Issues and Emerging Trends in Identity Management

Manish Snehi
Engineering Department
Infosys Limited
Chandigarh, India - 160101

Jyoti Snehi
Department of Computer Science
Chitkara University
Punjab, India - 140401

Renu Dhir
Department of Computer Science
NIT Jalandhar
Punjab, India - 144011

ABSTRACT

In today's digital age as companies are moving more and more amounts of important, sensitive data, information, applications, and infrastructure online there is a need to establish and maintain credentials on all the connected and disconnected systems, and grant rights or access to users. The main goal is to manage physical and logical resources and relate them to owners. Identity Management is emerging as a significant technology to help in handling the complexity of today's Business companies, dealing with security in the virtualized environment, strong authentication and dealing with threats from Insiders. This paper attempts to provide direction toward some of the issues, Challenges and Trends in Identity Management. Emerging Trends in Information technology involves identity audit, automated compliance, Role lifecycle management, authorization, Information centric identity, E-SSO and strong authentication, Open ID, Infocards, CardSpace, Governance, Identity management as a service, Risk management, and Compliance Modularity.

Keywords

IM (Identity Management), IMS (Identity Management Security), IAM (Identity and Access Management).

1. INTRODUCTION

Identity is defined as the distinct personality of an individual or any object which can be regarded as a persisting entity.

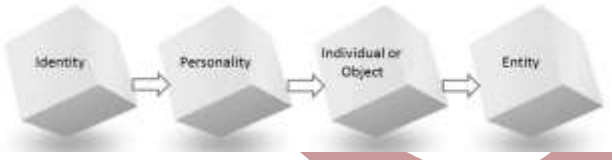

Fig 1: Identity

Identity management is a discipline which encompasses all the tasks used for different tasks viz. create a user, get user information, update or delete user identities in a computing organization. The Burton Group defines identity management as the set of business processes and related infrastructure for the creating, maintaining, and using digital identities. [1].According to Spencer C. Lee Identity Management refers to the process of implementing new technologies for the administration of information on the user identities and on the access control to resources. Identity management is a wide administrative area which deals with identifying individuals and control access to resources by associating the user rights and restrictions policies. It aims at increasing productivity and security and reducing the costs of managing users, their identities, attributes and access rights. It involves Usability, transparency, experience, customer service, convenience, compliance, availability and access to Information in a secured manner.[1]

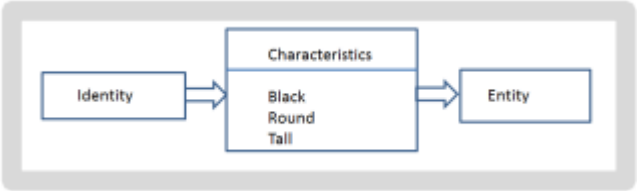

Fig 2: Identity Management

A systems administrator assigns a credential to a worker which allows the employee or user access to the network and determines the resources that can be accessed. Identity management provides managers a custom view of the IT environment for each user, determined mostly by job function and security concerns. Identity management enables session management, authorization, and authentication and user lifecycle management. Components of IDM involves Data sources and applications, Directories as a central component to store identity information, passwords, policy, Standards: X.500, LDAP,s meta-directories used as the base for the synchronization of data, for person identification and for managing passwords, Connectors for actual data synchronization, data conversion and logging of the processes and Auditing tools to provide the overview. [3]

Fig 3: Identity Management

2. IDENTITY AND ACCESS MANAGEMENT EVOLUTION

Traditionally Identity Management solutions provided automatic resource provisioning, self-service for tasks and centralized user lifecycle management. With systems becoming more open, Governance Risk Management and Compliance has become the driving force behind the identity management and IDM infrastructure has moved from being administrator centric to being business oriented known as Identity 2.0.

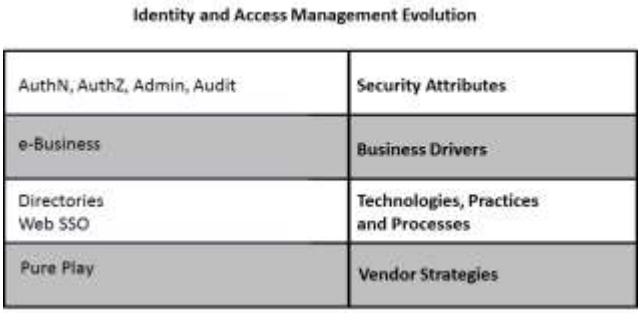

Fig 4: Evolution of Identity and access management

Identity and access management evolution involves vendor strategies, Technologies, Practices and Processes, Business drivers and security attributes for authorization, authentication, administration and audit. In 2008, a consortium was formed by the experts at Canfield University, Royal Holloway University of London, Sanford University and Consult Hyperion and Sunderland City Council to work on a project to pioneer innovations in the field of privacy and consent for Identity Management. [3]

3. ISSUES AND CHALLENGES IN IDENTITY MANAGEMENT

3.1 Single Sign On

Sometimes a user logs in multiple times in order to gain access to various business applications. Multiple logins and the need to remember the multiple passwords are the main reason behind causes of bad application experiences. The SSO faces the problem of users authenticating multiple times to a connected information system. Authentication and authorization solutions handle the authorization events by initializing authentication event, session management and multiple authorization events. [7]

3.2 Identity theft

Identity theft or ID theft is a crime which involves obtaining important and personal information by criminals, e.g. social security number and/or bank account details and/or driving license details, and they pose as somebody else. This sensitive personal information can further be misused for obtaining credit card details, and using these details posing victims' identity. Identity theft can be more dangerous as it can also give a chance to a thief with stolen credentials for immigration purpose or any other misuse. Identity theft can majorly be categorized into account take-over and true-name theft.

3.3 Strong Authentication and Authorization

Authorization means finding out if the person who was once identified is now permitted to have the resource. This is determined by finding out that person, his group and his eligibility for admission, or level of security clearance. Authentication is a process of verifying any individual as someone which they claim they are. It involves security measures like a username and a password, a smart card, retina scan, Finger prints voice recognition etc. [5]

3.4 Provisioning

Administrators manage Physical and logical resources using provisioning software solutions which aggregate all of resources and automate allocation of resources which is achieved using either rules or role based access control. Provisioning Provides account request, validation, create, approval, propagation, notification and capabilities.

3.5 Auditing

Auditing involves recording 'Who did what and when". Audits are driven by regulatory compliance to provide secure environment and mitigate risks involved in the system. The objective of the audit is to validate and evaluate user with assessment of any information .Identity control systems generates activity reports as identity audit solutions. ISO 27002 correlates to identity audit. Identity project involves identification of all identity related policies in the organization, implementing controls and auditing controls.

3.6 Entitlement Management

Entitlement management is authorization tool that can help in providing access to the set of technologies which are used to grant and revoke access privileges to identities. It is associated with authorization and enforcing the access rules, regulations and restrictions associated with business functions. [6]

3.7 Identity Aggregation

Identity aggregation is a term which can be referred to the technologies set which are used to help various applications aggregate identity information from different identity systems and reduces the complexity of data reconciliation, integration and synchronization. Technical challenges that identity aggregation technologies can address includes maintaining relationships for data transformations, Optimizing data CRUD operations which involves creation, reading, updating, deleting and synchronizing data.

3.8 Trust and Federation

A federation protocol enables parties to communicate. Trust schemes involve multiple business parties and federation technology captures the essence of real world trust relationships into a simple to understand and powerful trust models that will help in enabling various business scenarios. Federation represents products and standards are used for extending an authentication context to external parties.

3.9 Improving the Flexibility

Identity management involves policies, procedures and technology working together in creating a safe, secure and flexible environment for controlling access to online systems.

3.10 Identity Unification

It represents Directory, Virtual Directory, and Meta-Directory offerings by identity management. [4]The main focus is on creation of directory that synchronizes identity data sources containing user profile, his credentials, group, role and entitlement.

4. EMERGING TRENDS IN IDENTITY MANAGEMENT

4.1 Authentication and Authorization

The widespread use of User ID/Password as the predominant method for authentication will demand for wide adoption of alternate authentication methods which are secure and easy to use. Authentication is process of two ways matching between public and private identifier. It is mechanism in which

systems securely identify their users. It establishes trust relationship between provider and consumer. Authentication methods involves HTTP authentication, HTTP digest, Login form, X.509 certificates and custom authentication methods. Authorization is process which follows authentication and it is a mechanism of determining which access level any authenticated user can access resources. Authorization methods include access controls for URLs, Secure objects and access control lists.

4.2 Identity Assurance

The Identity Assurance program is an optional service which provides a set of standards for identity management procedures. Some online services, such as those related to financial aid and managing federal research grants, will require these profiles representing higher levels of assurance.

4.3 Governance, Risk Management and Compliance (GRC)

Governance, risk, and compliance management includes identifying risk-affected processes, assessment, implementing internal control system, and monitoring the control effectiveness, hence meeting internal and external legal requirements. GRC has become a driving force for Identity Management focusing on business-oriented Identity management.

Acceptance of role based access control is growing in production systems. The use of roles is potentially broader including use of data analytics for evaluating the effectiveness of organizations.

4.4 Identity Federation

Identity federation is a process of relating multiple identities in a manner that disparate systems can be integrated seamlessly and its capabilities enable the users to securely access cloud or other Web applications. Identity federation is a concept that makes sure that the user need not have to manually logon to multiple systems for accomplishing a given objective, it simply enables a user to navigate through the systems only by logging on once. SAML is broadly used as a standard protocol and successful business models have been implemented.

4.5 Identity Analytics

It provides vital identity intelligence with rich analytics and advanced compliance features that analyses, monitor, and govern the access of user to mitigate risk, satisfy compliance mandates and build transparency. Identity Analytics consists of a set of techniques and methodologies to predict the impact of investing in the space of Identity in a well-defined context and scenarios. Advanced data analytics adds value to different identity-based tasks/activities such as Authentication, context, purpose and auditing.

4.6 Internet Identity

It refers to online identity and digital identity. It can be user-centric or user-managed Identity technologies such as Info card/CardSpace and Open IDs are trying on technology and domain level for addressing the tension between ease of requirements and security.

4.7 Identity in the Cloud

Identity in the cloud establishes effective trust relationships between the enterprises and service providers, protecting the privacy and security requirements as required by customers and regulations. Identity as a Service (IDaaS) is a foundation for managing identities for Cloud Computing and federation are key requirements for a successful cloud strategy

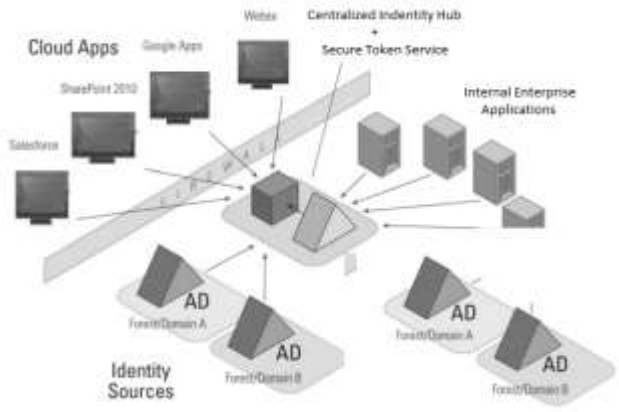

Fig 5: Identity as a service

4.8 Market Maturity

The Identity Management market is maturing day by day. Focus is being given to those practices of how to maximize investment in any enterprise. Enterprises are concentrating on system expansion and replacement.

4.9 Personalization and Context

Personalization means to understand the user, the user needs and to find semantically-related content. Context-awareness means to identify features that influence the user's current situation. Personalization can add value to online user experience.

4.10 Regulations

Regulation requires strong security and process of regulating identity involves active identity work to introduce new discursive practices of teamwork, partnership, etc. Regulations which impact IT security require logging the changes to financial data, attempting to access private information, authorizing and digital signatures.

4.11 Online Banking

Online banking has caught up significantly worldwide. Computers and broadband connectivity is within the reach of the common man today.

4.12 OpenID for Identity 2.0

Open ID is a key standard for Identity 2.0. It is a set of methods for identity verification using emerging user-centric techniques such as Information Cards or Open ID. InfoCards and CardSpace are becoming part of real life. Governments around the globe are participating actively in the OpenID concept.

4.13 SOA and IDM

SOA and IDM growing together

SOA define integration of widely disparate applications for web-based environment and to achieve the same, multiple implementation platforms are used. Collaboration between Identity Management and SOA is a key requirement. Investigations are on to arrive at services that can be executed to ensure end-to-end security. Identity Federation and use of virtual directories for flexible provisioning of Identity data will continue to grow.

5. CONCLUSION

Identity Management is a rapidly evolving market. Identity Management issues and challenges involves high number of IT help desk calls related to the passwords and lack of secure verification, quick resolution is required. Study of challenges and Issues will help in Promoting identity management and leading to new emerging trends which will be more secure for business and other organization.

6. ACKNOWLEDGMENTS

The authors would like to thank Infosys Limited and Chitkara University for supporting this research work. We also feel immense pleasure to thank Ms. Meenu Khurana (Dy Dean and HOD Computer Science, Chitkara University), Mr. Deepak Khurana (Project Manager, Infosys), Ms. Anju Chawla Takkar (Delivery Manager, Infosys) and Abhishek (Delivery Head, Infosys) for their able guidance and useful suggestions.

7. REFERENCES

[1]. Jamie Lewis, *Enterprise Identity Management: It is About Business*, Burton Group of Directory and Security Strategy Report, version July 2nd 2003.

[2]. Jason Bloomberg, Zapflash, *Enterprise and Identity Management: Essentials of SOA Prerequisite*, June 19th, 2003.

[3]. Jonathan Penn,VP & Research Director, Security & Risk Management, Forrester Research,2008,Identity & Access Management: Trends & Best Practices

[4]. Harjeev Dhingra, Identity Management – White Paper, Principal Security Architect, NetCom System

[5] Kahn, Jam. "HIPAA: Critical role of making strong authentication." Safenet. Apr.2002 [6] Langin, Daniel J. "Gramm-Leach-Bliley Security Requirements: Keeping Robbers and Regulators from the Door." Jun. 2002. 12 Nov. 2004.

[6] Lewis Jamie. "Emerging Infrastructure for ID&AM". Open Group in Conference. Jan. 2002. 15 Oct. 2004.

[7] Meta Group. "User Life-Cycle Management?" 800 to 94