ABAC Workshop Minutes

Prepared by Jeff Coleman (NSA), Paul Jacob (Booz Allen and Hamilton), and Vincent Hu (NIST)

Date: 17 July 2013

Location: National Cybersecurity Center of Excellence (NCCoE), 9600 Gudelsky Drive, Rockville, Maryland 20850

Meeting Summary

Mr. Paul Timmel, Director of the National Cybersecurity Center of Excellence (NCCoE) and Mr. Arthur R. Friedman, Chair – Identity and Access Management Working Group (IdAM WG), Committee of National Security Systems at NSA, began the meeting with review of the Agenda for the ABAC Workshop. The presenters stated that the primary goal of the ABAC Workshop was to briefly explain the importance of ABAC: to enhance security for protected resources in the Defense, Federal, Commercial and Healthcare Information Technology (IT) Sectors. Additional primary goals of this workshop were to present the highlights of the NIST Special Publication (SP) 800-162: "Guide to Attribute Based Access Control (ABAC) Definition and Considerations." The purpose of this document is to provide as guidance, an industry-based standard definition for ABAC; a synopsis of the current ABAC and Identity and Access Management (IdAM) models; use of frameworks, standards, guidelines, industry best-practices, and; development, design and deployment considerations for the successful realization of ABAC capabilities within an enterprise. A series of ABAC presentations, followed by Question and Answer (Q&A) sessions and technical sidebars allowed opportunities for attendees to identify, refine and guide the many interrelated considerations, challenges and efforts required to develop ABAC Guidance.

The afternoon sessions had ended the ABAC Workshop with limited live demos and booth presentations of available ABAC and IdAM Technologies from various Commercial-off-the-Shelf (COTS) Vendors.

In the subsections below, brief summaries are presented, detailing some of the highlights and discussion points that were covered during the ABAC Workshop.

Presentation: Importance of ABAC

The two presenters that discussed the Importance of ABAC were: 1) Mr. Jeremy Grant, NSTIC Program Manager, NIST, and Ms. Deborah Gallagher, Identity, Credential and Access Subcommittee Co-Chair, GSA. At various times, both Mr. Grant and Ms. Gallagher have spoken independently and collaboratively under this topic. The highlights are as follows –

- In order to ensure that the Identity Ecosystem is fortified to adequately protect resources and provide assured information sharing across the enterprise, a need for robust identity and authentication (I&A) schemes is required across cross-domains and multiple environments. The schemes includes the key premises:
    - Definitely proves who you are.
    - Enhances privacy.
    - Allows the minimized set of attributes need.
- Successful access control across the enterprise requires the development, deployment and operations and maintenance (O&M) of robust security mechanisms in order to address the required security controls identified to adequately and appropriately protect mission data/resources from compromise and provide mission assurance (MA). Through such tenets as validation of identity, level of assurance (LOA) and confidence of identity used for implementing the required security mechanisms to employ ABAC, potential threats to the mission, war-fighters, mission-oriented or other users/consumers can be avoided.
- There are four levels of assurance of identity:
    - Level 1 – For little confidence in identity (e.g. self-reported ID information on public web pages)
    - Level 2 – For some confidence in identity
    - Level 3 – For high confidence in identity (e.g. verified through secondary means)
    - Level 4 – For very high confidence in identity (e.g. PIV-I)
- Primary benefits and rationale for using ABAC include:
    - The ability to provide fine-grained access control and robust authentication mechanisms to provide various levels of authorization or access to protected resources;
    - The realization of assured information sharing and secure information exchange capabilities across the enterprise;
    - The minimization of duplication of data/mission resources for data sharing within a federation or across the enterprise, and;
    - The reduction of administration efforts in order to provision user accounts across various environments (i.e., cross-domain) for assured information sharing.
- The desire and need for ABAC to be selected as an attractive, architecture planning and design methodology to improve on the security posture to Healthcare IT Infrastructure was mentioned by some of the participants in the audience. Both Ms. Gallagher's and Mr. Grant's reactions were united; they concur that there needs to be follow-on, funded efforts and/or working groups to establish appropriate business cases for ABAC. Additional efforts that need to be executed should include the identification of standard, authoritative attributes across the enterprise. This should be done as a precursor to ABAC service definition.

- Relying Parties (RPs) must articulate what are the data requirements for their protected, mission data/resources that contribute to Digital Policies (DPs) and Meta Policies (MPs) for successful development, deployment and execution of ABAC.
- Healthcare has special problems for identity management with respect to identification and published attributes. An example is the Blue Button initiative where patients can view and download their own heath records. How do you share this information securely and to whom?
- The National Strategy for Trusted Identities in Cyberspace (NSTIC) has directed industry to provide solutions and is focused on robust commercial marketplace solutions.

Presentation: Overview of NIST SP 800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations

Dr. Vincent Hu (NIST and Lead Editor for the NIST SP 800-162) stated: originally, there was no ABAC guidance for all of the US government (USG). This document is currently in draft and while the deadline is passed, they are still accepting comments. Terminology in this SP is not meant to be authoritative, but is intended to be consistent. It extends fundamental concepts of policy, models and properties of access control. The next document related to 800-162 will be ABAC Formal Models. Expect a draft by the end of 2013.

Mr. Adam Schnitzer (Booz Allen and Hamilton, NIST SP Co-Editor) provided an introduction to Logical Access Control. Access control has evolved over time.

- Mandatory Access Control (MAC)/Discretionary Access Control (DAC)
- Identity-Based Access Control (IBAC) using tools such as Access Control Lists (ACLs)
- Role-Based Access Control (RBAC) using groups and roles to ease authorization decisions for larger groups of people
- Attribute-Based Access Control (ABAC) further improving and providing finer-grained control over access decisions
- Key concepts in ABAC include:
  Subject (Active Entity) – An entity needing access. While there are technical differences between users and subjects in formal models, they were combined for this SP
  Object (Passive Entity) – An entity for which access is needed
  Attributes – Information or characteristics of subjects, objects or environment conditions such as time, location or threat level
  Operations – Functions such as read, write, create, modify or delete that can be performed on an object
  Policy – Formal rules that could be access rules, relationships, etc.

This included the presentation of the ABAC Basic Fundamentals, which included: 1) a business case/operational scenario for ABAC; 2) the ABAC definitions; 3) the basic conceptualized ABAC model, and; 4) the more advanced and complex, ABAC model for enterprise operations.

To re-emphasize on the importance of ABAC, the presenters continued with the following ABAC benefits and rationale:

- No advance knowledge of requesters for protected data/resources are required;
- Individual attributes can be correlated from multiple authoritative sources;
- ABAC is highly adaptable to changing needs (i.e., conditions) or operational environments, and;
- Policy attributes and access decisioning engines can be managed centrally for large enterprises

Mr. Ken Sandlin (MITRE Corporation and Co-Editor for the NIST SP 800-162) ended the series of ABAC SP discussions with his presentation of the ABAC Enterprise Employment Considerations, which helped to foster open discussion among the ABAC Workshop participants regarding if the proposed considerations were adequate for their specific operational scenarios and environments that support their designated Industries.

ABAC works well for challenges in large organizations where you have unknown users, rapid changes or fine-grained access requirements. However, the tradeoffs include potentially lengthy implementations, reliance on authoritative entitlement data, and lack of native support in common Operating Systems (OSs). It is not for everyone.

Deployment of ABAC needs to include:

- Initiation Phase to properly define requirements
- Acquisition to include standardization and build out of attributes
- Implementation Assessment to specify attribute caching and minimization and availability of interface specifications
- Operations and Maintenance to ensure the availability of quality data and high availability

Questions and Comments:

- Attribute semantic interoperability is not addressed in the SP
- Network access devices – ABAC could apply but could be too costly
- Natural language to digital policy is a large, complex problem that needs work
- Temporal attributes can be dynamically ingested but can have problematic caching considerations
- The SP assumes that user=subject but they should be separated in formal models
- The SP assumes authenticated identity

Presentation: Framework for ABAC Models

Mr. David Ferraiolo (NIST Co-Editor for the NIST SP 800-162) explained that there is a need to formally define ABAC by using more formal models. The formal model describes two paths: Rules and Rule Hierarchies, and Relations and Relation Hierarchies. Mr. Ferraiolo described notation for basic model elements and showed several examples. A formal model lends itself to Graph Theory and can be developed as a predicate calculus. Although most of the presentation was a very abstract, yet complex ABAC modeling and mathematical-oriented brief, they were a few advantages in having this proposed framework for ABAC Models. They benefits/advantages were the following -

- The identified elements of the presented series of ABAC models allowed modularity in the organization of the elements to demonstrate various methods of data exchange and to establish appropriate relationships between the elements to realize such capabilities as user provisioning, rule definition and attribute association (AA) relationships.
- Apparently these identified elements within the framework that is derived from the selected ABAC models help to compute privileges based on policy combinations formulated in the ABAC framework. A separate function of these elements as defined in the proposed ABAC framework helps to maintain accuracy, validity and freshness (timeliness) of attributes (including identity attributes) from various authoritative sources.
- The proposed framework is based on Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC) and may enhance the capabilities of each access control model, thereby evolving ABAC.

Panel Discussion

Panelists were invited to the ABAC Workshop based on their extensive experience and talent with their bodies of work supporting Identity and Access Management (IdAM) and ABAC. Each of the panelists had briefly presented current projects that are IdAM and/or ABAC-related. The highlights for each of their projects, as detailed from their briefs are as follows:

- Dr. John Howard (DISA Deputy Chief Technology Officer (CTO)) – *DoD IdAM Strategy* – A problem is created by how we talk about ABAC. ABAC is key to the future but not completely different; Since ABAC was not marketed in an efficient manner that helps potential DoD Stakeholders to understand the full scope and capability of this design methodology for adequately enhancing the security infrastructure of existing enterprise services and information systems (IS) for protected mission data/resources, the Defense Information Systems Agency (DISA) has changed its terminology from "ABAC" to "Dynamic Access Control." The idea behind Dynamic Access Control (DAC) in supporting DISA IdAM objectives for service realization to the DoD is that IdAM Operational Capabilities such as DAC, satisfy the DISA primary mandate; DISA is mandated to deliver IT capabilities to DoD Stakeholders with service realization and deployment. Within the IdAM Data Flow via DoDAF Capabilities View (CV-1), Human

Users (Individuals) and Non-Person Entities (NPEs – e.g., Devices) can *securely* access all authorized DoD resources, anywhere at anytime.

- Ms. Amy Reiss (NSA Technical Director – IT Security Development) – CASPORT is NSA's authorization service and provides a single place to be compliant. In 2004 there was a need to share other agencies. This was followed in 2007-2008 with federated queries and searches as well as Non-Person Entities (NPEs). Now, objectives include data objects and controlling network enclaves to reduce complexity. The implementation efforts for CASPORT has allowed the NSA to use OASIS and Security Assertion Markup Language (SAML) Use Cases as basis in building and managing federated queries. In the development of CASPORT, the Agency has shifted the paradigm for access control from use of centralized systems (based on traditional IT infrastructure) to use of data centers (i.e., use of Cloud Technology). With the integration of such projects and systems as PVX, CASPORT has integrated quality for their implementation of enterprise IdAM. Ms. Reiss highly suggests that the considerations for ensuring quality implementation of enterprise IdAM include –
    - 1) Data Owners should use Quality Attributes, in terms of validity, accuracy and timeliness (freshness);
    - 2) Data Owners must know their data protection requirements, and;
    - 3) Data Owners must intimately know their data to properly characterize their data sets.
- Mr. Rick Kuhn (Mr. Rick Kuhn, NIST Computer Scientist) – *ANSI Enhanced RBAC Standard – O*ne of the most challenging problems in managing large networks is the complexity of security administration. Role Based Access Control (ABAC), as formalized in 1992 by David Ferraiolo and Rick Kuhn has become the predominant model (prior to ABAC) for advanced access control because it reduces this cost. Now through the continued work with various access control models since then, Mr. Kuhn has identified the benefits and disadvantages of the RBAC model in its current state. Therefore, his brief proposes a hybrid solution, development of a new RBAC-ABAC model, which enables some broader attributes other than roles to be used and may serve as an alternative for ABAC.
- Mr. Mark Smith (PM-ISE – ICAM Attribute Management Roadmap)– The Federal CIO Council FICAM program has an objective for identification and provisioning of attributes being market driven to ensure that what is deployed is what people really want to do. The National Strategy for Information Sharing and Safeguarding (NSISS) was signed by the President in December, 2012. Its Priority Objective #4 extends FICAM to all fabrics with primary governance by the Federal CIO Council. GSA is the lead working on a government-wide implementation plan with heavy emphasis on shared services. It is important that everyone does not have to do everything. Mr. Smith is performing as a contributor and strategist for establishing methodologies for attribute management and

definition. He stated that it is relevant to have suitable business cases leading to use case definition for AM. In addition, transparency should exist for quality of service (QoS) of shared, authoritative attributes between various organizations within a federation, who require AM capabilities in order to be National Strategy for Information Sharing and Safeguarding (NSISS) compliant.

- Ms. Karyn Higa-Smith (DHS Program Manager – Cyber Security Division) – *Department of Homeland Security (DHS) Backend Attribute Exchange (BAE)* – Based on the previous work with DISA and NSA with the Privilege Management Phase II Pilot over at Johns Hopkins University – Applied Physics Lab (JHU/APL), DHS has developed an attribute exchange service that is a core component of the Identity Management (IdM) Testbed that supports ABAC. The attribute exchange service is called the Backend Attribute Exchange (BAE). Development of the BAE is based on Security Assertion Markup Language (SAML Version 2.0) and BAE is a part of Federal Identity, Credential and Attribute Management (FICAM). At DHS, the Personal Identity Verification-Interoperable (PIV-I) / First Responder Authentication Credential (FRAC) Technology Transition Working Group addresses identity management challenges inherent in collaborating with local emergency responders and provides one voice to policy makers. This includes an incident scene access provisioning pilot and pushing emergency responder attributes to the field. They are developing and end-to-end attribute exchange using public standards including to mobile handheld devices. FEMA is operationalizing the test bed. Ms. Higa-Smith then presented the BAE System Overview along with an Incident Scene Access Provisioning Pilot that demonstrates the DHS Science and Technology (S&T) IdM Testbed (integrated with BAE) capabilities. She presented a slide that depicted an operational scenario that occurred between DHS S&T (in Washington, DC) and an undisclosed BAE Stakeholder Facility in Chester County, Pennsylvania. Ms. High-Smith closed her brief with her mention about IdM Testbed/BAE future work such as IdM Testbed and Mobile Device Interoperability and BAE and Global Federated Identity and Privilege Management (GFIPM) Interoperability.

The Panel Discussion ended with a Question and Answer (Q&A) Session. In the session, several questions and proposed answers were given regarding the way forward in evolving ABAC and its usefulness in various Industries and Operational Environments where critical data and resources require adequate security protection. The highlights of the ABAC Q&A Session are as follows:

Q: If SP 800-162 was published a year ago, how would it be used so far?

A: It would have helped with questions and been useful for developing a common lexicon.

Q: SP 800-162 included several principles, including the need to establish a business case. The cost of transitioning includes both hard and soft costs. The first priority in a business case should be operational capability, second is security, and third is cost savings. Various Industry

Representatives in the audience, including those from Defense, Federal Government, Commercial and Healthcare Industries have stated that some of the usefulness of the NIST SP 800-162 may not as effective to their particular operational environments due to the lack of adequate examples.

A: The NIST SP Editor and Publishing Team has asked participants to forward via email or other media, their business cases, particularly those on an enterprise level that may require ABAC as a solution. The NIST SP Editor and Publishing Team shall incorporate more business cases, real-world operational examples (including existing projects, reference implementations (where applicable), etc.) to cover the spectrum of potential ABAC Stakeholders.

Q: What are some of the most important considerations for ABAC implementation into the enterprise?

A: According to DoD, for example, as with DISA providing an ABAC Solution for the Joint Interoperability Environment (JIE), the three most important considerations are: 1), ABAC Solution must be able to support the functionality of the mission or information system (IS) that it is designed to protect, 2), ABAC Solution must be able to fortify (at a minimum) or enhance the security posture of the designated mission system or IS, and; 3), ABAC Solution has to be cost-effective with a moderately affordable, total cost of ownership (TOC). Of course, for various Industries, these considerations may be in a different order or may be replaced or interchangeable with other considerations that have not been mentioned.

Q: How can attributes be used to enhance privacy and protect Personally Identifiable Information (PII)? – How are attributes protected?

A: Some of the proposed security controls and mechanisms are identified in NIST SP 800-162. However, with strenuous Privacy Regulations and Laws that various Industries are mandated to comply, the Panel highly recommends the following –

- Various established agreements such as Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) and Data Use Agreement (DUAs) should be vetted, negotiated, concurred and then legally invoked between all Department/Agencies/Organizations (DAOs) prior to use, management and dissemination of the PII/Privacy Data amongst authorized Relying Parties (i.e., the DAOs), and;
- Not having to store attributes redundantly is an improvement. Note that a lot of subject attributes are not PII. These characteristics help make the capability inherently privacy-based. Also, confidentiality policies can be extrapolated and implemented.
- Adequate and robust security mechanisms are in integrated into the authoritative attribute databases, repositories and the ABAC system/solution to protect the PII/Privacy data-in-rest and data-in-transit.

Q: Is there a move towards real adoption, especially in the battlefield?

A: Yes and no. There is some organizational resistance. However, the Army is moving forward transitioning systems such as email. All active directories will be actively provisioned from the Enterprise automatically. Look for big changes in the next three to five years.

Q: As these capabilities are centralized, what assessment of capability of the infrastructure is planned especially with respect to confidentiality and availability?

A: Currently, a pod of email servers provide caching for availability. There must be local infrastructure redundancy, not just the enterprise infrastructure. There needs to be policy regarding the availability of attributes and failovers.

Q: Who decides what attributes will be made available from what Agency?

A: We should be looking for market-driven answers. Agencies have their own governance bodies. Note that the relying party has a lot of the responsibility for specifying it.

Q: Overall, attributes do not have personal information, but some attributes are inherently private. What is the vision for treating attributes with privacy characteristics?

A: Must make a distinction between attributes and payload and isolate as necessary.

Vendor Demonstrations and Poster Displays

The following Vendors/Organizations are as follows:

- Mr. Serban Gavrilla, NIST, Policy Machine
- Mr. Donald Graham, Radiant Logic, Federated Identity Service Based on Virtualization
- Mr. Jeremy Wyant, General Dynamics, Assured Information Sharing with Situational Awareness
- Mr. Dave Coxe, ID/DataWeb, *Online Attribute Exchange Network*
- Ms. Brynn Mow, Jericho Systems, Jericho's EnterSpace: ABAC Decisioning Deployed and Delivering
- Mr. John Tolbert, Boeing, Resource Metadata Tagging
- Mr. Koh EngKlat, Next Labs, ABAC for Data on the Move – Dynamically Controlling and Protecting Classified Data
- Ms. Sandy Trumbull, CA Technologies

Wrap Up

By Mr. Art Friedman (NSA) and Mr. David Ferraiolo (NIST), the meeting ended with a final discussion on the following identified action items that must be executed by NIST SP Editor and Publishing Team in order continue to mature and release the NIST SP 800-162:

ABAC Workshop Participants shall continue to provide technical review and comments to the NIST SP 800-162. Details on an invite for participants regarding the near-term re-review and edit of the current NIST SP shall follow. NIST expects final Release of SP 800-162 to be delivered by end September 2013.

NIST and NSA among other Defense Industry and Federal Government participants should foster continued dialogue and investment in ABAC and IdAM-related projects within various Industries, Private Organizations and COTS Vendors for evolution of ABAC capabilities. This can and should be done by investing in COTS Vendor ABAC Technology Development and Enhancement Projects (e.g. via contract award, SBIR, etc.).

Should SP 800-162 go through another public review?

- The SP is one solution in an ecosystem
- Some participants recommended another round of review
- Include asking OMB about authorization metrics
- There was agreement with the need to get it right, but publication should not linger. Therefore, make it a short suspense
- Get it published to avoid scope creep
- Avoid the path of SP 800-63 with two years between updates.
- It was recommended to have another workshop six weeks after publication in order to reinforce the guidance.
- There was a request for disposition of comments in the next draft.

There was a recommendation to attend a healthcare conference to give a briefing or tutorial regarding ABAC. Travel and convention funding for this may be an issue.

Expect a series of related, new documents regarding ABAC. For example, the next document is expected to be ABAC formal models.