archTIS

The tip of the ABAC iceberg?

Trusted Information Sharing as the broader architectural context for guiding and managing the implementation of Attribute Based Access Control (ABAC)

Copyright Statement

The Information Access - Security Challenge

Shortfalls in information sharing and management lead to disastrous outcomes – from terrorist attacks and global financial crises to the loss of commercial advantage and the exposure of intellectual property and sensitive information. As a result, government organisations and large enterprises have spent billions of dollars trying to resolve their lack of trust in their people, their processes and their information technology. To achieve these ends, organisations have focused on investing in network security and cybersecurity products to solve a problem that is often hard to define.

Investing in tighter 'perimeters' and 'plug-in' appliances is not necessarily the answer to the 'access + security' problem. While the deployment of perimeters and appliances might appear to gain quick wins in terms of security, this approach may lead to an environment characterised by:

- a misalignment of information services and business outcomes
- increased complexity and infrastructure costs, and
- a lack of information access that hinders the organisation's ability to 'do business'.

Business demands information management that meets their business and information needs. From an IT perspective, it means that stakeholders are demanding access to information services that reach far beyond the boundaries of the organisation. At the same time, they are also expecting the IT department to protect their high-value information assets and intellectual property.

How can you ensure that enabling remote and mobile access to your protected information services will not compromise your high-value information assets?

Attribute Based Access Control

The latest technology evolution in the solution space is Attribute Based Access Control (ABAC). The US Committee on National Security Systems Glossary (2010), defines access control as:

> *"The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances)." (2010, p1)*

Access control is the authority-driven layer of security that dictates who can access which resources within one or more networks or systems. Prior to events such as 9/11, Wikileaks and Snowden, role-based access control (RBAC) was considered sufficient for managing the exchange of information. It enabled access based on a person's role and/or group (e.g. Finance, Employee) within the organisation. These recent security incidents, however, have shown that role-based access control is neither granular nor flexible enough to enable the required security AND the sharing of information between organisations.

RBAC is not dynamic or scalable

RBAC is limited in its ability to scale, manage multiple roles or respond to changing circumstances. When associated with secure network perimeters, RBAC places significant restrictions on the business' information services and relies on policies that are hard to maintain and control.

While RBAC makes enabling access control easy, assigning access according to a specific role limits the granularity by which the organisation can restrict or enable access to its information assets. For example, personnel may fall into a number of different role subsets depending on their authority and work requirements at any given moment.

With RBAC, managing access to information requires the administrator to assign multiple system-level roles to a single person. This complexity can be compounded by the complexity of adhering to organisational policies. For example, when staff change roles within an organisation, the requirement to modify their permissions can be overlooked.

The 2014 QHealth fraud report depicts a clear example of this scenario. Even if role-based access had been deployed appropriately, organisational restructuring and changes in job roles and functions still allowed a staff member to retain control over financial accounts that he was no longer authorised to access. Moreover, this situation was compounded by a lack of assured workflows which meant that the staff member could 'side step' the required approval processes.

http://www.ccc.qld.gov.au/research-and-publications/publications/misconduct/qhealth/qhealth

The Benefits of ABAC

IT enterprises can no longer be seen as just a collection of applications, systems and networks. Instead, organisations need to focus on the information assets they hold and the information services they provide to their internal and external stakeholders: what is needed, when, where and by whom? How valuable is this information to the organisation and to outsiders? If there is understanding as to how the information lifeblood needs to flow through the organisation, and where the 'bottlenecks' are, then projects of work can be systematically undertaken to enable and control of these information flows in a coherent way.

Deploying ABAC in support of a trusted enterprise information architecture positions the technology to be used most effectively.

When implemented as part of a broader assured identity and information sharing capability, ABAC enables fine-grained, mandatory, dynamic access control that supports the sharing of information within and between oragnisations. It sets the conditions under which access can be granted to data, a device, or system, within any given context. For large enterprises, it presents them with the ability to consistently and dynamically allow, track and restrict access to information based on an entity's attributes such as: organisation, role, citizenship, geographic location, device being used, security clearance, need-to-know, authorities, and time.

An ABAC implementation then uses these attributes to determine what is known (and trusted) about every individual, device or system attempting to access information within a system, and then it assesses that entity against the attributes (metadata) required by the business and security policy (business rules) for the requested information asset.

Despite its potential to provide robust, dynamic and consistent services across an enterprise, ABAC is currently offered by vendors as attribute service capabilities within a hardware, software or virtual gateway solution. This approach to deploying ABAC is not only reinforcing the 'bottom-up' product focus of many IT departments, but it may introduce vulnerabilities and add complexity to the organisation's information infrastructure if not deployed correctly.

"As standards and technology mature, organizations will need to embrace concepts that enhance interoperability and promote higher assurance solutions while discarding proprietary, stovepiped solutions."

NIST Special Publication 800-192, 2014, p30

The Business Context of ABAC

On its own, ABAC is not a 'plug and play' solution. It is the access technology through which the organisation's information management 'rules' are implemented and enforced. To ensure its effectiveness, an access control solution needs to be part of the ICT enterprise architecture so that it aligns with the broader organisational context - its mission, objectives, and risk appetite - and works seamlessly with all information management systems and information workflows. ABAC can only benefit the business if it can articulate what it needs to know, what it has, what it wants to secure/use/delete, who should have it, where they need it, when and via which kinds of devices.

Implementing an ABAC solution or technology alone is not THE solution. ABAC does, however, play a role in addressing the trusted information sharing and management problem. The success of an ABAC solution is highly dependent on how well it is designed, implemented and operationalised to support and grow with the information services delivered and required by the organisation. To achieve this goal, ABAC must be delivered through a holistic architectural approach as part of a broader solution to meeting the organisation's information needs.

Managing the Potential Costs & Risks of ABAC Implementations

Managing the risk and cost of an ABAC implementation is of paramount importance to any organisation. In most cases, there will be only one opportunity to implement ABAC within an ICT environment. The costs and expense of a poor ABAC deployment are so high that a failure is likely to prohibit any future implementations. It must be done right the first time.

In January 2014, the National Institute of Standards and Technology (NIST) published their Special Publication 800-162, *Guide to Attribute Based Access Control (ABAC) Definitions and Considerations*. This publication provides guidance on implementing an ABAC solution, and largely considers ABAC from a technical perspective, without positioning it in the context of the business and its organisational benefits.

The guide identifies more than 40 issues and considerations which, if not addressed and managed appropriately, will have an impact on costs, timeframes, and the effectiveness of ABAC implementations. These risks include:

- Complexity
- Development and Maintenance Costs
- Transitioning
- Authorisation and Classification Requirements
- Trust Models and Security Capability Integration
- Establishing Attributes and Environmental Conditions
- Operationalisation, and
- Standardisation, Interoperability and Traceability.

These key considerations, which can be mitigated by broadening the scope to include the organisational context and taking an enterprise architecture approach to enable attribute based access control, are addressed in the following sub-section. Notably, the NIST publication provides very little guidance as to how these issues can be addressed or avoided.

Unless the quick tactical wins are aligned to deliver the operational and strategic objectives, a 'bottom-up' approach will only offer isolated benefits and will not solve the problem of trusted information sharing and management.

Complexity

Consideration: There is a risk that, within large enterprises, the complexity of interactions between existing applications, systems and networks can impact on performance and scalability (cost). These risks are likely to be realised if a technology, or 'bottom-up' solution is implemented. By adding yet another component to the mix, in the form of an ABAC solution, there is a danger of not only adding complexity, but also increasing the on-going costs involved in maintaining those components and resolving any issues it may introduce to the enterprise.

Mitigation - Enterprise Architecture:
There are definitely benefits to be gained through the implementation of ABAC. However, the risk for organisations lies in not implementing it within the context of the broader organisation. Taking a 'top-down' holistic architectural approach defines information access control business rules across the enterprise (regardless of the system that contains the information) through metadata structures. It then uses the ABAC solution to ensure that the business rules are consistently enforced.

Development & Maintenance

Consideration: There is a risk that ABAC solutions can incur high costs of development and maintenance; costs that "may exceed its benefits in the long term" (NIST Special Publication 800-162, p.19). This is particularly likely for bespoke solutions that are implemented without due consideration of the entire capability and associated enterprise outcomes. These customised solutions will require on-going maintenance and development to retain:

- their compatibility with and utility within the ICT infrastructure,
- their alignment with organisational structures and needs.

Even if the solution is not outsourced, it is difficult for organisations to retain the skillsets required to maintain bespoke systems over the long term.

Mitigation - Leverage COTS Capabilities:
In many cases, implementing ABAC can be delivered through leveraging existing ICT infrastructure and commercial-off-the-shelf (COTS) products. Using COTS products can not only achieve the same information management objectives, it has the potential to increase returns on existing and future capital expenditure through the better utilisation of existing capabilities and the alignment of information management services to the business needs.

Cost savings are enterprise-driven, not solution-driven. When paired with an architectural approach that consolidates networks and promotes component reusability, cost efficiencies can also be achieved through reductions in licensing, support and maintenance overheads. Another sustainment cost saving is the ability to source common technical skills off the market. By leveraging COTS products, long-term maintenance sustainability is assured. This manages the risk involved in having to retain bespoke solution-specific skills.

Transitioning to ABAC

Consideration: Transitioning to ABAC requires the establishment of associated governance and business processes, and the application of meta-characteristics to existing assets. Managing this change is crucial for the success of such an implementation, as the organisation may face resistance from users who face losing access to information they do not need. To alleviate some of the issues, NIST suggests the incremental implementations for specific areas of interest and user communication/training is vital for achieving a successful outcome.

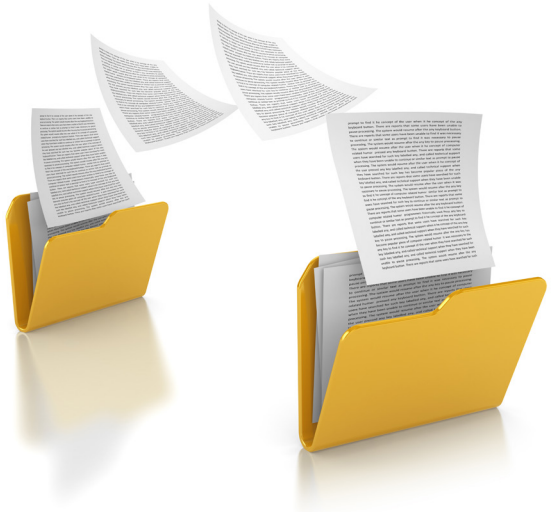
Mitigation - Maturity-Driven Change Management:
Proper change management is essential for all ICT transitioning initiatives. Taking an incremental implementation for defined communities of interest is one approach to managing the risks involved in transitioning to ABAC. Another approach is to take an enterprise-wide maturity-driven approach that drives the development and implementation of a change roadmap. This roadmap is developed in accordance with the organisation's current level of maturity and its desired end state. Changes can then be aligned to the desired business outcomes and priorities rather than as a technology decision.

Authorisation and Classification Requirements

Consideration: One of the critical success factors of any ABAC implementation is the selection of what data is to be managed and protected by the ABAC solution, the manner in which it must be protected and the determination of who is authorised to access it.

Mitigation - Information Management Architecture:
As each organisation works within an individual risk context, consisting of differing compliance policies, requirements and business objectives, a consultative approach to trusted information sharing (TIS) plays an integral role in achieving a successful implementation of ABAC. Clients frequently need help to distinguish which information assets are important for them to protect, and who has permission or authorisation to access that information. However, for large enterprises and government organisations, ALL of their information assets could potentially be valuable to external sources. Managing and protecting these assets must be done within the broader context of a Trusted Information Sharing architecture. Organisations must prioritise and value their information assets just like any other asset. Failing to do so means that their information is not being managed properly. Companies who understand and target information superiority as a priority are well-positioned to establish a competitive edge within their industry.

An access control management capability alone is insufficient for large private and public enterprises. Rather than plugging ABAC into an existing, poorly performing ICT infrastructure, an ABAC capability is embedded within the organisation's enterprise architecture to ensure access control capabilities are coherently aligned with all assurance capabilities from identity management, systems management, and information management through to workflow management lifecycles. This approach ensures that information is appropriately maintained and made available to the people who need it, while access to high-value information remains restricted to authorised users.



Trust Models and Secure Capability Integration

Consideration: To provide a holistic security capability, authorisation services must be integrated with all other security capabilities (e.g. security configuration management, monitoring, Data Loss Prevention, security audit, cyber defence) especially in distributed environments.

Mitigation - Architect Trust:
When implementing a technology solution, it is clear that trust models and security concerns must be considered. However, information security and sharing should be integral to an organisation's entire ICT strategy and architecture – not just component add-ons or after thoughts.

Security and sharing are NOT competing objectives, rather they are complementary objectives: if you do one properly you also enable the other. In order to trust an assured information management and sharing capability, and derive business value from information assets and services, the enterprise architecture understands how information capabilities support the desired business outcomes. These outcomes necessarily include:

- The provision of a superior decision-making capability – providing the people who need it with the right information at the right time and location,
- Compliance with all regulatory, security and policy requirements, and
- The mitigation of any risks presented by the possible exposure or corruption of sensitive organisational information assets.

ABAC is a technical enabler that can be employed to achieve these outcomes. While similar results could be achieved by combining quality information management practices with other forms of access control, ABAC currently provides organisations with greater granularity of control. Using ABAC as one of the technical enablers within a broader trust architectural approach means that organisations can exploit this capability to enable and control the sharing of information.

Establishing Attributes and Environmental Conditions for Exceptional Circumstances

Consideration: There is a risk that if attributes and conditions are not properly established, assigned and maintained, then data could be exposed. NIST recommends that attributes be "established, defined, and constrained by allowable values required by the appropriate policies" . Methods for provisioning these attributes and an architecture for storing, retrieving and checking them must also be established.

Mitigation - Agreed Attributes and Business Rules:
In most information-sensitive environments, the majority of these policies and business rules have already been established, assigned and maintained. The challenge is capturing them so that the required attributes and business rules can be defined and implemented. Once defined and suitably architected to properly manage flow of information between identities, systems and workflows, existing attribute stores can be leveraged and extended to offer the organisation greater granularity of information management and control.

This approach offers the organisation the ability to dynamically condition the enterprise environment in response to policy changes or the emergence of exceptional circumstances. The standardisation and management of attributes and their values are a critical element in any ABAC implementation especially if the information sharing is between different organisations and even between different industry types.

Dependency on External Information Services

Consideration: The availability of timely and quality data from outside services is a key dependency of an ABAC implementation. These dependencies present a risk to the enterprise when ABAC is considered as a standalone or 'plug-in' solution. There is a risk that the confidentiality, integrity and availability of the external information services do not meet the requirements of the ABAC solution. If the organisation is unable to assure or trust those systems that the ABAC solution is relying on, then the performance expectations cannot be realised.

Mitigation – Federated Assurance:
Instead of using an ABAC solution in an attempt to resolve a symptomatic issue such as a lack of granular access control, an architectural approach to Trusted Information Sharing enables and controls all flows of information within and external to the enterprise in a consistent and coherent manner. Those same interactions between services and systems that posed a risk for the ABAC solution, would be managed and controlled by assured workflows.

This federated assurance process enables the organisation to assess and manage the risk involved in trusted external data sources. It also enables the organisation to dynamically tune its authorisation decisions if the level of trust in these external data sources changes.

Operationalisation of ABAC

Consideration: There are a number of issues and considerations cited by NIST that relate to the operationalisation of ABAC. Firstly, one would need to establish 'deconflict rules' so that any access control discrepancies are identified and corrected early. Secondly, "New techniques are needed to coordinate and obtain the proper balance of sharing and protection", and thirdly, documentation of the 'rules' is required- policies and procedures must be in place.

Mitigation – Policy Development and Enforcement:
A standards-based architectural approach to the trusted information sharing problem is critical to enable organisations to implement the right balance between sharing and protection in their particular business context. From this, the organisation can develop the policies, procedures and services required to support and maintain this balance.

This approach identifies the appropriate level of automation required to embed desired best practice in the tools already being used by the business (e.g. identity management, 2-person integrity for the release of content, etc). It also aids in both the operationalisation of ABAC and in developing the capacity for the organisation to own, run and optimise such an implementation.

Standardisation, Interoperability and Traceability

Consideration: NIST recommends that organisations take a comprehensive standards-based approach to achieving interoperability and a flexible future deployment capability. The publication suggests that a series of products and capabilities should be used that meet "standards, specifications and standardized configurations"(p. 27).

Mitigation – Strong information management practices:
An enterprise framework is required to govern the assurance and trust models, the standards and the means of measuring the success of an ABAC implementation. Standardising products and solutions for greater interoperability is a logical and necessary first step to take. Achieving this goal, on the other hand, can be a very complex, long-term process. Large enterprises frequently have multiple networks, bespoke or legacy systems in place that do not meet current interoperability standards and are not integrated with the organisation's current networks/system. While these isolated assets are vital to the business, their value is not maximised across the enterprise.

Enabling a standardised access control capability will not resolve the information sharing issues faced by most large enterprises. Poor enterprise information management is why information services are not delivering to organisational requirements. Successfully undertaking a standardised ABAC implementation assumes a certain level of information management maturity within the organisation. Without a strong information management capability in place, standardisation, interoperability and traceability cannot be realised.

Implement TIS - not just ABAC

Despite the problem being known and articulated by the business, the IT industry continues to look for answers in technical solutions or products. ABAC is one such 'answer' that is currently being championed by many vendors and IT Executives. However the problem cannot be resolved by simply changing access control products.

IT must engage effectively with business to understand the problem, otherwise they will continue to provide services that fail to satisfy the needs and the expectations of the business. Moreover, by taking a bottom-up approach to addressing the information management problem, the costs and risks involved in implementing ABAC are likely to be realised without producing the much-hoped-for results.

The solution lies in taking a Trusted Information Sharing (TIS) architectural and maturity-focused approach. Instead of 'jumping to solutions', the TIS architectural framework emphasises a top-down approach that will help the organisation strategise, design, plan, build, implement and operationalise trusted information sharing capabilities that are uniform across the enterprise.

Establishing a trusted information sharing architecture will deliver assured information management and utilise the full potential of ABAC. It will align IT services with business outcomes and prepare the organisation for the future of information management – a future that enables them to dynamically change the conditions governing the access, use and security of information assets.

Are you considering an ABAC solution?

To deliver value, ABAC must first be designed and implemented within the broader business context of Trusted Information Sharing

archTIS

1300 ARCHTIS (Inside Australia)
+61 2 6247 3372 (Outside Australia)
info@archtis.com
PO Box 1234, Braddon ACT 2612
Suite 6, 6 Lonsdale Street, Braddon ACT 2612