Global Information Assurance Certification Paper

Identifying Identity Management

GIAC Security Essential Practical Assignment
Version 1.4b

By
Jason Jacys

July 2, 2003

Table of Contents

Abstract…… 3

Introduction…… 3

Provisioning…….. 4

Identity Federation……... 5
- Silo…… 5
- Closed Community…… 5
- Federation…….. 6

Identity Control…… 7
- SSO…….. 7
- CSO…….. 7
- Auditing……. 9

Vendor Products…….. 10
- Novell eDirectory……. 10
- Wavesset…….. 10
- Sun Microsystems…… 11

Summary…… 12

Abstract

The purpose of this paper is to provide a high level overview of important elements within identity management, and also some possible solutions for administrators. Many companies attempt to universally define identity management, however, this term has recently become a bit obscure due to this effort. As a whole, identity management consists of different elements. Not all elements are necessary; however there are a few essentials which form the fundamental basis for identity management.

Introduction

As companies with large IT departments expand both internally and externally, many issues impact the ability of the company to remain scalable and flexible. One major variable affected is the ability for administrators to effectively manage individual users. Typically, users have a variety of tools in which they have to enter personal credentials, usually a user id and password. A majority of the time these credentials differ, and users end up with a myriad of passwords, which are often forgotten, resulting in headaches for IT administrators. This in itself can be a great cost including lost user and administrator productivity and lost revenue[1]. Additionally, if companies have other security implementations such as biometrics, they have another entity in which they must sustain. Keeping the above in mind, there is a delicate balance in which administrators must maintain - the ability to allow legitment users or customer's access to the resources they request, while retaining an acceptable level of security. While there are many strategic solutions, one has been brought up extensively – identity management.

Identity management has many different, but closely related definitions. "Identity Management encompasses all applications, services and methods for creating, maintaining, revising and removing a database object representing a person as well as that object's attributes, rights and privileges whether granted directly or indirectly [6]." Although identity management includes many different variations dependant on the vendor; there are three major common elements:

- Provisioning
- Identity federation
- Identity control (single sign-on and auditing)

"By following these steps a business will be able to attain improved user experience, increased revenue, reduced management costs, enforced security policies and ultimately, achieve a dramatic return on your e-business investment [13]." These steps are the foundation in developing an identity management system. Not every element is necessary, however it would be in the best interest

of the enterprise to implement the majority so they may benefit from all available functionalities.

An information security consulting firm, Vigilar, claims identity management provides a company with solutions that may increase the productivity of the enterprise. Some of the proposed benefits include[10]:

- Centralized user management
- New Services can be deployed rapidly by leveraging user identity infrastructure
- Applications use one data store to authenticate users
- User Access can be terminated by deleting one central account
- User management overhead is reduced immediately
- Automatic propagation of user information
- Users can manage their own account information through a secure web portal

Much like project development, identity management remains a cyclical process. After development, administrators must look at what has been created so that they can tailor their identity management system to the needs of the company.

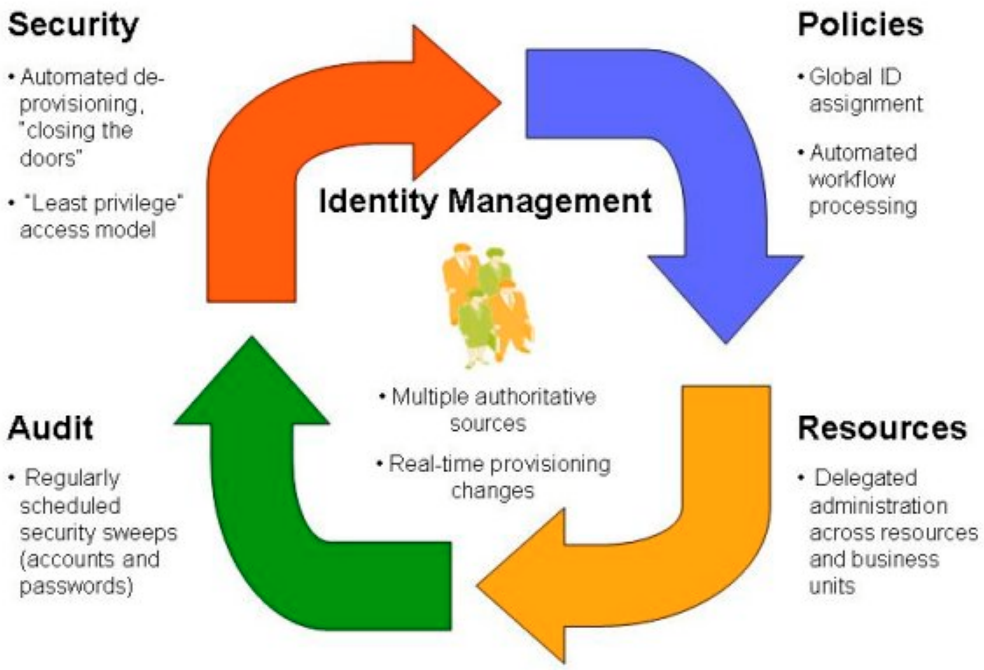

Figure 1: The Identity Management Cycle[2]

Provisioning

The first common element of Identity Management is provisioning. "Provisioning involves granting members of an organization secure access to the appropriate range of business resources, applications and systems that they need to effectively perform their work [5]." In other words, provisioning is the process of identifying user's basic business requirements and system accesses. There are many different ways to implement provisioning, however there are some important factors to include in the implementation of their identity management system. Michael Hunt provides some good direction to take when considering provisioning [4].

1. Implement global user ID naming conventions and enforce/ validate at provisioning run-time.

2. Leverage authoritative sources to provide real-time provisioning information.

3. Provide self-service capabilities wherever possible.

4. Implement a "least privilege" security model.

5. Regularly check accounts and passwords for security vulnerabilities.

6. Pick one authoritative source for each identity profile data element to be managed and allow multiple authoritative sources to drive automated provisioning.

These six steps provide an administrator with the means to successfully begin implementing an system. RSA also suggests deploying digital identities and access rights based on business policies for all entities to reduce problems. This should be centrally assigned and maintained[13].

Identity Federation

There are three main ways in which to make associations for an identity management system. According to RSA they are silo, closed community, and federated. Each have their own pros and cons, however it is important to determine what best suits a companies needs[13].

- Silo – This approach indicates that the company must have a unique identifier for all lines of business, including customers, employees, and any other third party vendor. One of the pros is that this is the easiest of the three to implement. Some drawbacks include difficulty in administration and the system requiring the same password and id for each tool[13]. This remains the most popular.

- Close Community - This second method involves a company, in association with all other related business, combining resources to define a central infrastructure. This would allow synonymous usage among practicing companies. The advantages of this method are one single infrastructure where maintenance of identities becomes more manageable across the lines of business. Some disadvantages include a single point of failure and one line of business that must maintain the infrastructure.

- Federation – This method allows participating companies to trust each others individual identities. Two such software packages are Microsoft .Net Passport and Liberty Alliance. Some positive aspects include the ability to trust other organizations so that only a single id and password are needed. The drawback is it would be difficult to find companies that are willing to trust another's secure information.

Identity Control

Single Sign On (SSO) is an attempt to provide a user with a seamless entry to all pertinent systems. In today's environment a user will have to use many different tools to accomplish their task. Many of these tools usually require a different id and password. With single sign on a user requires only one id and password to access the various systems in which they are authorized. With RSA's solution users are automatically presented with personalized pages that do not require multiple passwords. This allows them to"…securely navigate across multiple applications, resources and sites while authenticating only once. In turn, your business enjoys significant revenue generation and cost reductions[16]." This also increases user's productivity.

Another such solution is eTrust's single sign on software. This would provide the customer with an automated login process including single sign-on to any mainframe, client/server or web application, password management, and finally integration with biometrics, digital certificates and smart cards[7].

Although the solutions sound promising, many argue that SSO was not living up to expectation. Some companies claimed SSO was theoretically possible; however implementation of such as system was far from practical. Therefore Consistent Sign On (CSO) was formed[15]. CSO's goal was to use Lightweight Directory Protocol (LDAP) to synchronize the directories where password and ids were maintained. LDAP is used for accessing information directories based on the standards contained in X.500, but significantly simpler. Unlike X.500, LDAP supports TCP/IP, which is necessary for internet access[11]. Due to its simplicity, LDAP became the ideal solution.

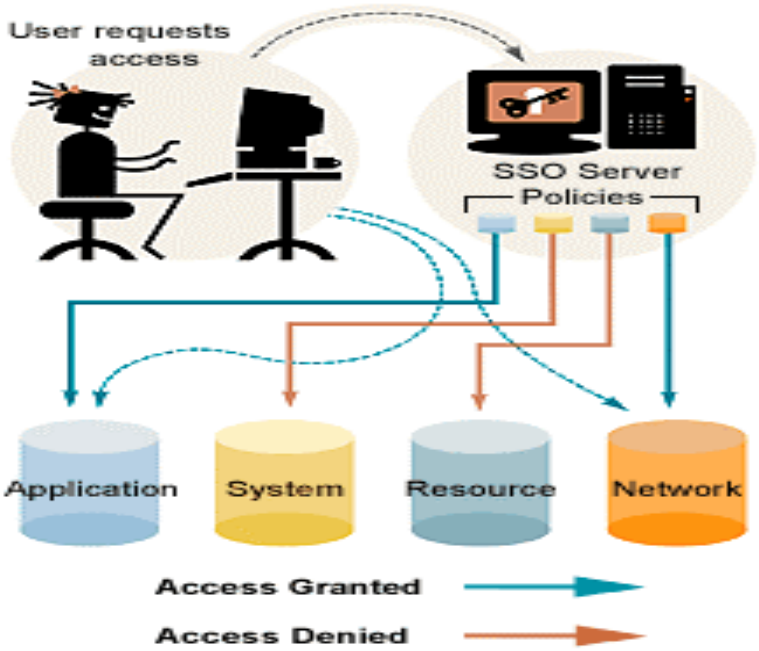

Figure 2: Single Sign On[7]

If a single sign on management system has been developed, an administrator needs to manage the passwords that are associated with the company's particular system. There are three important steps in password management[1]:

- Self-service password resets, which let users reset forgotten passwords by correctly answering "challenge questions"
- Password synchronization, which allows use of a single password for multiple systems. When one password is reset, all are updated automatically.
- Password policy enforcement, which requires new passwords follow not only operating system requirements (number of characters), but the network department's policies

The following is an example of an ideal password management system:

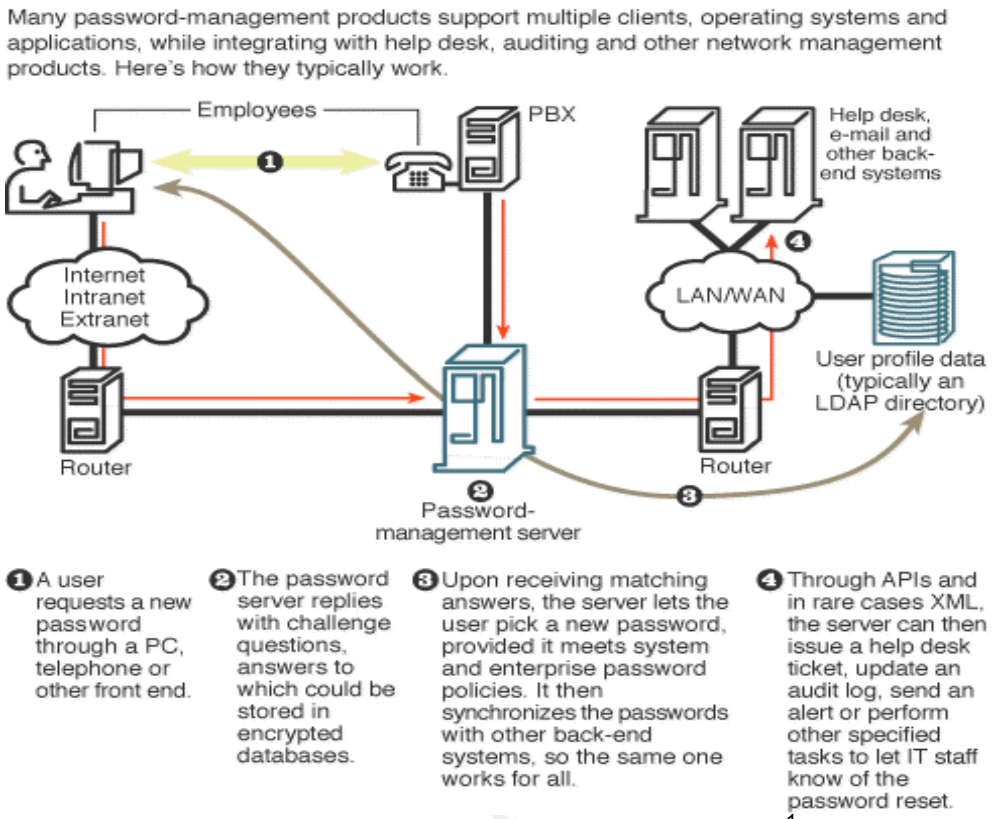

Figure 3: Password Management System[1]

Some important questions that administrators should consider regarding identity control are[1]:

- If the product encrypts answers, ask how. Some use hash algorithms that dice and scramble challenge-question answers for high security, but require answers to match stored data precisely

- Ask if a product uses its own database, relies on an existing source of user information, such as a directory or database

- Ask which client interfaces are supported and how. All support browsers for password resets. Some also support Windows and Unix screens, interactive voice response and e-mail[1].

Auditing remains another part of identity management that falls under the category of identity control. With all of these controls in place, it is imperative that one remains aware of what, who, and when things are changing within the new system. There must be a system in which administrators will be able to view the accessing of the system. When using a system like W*aveset,* designers claim the ability to view instantly who has access to what and why, with current, accurate views and reports of group memberships and role memberships on IT

resources, as well as administrative privileges on key systems to enhance security and comply with current laws[14].Government legislation proves to be a formidable factor in certain industries. A company in financial services or the health care industry are required to have strict auditing logs[9].

Vendor Products

Each vendor promises many successful options, however administrators must be careful in what they select. A larger, established company may face a more difficult implementation, while a smaller company will have the benefit of planning rather than retrofitting the system. In addition, administrators must decide how much capital they are willing to spend verses how many security controls they would like to implement. Administrators face the reality of high costs escalating from purchase of the product to the time of successful implementation choosing the right vendor will be crucial

Novell eDirectory

Novell has developed their own application for Identity Foundation – eDirectory 8.7. Novell's identity management claims to have "…cross platform capabilities while delivering a centralized, scalable foundation with control over the identities and access rights of your employees, customers, partners and suppliers[14]." eDirectory claims to have the most flexible interoperability among operating systems. Servicing operating systems such as AIX, Linux, NT, 2000, Netware, and Solaris. One of Novell's features is the ability to create or revoke a user's identity from the whole enterprise with minimal changes to one data store. eDirectory also incorporates SNMP management support and event publishing via LDAP to facilitate directory management and monitoring[14]. Other security features include Novell International Cryptographic Infrastructure; passwords encrypted over Secure Sockets Layer (SSL), RSA private key/public key encryption, Secure Authentication Services, smart cards and X.509v3 certificates[14].

Waveset

Another identity management software solution with unique elements is Waveset. Waveset leverages their 'Agentless' solution[11]:

> *IT is an architectural model that uses pre-defined "hooks." These hooks are exposed API's and known standards, including security standards such as SSL, in existing systems and applications that provide methods for achieving noninvasive identity management. Rather than relying on a piece of custom codes that is tailored to each system, and thereby affected every time that system is patched or updated, an Agentless models makes use of existing*

hooks where possible – translating to very rapid deployment times without loss of data integrity or privacy.

The purpose of Waveset leveraging Agentless solutions is to simplify integration. Waveset's four core products include a provisioning manager, password manager, Identity broker, and Auditing and Reporting. Waveset's Identity Broker allows synchronizations of profiles across different platforms. The goal of Waveset is to provide a company with an open-ended solution that can maintain scalability and flexibility. By using open ended protocols such as LDAP and SOAP, an enterprise can easily implement a solution that is understood by all applications. This avoids the need to develop specially tailored applications that are application specific.

Sun Microsystems

Increasing interest in identity management prompted Sun Microsystems to unveil its new plan for their own identity management software. iPlanet Directory Server, Access Management Edition 5.0, builds on Sun's existing iPlanet Directory Server, enabling customers to maintain personalized information access, create tighter security, and use integrated communications with partners[3]. Sun has already sold over 650 million licenses, possibly indicating an extremely valuable partnership for both Sun and its participating companies[3]. Sun products feature[3]:

- Web-based Single Sign-on, which enables a user to access multiple Web-based applications or services during a single session.

- Policy Management providing companies an easy, centralized way to control which applications and information are available to their employees, customers, partners and suppliers.

- Delegated Administration features providing companies a practical way to delegate administration of user policies to departmental managers, business partners or even end-users themselves.

Summary

Due to a rapidly growing number of vendors and vendor services, business decisions are more complicated. One thing to keep in mind is how your current system enterprise is set up today. Once the business requirements are determined, an administrator can make a more informed and successful decision. The preceding was described as a high level overview of considerations when developing an identity management system and the possible solutions. The three fundamental steps, provisioning, identity

federation, and identity control will allow a company to improve user and customer management, resulting in a higher profitability.

Reference

1) Bort, Julie. "Identity Management Begins with the Humble Password." April 2003 URL: http://www.nwfusion.com/supp/security2/password.html (21 October 2002)

2) Hunt, Michael. "Provisioning: The Key to Identity Management" April 2003 URL: http://www.itsecurity.com/papers/waveset1.htm (8 March, 2003)

3) Meyer, Sasha. "Sun enveils user identity management software" April 2003 URL: http://www.itweb.co.za/office/sun/0203220827.htm (22, March 2002)

4) Yasin, Rutrell. "What is Identity Management?" April 2003. URL: http://www.infosecuritymag.com/2002/apr/cover_casestudy.shtml (19 June, 2003)

5) "Active Entry" April 2003
URL: http://www.activeentry.com/dynasite.cfm?dssid=2733

6) "eProvision News: Industry News" April 2003
URL: http://www.businesslayers.com/site/newsletter.asp?nlID=32

7) "eTrust Single Sign On (SSO)" April 2003
URL: http://www.politec.com/etrustsso/

8) "Identity Management" April 2003
URL: http://www-3.ibm.com/software/tivoli/solutions/security/id/

9) "Identity Management" April 2003
URL: http://www.courion.com/sitemap.asp

10) "Identity Management" April 2003
URL: http://www.vigilar.com/sol_identity_management.html

11) "LDAP" April 2003
URL: http://www.webopedia.com/TERM/L/LDAP.html

12) "Novel eDirectory 8.7" April 2003
URL: http://www.novell.com/products/edirectory/quicklook.html

13) "RSA: Identity Management" April 2003
URL: http://www.itworld.com/itwebcast/archive/rsa_security/index.html

14) "Secure Identity Management Solutions" April 2003
URL: http://www.waveset.com/Solutions/Lighthouse/

15) “SecurPass-Sync & SecurPass-Reset” April 2003
URL: http://www.secure-pass.co.uk/

16) “Single Sign On” April 2003
URL: http://www.rsasecurity.com/solutions/sso/

17) “Understanding Single Sign On”
URL: http://www.intranetjournal.com/articles/200205/se_05_28_02a.html (28 May, 2002)