

WHITE PAPER

PLANNING FOR SINGLE SIGN ON

Rion Dutta
rdutta@mielesecurity.com

9:00 a.m. on Monday morning. You can't log in to the intranet. Your previous password expired last week and you entered a new password at the prompt, in line with your company's dynamic password policy. The problem is that you've forgotten what it is. There are just too many passwords to remember these days.

Organizations spend \$25 each time they have to process a 'lost password' incident (Meta Group). And this is only part of the problem. Despite measures taken by the user and the administrators to ensure the integrity of passwords, the vast majority of network users tend to use the same password wherever possible, posing inherent security risks.

Enterprises today are seriously considering the use of Single Sign On (SSO) technology to address the password explosion because they promise to cut down multiple network and application passwords to one.

While the temptation to purchase readily available SSO Solutions in the marketplace is great, organizations need to plan the process and evaluate options in line with their security policies and business objectives. Why? It's not going to be effective unless it is planned and implemented properly. The cost is too high a risk, and worse, it could end up costing millions and exposing new vulnerabilities in your systems.

What is Single Sign On (SSO)?

SSO allows users to log in once, using what appears to be a single method or credential to gain access to multiple hosts and applications, thereby eliminating the need for multiple logins accompanied by multiple passwords.

Most SSO solutions available today provide *Authorization* as well as *Authentication*. Authorization policies can restrict which applications the user has access to and what the user can do once logged in.

There are two common approaches to a SSO solution – tokens and proxies. Both methods employ a *Centralized Authentication Server* that authenticates the user and brokers the authentication and login to the back end system.

In the *Token model*, a single encrypted token is issued to the user after successful authentication. This token is then presented to multiple back end systems as needed. The most common instance of this type of SSO employs the Kerberos Network Authentication Protocol developed by MIT, often in conjunction with the Open Group's Distributed Computing Environment technology (DCE). Microsoft's Windows 2000 and XP use a version of Kerberos v.5 for default network authentication protocol.

One of the biggest drawback's of the token approach is that it requires acceptance of the token by all the back end systems, i.e. a back end system must be 'token enabled' to support SSO. This can prove to be a costly and time consuming exercise, since some systems may need to be re-architected to accept the token.

The disadvantages of the token approach led to the development of *Authentication Proxy Servers*. Instead of logging in directly to the application or presenting every application with a token, the user logs into the authentication proxy server. The server brokers the user authentication request by presenting the correct user credentials (i.e. password, certificate, token) to the native application, server or OS. Then the authentication proxy server manages the user access based on the native system's response.

Authentication proxies are also used by *Web Based SSO solutions*. Web based SSO allows users to log in via a web page and then access systems and applications through the web interface. Primitive web based SSO solutions use cookies, but these are not suitable for organizations that have large, distributed web farms or complex applications that have application specific logins that are coded into the application itself. Also purely web based SSO solutions may not have support for multiple authentication methods such as smart cards and tokens or for applications that are not accessed in ways other than a web browser.

To address these shortcomings, many web based SSO solutions have been upgraded and expanded to incorporate support for multiple modes of authentication and interfaces.

Business Benefits of SSO

The benefits of reducing multiple usernames and passwords may seem obvious. But this intuitive reasoning needs to be backed by with analysis of the benefits and the risk. The specific benefits of reducing passwords vary across enterprises and even across departments. In addition to this, companies need to examine whether SSO makes sense from a hard numbers perspective. If all these questions can be answered, and the benefits outweigh the risks, then SSO may well be the technology that you need.

Reduction in Total Cost of Ownership (TCO)

How much does it cost your company every time a password is reset? Depending on the organization and the relationship of the user to the password, administration costs range between \$1 and \$30 for every password change (higher costs are due to instances where transaction values are high and there are many different users that need to access a central support center, for example, users of online banking or financial services.)

Potential Increase in Security

If users need to guess one password, there is a greater chance that they will user 'stronger' ones and a lesser chance of passwords being visible to third parties because of poor protection by the user.

Support for multiple authentication Methods

Most companies reject stronger multi-factor authentication solutions because they fear that they will be too difficult to manage or too hard to incorporate into existing authentication systems. Choosing an SSO solution that supports multiple authentication methods can reduce the implementation costs while providing strong authentication security.

Integrating External and Internal users

Most companies with a large web presence require authentication login support for two very different populations – internal employees and outside users. Because the security rules and policies that apply to the two groups are different, companies prefer two separate authentication databases. As the use extranets and access to remote systems grows, MIEL sees a trend in companies moving towards consolidation of the two user bases. An appropriate SSO solution could enable a company to integrate and consolidate the management of these two user bases under a single system.

Risk Factors

Consolidating passwords and logins also results in consolidating the points of risk – potentially exposing your enterprise to threats and vulnerabilities. This section will outline the potential risks and will help you balance the business benefits against these risk factors.

Single Point of Failure

Since a single password affords access to multiple systems, if it stolen, the damage done with it will be much greater. Even if the passwords are not stolen, storing passwords on a single server makes that server a single point of attack. If the server's security is compromised, then the attacker potentially has access to all the systems the server protects.

Vendor Reliability

Before purchasing an SSO solution, an organization should research the vendor with due care.

Some questions to ask: Has the vendor had the solution reviewed by a third party audit? How long has the company been in business? How many customers does the vendor have? Will any customer act as a reference? Are there any published attacks against the vendor's solution and if so has the vendor addressed and corrected the vulnerabilities?

User and Administrator Training

Organizations planning an SSO must also plan 'Safe Password' training classes for their employees, educating users to select passwords that are difficult to guess and explaining the importance of never sharing passwords with third parties. Users need to understand the basics of password security irrespective of SSO. In this instance, the incremental cost of SSO education needs to be measured. Also, the head count of support and administrative staff needs to be examined, in addition to training for administrators.

Cost to Implement / Complexity of the Environment

The potentially high cost of implementation in complex environments is often overlooked by companies. There are often restrictions on what solution can be used, imposed by the existing technical landscape. Creating a single sign-on solution for an all web environment is much simpler than creating SSO in a heterogeneous landscape.

Organizations that need authentication to multiple legacy systems comprised of systems like AS/400 and S/390®, and custom applications should select a solution that supports as many of

these systems as possible such as Resource Access Control Facility (RACF) from IBM® or Computer Associates' eTrust CA-Top Secret for S/390 mainframes, Pluggable Authentication Modules (PAMs) for Unix systems and Graphical Identification and Authentication (GINA) for Windows.

Also, many companies that have attempted SSO in the past may have legacy Kerberos/ DCE based authentication. If your enterprise has already spent time and money in providing some SSO via DCE, the costs of replacing the existing infrastructure need to be considered against the benefits. Or, look to an SSO provider that can incorporate the existing architecture into an overall framework that supports future needs.

Companies with dial-in or remote populations may need support for RADIUS. Companies that are using directories will probably benefit from the ability to integrate directories, via LDAP into SSO.

Wireless authentication is something that needs to be considered for long term SSO planning, as WLANs are becoming common, making authentication for wireless clients critical to SSO strategies. The IEEE 802.1x authentication standard uses the Extensible Authentication Protocol (EAP) for wired and wireless networks and supports many authentication standards such as RADIUS and Kerberos.

Another point to consider in complex architecture is the varying level of authentication needs, such as multi-factor authentication to highly restricted systems and simple password authentication for less protected ones.

Summary

While 'fewer passwords' is a common end goal for many companies, SSO solutions do not come in a 'one size fits all' package – rather, what is appropriate for Company A may not be for Company B. This is why it is critically important for a company to analyze its situation, specific business benefits and potential risks objectively before selecting a solution.

By taking the time to understand the potential business benefits, including the business needs, objectives and security risks, you will be able to avoid the common pitfalls of SSO implementation. Without an objective, hard number analysis of the costs and benefits associated with SSO.

A security implementation that has not been planned effectively will result in cost overruns, mismanaged systems, and reduced security overall.

By keeping expectations in line with reality and planning ahead, your company can enjoy the convenience of fewer passwords without the pain and the high cost of a poorly planned rollout.