IMPLEMENTING ATTRIBUTE BASED ACCESS CONTROL IN THE FEDERAL ARENA

Recently, the United States Government has shown a considerable interest in Attribute Based Access Control (ABAC) as a means to improve information sharing and IT security. The Federal government is making it a priority to update existing access control infrastructures that use authorization leveraging Role Based Access Control (RBAC) or Identity Based Access Control (IBAC) using Access Control Lists (ACL). Some organizations have even older models such as Discretionary Access Control (DAC) and Mandatory Access Control (MAC).

In 2005, Hurricane Katrina (and similar national emergencies since) emphasized the need for multiple Federal, state, and local agencies to share information in a dynamic and flexible manner. The WikiLeaks Incident in 2010 highlighted the government's needs to further protect and secure its classified materials. The focus on ABAC is a reaction to very real events in our nation that have highlighted the need for a more dynamic, more adaptable logical access control method to protect its resources.

The Federal Requirements

Implementing ABAC in the Federal arena became a major priority with heightened visibility when President Obama signed Executive Order 13587 in October 2011[1]. This action made it one of the five priority areas for structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information. Understanding the history and purpose behind the Federal mandates is vital to ensure goals and deadlines are accurate and the project approach is appropriate.

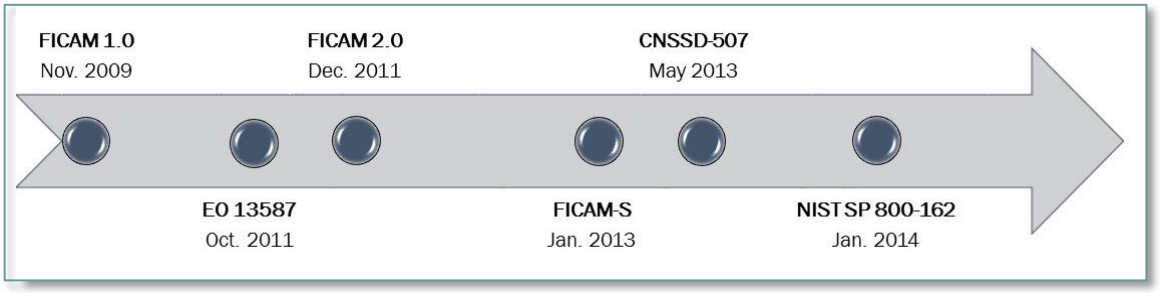

Figure 1 – High level timeline of ABAC related requirements and guidance

The Federal Chief Information Officers Council (Federal CIO Council) published the Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Plan version 1.0 in November 2009, which provided direction to Federal agencies to progress their logical access control architectures to include attributes in the decision process. Executive Order 13587, as mentioned previously, was distributed in October 2011 and established the Senior Information Sharing and Safeguarding Steering Committee (SISS SC) that developed what are referred to as the "Five Priority Areas", one of which is Access Control. Soon after, in

[1] Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011

December 2011, FICAM Roadmap and Implementation Guidance version 2.0 was released which specifically called out Attribute Based Access Control as the recommended model to improve the security and responsible sharing of classified information and networks. The Committee on National Security Systems (CNSS) also released Recommendations for Implementing FICAM on U.S. Secret Networks in January 2013, and soon after, CNSSD-507 was released in May 2013 to establish the mandate to implement the capabilities embodied within FICAM 2.0 on the Secret Fabric (secret applications, systems, and networks owned, operated, or maintained by the Federal government). Most recently, in January 2014, the National Institute of Standards and Technology released NIST Special Publication 800-162 in an attempt to define Attribute Based Access Control and provide Federal considerations for implementation. This document has become the primary reference for the Federal ABAC definition.

Additional ABAC policy drivers exist that are not mentioned above, and Federal agencies must understand all of the guidance provided to support their compliance. One major way that agencies remain compliant with these mandates is by answering affirmatively to the Key Information Sharing and Security Indicators (KISSI). Several KISSI questions are specifically related to implementing ABAC at a Federal agency:

- Does your agency have an Implementation Plan?
- Do you have the capability to provision user attributes to support ABAC?
- Are your applications integrated to use the interoperable ABAC infrastructure facilities?
- Is it integrated with PKI authentication?
- Do you have the capability to federate attributes across organizations?
- Do you tag or mark new and legacy data with access-relevant attributes?

These questions point towards a Federal government with a well-established, fine-grained, and federated ABAC model, implemented across classified domains with enhancements to interoperability made to multiple IT infrastructures.

What is Attribute Based Access Control?

The main difference between ABAC and access control models that use RBAC or ACLs is the use of dynamic policies that evaluate many different attributes, including real time environment conditions (like time of day) instead of preset access lists or user roles to make access control decisions. The following diagram depicts how an ABAC model generally functions.

Attributes associated with the users, environment, and objects being protected are at the heart of an ABAC model. Examples include:

- Subject (or user) Attributes: Clearance level, whether they are a contractor or Federal employee, and office title.
- Environment Conditions: Time of day, current security level, or location of user.
- Object Attributes: Classification of information or office who created the file.

A potentially large number of attributes need to be managed and understood for an ABAC solution to work, and they must best selected by an authority with technical, security and business process knowledge.

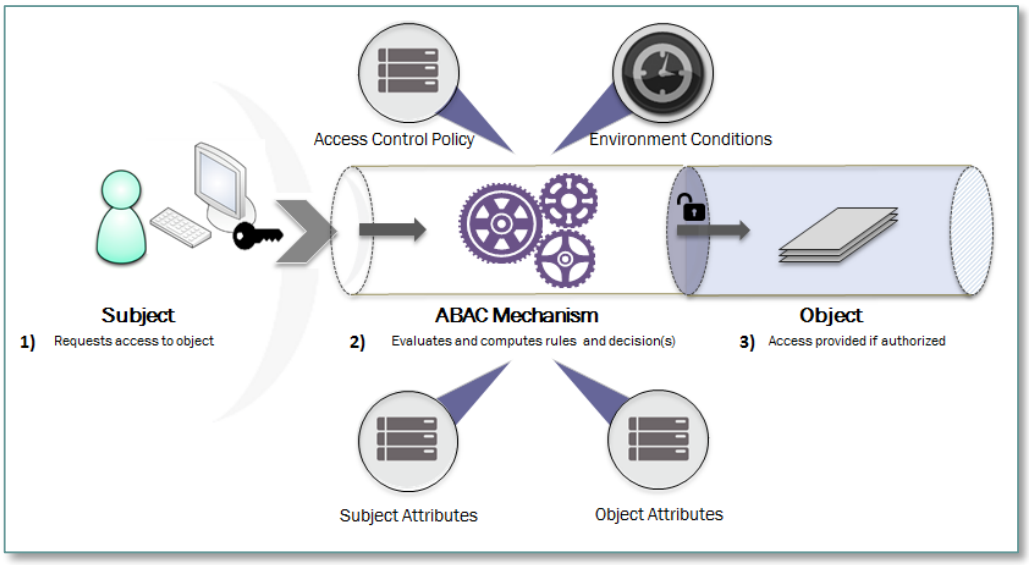

Figure 2, ABAC Model Functionality

The purpose of logical access control is to protect information resources, such as data, applications, network devices, or other types of information technology, from unauthorized operations or access. This real time authorization is done by installing access control mechanisms that mediate requests from subjects or users. As networks grew and the need to limit access to specific protected objects increased, access control models have evolved from using roles and groups to even more dynamic access control methods, like ABAC.

The basic architecture to manage the rules, policies, algorithms and subject, object, and environment attributes following an ABAC model include four basic elements:

1. Policy Decision Points (PDP)
2. Policy Enforcement Points (PEP)
3. Policy Administration Point (PAP)
4. Policy Information Point (PIP)

It is important that these policy points are considered when determining what solution can be used by a Federal agency to meet the mandates outlined in KISSI and other policy. The following diagram (recreated from NIST SP 800-162) shows how the policy points interact with each other and attributes to grant or deny access:

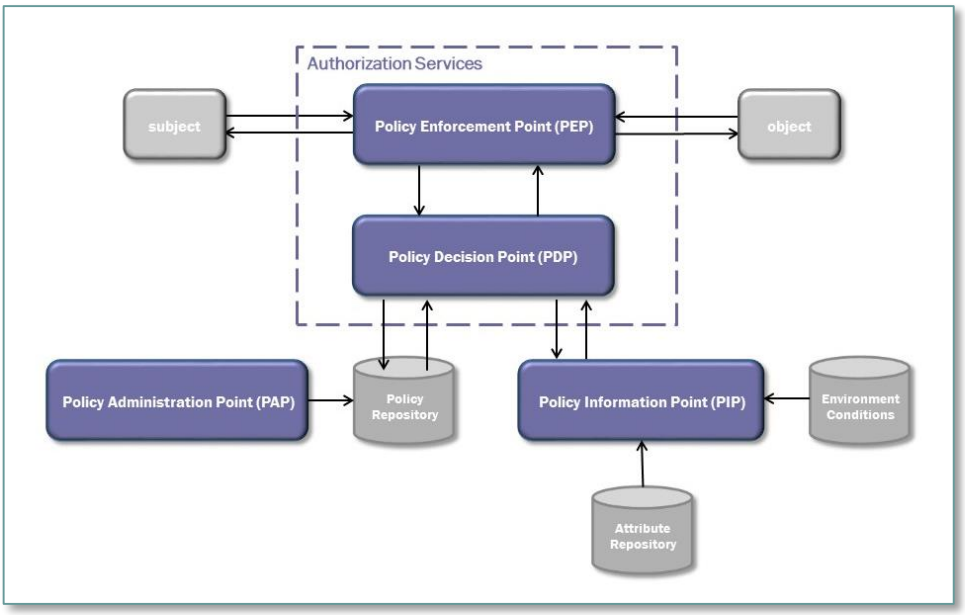

Figure 3, ABAC Element Interaction, based on NIST SP 800-162

Benefits of ABAC

The overarching benefit of Attribute Based Access Control is that it ensures the right people get the right information when they need it. NIST highlights a variety of different benefits in their special publication, but the three most significant benefits are:

- **Single Point Provisioning of Users.** With ABAC, a system administrator no longer has to review a user's account and to either assign one or more roles in a system or enter them into an ACL based on an external approval process. There no longer is a dependency on a manual exchange (normally via email) between the system administrator and the authorizing manager. Instead, the ABAC solution automatically knows what the user should and should not be able to access based on the established policies and attributes assigned external to the application. Attributes are managed centrally and can be pulled from authoritative sources, such as LDAP or Active Directory repositories. This approach accommodates new users, as well as external and unanticipated users, with no changes to the existing rules as long as the attributes are standardized.
- **Dynamic Access Control Based on the Most Current Policies**. As digital policies change in real time to address security concerns, including environmental conditions such as the nation's security level or time of day, ABAC reads these changes as reference data for its policy decisions. This enables flexible access control that responds as the needs of the resource or organization change. Further, central policy management through an enterprise ABAC solution simplifies standardization and policy compliance across an organization.
- **Finer Grained Access Control**. Many Federal agency applications use RBAC to manage authorization, but this quickly results in "role explosion" when administrators create a roles for a small subset of people as different levels of access develop. ABAC allows for precise access control by pulling from a higher number of attributes for decision making, creating a larger set of possible rules and options without the need to manage

groups and roles. As NIST put it, an ABAC solution "is limited only by the richness of the available attributes"[2].

Challenges of an ABAC Implementation

Implementing an ABAC Solution is not without its challenges. The primary challenges related specifically to the Federal arena are:

- **New and Emerging Technology.** The ABAC marketplace is still working to understand the customer's needs, specifically in the public sector. The Federal definition of ABAC (NIST SP 800-162) was only published at the beginning of 2014, and viable ABAC options in the market today are considered young and have not been thoroughly tested through a sufficient number of robust Federal implementations. Only a small number of ABAC pilots have actually deployed commercial off the shelf (COTS) solutions into production. Some Federal agencies have used OpenSource or modified their Central Authentication Service (CAS) in a Government off-the-shelf (GOTS) approach, thereby avoiding the heavy burden of the Federal procurement process, but this introduces an increased cost of maintaining the compliance of the in-house solution as technical and operational standards change. At a minimum, agencies should strongly consider eXtensible Access Control Markup Language (XACML) and SAML data format for exchanging authentication and authorization so they maintain compliance with federation and general solution evolution and improvements over time.

BENEFITS OF ABAC
Single Point Provisioning
Dynamic Access Control Based on the Most Current Policies
Finer Grained Access Control
CHALLENGES OF ABAC
New and Emerging Technology
Sensitive Federal Environments
Limited Models to Follow
People Change, Process Change
Tight Federal Timeline

- **Sensitive Federal Environments.** In the complicated technical environments that exist in Federal agencies, multiple application types that must be enabled with attribute based authorization exist. The Federal space is unique in that many of the networks being protected by ABAC are classified and purposefully air gapped. This makes federation and the use of enterprise wide policies and attributes a significant risk and not just a technical challenge. The users that use the application may only be a handful, but due to the mandates, an ABAC solution must still be implemented. Each application serves a different purpose and may have a unique platform, coding language, or operating system to be considered to ensure no modifications need to be made to the chosen ABAC solution. In addition, the hardware itself may need to be considered if application code is executed directly.
- **Limited Models to Follow.** There is no widely accepted ABAC model as there are with the more established access control approaches. NIST has provided some standards and a solid definition, including the elements of an ABAC solution, but has not provided a specific model for agencies to follow or a core set of attributes to be used in federation across agencies. Government working groups, such as the Access Control and Attribute Governance Working Group (ACAGWG), have been established to create

[2] NIST SP 800-162

and gain consensus on an initial list of attributes to be used government wide, but have so far been unable to provide them.

- **People Change, Process Change.** One of the key concepts of ABAC is the idea of centralizing authorization decisions. This causes the most notable challenge to implementation. Application owners in the Federal arena struggle to allow the access control to be performed outside of the application. Legacy applications were not initially built to give up these internal controls, and transitioning that functionality to an external Policy Decision Point (PDP) can involve a great deal of development time and effort, as well as a significant cultural shift.
- **Tight Federal Timetable**. FICAM-S has suggested that the Federal government begin to integrate ABAC services by the end of 2016 and be fully interoperable (federated) with other agencies by 2018, and some agencies have even more aggressive deadlines have been outlined for many agencies internally. This means that there is less than a year to plan, survey the environment, analyze the information, procure a solution that will work for the entire agency, pilot that solution, and begin implementation to show progress, as outlined by the Federal requirements. There is a need to correlate information, policies, and attributes from many sources internally and externally, which typically requires a lengthy implementation lead time.

Guidance

The Federal government is moving towards an ABAC model in response to very real threats that are only increasing in likelihood and impact to the American people. Information sharing and IT security will improve across the Federal government as agencies reduce risk through dynamic, meaningful digital policy for access control decisions; centralize authorization services; and avoid timely user provisioning. The challenges associated with implementing an ABAC solution lie not only with technology, but with a change in the way people think and processes are managed. No two agencies are the same, but we have established a standard, but adaptable methodology that provides a roadmap to guide implementations.

First, agencies are encouraged to establish a Department level program management office (PMO) specialized for ABAC. As the center of information governance, this structure will guide and enforce the implementation and associated enterprise policies. The PMO ensures decision authority is assigned, transparent, and understood by those business and technical owners affected by the implementation. It also begins the cultural shift toward centralization by collecting the Department's digital policies and attributes to facilitate information control. Formalizing this governance structure out to those being managed may be an essential step.

Second, it is important to define what success by defining what the ABAC requirements mean to the agency and what the agency thinks is the best way to address those requirements, based on its specific time and cost constraints and quality definitions. Framework decisions need to be made by leadership regarding the level of enterprise interoperability, the continued use of existing supporting solutions, and a preference towards a COTS or GOTS solution. A maturity model should be created during initial planning sessions to define and communicate the level of ABAC sophistication through time. Once approved, the maturity model becomes the stakeholders' guide for developing a clear and actionable implementation roadmap.

Third, success increases among agencies who establish and facilitate regular working groups for stakeholders impacted by the implementation. The working group acts as a touch point throughout the implementation and a forum for addressing technical and operational issues. The sessions also allow the PMO to monitor and control the process and to understand

challenges and make course corrections to the implementation roadmap when necessary. Early identification of issues and their resulting adjustments to the implementation plan will minimize their impact on the tight timeline.

Fourth, a technical survey of all effected environments will document current attributes and digital policy to use in planning and negotiating the future ABAC solution. The information and knowledge gathered from the technical survey supports the procurement of an ABAC solution (i.e., COTS or GOTS product), and the macro-set of attributes enables creation of a master attribute set that should be controlled at the Department level.

Finally, a reference implementation, with the full support of the PMO and lessons learned for continuous improvement, as the first installment into production provides a strong initial stage for a Department's ABAC deployment. The PMO provides full support during this initial stage to document the ABAC solution, to create guidance materials that will be used as the solution is deployed, and to track and monitor ongoing compliance. The reference implementation should be transparent to facilitate learning across the Department, and participation in testing and other aspects should be encouraged. A Department level Tier 4 help desk and a test lab to support application onboarding should also be considered.

Conclusion

In today's environment of constantly changing security threats, the Federal government is continually evolving its security capabilities to protect this nation's assets. ABAC offers a dynamic way to control access at a very fine-grained level, which is essential to minimize today's security risks, but it is not easy to provide a blanket capability across the vast, diverse IT infrastructure that has grown organically to date. The aggressive timelines required by Federal mandates mean that Departments need to establish a clear, comprehensive directive to guide subordinate components and to develop a comprehensive roadmap so that progress can be monitored and managed appropriately.