ASP and BPO Authentication Issues

A Sevan White Paper

sevan networks

Introduction

This Sevan White Paper catalogs authentication issues that have been reported by Application Service Providers (ASPs) and Business Process Outsourcers (BPOs). The paper also discusses the impact of the choice of user authentication methods on these issues.

As background, ASPs provide applications (e.g. database, ERP, or CRM), and BPOs host processes for supporting specific types of businesses (e.g. medical offices, credit unions, and travel agencies). Since we have found that ASPs and BPOs face similar issues, we group them into a single entity, which we call "providers". We refer to their offerings simply as "services".

User Authentication Issues

The following table presents the issues raised by the providers as well as the end customers (the provider's customers):

ASP and BPO Authentication Issues			
Issue	*Description*	*End Customer's Concern*	*Provider's Concern*
1	Security	Customers demand that the provider protect their information. Only users authorized by the customer can access the information. This concern is especially acute when customers are competitors. The security mechanisms must not interfere with the customer's business.	Providers must minimize their liability stemming from inadvertent access to sensitive information. Providers must have responsive, secure and inexpensive means of administering and enforcing authorized users. Providers must limit security's demand on the help desk.
2	Reliability and Availability	The services are available when and where needed. Customers demand high up-time and internet availability.	Unavailability translates into lost revenue and dissatisfied customers. Reliable applications and internet access reduce the provider's operating costs.
3	Optimal Services	Customers demand services that fit their business. Some customers might demand the most up-to-date tools, while others seek the stability of staying with proven solutions. Customers cannot be satisfied with a common service.	Providers must quickly, reliably, and cost effectively roll out new services. Providers must minimize the costs caused by multiple applications.
4	Cost Effectiveness	Customers demand the highest value, which generally means the lowest subscription costs.	Providers demand a return on their investments, which translates into low total cost of operations.
5	Ease of Use	Customers demand user convenience. User authentication must not impede the business.	Providers must keep help desk costs down. Providers must have satisfied customers.

Comparing User Authentication Choices

A provider's ability to address these issues is influenced by its choice of user authentication methods. This section illustrates the impact of authentication technology by comparing two user authentication methods:

- password-based authentication; being the most commonly deployed
- certificate-based authentication; being the most discussed successor

Password Authentication

Almost all providers depend on user names and passwords to control access. Each user is assigned a unique name and password and must provide it in order to access the service. Password systems have been used for decades. They are well known and are widely considered "best practices" for IT security. Password systems can differ in the following respects:

- Location of the access control. Typical locations include:
  - a native function of the application (service),
  - a native function of the server's operating system,
  - an access control solution added to the server, or
  - an external access control gateway.

- Administration of the authorized users. Options include:
  - the provider administers the users
  - each customer administers his users

- Password policies: Options include:
  - length and obscurity of the password
  - age restrictions for the password
  - restrictions on password sharing

- Method of password reset, which include:
  - manual reset by provider
  - manual reset by customer
  - self-service reset by user

When security concerns are especially high, passwords can be augmented with one-time-password tokens. Security is strengthened because access is granted only to those users who possess the token as well as know the password. The tokens are not widely used because users don't like them. The most widely used token is the SecurID™ product from RSA.

Password-based authentication is especially attractive when the security demands are modest. Unfortunately, as the security requirements become more demanding, the cost of operating password systems increases rather dramatically. Processes that deal with lost passwords and periodic changes to passwords tend to be costly. There is a good deal of interest in finding alternatives to passwords for those environments where the passwords are either too costly, complex, or inconvenient.

Certificate-Based Authentication

For over a decade IT professionals have looked for alternatives to password authentication. One of the most promising technologies is based on public key cryptography, which is commonly and erroneously referred to as "certificate-based" authentication. Unfortunately, the promise of certificate-based authentication has been stifled by the cost and complexity of setting up the requisite infrastructure: PKI

Certificate-based authentication is characterized by the following:

- Users are authenticated through their SSL certificates.
  - Authentication can be automatic and transparent to the user.
  - Certificates and keys can be stored on the user's computer – nothing to forget or lose
  - Portability can be achieved by storing certificates and keys on tokens or smart cards
  - No user software is required, since the authentication operations are natively supported by all major browsers.
  - Certificates can be used as the sole form of authentication or can be combined with passwords

or biometrics.
- Certificates can be created so they cannot be replicated or shared.

Sevan's Identity Authentication™ makes it possible to simply deploy certificate-based authentication without an infrastructure. Identity Authentication is characterized as follows:

- Identity Authentication is delivered as an appliance, which installs as a gateway in front of the web servers.
  - The appliance is transparent to the services, servers, and networks.
  - The appliance is self-contained – no additional hardware or software is required.
  - The appliance is hardened to provide the highest levels of security.

Passwords and certificate-based (specifically Identity Authentication) are compared in the following table:

Comparing Passwords and Certificates			
Authentication Issues		*Password-Based Authentication*	*Certificate-Based*
Security	*strength*	Passwords tend to be easy to lose, guess and forget. Procedures for recovering lost passwords are the weakest point of the security system.	Public key cryptography is stronger than passwords. Certificates are far less likely to be lost or stolen.
	strength	Password systems that are part of an application or operating system are only as strong as the underlying application or operating system. This comment also holds for access control solutions that are added to servers.	Identity Authentication is delivered in an appliance that hardened against attacks. This secured appliance must be broken to defeat Identity Authentication.
	unified solution	Relying on password systems that are part of an application or operating system can mean multiple authentication systems, which weakens security by confusing administrators and users.	A consistent authentication mechanism reduces the possibility of security beach through mis-configuration or misuse.
	password sharing	When users share passwords, reliable audit is impossible.	Certificates can be generated so that they cannot be shared. Each access can be traced to a single user or computer.
	site partitioning	It is common to host multiple customers on a single server or even application. The authentication mechanism must enforce strong partitioning so that one customer cannot examine the information of another.	Identity Authentication allows the provider to securely partition his site, servers, and even applications into independent resources. Users are authenticated and authorized only for their resources.
Reliability and Availability	*web access*	Wide availability means access through browsers: password authentication through standard HTTP and HTML mechanisms.	Identity Authentication leverages standard features found in all browsers – no need for additional client software.
	redundancy	An external authorization solution can become a performance bottle neck and a single point of failure – redundancy is a must.	Identity Authentication supports redundant configurations for scalable performance and reliability.
Optimal Services	*ease of upgrade*	Relying on password systems that are part of the applications makes it difficult to upgrade or add new applications, since the security mechanisms must be verified before each upgrade. This significantly increases the time and cost of application and server upgrades.	Since authentication is independent of the applications and operating systems, the provider is free to add, upgrade, or change applications and operating systems.
	independent solution	Integrating authentication solutions into your applications or servers provides a common solution. Unfortunately, changes may require a significant reintegration effort. Once again, security solutions become a ball-and-chain.	Identity Authentication is delivered in a manner that is independent of the applications and servers.

Comparing Passwords and Certificates			
Cost Effectiveness	*account sharing*	A single account can be shared among multiple users by sharing the password. This results in lost provider revenue.	Certificates can be generated so that each user needs his own certificate. The provider can easily monitor (and bill for) the number of certificates used by each customer.
	unified solution	Relying on password systems that are part of an application or operating system can result in multiple authentication systems, which are expensive to maintain and use.	A common authentication mechanism reduces training costs and operating expense. A common user interface lowers help desk costs.
	delegated user administration	It is costly for the provider to administrate users. User administration must be delegated to the customers.	Identity Authentication supports simple, delegated user administration. Each customer can determine which users are allowed access.
	usage logs for billing	Value-based billing requires dependable usage statistics, which are usually not available from password-based solutions.	Identity Authentication maintains full logs of user activities. The service provider can bill on the basis of time, resources accessed, or data transferred.
Ease of Use		When password policies are stringent, passwords become a burden to the users: passwords must be memorized, protected, reset, and repeatedly typed in.	Identity Authentication can be configured to be automatic and transparent to the users -- authentication couldn't be easier on the users.

The Sevan WSA™

Sevan Networks delivers its Identity Authentication solution in a self-contained appliance. The Sevan WSA is located between the servers and the network. It is transparent to users, applications, servers, and networks and requires no changes to the provider's web site – simply plug and play.

The WSA partitions the provider's site into independent sets of resources for each customer. When a user attempts to access his resources, the WSA creates a secure SSL session between itself and the user, while authenticating the user through his SSL certificate.

Illustration 1, suggests a WSA installation supporting 3 customers to 4 services. Each user has his unique certificate, which gives him rights to access the set of services for which his employer subscribed. The WSA prevents the customers from accessing each other's services. User administration can be performed by the provider or delegated to the customers.

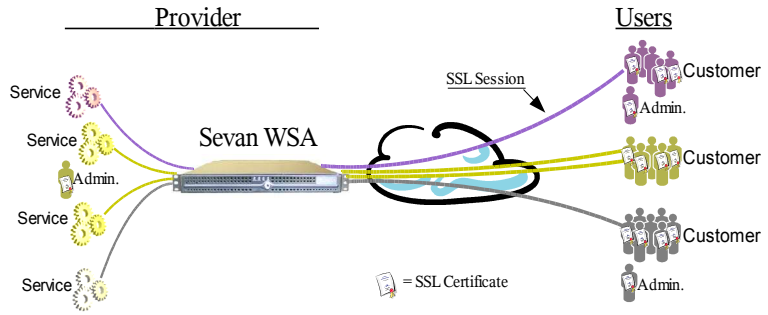

Illustration 1-- adding a Sevan WSA to a provider's site

Sevan Networks, Inc
1310 Hollenbeck Ave, Ste F
Sunnyvale, CA 94087
Tel: 408.830.1000
Fax: 408.830.1001
www.sevannetworks.com