ISSN:0975-9646

Web Applications Access Control Single Sign On

Anitha Chepuru ,
Assocaite Professor IT Dept,
G.Narayanamma Institute of Technology and Science (for women),
Shaikpet, Hyderabad - 500008, Andhra Pradesh, India

Dr.K.Venugopal Rao ,
Professor CSE Dept
G.Narayanamma Institute of Technology and Science (for women),
Shaikpet, Hyderabad - 500008, Andhra Pradesh, India.

Amardeep Matta
Application Security Solution Consultant, Identity and Access Management –Practice,
Mahindra Satyam Computer Service Ltd, Hyderabad,
Andhra Pradesh, India

Abstract-Access control mechanisms are a necessary and crucial design element to any application's security. Authorization is the act of checking to see if a user has the proper permission to access a particular application or perform a particular action, assuming that user has successfully authenticated him. Web access control (WAC) systems are central to this evolution. While WAC systems are not new, pressures around cost control, compliance, and growth and emerging technologies such as Web Services, Federation, and user-centric identity are causing organizations to rethink and often dramatically expand their WAC strategies. Organizations must adopt new and more advanced authentication systems, implement risk-based security policies, and federate identities with other organizations to compete effectively in the Web-enabled world. Single sign-on (SSO) is mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where he has access permission, without the need to enter multiple passwords. Single sign-on reduces human error, a major component of systems failure and is therefore highly desirable but difficult to implement. This paper presents how a Web Access control Single sign-on (WAC SSO) system protects and controls access to your Web applications, records user and administrator activities, and is responsible for creating a seamless single sign-on experience for any user including employees, partners, and customers.

Key words: Access control, Web access control, Single sign-on, Authentication, Authorization.

1. INTRODUCTION

In an Organization - customers, partners and employees fully expect anytime, anywhere access to critical applications, information and services. The proliferation of intranets, B2B extranets and e-commerce websites presents opportunities to Increase revenues, manage costs and deepen relationships with users. But opening organization via the Web also presents significant security, management and compliance challenges

WAC SSO lets you manage and deploy secure web applications to:

- Increase new organization opportunities
- Manage costs
- Improve security to mitigate risk
- Ease compliance

WAC SSO can handle your secure Web-enablement challenges and enhance your enterprise identity and access management strategy. This WAC SSO solution helps you

- Create a seamless experience for users, including access to partner systems
- Reduce costs with delegated administration and simplified management
- Respond to organization needs with the latest features, including strong authentication
- Move beyond retroactive audits and toward continuous compliance

WAC SSO addresses all of your security management concerns so you can stay focused on your important organization challenges. WAC SSO delivers unparalleled reliability, availability, scalability and manageability. WAC SSO is also automates the administration of user identities and ensures only properly authorized users can access critical IT resources from the Web to the mainframe

2. WHAT DOES A WAC SSO SYSTEM NEED TO DO?

From a organization perspective, the WAC SSO system needs to help organizations respond too many important questions, including:

- Are Web resources adequately protected? How can we provide a seamless experience for users given our disparate application environments?
- How should we authenticate users and can different approaches be used based on criteria we define?
- Is it easy to create and manage access policies and does the system offer us the flexibility we require?
- Can the system help us reduce security administration and related operational costs?
- Will a company acquisition force us to rethink our deployment strategies?
- Can we tie the system into our existing auditing processes?
- As our usage increases, will the system continue to be responsive and easy to manage?
- Can the system itself be compromised and how reliable is it?
- Can we offer a secure and simple means of authenticating users without requiring them to remember passwords?

- An employee looks up a colleague's phone number in the corporate phone directory.
- A manager retrieves employee salary histories to determine an individual's merit raise.
- An administrative assistant adds a new hire to the corporate database, triggering the company's health insurance provider to add the new hire to its enrollment.
- An engineer sends an internal URL for a specification document to another engineer who works for a partner company.
- A customer logs into a company's web site and looks for a product in their online catalog.
- A vendor submits an invoice to the company's accounting department.
- A corporate human resources administrator accesses an outsourced benefits application.

3. OVERVIEW

WAC SSO can be used to authenticate and manage users in a multi-user, multi-repository environment and to store and retrieve the credentials that are used for logging into various content and workflow repositories.

Applications can use the single sign-on system to provide users with seamless access to content that is stored and managed in disparate systems without requiring the user to log on multiple times. The system includes an application programming interface (API) for creating a single sign-on implementation and a service provider interface (SPI) for creating authentication plug-in modules that interface with existing authentication standards. Also included are two implementations of the Single Sign-on SPI. Both implementations are instances of a password vault, an encrypted store for repository user names and passwords. The first implementation, called the reference single sign-on system, uses the embedded data store. The second implementation, called the LDAP single sign-on system, uses Lightweight Directory Access Protocol (LDAP) users and authentication and stores the encrypted credentials in the LDAP store. Other implementations can be created by using the Single Sign-on SPI. The single sign-on system provides applications with the ability to manage single sign-on users and manage single sign-on user's repository credentials.

4. OBJECTIVES OF WEB ACCESS CONTROL SINGLE SIGN ON (WAC SSO)

WAC SSO eliminates the challenge of multiple user logins by enabling single sign-on for seamless access across multiple diverse web applications, portals and security domains.

WAC SSO systems are the key to enabling organization over the Web while limiting your security risk. A WAC SSO system protects and controls access to all critical Web applications, records user and administrator activities, and is responsible for creating a seamless single sign-on experience for any user including employees, partners, and customers. An effective WAC SSO system must be a shared security service for applications throughout the enterprise. It's not enough to simply meet basic requirements enterprise WAC SSO deployments need to support complex single sign-on scenarios and nonstop operations. They must be easy to administer, monitor, and manage. Deployment alternatives are necessary so that the system can be adapted to an organization's specific requirements. In addition, the system needs to be extensible and pervasive in terms of its platform coverage and capabilities.

As mentioned in section 3 transactions, the company must determine who is allowed to view the information or use the application. Some information such as product descriptions and advertising can be made available to everyone in a public online catalog. Other information such as accounting and human resources data must be restricted to employees only. And other sensitive information such as pricing models and employee insurance plans is appropriate to share only with partners, suppliers, and employees. This need for access determination is met by WAC SSO.

When a user or an external application requests access to content stored on a company's server, a policy agent PEP (installed on the same machine as the resource you want to protect) intercepts the request and directs it to WAC SSO which, in turn, requests credentials (such as a username and password) for authentication. If the credentials returned match those stored in the appropriate User data store, WAC SSO determines that the user is authentic. Following authentication, access to the requested content is determined by the policy agent who evaluates the policies associated with the authenticated identity. Policies are created using WAC SSO and identify which identities are allowed to access a particular resource, specifying the conditions under which this authorization is valid. Based upon the results of the policy evaluation, the policy agent either grants or denies the user access.

Single Sign-On (SSO) across Web applications is one of the most visible features of a well-designed WAC system. Most WAC systems address basic SSO requirements through the use of an HTTP session cookie. But challenges emerge as the deployment scale grows or as the Information Technology (IT) infrastructure from different organizations is combined. WAC includes three additional SSO features to address these challenges: ***Security Zones, Cookie Providers,*** **and** ***Identity Mapping*****.**

Security Zones

SSO across applications within a common cookie domain can be restricted through the use of WAC Security Zones. This allows a single cookie domain to be partitioned to allow for different security policies without a requirement to establish Domain Name System (DNS) sub domains. Administrators first organize applications into groups (or zones) with similar SSO requirements. Then, WAC generates a separate session cookie for each zone. End users benefit from SSO within each zone and administrators are able to enforce different security policies for applications in different zones. Security Zones make it possible to have:

- Different session time-out settings for applications in each zone

- Different user directories for authentication in each zone
- Different authentication methods and protection levels in each zone

Cookie Provider

SSO can be extended across multiple DNS domains with the WAC Cookie Provider feature. In this configuration, WAC challenges the user to authenticate in the first DNS domain (company.com) but does not challenge the user when they navigate to subsequent domains (subsidiary.com). The Cookie Provider feature is popular for cross-domain SSO where a single WAC environment is protecting resources in each domain. The federation capabilities of WAC provide a better solution when there are many different domains or when there is no WAC infrastructure in the other environments.

Identity Mapping

WAC Identity Mapping can be used to extend SSO across independent WAC deployments. This might be useful when two organizations merge and each was previously running different WAC systems (and different user directories) and it is not possible or desirable to merge the infrastructure. Also known as auth-validate mapping, Identity Mapping makes it possible for a user to be authenticated to a user directory in one WAC system and be mapped to the same user identity in a different authentication store on another WAC system. The two systems need only share or synchronize their WAC key stores. The federation capabilities of WAC can also be used for this purpose.

5. SOLUTION:

WAC SSO is a comprehensive security management solution that addresses these important questions. This paper discusses how the component architecture of WAC SSO enforces security policy, why it performs so well, and how companies have scaled WAC SSO deployments to support thousands of Web applications and tens of millions of users. The key WAC SSO functions that WAC supports, including authentication, authorization, single sign-on and auditing are also discussed.

The Basic Architecture of WAC SSO

WAC consists of two basic run-time components and an administration component WAC AGENT acts as a **Policy Enforcement Point (PEP)** and also performs the services of authentication management and single sign-on. Agents can also support optional requirements such as securely passing user entitlements to protected organization applications.

WAC SSO policy server acts as the **Policy Decision Point (PDP).** The Policy Server authenticates users on behalf of the PEP, evaluates security policies, and makes authorization decisions that are communicated back to the PEP. The Policy Server also audits each of these events. The Policy Server supports various providers and platforms for the user directory and for its policy and key stores. As Policy Servers are added for increased capacity and high availability, they connect to a common policy store to determine available infrastructure and the security policies they need to enforce. They also connect to a common key store to enable secure single sign-on.

WAC SSO administrative UI serves as a secure **Policy Administration Point (PAP).** One instance of the Administrative UI server can connect to and manage multiple Policy Servers.

WAC Centralizes Security Policy

WAC provides the centralized security management your organization needs to authenticate users and control access to web applications and portals. Across Internet and intranet applications, it enables the secure delivery of essential information and applications to your employees, partners, suppliers and customers. It also scales to meet your growing organization needs with flexible administration tools that can support either centralized or distributed administration.

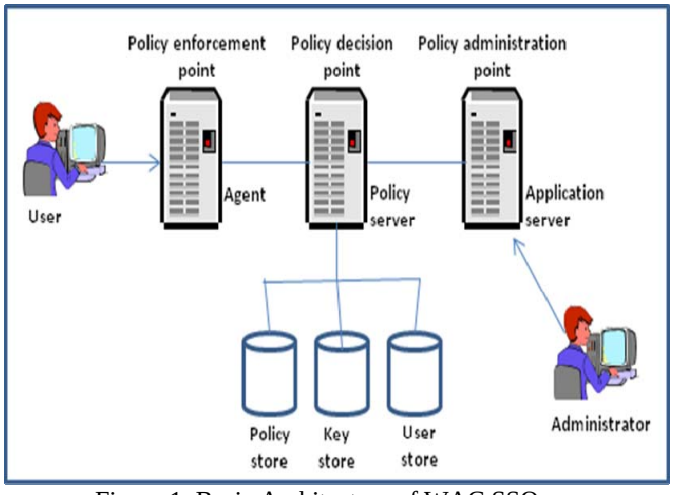

Figure 1: Basic Architecture of WAC SSO

Authentication

User authentication is the first step in securing Web applications, establishing a user identity, personalizing the user's experience, and determining what each individual can do. WAC SSO supports and manages the use of a broad range of authentication methods including passwords, tokens, X.509 certificates, smart cards, custom forms, and biometric devices.

Authentication methods can be designated a protection level, and minimum protection level scan be associated with applications to provide greater assurance of the user's identity where sensitive applications and information are exposed.

Centralized Policy bases Authorization

Organizations need flexible security policies that can be easily leveraged over multiple applications and services. They need to implement a single shared security service to simplify administration, ease compliance-related reporting, and reduce the security-related burden on application developers. Without WAC SSO, web application developers must implement security logic entirely inside their applications. This leads to compliance exposures and development challenges. For example, the required security development skills would depend on the type of Web server,

operating system, and programming language used for the application. WAC SSO centralizes the management of user entitlements for customers, partners and employees across all web applications through a shared service. Centralized authorization greatly reduces development costs by allowing developers to focus on the application's organization logic instead of programming security policies. In addition, provides the ability to enforce security policies across the enterprise, which eliminates the need for redundant user directories and application specific security logic.

WAC SSO centralizes the access management for customers, partners and employees across an enterprise's web applications. This eliminates the need for redundant, application-specific security logic and provides a lower cost approach for ensuring an enterprise's ability to meet compliance requirements. WACSSO policies are rules or rule groups that allow or deny access to a resource. Access can be restricted by user attributes, roles, groups and dynamic groups and determined based on location and time. Authorization can be conducted at the file, page or object level. In addition, controlled "impersonation" — where one authorized user, such as a customer service representative, can access what another user can access — is also defined by policies. An embedded policy analysis engine, reporting system, and out of the box reports support an organization's evolving needs for compliance and governance reporting.

Password Services

Password Services encompasses a range of topics, including password policies, changing passwords, password expiration, password recovery, and account disablement. Password services are provided by some user directories and by some WAC systems. When configured, WAC SSO invokes a password policy whenever a user attempts to access a protected resource. If the user's password has expired based on criteria defined in the password policy, the user's account can be disabled or the user can be forced to change the password. Password policies can be associated with an entire user directory or a subset. Multiple password policies can be configured for the same user directory, in which case they are applied according to priorities that you can specify for them.

Auditing

Organizations must closely track how applications and data are used, and how the security system is helping to provide controls. System administrators need detailed system data to fine tune performance. Organization managers need activity data to demonstrate compliance with security policies and regulations.

Performance, Availability, Reliability, Scalability

Use WAC SSO to deploy critical organization applications to multimillion user populations and be confident that its performance has been verified through independent testing to provide significantly higher transaction rates, reliability and manageability than alternative solutions.

Reliability, availability and scalability are supported by features including:

- Dynamic load balancing
- Two-level caching
- Policy Server clustering and cluster-to-cluster failover
- Policy Store and user store replication

6. WEB ACCESS CONTROL SINGLE SIGN ON WORK FLOW

Step 1 : The user attempts to access a protected application on a Web browser.

Step 2 : A policy agent installed on the Web server or application server intercepts the access and checks for a valid SSO token, which is typically presented as a cookie. You can deploy policy agents to a range of Web servers, application servers, and even enterprise applications from vendors such as Lotus, SAP, and Siebel.

Step 3 : The policy agent redirects the user's browser to a login page and earmarks the URL originally requested by the user as a parameter.

Step 4 : The user authenticates to Access Manager, typically by typing in a user ID and an associated password. Afterwards, Access Manager creates a session with a specific lifetime. For the duration of that session, the user is signed on according to the policies that are in place.

Step 5 : Access Manager sends the user's browser a cookie that contains an SSO token and redirects the browser to the originally requested URL. Afterwards, the user's browser repeats the request in step 1, this time with the token-included cookie.

Step 6 : The policy agent finds the cookie, extracts the SSO token, and validates it with Access Manager.

If Access Manager's policies have granted the user access to the requested application, the user can proceed. Otherwise, the policy agent denies the request with either an HTTP error or a redirect to a page with an "access denied" message. Subsequent requests for other protected applications will include the SSO token. Again, the Policy Agent validates the SSO token and the user's authorization and then allows or denies the request, as in Step 6. This sequence of events can repeat until the user's session expires or until the user explicitly logs out.

CONCLUSION

Web access control SSO systems perform a vital role in today's environment by securing the delivery of information and applications over the Web without the code to run for all applications.WAC has the best performing and most scalable architecture available today to secure all of your Web applications, even those destined for global scale deployment and tens of millions of users. Applications can use the single sign-on system to provide users with seamless access to content that is stored and managed in disparate systems without requiring the user to log on multiple times .Single sign-on features, flexible deployment and auditing options, and broad platform support make it possible to optimize a WAC deployment to your organization's specific requirements. The single sign-on system provides applications with the ability to manage single sign-on users and manage single sign-on user's repository credentials.

REFERENCES

[1] www.ca.com
[2] www.oracle.com
[3] www.ibm.com
[4] www.sun.com
[5]www.searchsecurity.techtarget.com/definition/single-sign-on
[6]http://www.imprivata.com/products-and-solutions/single-sign-on/onesign-single-sign-on