Global Information Assurance Certification Paper

An Overview of Secure Identity Management (IdM)

GIAC Security Essentials Certification (GSEC)
Version 1.4b
Nishanth Chandran
17 July 2003

Table of Contents

Introduction

Identity Management (IdM) is about providing the right people with the right access at the right time. In the past the challenge has always been how to keep people out of your IT systems - today the challenge is bringing the right people in.

A solution to resolve the challenges of managing user information will not resolve all security issues faced by an organisation. The fundamental elements of security i.e. authentication, authorization, administration and monitoring, cannot effectively address all the security issues in large-scale environments without examining the methods in which user data is managed, accessed and interpreted by applications and resources that organizations wish to secure.

Secure Identity management is a framework for securely maintaining a complete set of electronic identity information for a person. It can span multiple business contexts and boundaries. It is not a single product and requires both the integration of technologies such as directories, single sign-on (SSO), provisioning and delegated administration, as well as coordination with business processes surrounding the management of user information, access rights and related policies. It should unify a person's disparate identity data to improve data consistency, data accuracy and systems security in an efficient manner.

Business Drivers for a Secure IdM solution

Due to the rate at which changes currently occur within large enterprises, and to its people and technology, the ability to ensure appropriate security over access to business services and information assets is turning out to be an inherent and significant risk.

This is further compounded by having many disparate systems and groups within these organisations performing access administration at various layers, such as operating systems, databases and applications.

Whilst efforts to implement new processes and technology to standardise access control administration have been underway in organisations, it has been acknowledged that the progress in this area is slow. It is also recognised that staff and customers have many identities to gain access to organisational systems/services. Often, authority is either inconsistent with the user's role and responsibilities or detrimental to the group in terms of poor segregation of duties. As a result, there remains an ability to potentially perform inappropriate activity.

Efforts are currently underway by many organisations to improve this situation, but they are struggling to regain control over their information systems. After empowering employees, customers and partners with more and more information systems, companies now are trying to understand who

needs access to what information and when. This is not an easy question to answer, but by neglecting it, enterprises suffer serious security vulnerabilities and organisational inefficiencies.

Effective management of users' identity, credentials and access rights needs to be implemented to address security, business and user expectation. Appropriate identity management and user provisioning would ensure that customers and staff have access commensurate with their role and would not allow conflicting access. This would prevent inappropriate system activity such as unauthorised transactions and changes to systems.

IdM solutions can deliver significant value to the business and if implemented properly can demonstrate rapid return on investment. The value to the business is derived from one or more of the following categories:

- Reduced Cost - The cost of administering users is high, especially in organisations with a global presence and large user communities. The combination of technologies in an Identity Management solution leads to a reduction in both system administrator and helpdesk staff that brings direct cost savings. In addition, there are indirect cost benefits since speeding up user account creation and password reset processes means that staff get or regain access to their IT systems quicker, minimising both frustration and lost productivity.

- Increased Security - IdM technologies provide a centralised, authoritative source of user identities, privilege and access information, enabling real-time enforcement of access rights based on a user's role. Providing a centralised point of control improves security by reducing or eliminating the risk of unauthorised access to resources, or disclosure of confidential information. The ability to remove terminated easily and automatically revoke all of their system access rights is also a powerful security feature.

- Increased Compliance - The strong controls over access to systems and data delivered by IdM enhance an organisation's ability to operate in regulated environments and its ability to respond to changes in policies, practices and procedures. IdM solutions provide organisations with a central source of management of user access rights, with powerful reporting features that help organisations audit these access rights.

- Increased Usability - The importance of delivering security systems and measures that are easy to use cannot be overstated. Cumbersome or onerous security measures often end up being circumvented by legitimate users of the network in order to get their work done. The combination of RBAC and reduced sign-on or SSO inherent within an IdM programme delivers a high degree of usability, based around the integration of systems and resources across the enterprise.
- Flexibility of User Management - Traditionally, enforcing centralised user management is a simple way of improving security. However, in the distributed enterprise, delegation of user management to business units can be the key to efficiency and scalability. IdM delivers the ability to address both of these apparently contradictory requirements, providing

centralised creation of user roles whilst also enabling the controlled delegation of routine user administration to business unit level.

An Approach to a Secure IdM solution

An enterprise IdM architecture to administer customer and staff access can be developed through the rationalisation of business processes along with standardisation of authentication mechanisms, authorisation systems, application development and a common credential store. This will lead to a transformation of the current operational access control function within the organisation, into a business enabling function, also resulting in security solutions being derived from business requirements. This will require a change in behaviour, culture, process and awareness.

Some of the key concepts within a Secure IdM solution include

- Single User Identity - Single user identity is a single view or instance of an identity. A single identity may be associated to a number of user accounts.
- Federated Identity – Federated user identities are those that span across company boundaries, enabling businesses to offload identity and access management costs to business partners within the federation.
- Identity Domain: An identity domain comprises of a group of systems, applications and access channels.
- Least Privilege Approach: A user will only be granted the privileges necessary to perform their user roles. Applications will only be granted the privileges necessary to interact with other applications.

In order for organisations to develop a Secure IdM solution, they need to consider and develop an to approach that would include

- Role Based Access Control (RBAC) system, supported by relevant standards and operational procedures. It should allow the rationalisation of permission management and ensure a policy of 'least privilege' access based on a person's job/role to access business services.
- Password synchronisation and self-service features with password reset facility to address the exposures and risks due to staff and customers having to remember numerous IDs and passwords.
- Reduced or Single Sign-On (SSO), which would allow users to access and carry on throughout multiple business services with a minimum number of log-ons. Where possible once credentials have been provided in the initial instance, they should be passed to other associated systems and applications with the same level of required authentication or less, without the need to re-authenticate. This principle must be applied in conjunction with the Least Privilege Approach principle in order to mitigate potential risks.
- Strong authentication and permission controlled through the use of 'roles' would mitigate any risks associated to providing a 'single key to the door'.
- Centralised User Administration, the ability to administer users and domains from diverse locations, support delegated management.

- Centralized logging and reporting facilities, that provide auditing and monitoring capability from a central location. It should capture all security events and assist in the detection and prevention of security incidents.
- Enterprise platforms and applications integration and compatibility, that provide the facility to easily integrate the current enterprise systems, including legacy systems and allow the provisioning of users into these systems.

There are significant benefits and savings to be realised, some of which include:

- Reduced user administration, through role based access standards
- Improved user productivity as a result of reduced user provisioning wait-time and self-service facilities
- Simplified access workflow processes and reduced costs associated with current system access requests (add, move, change, disable & delete)
- Improved segregation of duties and role incompatibility management to prevent ability for users to perform functions outside the authority and responsibilities of their assigned role(s)
- Productivity gains, minimisation of administration overhead, help desk efficiency and more appropriate allocation of IT resources through consolidation and streamlining of authentication and authorisation protocols.

Secure IdM Architecture

Secure IdM architecture would include the following key security related sub-systems

- Identity Management Services– is the online component for the administration of users, that provides centralised, role based, and policy-based administration, plus delegated and self-service channels for business units. Identity Administration also provides a centralised or single point of administration for the assignment and subsequent retraction of these access rights.

- Provisioning Services – addresses the granular management of accounts, including set-up, modification and revocation. User provisioning can extend beyond applications and data, and can include other required business resources that would be issued to new or existing employees.

- Access Management Services – key functionality includes authentication and authorisation. This facility provides a common approach for authentication and authorisation to multiple applications across the organisation
    - Centralised Authentication – is the user-facing component of the conceptual architecture. Authentication is the process that verifies the identity of a user so that access to protected resources can be correctly granted or denied. These authentication credentials can

then be forwarded to other systems to achieve single sign on / reduced sign on. Authentication techniques range from a simple login based on user IDs and passwords, to more powerful mechanisms such as tokens, public-key certificates and biometrics.
    - Centralised Authorisation - is the component that facilitates centralized coarse grain authorisation by policy based RBAC.

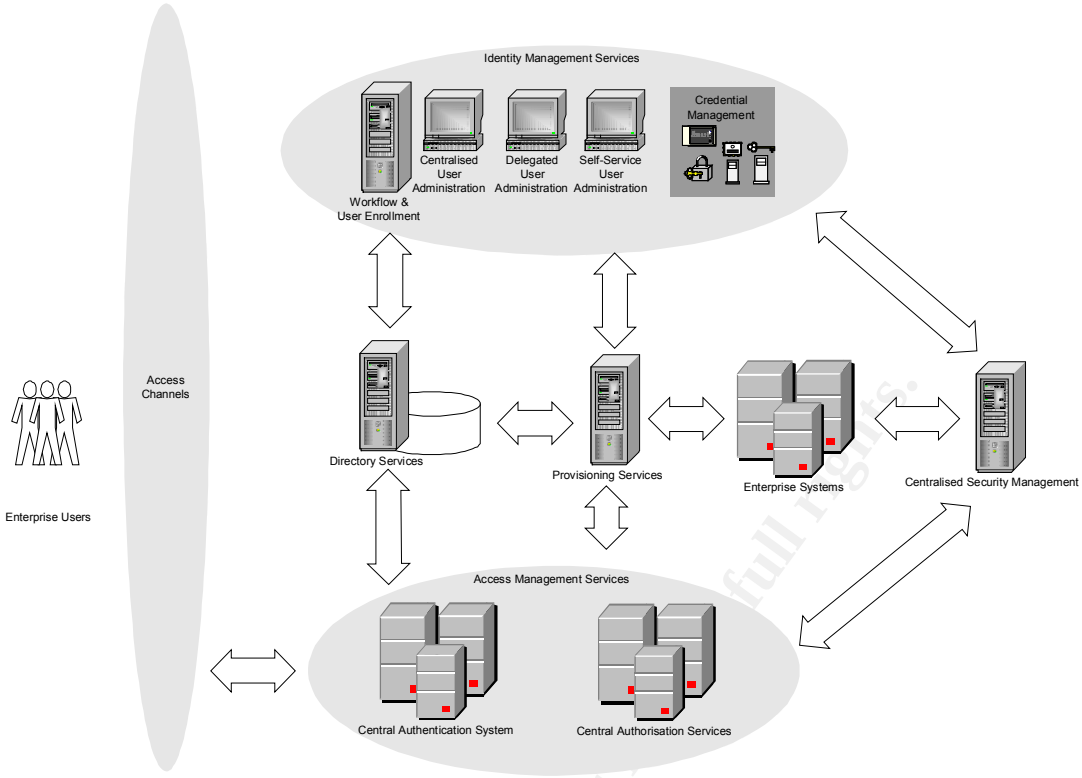
- Directory Services – is the component, which centrally stores identity and Nominee User profiles, and coarse grain system access policies. This repository is most commonly established by the implementation of a directory.

When fully implemented a secure IdM architecture would be expected to realise the following:

- Increased ability to manage enterprise information assets;
- Centrally managed from diverse locations, cross-platform environment;
- Centrally managed logging and reporting of administration activities;
- Simplified operations and administration activities;
- Decrease administrative/help desk overhead;
- Assure authentication across multiple platforms;
- Secure data and network access by internal and external resources;
- Reduction in the number of logins/passwords associated with a user and required to access systems (Single Sign-on / Reduced Sign-on); and
- Efficient and effective support of high user turnover and flexibility for growth.

The key components of the IdM architecture include

- Access Channels - Enterprise users currently gain access to systems via a number of access channels and they are expected to be integral part of any security architecture. The architecture should facilitate existing access channels and provides extensibility to support the addition of future access channels (e.g., wireless technology).



- Access Management Services - Access Management Services comprises of two key components:

    - Centralised Authentication System – It is a central service in which a user must provide authentication details to gain access to enterprise systems. Central Authentication facilitates:
        - Single sign on / reduced sign on between applications and enhances user management capabilities. All Access Channel authentication will pass through a centralised authentication system, enabling user authentication to occur once, updating the users current authentication state and have the authenticated credentials passed to applications within a trust relationship (so long as the users state does not change). Where Legacy systems do not support such functionality the user will be required to re-authenticate to the legacy system.
        - Improved efficiency and effectiveness in the management of user access (e.g. a user account can be disabled within the centralised user repository, and their access to all systems can be disabled instantaneously) and user access policies (eg, number of allowed concurrent logins).
        - Centralised enforcement of access control policies contained within the central user repository (eg, number of concurrent logins)
        - Audit logging, maintaining a centralised history of all access enterprise resources, including all failed attempts.

- Centralised Authorisation Services- The central authorisation service supports the following functions:
  - Policy based RBAC- Applications and infrastructure access based on Role Based Access Control (i.e., where the Nominee User role defines the type of rights and privileges of a user. Policies should determine how the rights and privileges are defined at both a coarse grain and fine grain level).
  - Central User Repository - Coarse grain authorisation information will be contained within the Directory Service. The Access Management Services will interface with the Directory Service to perform coarse grain authorization.

  The Access Management Service will pass the authorisation credential information to applications, which are responsible for the enforcement of finer grain authorisation policies. The solution should also supports the management of legacy ACL's.

- Directory Services - Directory Services provide a secure and resilient repository for user/resource profiles. The user credentials and authorisation policies stored within the Directory Service are used by the authentication and authorisation services to provide centralised access control to multiple or diverse applications. The solution should support a directory implementation, which may be split over a number of different physical devices and logical stores. This can be achieved through the use of Meta Directory products. Where an application is unable to connect to the Directory Service it will be the responsibility of the provisioning system to provision user accounts and ACLs in the application, based on user information contained in the Directory Service.

- Identity Management Services - Identity Administration provides the services to enable the registration and enrolment of users to gain authorised access to organisation systems. The key components of identity management services, include:
  - Workflow and User Enrolment will enable electronic identity administration request, approval based on approval policies. Subsequently these would be forwarded to provisioning services for both planned and unplanned conditions. Provisioning could be a combination of automated and manual processes.
  - Centralised User Administration will enable the administration of the enterprise users and systems from a central location and enabling the management of delegated and self-service user administration.
  - Delegated User Administration will enable segregation of user and system management to multiple parties to manage their user base.
  - Self Service User Administration, provides the ability for user's to request additional system privileges and to perform self-

management of their information (eg, personal details, password resets)

- Authoritative data feeds from other enterprise systems such as HR and customer databases or external partner databases.

The above components facilitate consistent application of policies for enrolment and approval, credential management (eg. password strength) and role management.

Managing an Identity is all about the being able to:

- Register users
- Managing user and their credentials through a centralised approach to defining and enforcing user and credential policies that is stored in a central user repository.
- Establishing and managing enterprise roles and authorisation policies (RBAC Policies)
- Associating credentials to identities
- Associating roles to identities
- Centralised logging of all identity administration activities.

- Provisioning Services-The central provisioning service supports the following functions:
  - Automated Provisioning. The provisioning system publishes information relating to an identity, Nominee User or access control policies and roles to the Central User Repository based on information feeds from Identity Administration and Access Management components. As the systems administration is automated and based on set policies and templates the provisioning system ensures Identity Management activities are consistently applied to systems.
  - Legacy System Management - Where legacy systems do not support the use of a central repository the automated provisioning system should facilitate legacy system management.
  - Tokens / Strong Authentication Management. The provisioning system interfaces with token management systems to support strong authentication credentials.
  - Reconciliation – where user credentials may be replicated over a number of systems, the provisioning system should identify any changes made and reconcile this information against authoritative data sources prior to replicating / rolling back the change.
  - Centralised logging of all provisioning and de-provisioning activities.

- Security Management-All systems within the secure IdM architecture should produce logs on system and user activity to comply with the

functional requirements. Security management tools should be implemented to log, monitor and report on all identity management and user provisioning activities.

These logs would be either visible to or replicated to a centralised management system to facilitate data sorting and filtering for system monitoring activities. This can be used to measure compliance with organisation's internal policies, privacy and other legislative requirements.

The security management component should facilitate the ability to prevent, detect and react to any attempted modifications to audit records.

A IdM solution does not stand by itself but is part of a complete security architecture and hence should be supported with the following:

- Policies that have buy-in from the business and that are reviewed and implemented
- Security education and training for employees
- Incident response policies and procedures
- Network protection strategy
- Strategy for future security needs
- Proper management structure and process to support security initiatives

Reference

- Exploring Secure Identity Management in Global Enterprises, A Joint Study by Novell Worldwide Services, Stanford University and Hong Kong University of Science and Technology, March 2003
- Identity Management Design Guide with IBM Tivoli, Bücker, A., Camp, A., Cohen, R., Edwards, D., Penman, C., Sant'ana, T., July 2003, http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/sg246996.html?Open
- Security Provisioning: Managing Access in Extended Enterprises, Pikover, Y. & Drake, J., 2002, Information Systems Audit and Controls
- What is Identity Management?, Yasin, R., April 2002, http://www.infosecuritymag.com/2002/apr/cover_casestudy.shtml
- Identity Management Begins with a humble password, Bort, J., October 2002, http://www.nwfusion.com/supp/security2/password.html
- Identity Management, The Open Group Conference, January 2002 http://www.opengroup.org/security/An_index.htm
- Identity Management – A White Paper, The National Electronic Commerce Coordinating Council Annual Conference, December 2002 http://www.ec3.org/Downloads/2002/id_management.pdf
- Towards Federated Identity Management – A white paper, Norlin, E. & Durand, A., December 2002, http://discuss.andredurand.com/stories/storyReader$320

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event