Identity Management Practices and Concerns in Enterprise Cloud Infrastructures

Dan Daniels
Oakwood University
School of Business and Adult and Continuing Education
Huntsville, AL USA

***Abstract*—This paper reviews both scholarly and trade literature for contribution into a greater body of knowledge in identity management (IdM) practices and applications in cloud infrastructures. Identity management is a lateral iteration in the field of information security. In this paper classical and emergent identity management views are defined along with practices and applications. The benefits and challenges in identity management are surfaced, the cloud environment is defined, and the case is made for security within the environment and how identity management facilitates greater control over the access and confidentiality of user and enterprise data both stored and transmitted. Advances in identity management, cloud systems, and private and public key cryptosystems are also explored with a specific review of the three main IdM cloud practices: OpenID, security assertion markup language (SAML) and Microsoft Infocard.**

Keywords-identity management; security; cloud; OpenID, SAML, Infocard

I. INTRODUCTION

There are several benefits to traditional identity management (IdM) such as lowered security management costs and reduced costs of IT administration [2]. Improved employee productivity is increased since less time is spent dealing with the frequent issue of credential management which has primarily been the responsibility of the end user. Also, by delivering user identity information from a single source, end-user verification is made available, on demand, to logical peripheral systems. This paper provides a review of practical and theoretical work in the area of information security and, more specifically, identity management, to effectively draw a knowledge map of the field as it relates cloud security practices and management.

Ohio State's Identity Management program defines IdM as "a set of processes used to manage the identities in an identity store which includes the process of collecting information from the authoritative sources into a single location." [16]. For this paper the selected literature was reviewed and categorized into one of three groups covering cloud infrastructure, general information security, and identity management. The fields were evaluated topically then identity management current practices were identified and summarized.

Identity management affects more than those specifically within the field and technical vocation of information systems and technology. In a recent survey of small business owners conducted for Bloomberg Businessweek.com by the professional social networking site LinkedIn, three-fourths of the 65 respondents cited IdM as their biggest concern over cloud-based apps [5]. It is important to address issues that may be found on the periphery of cloud security, identity management practices and concerns, network security and cryptographic systems so that such information can be converted to high-level knowledge that can be made useful by those in higher, non-technical levels of management. These individuals would primarily be concerned with leveraging risk and its associated costs, and taking information from the independent, departmental knowledge silos and distributing it appropriately across the cloud reliably and securely.

II. THE PROBLEM OF SECURITY

Organizations implementing an information security program are often faced with several challenges with concerns surrounding data transmission, storage, migration and recovery. In a cloud environment additional concerns arise when considering stored end-user attribute data and profiles, public/private cloud partnerships, and public key infrastructure authentication mechanisms. While organizations are in wide support of the transition from IPv4 to IPv6, there is still an issue with bringing current products up to IPv6 capability as it is a separate protocol and as such brings new security risks. Until there is substantial assurance that the increased number of available IP addresses will have the same protocol transparency and governance from IPv4 the end-user is still vulnerable to the same content-based threats [6]. Organizations need to be persuaded to fully adopt and secure the IPv6 network structure in consideration of implementing any cloud infrastructure.

III. THE CLOUD ENVIRONMENT

Cloud computing is an emergent, employable tool for organizations to use in order to cut data storage costs, reduce the time to move an application from a development to a production environment, lower virtualization costs and deploying decision systems modules to end-users. According to Ramgovind, Eloff, and Smith [18] cloud computing is used

to keep IT budgets down, keep conceptual investments costs low, and can be part of a larger organizational solution by placing key applications within the cloud to take advantage of the cloud's processing power, while keeping mission critical systems on organizational resources thereby leveraging the computing power so as not to drain services.

As more organizations, as well as individual end-users, begin to employ cloud software, hardware and platform services the need to keep stored and transmitted data reliable and secure increases. Cloud security is, as it should be, an iterative process meaning that there will not be one clear solution that stands out regarding practices, protocols and governance for all cloud service providers (CSP) but a feedback loop with continual progression as to the practical applications of security management. The type of cloud an organization chooses to employ will inherently define its own security criteria and hardware needs. Currently, there are three types of clouds: public clouds which connect users to the Internet, private clouds which typically run internal applications and store data locally, and hybrid clouds that essentially provide the organization with an internal and external web-based presence.

IV. Security Concerns Within the Cloud Environment

An overview of literature on this topic brings forward not only the narrowed perspectives and solutions provided by those studying industry practices and concerns, but access to a host of implicit and inferred issues on the periphery identifying issues involving data storage, physical security, end-user privacy, data integrity and availability, and identity management. Mather, Kumaraswamy, and Latif [12] identify two broad categories when classifying multiple security issues: Security issues faced by cloud providers (organizations providing Software-, Platform-, or Infrastructure-as-a-Service via the cloud) and security issues faced by their customers. As such, literature proposing new security management frameworks and analysis data obtained through case study is substantive and readily available.

Just as the types of clouds are dissimilar, so are the concerns regarding privacy and security different depending on the type of cloud service being used. For example, an organization with a hybrid cloud infrastructure will be concerned about both maintaining the privacy of internal, confidential data such as research and development, as well as making sure that user data is not compromised as moves from the private to the public cloud by hyper-linking to a vendor site from within an organizational dashboard accessed using a single sign-on authenticated method.

IBM is also focused on the security within hybrid cloud infrastructures. In the June 2011 issue of NetworkWorld, a trade publication, Steve Robinson, a general manager for IBM security solutions stated that "enterprises using clouds should be able to establish means of authentication, provisioning of resources and de-provisioning of them in an automated way" [14]. IBM is researching monitoring systems which would have the ability to determine breaches in security and policy violations in real-time. The system, which is developed using IBM's own Infosphere stream data analysis tool, Cognos business intelligence and IBM's predictive analysis SPSS software used for audit control will potentially have the capability to "detect an upset employee who comes in on a Saturday and walks out with 4GB of data" [14] according to Robinson.

V. Traditional Identity Management

Identity management is similar to information security; specifically traditional biometric systems in that it involves the identification and authentication of humans across computer networks. The term "identity" for the purpose of this paper is synonymous with personally identifiable information (PII). This can include but is not limited to an individual's email address, financial and medical records, criminal history, social security number, biometric records, and passport numbers [13].

According to the University of Buffalo [21] information security office, identity management can be given three perspectives: pure identity paradigm, user-access or logon paradigm, and service paradigm. In the classic pure identity model general identities are constructed from a small set of principles. All identities are unique and distinctive and have a specific relationship to corresponding entities in the real world. The model is not restricted by its applied context and can have multiple identities, each consisting of multiple attributes and/or identifiers thus providing a virtually pure identity. Josang and Pope [7] identify, in their research, the conceptual relationship between entities, identities, and their attributes/identifiers. The user access and service paradigms involve familiar log-on, organizational perspectives and are integrated systems of processes, policies and technologies that aid in protecting confidential information from unauthorized access [21].

VI. Challenges in Traditional Environments

With the inherent benefits organizations can realize with identity and access management software it is not without complications in configuration, implementation and use. It can be common to have long implementation times to integrate each application, and laborious development and maintenance efforts which translate into longer time to introduce into the production environment to demonstrate value for the organization. The total cost of ownership can also be high with initial startup costs, services-to-license ratios, and the need for specialized IT support staff. Federated identity can potentially increase the complexity of an organization's security model, as each system is required to establish a trusted link with every other system, creating a star-based topology of connections [10]. Also, the process of de-provisioning is open to error and omission. Former employees can be blocked off from the

corporate network but may still retain access the public cloud (Internet) or other web services.

VII. Identity Management in the Cloud

As single-sign-on (SSO) applications helped to enhance enterprise information security on the desktop and network levels, there is now a need to extend identity and access management (IAM) models into the cloud infrastructure. The barriers to entry of an IAM model in the cloud is often compared with the barriers that preceded them within traditional identity management frameworks such as high upfront costs, hidden maintenance costs, vendor lock-in and reduced scalability.

There are three main federated identity protocols [9]:

- Security Assertion Markup Language **(**SAML)
- OpenID specification and
- InfoCard specification underlying Microsoft's Windows Cardspace

SAML is used by most organizations however is gaining increasing notoriety. SAML is an XML-based standard for exchanging authentication and authorization data between both producers and consumers of assertions otherwise known as identity providers and service providers. SAML attempts to solve the Web Browser Single Sign-On (SSO) problem which is also addressed by OpenID.

OpenID is the open standard that examines how users are authenticated in a decentralized manner, eliminating the need for organizations to develop ad hoc systems and allowing users to consolidate their digital identities [4]. In the OpenID protocol, which does not rely on a central authority to authenticate a user's identity, "neither services nor the OpenID standard may mandate a specific means by which to authenticate users, allowing for approaches ranging from the common (such as passwords) to the novel (such as smart cards or biometrics)" [4].

VIII. Conclusion

Enterprise cloud infrastructures require unique and anonymous storage, message authentication, encryption and decryption. Currently, end-users accessing resources from multiple providers have authentication issues due to the separate requirements of each individual provider. Bertino, Paci, Ferrini, and Shang [1] propose an answer to this issue through an Aggregate Zero Knowledge Proof of Knowledge (AgZKPK) solution for managing authenticating users from the client to the cloud service provider (CSP). This is possible by allowing one entity to submit (client-side) identity attributes to the provider via a portal and the CSP verifies that the values match syntactically and semantically through ontological mappings providing a multi-factor type of authentication.

Oracle is also developing new service-oriented capabilities in identity management with the 11g Identity Management product line. This service aims to "optimized and support the evolving needs of modern enterprises, such as cloud computing, with a unified, secure easy-to-deploy set of identity management functions" [17]. In this paper, the overall issue of security was addressed. The traditional identity management framework was explored identifying key attributes or identifiers associated with user identities specifically as it relates to single sign-on platforms. Current and emerging practices in identity management were also identified keying in on barriers of entry as well as best practices to help ensure successful implementation. The literature provides much promise to the future of identity management and enterprises would benefit from further research in this area specifically as it relates to scalable data-grid centers, virtualization, and connecting internal and external clients via hybrid cloud systems.

IX. References

[1] Bertino, E., Paci, F., Ferrini, R., & Shang, N. (2009). Privacy-preserving Digital Identity Management for Cloud. Microsoft Research. Microsoft.com Retrieved from: ftp://ftp.research.microsoft.com/pub../debull/A09mar/A09MAR-CD.pdf#page=23

[2] Blount, S. (2010). Improving the Operational Efficiency of IT Security Management. CA Security Management Retrieved from: http://image.lifeservant.com/siteuploadfiles/VSYM/99B5C5E7-8B46-4D14-A53EB8FD1CEEB2BC/4B11FB0C-C29A-8FCE-45B041FFE30483A2.pdf

[3] Eldon, E. (2009). Single Sign-on Service OpenID Getting More Usage. SocialBeat.com Retrieved from: http://venturebeat.com/2009/04/14/single-sign-on-service-openid-getting-more-usage/

[4] Hesseldahl, A. (June 2010). Businesses Confront the Cloud Security Threat. Business Week. Retrieved from: http://www.businessweek.com/technology/content/jun2010/tc20100616_394524.htm

[5] InfoSecurity.com. (2011). Transition to IPv6 Poses Information Security Challenges. Retrieved from: http://www.infosecurity-us.com/view/17561/transition-to-ipv6-poses-information-security-challenges-says-fortinet/

[6] Josang, A., & Pope, S. (2005). User Centric Identity Management AusCERT Conference Retrieved from: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.1563&rep=rep1&type=pdf.

[7] Landau, S., Le Van Gong, H., & Wilton, R. (2005). Achieving Privacy in a Federated Identity Management System Retrieved from: http://www.futureidentity.eu/documents/Achieving_Privacy.pdf

[8] Lasance, M. (2011). ID and Access Management Challenges in the Cloud. Asia Cloud Forum. Retrieved from: http://www.asiacloudforum.com/content/id-and-access-management-challenges-cloud

[9] Liang, Y., Chunming R., & Gansen Z. (2009). Strengthen Cloud Computing Security with Federal Identity Management Using Hierarchical Identity-Based Cryptography. CloudCom 2009, LNCS 5931, pp. 167–177

[10] Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. Sebastopol:O'Reilly

[11] McCallister, E., Grance, T., & Scarfone, K. (2010). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). National Institute of Standards and Technology. Retrieved from: http://www2.illinois.gov/bccs/security/Documents/Guide_to_protecting_PII.pdf

[12] Messmer, E. (June 2011). IBM building security into cloud fabric. Network World. Retrieved from: http://www.networkworld.com/news/2011/060911-ibm-security.html?hpg1=bn

[13] Mullen, M. (February 28, 2011). Chairman's Quote. Joint Chiefs of Staff. U.S. Strategic Command Change of Command, Offutt Air Force Base

[14] Ohio State University. (2011). Office of the Chief Information Officer Retrieved from: http://cio.osu.edu/projects/idm/idm_terms.html

[15] Oracle.com (2010). Oracle announces significant advances in application security with Oracle Identity Management 11g. Oracle Press Release. Retrieved from: http://www.oracle.com/us/corporate/press/154293

[16] Ramgovind, S., Eloff, M.M., & Smith, E. (2010). The management of security in Cloud computing. *Information Security for South Africa* (ISSA), 2010 , vol., no., pp.1-7, 2-4 Aug. 2010 doi: 10.1109/ISSA.2010.5588290

[17] University of Buffalo (2007) Electronic Identity Management. UB Information Security Office. Retrieved from: https://security.buffalo.edu/identitymanagement

AUTHORS PROFILE

Dan Daniels is currently an Instructor for the School of Business and Adult and Continuing Education at Oakwood University in Huntsville, Alabama. His current research involves an investigation into the availability of open-source intelligence through an examination of the security behavior of technology knowledge workers. Additional research interests include knowledge management systems, symmetric key distribution systems, and advanced penetration testing and analysis techniques. Daniels received a BBA in Information Technology from Oakwood University, an MS in Management Information Systems from Nova Southeastern University, and is completing his PhD in Information Technology at Capella University. He holds both Network+ and Security+ certifications, and is a member of IEEE, ACM, and the North Alabama Information Systems Security Association.