Comparing Web Authentication Methods

A Sevan White Paper

sevan networks

This Sevan White Paper presents commonly used methods for user authentication. It compares these authentication methods with Sevan's Identity Authentication™.

All user authentication is based on one or a combination of the following:

1. something the user knows
2. something the user has
3. some physical trait of the user

The most commonly discussed (not necessarily deployed) methods for user authentication are:

- user name and passwords
- hardware tokens that generate time-varying passwords or responses to challenges
- biometrics
- PKIs

Each of these methods are discussed below:

User Name and Password

This is the most widely used method of authentication. It is based on “something the user knows”. Its popularity stems from the following:

+ Passwords require no special software on the users' computers
+ Passwords are portable if the users memorize them.
+ Passwords authenticate the user directly because only the user knows the password.

Password systems suffer from the following problems:

- Users can't remember strong passwords, so they write them down. This makes the passwords vulnerable to password thieves.
- When passwords are forgotten, the password must be recovered, which is either expensive or insecure.
- Users can share passwords. Revenue is lost when multiple users share an account. Also,the ability to audit or otherwise trace access to a particular user is lost when users share passwords.
- A password is a shared secret: it is known by the web site as well as the user. An administrator can discover the password and use it to masquerade as the user.
- A single password cannot be safely used with multiple web sites, since each site administrators can discover the password. The user must have a unique password for each site.

Hardware Tokens

Hardware tokens are widely used to augment password-based authentication. Tokens are examples of authentication through “something the user has”. Tokens have the following positive features:

+ Tokens prevent a thief with a stolen password from accessing the web site. The thief must steal the physical token as well as the password.
+ Tokens prevent accounts from being shared since the token must be duplicated.
+ Tokens are portable, so the users can take the token with them.
+ Tokens require no special software on the user's computer.

Tokens suffer from the following problems:

- Tokens are expensive and must be replaced or refurbished every few years.

- Token are easy to misplace or damage. A lost token prevents a valid user from accessing the web site, which disrupts business or commerce.
- Tokens are inconvenient since the user must manually enter the value of the token as well as the password.

Biometrics

The promise of biometrics is compelling: authenticate a user through a unique physical characteristic. Typically this is a finger print,voice, face, typing pattern, etc. The hope for biometrics is based on the following:

+ Biometrics directly authenticates the person, not indirectly through a password or token.
+ Biometrics features are difficult to steal; thereby making biometric authentication very strong.
+ The biometric feature is eminently portable, and is unlikely to be lost.

The reality of biometrics is clouded by the following:

- The user's computer must include the appropriate biometric sensor and software. Reliable sensors tend to be expensive.
- Most inexpensive biometric authentication schemes exhibit poor trade off between false-positives (wrongly accepting an invalid user) and false-negatives (denying a valid user).

Public Key Infrastructure

This broad marketing term is applied to authentication methods using public key technology, especially those employing digital certificates. Details on these technologies can be found in our white paper: “User Authentication with Public Key Cryptography”.

The following features make PKI authentication attractive for web access control:

+ Every modern browser has the built-in capability for public key authentication.
+ Public key authentication can be automatic and even transparent to users.
+ Public key authentication is much stronger than passwords, because the authentication “secret” is stronger and is not shared with web sites.
+ A single certificate can be used for many web sites, since the “secret” is not shared.

PKI authentication has not been widely deployed. The main reason for this is the complexity of the infrastructure:

- The PKI model requires that the digital certificate binds the proofed identity of the user to the value of the user's public key. This seemingly simple requirement generates a great deal of complexity: how is the identity proofed, who does the proofing, what are the liabilities if the identity proofing is wrong?
- The PKI model focuses on identity and does not address the authorization problem: what is a user allowed to do? As such the PKI is a partial solution.

Sevan Web Identity Authentication

Sevan's Web Identity Authentication is a hybrid of password and public key technologies. We combined these technologies in such a way to cover the weakness of one with the strength of the other. Specifically, WSA solves the problem of forgotten and weak passwords, while avoiding the need for a PKI.

WSA is based on the observation that public key authentication is ideal for maintaining trust (accessing the web site day after day) and passwords are ideal for establishing trust (authorizing the initial access). So, we use passwords to establish the trust in the user's certificate and the certificate to maintain the trust. As such, there is no need for a PKI to generate a trusted certificate. Furthermore, after the certificate becomes trusted through the password, there is no need to remember the password.

WSA directly supports today's business practices and as such it avoids the legal pitfalls of PKIs. Since we use passwords to establish trust, the trust is solely between the user and the web site – there is no need to trust a third party running the PKI. If the web site decides that the user is no longer trusted, it is a simple process to revoke the trust in the certificate.

WSA also affords flexibility in the web site's and user's certificate policies. For example, the user can use one certificate for all web sites, or can use a different certificate for each site. This allows the user to control her identity and privacy. The WSA's ability to issue certificates on-demand, makes it trivial for users to obtain as many certificates as they need.

This flexibility extends to the web site's owner. The owner can decide to accept any certificate (no trust in the certificate) or can restrict itself to certificates from specific issuers. The web site can select from the full spectrum of trust: from anonymous certificates to certificates carrying full X.509-like identity proofing.

sevan
networks

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