2011 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
VEHICLE ELECTRONICS AND ARCHITECTURE (VEA) MINI-SYMPOSIUM
AUGUST 9-11 DEARBORN, MICHIGAN

Attribute-Based Access Control (ABAC)- Is it the Solution for a Mobile Net-Centric Army?

Joseph Mangin,
CISSP, ISSAP, ISSMP
Control Point Corporation
Goleta, CA

Jonathan Dorny
Control Point Corporation
Goleta, CA

ABSTRACT

Access Control sets the bounds directing use of a resource. Equipment, applications, and information in a military environment require access control to provide security where intelligence superiority is an integral part the battlefield. The Role-Based Access Control (RBAC) employed for Information Systems and IT networks where permissions for Army roles change slowly do not scale to the dynamics of distributed mobile systems in a rapidly changing tactical environment. As ground systems fulfill the Net Centric Warfare (NCW) charter, Attribute-Based Access Control (ABAC) provides a distributed, rule-based approach to support dynamic attributes for access control.

INTRODUCTION

This paper identifies strategies for achieving access control for ground systems within a tactical environment where resources and users are changing quickly. Rapid adaptations by enemy combatants and unfriendly foreign powers require rapid responses to change rules for new security policies. The strategies identified herein can be extended to encompass the Army enterprise at the tactical and national level with consistency across these domains to enforce consistent resource access and data strategy policies.

PROBLEM STATEMENT

Access control may be defined as guarding the use privileges for a resource. Examples of a resource are equipment (e.g. computing communication), software (e.g. service, application), or information. The Net Centric Warfare Key Performance Parameter (NCW KPP) has applicability to all warfighter systems and business systems in the Army and is enforced to ubiquitously share information throughout the Army. The value of shared information and readily available software services is apparent. However, the network connectivity of all systems is in direct opposition to the most fundamental security tenet which is to eliminate physical access.

The primary problem is one of offering an optimal level of resource service availability while restricting use to those currently authorized to perform a task utilizing that resource. A “plug-and-play” Mission Equipment Package (MEP) introduces an additional level of complexity since it needs to inherently carry access control of the MEP resources in context of when and where they are installed. Context is important in that a user or application that has permissions in one environment may not be granted permissions in another environment.

Access control in the Army, especially in the tactical warfighter systems, needs to provide flexibility and ease in making rapid adjustment to those able to use resources. The ability to do this requires a holistic methodology that accommodates policies and doctrine of the Army, Standard Operating Procedures (SOP) of a unit, and tactical field adjustments without changing the Military Occupational Specialties (MOS) in place. It must simplify the ability to make rapid changes. Essentially, the objective is to create a highly adaptive service oriented architecture (SOA) that will provide the right resources to the right people or applications to perform their job at the right time, regardless of location.

Challenges

The challenge of implementing this type of access control is in defining the relationship between requestors, resources, and use permissions. The complexity increases exponentially with the number of users and resources available. Simplification is achieved through reducing the kinds of users or resources. A corollary to this is a reduction in the resolution and distinction between users and resources. The complexity is further exacerbated when permissions are conditional on the operation being performed, the business process workflow, or the environment. An example of this is a supply clerk's access to the supply information system. Access may always be granted to the system, or additional specificity may be provided to order parts (operation), or to order parts that have been approved by a supervisor (workflow), or with the additional stipulation that it must be their shift (environment). More finely-grained access control rules may provide higher levels of security, but need to be weighed against flexibility, complexity, and maintenance.

A mobile environment invokes additional challenges. Centralized decision tools holding and enforcing the access rules provide the best method for consistent policies across the enterprise. In a mobile workforce these tools are often not available. Without this availability, there is a need to distribute access permissions to a local computing device prior to network disconnection. If this is not done, then all access is disrupted between all users and all resources, even those resources that are still connected locally and would ordinarily be available. Backdoor "super user" login mechanisms to avoid this total system failure introduce an unacceptable vulnerability.

Additionally, ground systems in the Army are often re-assigned for operational control outside of their property assignment and may be supported by another organization. Individuals are allocated dynamically based on op-tempo and mission needs. This dynamic assignment further establishes a challenge in setting up and administering permissions that enforce access control.

POTENTIAL STRATEGIES

In support of information sharing initiatives, the DOD is evaluating access control mechanisms that provide fine-grained access control to anticipated and unanticipated users within dynamic communities of interest (COIs) at the tempo of mission operations. Several potential strategies are defined further in the sections below.

Access Control List (ACL)

The ACL paradigm centers on the traditional need to know policy. There is a direct connection between a requestor and a resource. In an ACL environment, each resource has its own mappings of requestors and their set of actions allowable. As an example, an individual may be given rights to add, delete, or modify data in a database. Setting up ACLs for individual resources is an administrative burden when large groups of resources are involved or when people need access to multiple resources. In addition, there is limited scalability at the enterprise level, increased security risk, and inability to support dynamic mission operations.

Role-based Access Control (RBAC)

RBAC technology addresses some of the issues with the ACL paradigm. RBAC defines access control policy based on the relationship between the requester and the organization or controlling owner of the resource. Individuals or applications are categorized into roles that govern their permissions based on function or operation. Users are then assigned a role. In addition, RBAC allows for hierarchies and inheritance of permissions where an individual can belong to various roles enjoying the union of access rights. RBAC integrates at the application level, fostering scalability where a single middleware product can control access to multiple systems and resources. This is favorable in a NCW SOA environment.

RBAC inherently contains several disadvantages that prevent it from fully meeting operational needs of a mobile ground system. RBAC is unable to define granular access controls for subsets of users without defining a large number of roles. For example, a maintainer from Company A cannot be excluded from using maintenance equipment in Company B without establishing separate roles. This commonly leads to the proliferation of roles that over time often become difficult to manage, maintain, and enforce. Furthermore, RBAC still requires a registration process to assign a user to a role and ultimately provide a user access to resources. This pre-registration imposes a skilled administrative burden and is ineffective to support dynamic mission operations. RBAC operation requires roles to be under a single administration or to have a consistent role definition across domains, which makes distributed applications in a mobile workforce environment challenging.

RBAC is effective in applications where permissions associated with an organization's roles change slowly over time, but dedicated, skilled IT personnel may be added, removed, or change roles of users rapidly. [1]

Attribute-based Access Control (ABAC)

In order to address such concerns, ABAC provides a method to dynamically and autonomously discern an individual within a group and selectively direct access based on a fine grained set of attributes. ABAC enforces access control decisions based on attributes of the requester, the resource, and the environment within the context of a workflow transaction. ABAC process begins with a requester presenting their attributes (e.g. perhaps extracted from a CAC card) and an access request to a policy enforcement point (PEP). A Policy Decision Point (PDS) supports the PEP evaluating the attributes (requestor, resource, environment) in context of the applicable workflow policies. If approved, the PEP grants permission for the context of that transaction. ABAC promotes the use of attributes for rule-based access control decision making, which begins to address some of the needs of today's dynamic environment. However, a limiting factor of the ABAC method is the potential for inconsistent attributes and access control policies across domains in an extended enterprises such as the DOD. In a global or enterprise wide environment, it is necessary to harmonize access control strategies in order to meet enterprise governance requirements, support dynamic communities of interest (COIs) and include unanticipated users.

To summarize, ACL provides access to resources (e.g. can read and write the logistics database). RBAC provides permissions by operation (e.g. can add a fault, but not modify it). ABAC enables permissions associated with workflow (e.g. maintainer from another unit is denied entering a fault, because they are not part of this unit's workflow).

OUR APPROACH

Our access control approach implements the ABAC strategy utilizing workflow enforcement tools for a mobile environment. Our strategy includes:

1. Definition of access control organizational rules in the context of workflow responsibilities that include requestor, resource, and environment attributes
2. Centralized repository managing access control rules across domains
3. Distribution of workflow access control rules to mobile nodes for delegated local enforcement
4. ABAC execution locally, connected or disconnected, utilizing available attribute information

To support warfighter operations, the access control function needs an adaptive framework to accommodate increased mission tempos and changing mission needs. In this framework, users gain access seamlessly without pre-registration, while at the same time protecting services and data from exploitation.

Access Control Framework

The use of a well-structured and documented *Access Control Framework* will help coordinate permission policy definition and execution across the Army in support of a net-centric mobile ground force. The Access Control Framework should provide:

1. Alignment of policies, procedures, and strategies across domains for access to resources within the constructs of Army business processes
2. A holistic architecture that accommodates centrally-managed access permissions rules for connected, disconnected, and resource constrained computing devices fulfilled through distributed, adaptive execution
3. A technical foundation for tools that empowers a COI to establish a business-centric definition of access control rules
4. Foundational solutions that enable the execution of ABAC rules in a highly flexible and reconfigurable mobile environment

As depicted in Figure 1, the Access Control Framework provides a vision of the mechanisms required to confine the complexities to the analysis and design of interoperable net-centric systems. Effectively communicating the processes and architecture to MEP suppliers, Ground System suppliers, and Information System suppliers enables the responsible Information Assurance/Security authority to meet their objectives. This will simplify field support, minimize review of network additions for vulnerabilities, and accelerate approvals to operate. A common framework will also enable the selection of tools and products that will further speed the process and provide consistency of approval expectations.

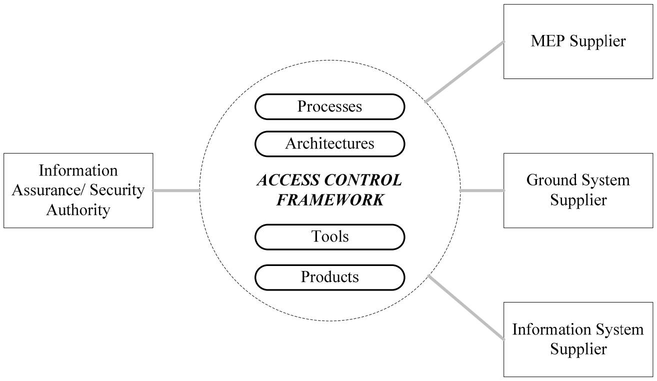

Figure 1 – Access Control Framework

Failure of suppliers to adhere to the framework will incur significant degradation of the advantages of ABAC to provide a flexible, scalable, and dynamic solution for access control where users, roles, and permissions do not need to be statically assigned a priori.

Business Process Alignment

The ABAC methodology is well aligned with the current DOD approach to integrated architectures. ABAC wants to associate the requestor (producer) with the resource (consumer) in context of a business process flow that considers the environment in which the transaction is invoked. The Department of Defense Architectural Framework (DODAF) identifies a number of views that identify resources and the services provided to requestors (ref. Table 1). The Event Trace models the allowable use of resources within business process flow and is used to gain consensus within doctrine, policy, and procedural constraints.

Table 1 - DODAF Views Enabling Alignment

DODAF View	Description
SV-6c Systems Resource Flow Matrix	Provides details of system resource flow elements being exchanged between services and the attributes of that exchange.
SV-10a Systems Rules Model	Identifies constraints that are imposed on systems functionality due to some aspect of system design or implementation.
SV-10c Systems Event-Trace	Identifies system-specific refinements of critical sequences of events described in the Operational Viewpoint.
SrcV-6cServices Resource Flow Matrix	Provides details of service Resource Flow elements being exchanged between services and the attributes of that exchange.
SrcV-10a Services Rules Model	Identifies constraints that are imposed on services functionality due to some aspect of system design or implementation.
SrcV-10c Services Event-Trace	Identifies service-specific refinements of critical sequences of events described in the Operational Viewpoint.

The Rules Model establishes the environmental attributes and permission constraints imposed on the resource functions within the context of a transaction within a workflow. The Resource Flow Matrix solidifies the attributes that must be presented by a requestor to invoke a transaction with a resource.

It is essential to overcome one of the weaknesses of ABAC that consistency of attributes and rules be established across domains within the Army. DODAF tools provide an environment where different systems can integrate their architectures to achieve interoperability. The DODAF does not specify the format required to express those views. Therefore, it is proposed that the Access Control Framework dictate the format for expression. The Unified Modeling Language (UML) provides a good representation for Event Trace. The Organization for the Advancement of Structured Information Standards (OASIS) has established an open industry standard eXtensible Access Control Markup Language (XACML) for expressing the rules and governing interpretation for ABAC. Our approach recommends XACML as the standard format for expressing the Rules Model for a system. To facilitate holistic access control, domains that interoperate should integrate their DODAF models together.

Central Management, Distributed Control Architecture

As previously discussed, mobile ground systems in a tactical environment cannot rely on “always-on” connectivity for centrally controlled access permissions. Ground systems, their MEP and their support equipment can be classified as resource-constrained computing devices. These devices are characterized by limited memory, limited storage, limited processing power, and limited or unreliable network connectivity. These types of devices become more powerful as they are dynamically organized into networked resource pools available to any requestor with permissions.

Often these types of devices in the Army will be configured in the field to fulfill immediate real-time operational threads or non-real time business workflows as tactical situations dictate. All of the resources are then available, but they cannot depend on a connection to the Global Information Grid (GIG) to support them in centralized access control.

However, a centrally managed repository of ABAC rules is advantageous for version control, integrity, compliance, and reuse. As business workflows often span across computing devices, nodes, networks, and domains a central application (whether monolithic or federated) that distributes local rules to middleware co-located with specific resources provides a strong deployment architecture for a mobile, net-centric Army. As noted in Figure 2, the architecture required for this dynamics reconfiguration of resource pools is dependent on equipment inherently maintaining and providing attributes about themselves or those they represent (e.g. display represents the user and their entered attributes).

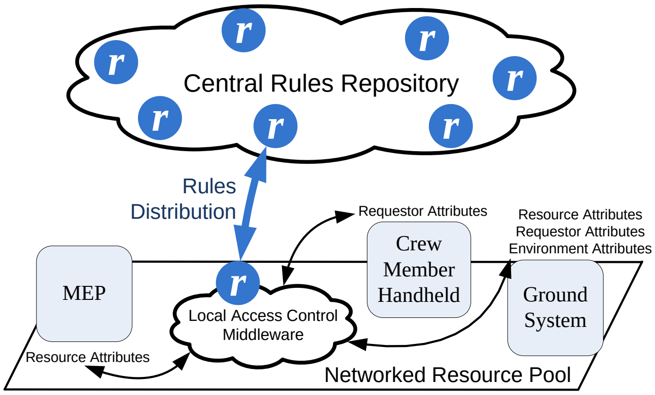

Figure 2 – Distributed Rules Architecture

This deployment architecture where rules are centrally managed, but distributed for delegated access control at resource constrained devices is essential to overcome the burden of managing the ABAC rules in a very distributed application environment.

Access Control Framework Tools

With the architecture understood and in place, the next need of the Access Control Framework is to provide tools for defining and authoring workflows and their associated XACML policies and rules. This is an area that requires additional work in the future. Some tools exist for authoring workflow that are deployable for execution, such as Business Process Execution Language (BPEL) tools. However, these tools do not automatically create XACML documents.

There are some XACML authoring tools available, such as XpressRules, a SBIR-stimulated software developed with the non-programmer policy officer in mind. This is essential if access controls are to be modified by those who are able to change SOP in real time to meet mission demands. The tools need to provide a simple way for them to describe the new SOP, have it accepted within the central rules repository, and have all of the middleware for all participating requestors and resources update.

Industry continues to clamor for additional tools, which is a benefit to the Army. As XACML is an open industry standard, there are a number of commercial companies that will continue to advance the state-of-the-art in tools for authoring and the Army will benefit over time.

Foundational Solutions

The greatest concern in any framework is the practicality of implementation. Complex systems are defined as those where the sum of the parts exhibit a behavior that was unexpected. Army ground systems in a net-centric environment responding to ever-changing tactical missions definitely fit the definition of complex systems. Is the architecture implementable?

There is an associated programs, the Common Logistics Operating Environment (CLOE) that has addressing this reconfigurable, net-centric ground system environment for the last six years. Recently, the US Army's Logistics Innovation Agency (USALIA) and Control Point Corporation have demonstrated a Common Information Management Service (CIMS) within a System Integration Lab (SIL) environment proving the ability to centrally manage, distribute, and execute business rules within a workflow. The capability to execute a workflow or enforce business rules is not new. However, proving the ability to coordinate this across nodes that are often disconnected is significant. Unique is the ability for nodes to dynamically organize in a peer-to-peer topology for information sharing rather than a "hub-spoke" topology. This is essential for dynamic resource pools and the local access control they require within our framework.

CIMS is targeted for logistics information sharing, but at the core of CIMS is a commercially available product the Information Management Grid Service (IMGS). As illustrated in Figure 3, IMGS contains capabilities that can be configured to implement the Access Control architecture. Messages from a Requestor are placed on a service bus including their attributes within the message. IMGS validates the message is valid and from an expected source according to the workflow control (ABAC PEP functionality). Then, the decision rules associated with that message are retrieved from the local repository (ABAC Policy Store functionality). IMGS processes the decision rules to determine the access control action to take utilizing requestor, resource, and (ABAC PDP functionality). If the algorithm is successful, then the workflow control mechanism formulates (e.g. transformation, generation, or forward) a message and coordinates transfer to the Resource to fulfill the business transaction. When new policies and rules are established the rules synchronization capability assures that the correct version of the rules is synchronized with the central version repository.

Essentially, there are three stages in the access control process. First, validate the message is good. Second, confirm the requestor is permitted to request that resource perform that action. To do so, the Requestor attributes are received in the message, the Resource attributes are stored at the node, and the Environment attributes are collected at the node. Finally, the next action in the transaction is invoked, providing access control at a granularity down to an individual transaction within a workflow.

CIMS continues to mature and is expected to increase confidence that there are foundational tools available currently that support the Access Control Framework presented.

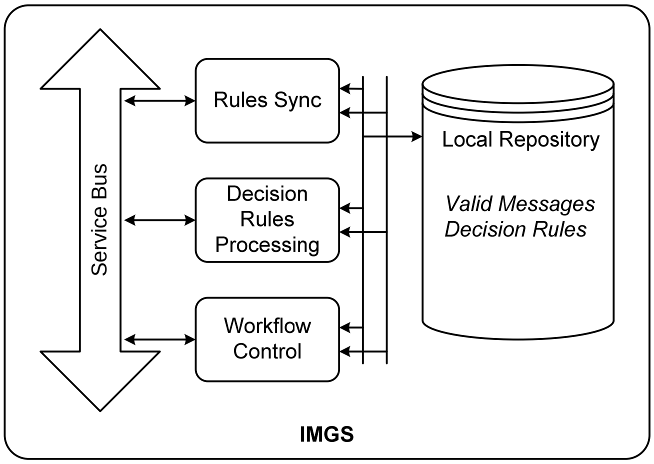

Figure 3 – Foundational Solution Capabilities

CONCLUSIONS

Attribute Based Access Control (ABAC) is a viable option for net-centric mobile ground systems when combined with a holistic Access Control Framework that overcomes the liabilities of ABAC in standard IT environment. The framework presented can accommodate unexpected users, plug-and-play installation of Mission Equipment Packages, and rapidly changing policies. The administrative burden is minimized and the analysis required to initially set up a deployment is virtually eliminated as it is incorporated within the standard architectural expectations of the acquisition process. However, the success of this approach is dependent on all systems employing the same strategy.

REFERENCES

[1] *Adding Attributes to Role-Base Access Control*. **Kuhn D. Richard, Coyne Edward J., Weil Timothy R.** IEEE Computer Society，79-81. （0018-9162/10.