Passwords and Subscriber Services
A Sevan White Paper

Businesses are increasingly turning to Web technology to distribute sensitive or valuable information. Corporations are basing more of their enterprise systems on the web; allowing employees, customers, and partners to access mission-critical information. Merchants and service providers are also using the Web to reach consumers of services, information or entertainment.

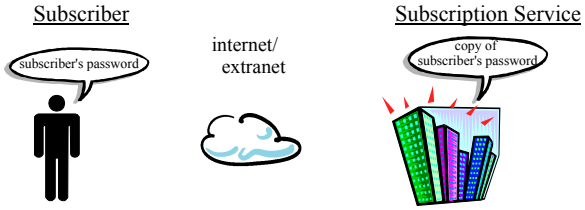
These high-valued Web-based services are underpinned by the concept of a *subscription*: the consumer of the information or service has a subscription relationship with the provider of the service. The subscription has a set of implicit and explicit rules concerning the use of the service and the compensation for the service. These subscription rules are manifested in many fashions. Examples include:

- employment agreements,
- user license agreements, and
- consumer subscription agreements.

A Web-based delivery of a subscription service must enforce the subscription rules.

Passwords

Today, most subscription services use passwords to limit access to only subscribers. The password scheme is based on the simple assumption that only those users knowing the appropriate passwords are subscribers and can therefore access the service.



Experience with password systems have shown significant drawbacks, which include:

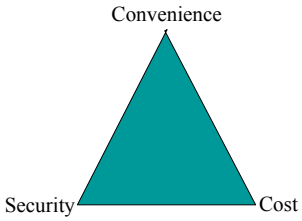
- Passwords are inconvenient for the subscribers, since subscribers must remember the password and type it every time they wish to access the service.
- Strong passwords tend to be hard to remember and are generally written down, which can expose the passwords to non-subscribers
- Strong passwords should be changed often, making it even more difficult for the user to remember. Security-conscience organizations require the subscribers to change passwords every 30 days., making it difficult to remember passwords.
- Strong passwords tend to be easy to forget, which requires a mechanism for the subscriber to recover his forgotten password or to get a new one. Password thieves focus on this recovery mechanism to steal subscriber passwords. Recovery mechanisms that prevent password fraud tend to be expensive to operate.
- Non-subscribers can steal access to the service, when subscribers share their passwords with non-subscribers
- Password thieves can easily guess simple, short, or otherwise convenient passwords.
- A dishonest service provider can obtain a password used on his service to access the subscriber's other services when the subscriber uses the same password on multiple services.

Password systems exhibit the classic tradeoff between security and cost to the subscribers and providers. Password systems that are easy to own, tend to be vulnerable, and hence provide little real security. On the other hand, password

systems that are secure tend to be difficult to manage and require a great deal of effort on the users.

So, even though password systems are widely used to enforce subscription services, passwords tend to be:

- cumbersome for the subscribers,
- expensive to maintain for the service providers, and
- open to fraud (weak security).



So, the service providers and subscribers must make the trade-off between security, convenience, and cost.

Fortified Password Systems

There are a number of schemes for improving password systems. We will consider two: single sign on and tokens.

Single-sign-on schemes make passwords more convenient to the users by automating the management of multiple passwords and automatically using these passwords in multiple subscription services. The user employs a single password to activate the single-sign-on mechanism. To date, single-sign-on is too complex except for the simplest environments.

Token schemes solve the problem of stolen passwords. The most widely deployed token is a small device that generates a number every minute or so. When the subscriber wishes to use a service, he must type in the number from the token as well as his password. This means that the subscriber must know the password as well as have the token in order to access the subscription service. This is the most widely used example of "two-factor" authentication. Token-based systems are considered far stronger than password-only systems, but they exact a high cost of ownership and subscribers tend to despise them (yet another "thing" to carry around and another number to manually enter).

Summary

Passwords are appropriate for some subscription services and will probably remain so in the future. However, passwords become less attractive for those services handling valuable or sensitive information. This is because the value of the information tends to demand more security, which in turn drives up the cost and inconvenience of the password systems. There are many ways of augmenting password systems to make them better, but such hybrid systems preserve the fundamental limitations of passwords.

The cost-convenience-security tradeoffs of passwords is one of the factors holding back the deployment of high-value subscription services on the Web. Therefore, it is important to come up with an alternative to passwords that exhibits a very different cost-convenience tradeoff. This is the motivation behind Sevan's Identity Authentication™, which provides the subscribers and the service providers a much more attractive tradeoff between convenience, security, and cost.

sevan networks

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