GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Michael Kelly
Version 1.2e

Is Single Sign on a Security Risk?

Introduction

There used to be a time when the majority of computer operators and people alike maintained one user ID and password. With the introduction of platforms such as Microsoft Windows, and with the continual lowering of hardware costs capable of hosting Unix systems. This is no longer the case. Many of the applications hosted by high end systems like Mainframes have been distributed amongst multiple client server systems. If this didn't cause organizations enough foods for thought, lets add e-commerce to the equation. With each different OS, Application and security database introduced comes its own unique group of issues. Every day that passes organizations change not only the technology they use but also the people that maintain the environment. This extremely fast progression has introduced many concerns for organizations large and small.

What is the issues progression has introduced?

It is inevitable that with progression comes some amount of pain. Without understanding all the issues it would be very difficult to investigate an SSO Solution. Once the issues are understood it will be easier to determine if SSO is a security risk or a technology that helps alleviate security risks. Some of these issues are.

Introduction of new OS, Application and Security Databases
Social Engineering
Continual changing of human resources
Security

Introduction of new OS, Application and Security Databases

There are hundreds if not a thousand of different OS/Applications and Security databases within the industry today. Many organizations have internally developed applications that authenticate to proprietary databases. As it is rare that all these different components are managed and maintained by the same (Ever changing) department, it is less likely that standardization has taken place. User name and password restrictions would all benefit from standardization. The many user ids and passwords that users have to manage causes confusion. A good percentage of a users time is spent login onto system resources.

"The Securities Industries Association, based in Washington, D.C., found that users spend an average of 44.4 hours a year logging on to (an average of) four applications a day."

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

www-4.ibm.com/software/network/globalsignon/library/whitepapers/overview.html

More and more organizations are moving towards e-commerce. Providing services and product to customer's worldwide introduces an even greater need for user control. Many of the databases previously used for internal applications only have now been web enabled. It is important that a mechanism be in place to allow customer to transparently navigate across multiple web servers.

Social engineering

With the introduction of so many systems it is possible that users will forget their user id or password and eventually lock themselves out. Unfortunately this happens frequently. Help desk personnel are overwhelmed with the amount of calls regarding password reset and account activation.

"META Group reports that 15-30% of all support calls are caused by forgotten or expired passwords. The cost to manually reset passwords ranges from $15-30 per call, and on average, users call help desks with a password problem 4 times a year.."

http://www.courion.com/solutions/index.asp

This can increase the possibility of an individual social engineering the Help Desk. Under high stress people are less likely to follow the guidelines that are in place. Guidelines that dictate being absolutely positive the person that is requesting the password reset is who they say they are. Solutions have been developed to reduce the security risk of social engineering.

These types of systems allow end users to answer a variety of questions through automated telephone services. Once the correct response has been entered the account is reset and in some cases e-mailed back to the end user. These types of systems are widely used within the Internet community. If you forget your password on one of the popular search engine e-mail systems, you can select to have a new one created. Answering the correct question will reveal a new password.

Continual changing or human resources

The technology is not the only frequent change within an organization. People come and go and along with that come the variety of user accounts across the enterprise. As users have so many accounts it becomes extremely hard for administrators to track and deactivate/delete accounts as people leave the organization.

Security

Each operating system and application has its own set of security requirements for both user id and password. Some security databases by default requires that the first character

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

of the password be a numeric. Other operating systems will not allow repeating characters within a password. For example AAMIKE would fail because the letter A follows the first letter A. As many operating systems have such a diverse set of restrictions it is possible that organizations will remove the restrictions (Where possible) to reduce the amount of user frustration and calls to the help desk. This also is in an effort to reduce the amount of sticky notes taped to monitors containing the user id and password. Security often competes with convenience in many different areas within an organization. Reducing password restrictions for end user convenience may or may not be an acceptable sacrifice.

What is Single Sign On?

SSO in short is the ability to authenticate once and never have to repeat the process for the duration of the session. Many solutions are available throughout the market that provides SSO capabilities. As a whole they all provide some form of Authentication, Authorization, Access control and password synchronization. SSO solutions are available for both organizations moving towards e-commerce as well as enterprise networked environments.

Authentication and Authorization

Authentication is the process of a user being identified as who they say they are. SSO applications either take advantage of the existing databases within the organizations or require the implementation of a proprietary database. Software vendors such as Novell and Microsoft have developed highly scalable Databases (Also known as Directories) that can be implemented into existing environments. These databases provide central repositories for user information and can be integrated into some of the available SSO solutions. Once a user has successfully authenticated they are then authorized to access various system resources. There are different types of authentications

Single Factor—Single factor authentication is when the user is only required to produce one piece of information. The most common single factor authentication method would be passwords (Something you know). Biometrics (Something you are) although considered more secure than a password, when used independently it is still referred to as Single Factor Authentication.

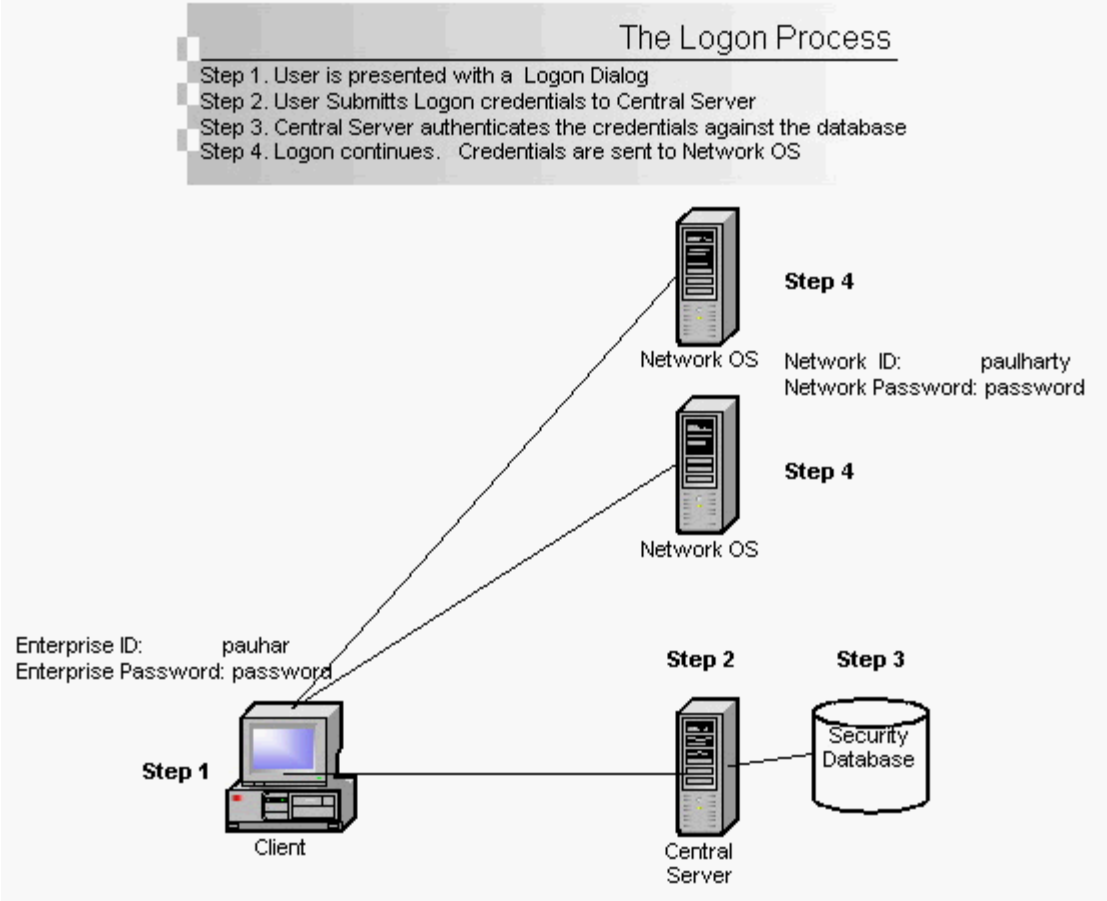
Two Factor —Two factor authentication is the combination of two single factor authentications. During an authentication process if a user is asked for both his password (Something you know) and a digital certificate (Something you own) then this would become a two factor authentication.

Typically SSO products contain a central server. The central server is responsible for authenticating the user against one of the security databases within the organization. This is usually the database where all the users accounts exist. Security databases such as Windows NT SAM, Active Directory and IBM's RACF are common authentication

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

options with SSO Products. These all provide single factor authentication. Extending security databases to support tokens and PKI would provide two factor authentication.

Within an enterprise environment users authenticate to the central server with the aid of client code. Once the user has successfully authenticated to the central server the network logon is allowed to continue.



Access Control

The level of access control that SSO can provide will differ depending on the solution as well as the intended end users.

SSO solutions for Web Servers typically provide content protection for web-enabled applications. After a user has successfully authenticated they are then allowed to access areas of the web server that the associated roll permits. A role is a list of ACL associated with one or more user Id's. Once authenticated, the user is then granted a session id. The session can be used to validate the user as they move about multiple web servers without requiring multiple authentications. This provides SSO for Web Users.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Users of corporate networks are presented with a graphical interface of applications they are allowed to access. The user points and clicks the application they want to launch. The credentials for that user (e.g. Non standardized user id) and application information are retrieved from the central server and provided to the application.

SSO products achieve transparent sign on in one of two ways.

Scripted—Scripted Sign On is the process of playing keystrokes back to an application. When the application is launched, the keystrokes are played back to the application as if the user was typing it in. The user Id and passwords are stored in the scripts as variables. Storing critical information as variables allows one script to be shared by many users for the same application. The variables values are pulled down from the central server at application launch. Scripted Sign On has to be initiated by the end user. Automatically launching the applications at logon would create multiple unnecessary active sessions to the applications

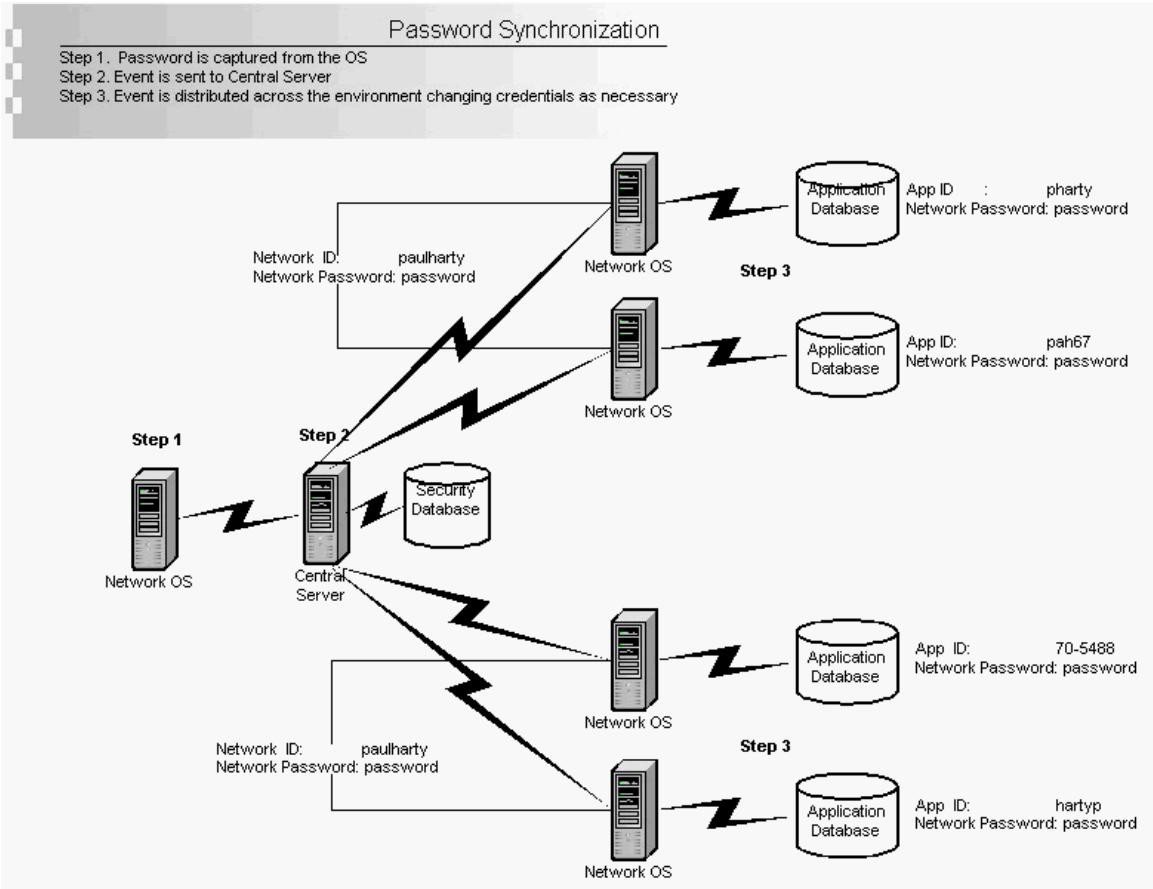
Integrated—Integrated SSO allows for tight integration with applications. Applications that have been developed to integrate with SSO allow for information to be passed about the user without the need for scripts. The process is invisible to the end user. In addition the SDK's provided with SSO solutions allow for the same integration with proprietary applications.

Password\account status Synchronization

Password synchronization is the ability to synchronize passwords around the corporate network. This is a vital aspect for SSO and can be considered the Back Bone of the solution. Passwords are captured from one or more security databases and then distribute vie the central server around the enterprise network.

The central server is typically the controlling component of a SSO solution. Disabling accounts from the central server triggers a chain of events that propagate down to the desired systems disabling the user account. The propagation of account status would also occur if the maximum bad logon count was reached.

© SANS Institute 2000 - 2002, Author retains full rights.



Conclusion

Security Personnel become concerned that SSO and password synchronization creates a security risk. If the password is the same across all security databases then the users account is only as secure as the weakest operating systems security. There are many aspects of SSO that counteract the concern.

- Less Secured systems can be excluded from the SSO Enterprise environment. Many of the solutions available are multi tier by design and don't require all users or systems to participate. Careful consideration can be given to who and what is included within the SSO Enterprise.

- Administrators are able to enforce more stringent password restrictions across the environment from the central server. Restrictions such as minimum length, password expiry time and invalid dictionary lists. Individual OS and application restrictions can be brought inline with the central servers configuration.

- Password Synchronization reduces users confusion. With only one password to remember it is less likely that the password will be wrote down on a piece of paper.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- SSO products that allow end users to reset the password after successfully answering a variety of questions reduces help desk cost and risk of social engineering.

- Employees that leave organizations can quickly be deactivated on all systems from one location.

- Authentication to less secure operating systems can be enhanced with two factor authentication.

- With little intervention required to sign on to applications the process is less likely to fail and cause volume helpdesk calls

Systems are vulnerable to attack. The strongest security databases have weaknesses that can be exploited. Host based and Network based vulnerability assessment tools help to ensure that system configuration is inline with internal policy's. SSO facilitates the authentication process and removes a good deal of pain from end users, helpdesk and administrators.

SSO, Vulnerability assessment and intrusion detection can all help to improve the level of security within an organization. After all, Security is all about layers.

http://www.eu.microsoft.com/windows2000/sfu/psync.asp

http://www.novell.com/products/nds/details.html

http://www.networkcomputing.com/1006/1006f12.html

http://www-4.ibm.com/software/network/globalsignon/library/whitepapers/overview.html

http://www.microsoft.com/windows2000/server/evaluation/features/dirlist.asp

http://www.courion.com/solutions/index.asp

http://www.fipass.com/corporate/authentication.asp

http://www.win2000mag.com/Articles/Index.cfm?ArticleID=526

http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=53&PID=3449195

http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=55&PID=3449195#sso

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

http://www.blockade.com/products/blk_prod_ov.pdf

http://www.hut.fi/~totervo/netsec98/sso.html

© SANS Institute 2000 - 2002, Author retains full rights.