilities of the device through which a user is trying to access a resource. Examples of terminal attributes are the hardware model, the type of encryption used to locally store data, and the type of connection to the terminal (e.g. SSL).

Second, the CPR (access control) policies are structured in two distinct sub-policies:

- a release policy, taking into account user, resource, and contextual attributes
- a protection policy, taking into account resource, terminal, and contextual attributes.

This enables separation of policy management roles and reflects the current procedures used within international and govern-mental organizations, including NATO. For example, consider the situation in which a user wants to access NATO classified information. This requires, on the one hand, connecting to a network infrastructure used for processing NATO classified information. To do this, a terminal must satisfy a number of technical requirements related to hardware and software configuration that are precisely defined in NATO technical directives and guidance documents. On the other hand, the security policy governing user access to the documents stored in the network is defined in a separate set of directives and guidance documents.

Third, access in CPR is content-based, i.e. decisions about the release of information are derived from content metadata. (For simplicity, a read-only mode for accessing information is considered in this paper.) Depending on the granularity with which content metadata is associated to (pieces of) a resource, access requests are then answered with *permitted views*, i.e. selected pieces of a resource that the user is allowed to access, and not with a simple "permit/deny" answer. Granular association of content metadata to information is particularly suited when resources are structured as containers of information that may recursively contain other structured or atomic resources, each one with its own content metadata. A mechanism for the fine-grained association of attributes to selected pieces of information in structured resources is NATO XML-labelling [4], which allows for the binding of extensive content-metadata structures to subsets of an XML node set. In general, a typical structured resource is an XML document in which content metadata is captured in XML attributes for each of the elements in the document. Access control systems for XML documents have already been proposed in the literature. While we believe that some of the techniques used in these works (e.g. [1]) can be adapted to enhance the performance of the CPR access control system when mediating access to XML documents, our work is more general as it aims to mediate access to a variety of structured resources (ranging from PDF files to military documents in proprietary formats) in a way that is transparent to the user.

Abstractly, the CPR access control system mediates the request to read the content of a structured resource *r* submitted by a user *u* with a terminal *t* in two phases. First, it retrieves the attributes of *u* and *t* together with those of all the (sub-)resources contained in *r*; let *R(r)* be their set. Second, it builds the permitted view of the resource derived from *r*, which is composed of only those resources in *R(r)* that *u* is permitted to view by using *t* according to the given release and protection policies. When none of the resources in *R(r)* can be accessed by *u*, "deny" is returned.

3. Architecture of the CPR Access Control System

The OASIS standard XACML (eXtensible Access Control Markup Language)[1] is an ABAC framework, in which attributes associated with requesters, resources, and the context are used to decide whether a given user may access a resource in a particular context. The XACML standard defines, in addition to a declarative access control policy language implemented in XML, an architecture for the enforcement of policies describing how to evaluate authorization requests according to the rules defined in policies. Since CPR policies can be seen as a refinement of ABAC policies (as argued in Section 2), we propose an architecture for the CPR access control system that can be easily integrated with the XACML framework. Figure 1 shows the architecture of the CPR access control system. Readers familiar with XACML can easily

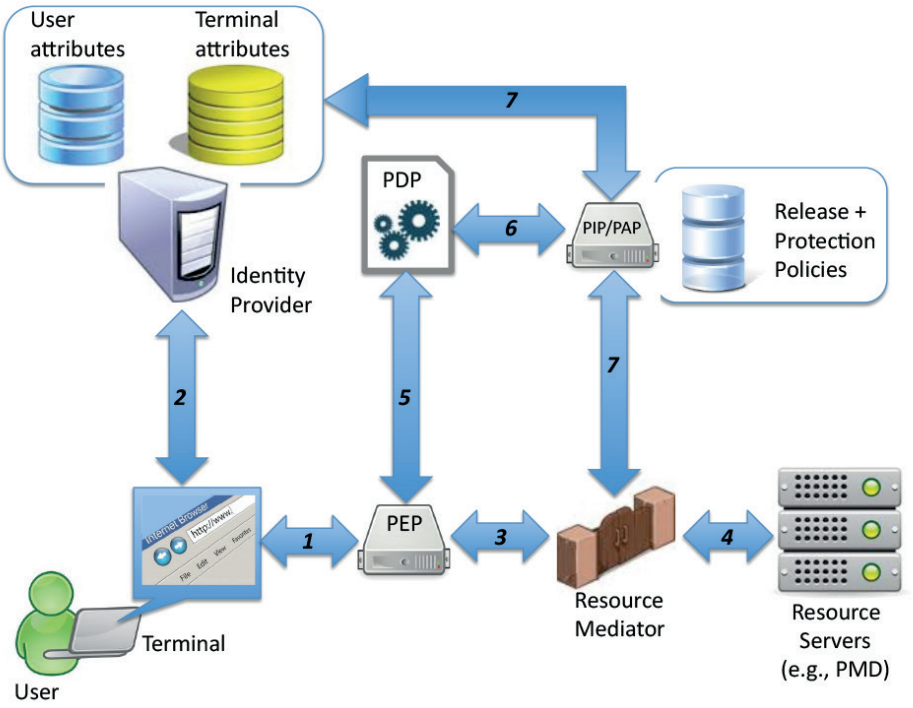

Figure 1: CPR Access Control System Architecture

recognize the use of four modules (PEP, PDP, PIP, and PAP, whose role is explained below) that are part of the XACML architecture for policy enforcement defined in the OASIS standard. The integration of these components in the CPR access control system has been designed to solve three main issues that are specific to information sharing in NATO missions.

First, CPR policies take into considerations terminal attributes in addition to users, resources, and contextual information (as is standard in ABAC). In XACML 3.0, the *AttributeDesignator* construct allows for the addition of attributes to pre-defined categories (i.e. *subject, resource, environment*, and *action*) and the definition of attributes for custom categories, such as one for terminals in CPR. In the architecture of Figure 1 (upper left corner), user and terminal attributes are encapsulated in credentials that are stored in two databases, managed by an Identity Provider (IdP).
This offers support for the authentication of users via, e.g., Single-Sign-On (SSO) solutions, and of terminals (devices) by using, e.g., Trusted Platform Modules (TPM). When the condition of a rule in an XACML policy involving users or terminals needs to be evaluated, their credentials are retrieved from the appropriate database.

Second, CPR policies base authorization decisions on the various pieces of information contained in a resource. Since NATO missions involve several types of resource, the role of the Resource Mediator (bottom of Figure 1) is to maintain the association between identifiers (e.g. URIs) of composed and atomic resources with their attributes. For this, it is assumed that dedicated sub-modules that are capable of retrieving both the identifiers and the attribute-value pairs of atomic resources are available. Indeed, the design and implementation of these sub-modules depend on the types of resources. There are some general approaches that can be taken to address this task. For example, the XACML 3.0 Hierarchical Resource Profile[2] may be used to handle resources organized as hierarchies. Another approach could be the use of the NATO XML-labelling specification [4] that permits the association of content labels to a variety of resources.

Third, access decisions are not simply "permit" or "deny" but consist of permitted views of the requested resource, containing only that information that can be accessed by the requester. This implies that a request to access a composed resource *r* must be expanded into several access requests, one per resource contained in *r*. This is made possible by the Resource Mediator, which is capable of extracting both the identifiers of each resource in *r* and their associated attributes. In this way, a set of multiple resource access control requests can be formed, once the attributes of users, terminals, and environment have also been obtained. XACML 3.0 offers support for multiple requests via the so-called Multiple Decision Profile, which allows performance improvements by packing multiple access queries into one XACML request.

We now describe the data flow underlying the architecture in Figure 1, where the double arrows stand for request-response interactions. A user *u*, via a terminal *t*, makes a request to the available *Resource Servers (RS)* using a browser. The request is intercepted (arrow 1) by a *Policy Enforcement Point (PEP)*. If *u* and *t* are not yet authenticated, the browser is redirected (arrow 2) to the IdP, which is responsible for authentication. Then the PEP forwards (arrow 3) the request to the *Resource Mediator (RM)*, which selects the appropriate RS and forwards (arrow 4) the request to it. The RS retrieves the resource from a database or performs some computation to build it. Once available, the resource is passed back to the RM, which assigns it an identifier *r* and extracts the set *IAV (r)* of pairs $(r', A_{r'})$ where *r'* is the identifier of a resource in *r* and *A_r'* is the associated set of attribute-value pairs (if *r* is atomic, then *IAV(r)* contains just one pair *(r, A_r)*). At this point, the RM sends to the PEP (arrow 3) the set $R(r) = \{r' | (r', A_{r'}) \in IAV(r)\}$ of resource identifiers in *r*. In turn, the PEP sends to the *Policy*

[1]http://docs.oasis-open.org/xacml/3.0/
[2]http://docs.oasis-open.org/xacml/3.0/xacml-3.0-hierarchical-v1-spec-cd-03-en.html

Decision Point (PDP) (arrow 5) a tuple composed of the identifiers of *u* and *t* (e.g. the tokens obtained from the IdP during authentication) together with the set *R(r)*; such a tuple encodes the (multiple) request of the user *u* to get access to all those resources in *R(r)* that he/she is allowed to view using terminal *t*. The *Policy Information Point (PIP)* is asked (arrow 6) to retrieve the attributes of *u* and *t* from the databases (right-angled arrow 7) together with the attributes of the resources in *R(r)* from the RM (vertical arrow 7). The latter can be easily extracted from the set *IAV(r)* that is stored in the RM.

At this point, the PDP returns to the PEP (arrow 5) the collection of decisions for the multiple resource request under the pre-defined CPR policy (obtained as a combination of release and protection policies). This has also been retrieved by the PIP, which also acts as a *Policy Administration Point (PAP)* in our architecture. The reason to merge the PIP and the PAP is to provide the possibility to pre-process policies so that only those constraining the attribute values of *u*, *t*, and (most importantly, because of the variety of the type of resources and potentially large number of associated attributes) *r* are included, as those that do not mention them are certainly not applicable. In this way, a "permit" or a "deny" decision is associated to each resource identifier in *R(r)* and the PEP can ask the RM to compute the permitted view *r'* of *r* by including only those resources in *R(r)* for which the PDP has returned "permit." Finally, the PEP sends *r'* back to the browser (arrow 1). We have implemented the architecture in Figure 1 on top of the WSO2 Security & Identity Gateway Solution[3] that supports authentication based on SAML 2.0[4] and authorization through XACML.

4. The NATO Passive Missile Defence Demonstration

The goal of the NATO Passive Missile Defence (PMD) system is to minimize the effects of missile attacks. The PMD system runs simulations of a missile attack in a given geographic area by taking into account several parameters, such as the type of missile employed in the attack and weather conditions. As a result of the simulation, a map of the predicted missile impact area is calculated, enriched with annotations about a description of the consequences of the impact at several locations, hazard areas with risk analysis, the trajectories of the threatening and intercepting missiles, sub-munition locations and descriptions, etc.

The maps are represented in the XML-based Keyhole Markup Language (KML) so that, e.g., Google Earth can be used to visualize them (see e.g. Figure 2). The PMD system is an important component of NATO missions for crisis-response planning and disaster preparation. In this context, missions require the coordination of coalition partners with civilian organizations (e.g. for rescue and medical operations). Thus, sharing (selected parts of) the content stored in KML

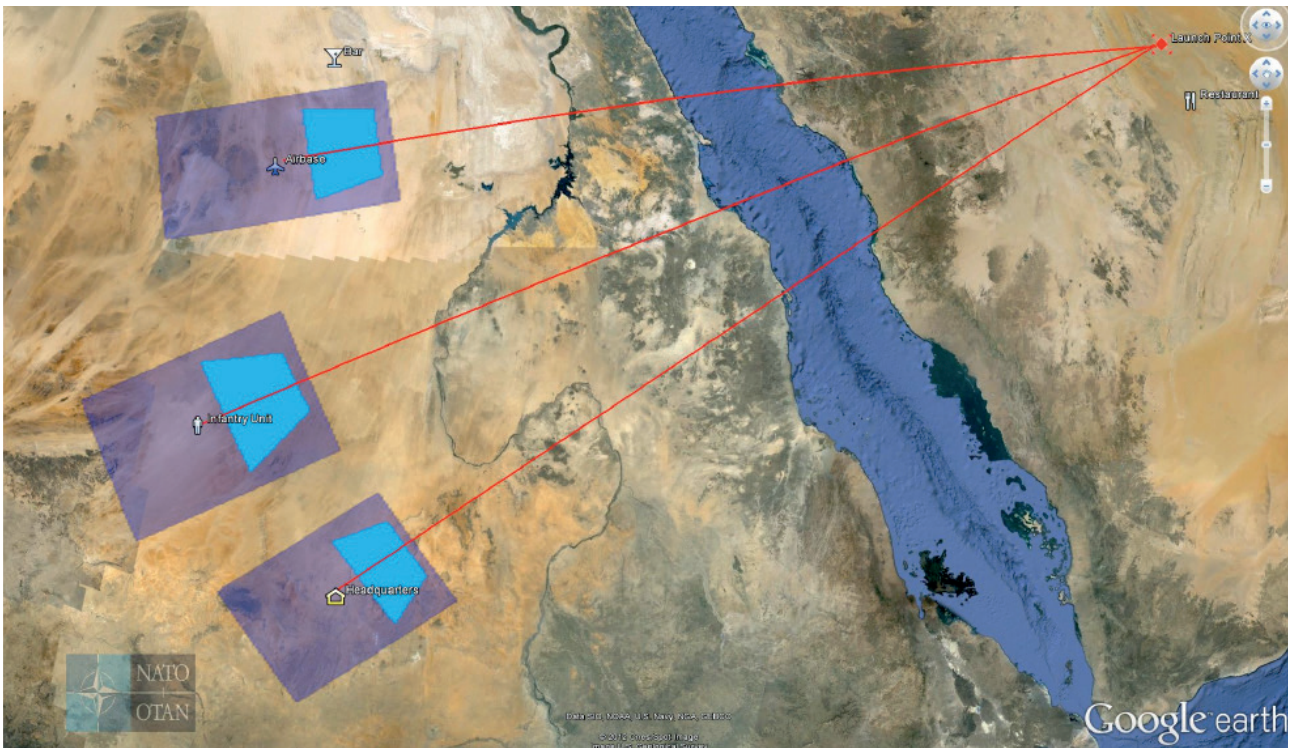

Figure 2: A KML map generated by the PMD system with missile trajectories and hazard areas

[3]http://wso2.com/solutions/security-and-identity-gateway/
[4]http://docs.oasis-open.org/security/saml/v2.0/

maps created by the PMD system is crucial for the success of a mission. When we demonstrate the system, we show that the CPR access control system of Figure 1 can support the disclosure of information depending on suitably defined CPR policies, such as *(a)* a soldier may see sub-munition locations and descriptions while a civilian cannot (this depends on the clearance of the user and is part of the release policy), *(b)* a soldier taking part in the operations in the area of the PMD simulation can access the map, but a soldier not involved in the mission - even one with a high rank - cannot (this is an instance of the need-to-know principle and is again part of the release policy), and *(c)* to access the description of the consequences of intercepting the missile, the terminal should have an enhanced configuration guaranteeing a secure connection and local encryption of data (this condition depends on the capabilities of terminals and is part of the protection policy).

The system demonstration is structured as follows. First, we illustrate the CPR policies and some sets of attribute values that characterize typical users and terminal profiles in military and civilian organizations. We show a complete KML map that the PMD system has generated as the result of running a certain simulation; for an example, see Figure 2. We then consider the map as a KML file and its graphic rendering by Google Earth. We make explicit the relationship between the graphical objects and the corresponding KML resources together with their identifiers and attributes (content metadata). This concludes the overview of the attributes and allows us to present excerpts of the XACML file containing the CPR policy sketched above: the evaluation of some conditions on the attributes will be demonstrated on the users, terminals, and resources previously considered. The demo is concluded with a step-by-step execution (cf. the dataflow in Figure 1) of some resource requests and a comparison of the permitted views of the same map accessed by different users and terminals.

5. References

[1] E. Damiani, S. De Capitani di Vimercati, S. Paraboschi, and P. Samarati. A fine-grained access control system for XML documents. *ACM Trans. Inf. Syst. Secur.*, 5(2):169-202, May 2002.

[2] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, and P. Samarati. Access control policies and languages in open environments. In T. Yu and S. Jajodia, editors, *Secure Data Management in Decentralized Systems.* Springer, 2007.

[3] X. Jin, R. Krishnan, and R. Sandhu. A Unied Attribute-Based Access Control Model Covering DAC, MAC and RBAC. In *DBSec'12: Data and Applications Security and Privacy XXVI.* Springer, 2012.

[4] S. Oudkerk. NATO Profile for the `Binding of Metadata to Data Objects' - version 1.0. Technical Note 1455, NC3A, The Hague, Netherlands, 2011.

[5] K. Wrona and G. Hallingstad. Development of High Assurance Guards for NATO. In MCC'2012: Military Communications and Information Systems Conference, 2012.

For more information contact us:

Dr Konrad Wrona
NATO Communications and Information Agency
Cyber Defence and Assured Information Sharing
konrad.wrona@ncia.nato.int

Mr Vassil Iordanov
NATO Communications and Information Agency
Missile Defence, Service Supply
vassil.iordanov@ncia.nato.int

NATO Communications and Information Agency
Agence OTAN d'information et de communication

Bâtiment Z
Avenue du Bourget 140
1110 Brussels
Belgium
www.ncia.nato.int

NCI AGENCY