Author(s): Jahankhani, Hamid; Talaimojeh, Soheil
Title: Review of identity and access management systems
Year of publication: 2007
Citation: Jahankhani, H.; Talaimojeh, S. (2007) 'Review of identity and access management systems' Proceedings of Advances in Computing and Technology, (AC&T) The School of Computing and Technology 2nd Annual Conference, University of East London, pp.53-60
Link to published version:
http://www.uel.ac.uk/act/proceedings/documents/ACT07.pdf

REVIEW OF IDENTITY AND ACCESS MANAGEMENT SYSTEMS

Hamid Jahankhani, Soheil Talaimojeh
Innovative Informatics Research Group
School of Computing and Technology
hamid.jahankhani@uel.ac.uk

Abstract: Identity and access management is rapidly becoming the top business issue as organizations look to increase security, reduce risk and decrease operational costs. In order to evaluate adequately the emerging maze of technologies brought forward by various vendors it is necessary to critically analyze many aspects of the identity related security terms and techniques. The emerging development of techniques assisting in the consolidation of dispersed yet somewhat related Identity components across the enterprise-wide systems could very well reduce the cost of management, while increasing the control over enforcement of governing Compliance and internal security policies. But as always there may be tradeoffs that could damage the organization if not planned properly. The fascinating fact is that Identity Management is 80% politics and business and 20% technology. Identity Management is a set of processes and supporting infrastructure for the creation, maintenance and use of digital identities (unique ids, attributes, credentials, entitlements. This paper aims to discuss what Identity Management means in the context of Information Technology and to provide an over view of the important components that makeup Identity Management Systems.

1. Introduction:

"Identity management solutions address enterprises' need to administer (create, modify and delete) user accounts, user profiles and corporate policies across the heterogeneous IT environment via a combination of user roles and business rules.", (Gartner, 2003).

Above Gartner Group refers to the technology as Identity Management (IdM) Solution. Oxford Computer Group an Identity Management Solution Providers defines Identity and Access Management (AIM) as; "A system of procedures, policies and technologies to manage the lifecycle and entitlements of digital identities. More simply, efficient and auditable mechanisms for ensuring the right people have access to the right resources at the right time", (Abagnale, 2006).

In effect the emerging technology frequently referred to as "Identity Management" (IdM) and sometimes called "Identity and Access Management" (IAM) are a set of technologies that are aimed at improving the existing state of affairs surrounding creation, maintenance and eventually deleting Identity related credentials.

The key question is; what are the improvements that IdM can bring to the existing state of affairs in relations to the Identity and its credentials?

There are number of fascinating categories of improvements and advantages to gain by implementing the new technologies of IdM into the existing systems. The question is; Why do we need Identity Management Systems?

This paper aims to list the basic necessities of components that make up IdM systems as well as the elements that are meant to be effectively controlled by implementation of Identity Management Systems. For the purpose of this paper we shall consider users/employees/consumers (Human) rather than resources or services as Digital Identities in the system.

2. Identity Management components and Services:

The emerging technologies of IdM shall much more effectively create new Digital Identity(ies) and manage the Identity Lifecycle in an Automated fashion known as Provisioning and if no longer needed De-Provision such an Identity.

The whole purpose of using Identity & Access Management Systems is to be able to exert maximum amount of desired Governance Compliance and Corporate Policies, with minimum Human Intervention whilst ensuring to keep track of (Auditing) all changes and activities throughout the enterprise and beyond if necessary in order to achieve highest level of cost saving while maintain and highest level of Security within the entire system that may span across a Federated Identity Managed (FIM) environment.

IdM Systems access EDS (Enterprise Directory Services) in order to Identify, Authenticate and Authorize users for various purposes. Today's EDS based systems mostly are based on LDAP Version 3. Adequate IdM systems must have support for X.500 (Global White Pages directory). One of the selection criteria's for IDM Systems must be its wide range of compatibility with Systems & applications Databases, Flat Files etc that they use as Repositories of Users' Credentials for Reference Monitoring within Silos of Dissimilar and Heterogeneous information systems.

Examples of EDS (Enterprise Directory Services) are Microsoft Active Directory, Novell eDirectory, Oracle Internet Directory (ODI), and IBM Directory Services (LDAP), and Sun LDAP-based Directory Service part of Sun Java Enterprise.

Most implementation of IdM Systems is likely to interact with Active Directory a Microsoft's proprietary implementation of an LDAP-compliant directory service. Of course other proprietary alternatives EDS such as Oracle Internet Directory may be used. There are also plenty of open-source tools to create directory services, including OpenLDAP and the Kerberos (protocol).

However the core components of IdM environment in most cases is provided by amalgamation of information available from all Reference Monitoring Repositories mentioned above into a separate MetaDirectory or Virtual Directory under the total control of IdM System. Almost always the user shall receive a Unique Identifier (This may be supplied by HR as Employee number or Student Number, Social Security number or generated by the system) across the entire enterprise in order not to clash with any previously specified Identity.

Of course adequately designed IdM systems may systematically allow bidirectional access and possible changes into their MetaDirectory for scenarios where changes in part of the system that may not necessarily use the IdM management interfaces be allowed to be captured into the global MetaDirectory in order to reflect those changes into the wider system. There are heavy penalties to pay should the highest level of attention lapse when designing the control of the

bidirectional changes of the MetaDirectory.
Data Feeds and Connectors are used to transfer data between dissimilar systems, applications etc. Data being transferred through these Connectors include configuration information, request for Identification, Authentication & Authorization etc. The type of information going through the Data Feeds and Connectors would be limited by the capabilities available in the IdM software and any IdM intended Standards that may apply particularly in a Federated Identity management Environment. Attribute and Group Services is via a combination of user roles and business rules and Support Software Systems (logs, maintenance web pages, diagnostic tools, etc.).
Segregation of duties are also achieved through Workflow in as many aspects as the vendors and Solution Providers imagination and expertise can provide for the specific needs of the end users with as much granularity as they are capable of or required by their clients.
Enforced and Automated Auditing is another extremely valuable part of all adequate Identity Management Systems in order to keep tracks of changes to the system and any Authorization or failure.
Identity Management also includes such components as SSO (Single Sign On) which in effect allows the user to provide one password for all chosen systems, Applications and services etc within the Identity Managed environment to avoid having to remember and reenter many different passwords every time the user may require access to his/her Authorized resources and services.
Of course the Identity Management Systems may go further to challenge the issues that matter within the entire IT infrastructure in a much wider, perhaps global scale. These are contrasting issues combining highly desired Security & responsibility within the Identity Management space.
This is then referred to as Federated Identity Management (FIM).
FIM in turn demands strict Standards for interoperability amongst dissimilar and distributed Identity Management systems, there are number of standards such as Shibboleth, SAML (Security Assertion Markup Language), SPML (Security Provisioning Markup Language) etc, with number of organizations involved such as Liberty Alliance & OASIS etc.
Security goals are usually acronymic to CIA *Confidentiality*, *Integrity and Accountability*.
However the need has never been greater to add '*Anonymity*' amongst the goals.
In fact all the above goals play an important part of a well thought IdM architecture. Identity could include many attributes of an individual. For example;

- *Confidentiality* is essential when you trust your Credit Card details with an online merchant
- *Integrity* of say data held by Health Authorities for your state of health is paramount should you need to receive treatment or purchase Insurance
- *Accountability* is the key to hold responsible anyone dealing with your sensitive Identity orientated information
- *Anonymity* is an issue raised time and time again when someone's Identity being exposed to others can have catastrophic results.

3. Relationship between Identity & Authentication:

Let's start by looking at the definitions and analyses concerning the core security principles required to adequately identify and authenticate a user into an identity managed system.

Identity

A security principal (you or a computer, typically) wants to access a system. Because the system doesn't know you yet, you need to make a declaration of who you are. Your answer to the question "Who are you" is the first thing you present to a system when you want to use it. Some common examples of identity are user IDs, digital certificates (which include public keys), and ATM cards. A notable characteristic of identity is that it is public, and it has to be this way: identity is your claim about yourself, and you make that claim using something that's publicly available, (Riley, 2006).

Authentication

This is the answer to the question "OK, how can you prove it?" When you present your identity to a system, the system wants you to prove that it is indeed you and not someone else. The system will challenge you, and you must respond in some way. Common authenticators include passwords, private keys, and PINs. Whereas identity is public, authentication is private: it's a secret known (presumably) only by you. In some cases, like passwords, the system also knows the secret. In other cases, like PKI, the system doesn't need to possess the secret, but can validate its authenticity (this is one of many reasons why PKI is superior). Your possession of this secret is what proves that you are who you claim to be, (Riley, 2006).

Authorization

Once you've successfully authenticated yourself to a system, the system controls which resources you're allowed to access. Typically this is through the use of a token or ticket mechanism. The token or ticket constrains your ability to roam freely throughout the system. By "caching" your authenticated identity for subsequent access control decisions, it allows you to access only that which the administrators have determined is necessary, thus enforcing the principle of least privilege.
Authorization is usually not an area of confusion, although this may be challenged on the point that some security attributes may be lost if a resource such as a file was to be replicated across dissimilar systems particularly in a heterogeneous enterprise-wide environment where IdM systems usually play their part.
There is a trend in merging identity and authentication. This is worrying many researchers, as it is believed that identity and authentication must remain distinct. (Riley, 2006) has highlighted this by three different scenarios.
Scenario 1:
"Consider a system that has no passwords. You log on by entering only your user ID. This works fine, I suppose, if you're the only user of the system and if no one else can get to it. How about a multi-user system or a network?
Someone else could simply enter your user ID and get access to your information. Generally, user IDs are also e-mail addresses, so you can't rely on the fact that user IDs are secret. Also, what happens if

two people have the same name? How will you create unique environments for each person?"

Scenario 2:

"Consider a system that requires entering only a password -- no user ID -- to log on. Passwords are secret and they're not acting as e-mail addresses, so this should work, right? Well, if your password now serves double duty -- identifying you and authenticating you -- then problems arise. Say you're changing your password to "p4ssw0rd" and, unknown to you, someone else has already decided to use that password. You can't use it! Indeed, the system will probably raise an error: "That password is already in use. Please try another." What have you just learned? The password to someone else's account of course! Now you can be a bad guy. Actually, there are no real-world systems that attempt to use passwords as identifiers; however there are papers describing how a system without user IDs is a really great idea. Obviously, ones disagree.

Scenario 3:

"A system must maintain distinct mechanisms for identity and authentication. Identity must be unique: there can be only one "jsmith" in the system or domain (but not necessarily in the world). Authenticators, however, don't have to be unique -- only secret. Both "jsmith" and "mjones" could be using the same password, but neither of them knows this. Having such a public/private pair (hmm, "public/private," sounds familiar, doesn't it?) also makes it easier to address theft. In this system, if a bad guy learns your password, you just change it. You don't need to go through the hassle of getting a brand new account. You can revoke and reassign passwords as often as you wish. How would an ID-only or password-only system handle that situation?".

Identity and authentication are distinct components of the steps necessary to use a secure computer system. Identity without authentication lacks proof; authentication without identity invalidates auditing and eliminates multi-user capability (consider Windows 95/98, which supported a password as an authenticator but no user ID). If biometrics becomes important to you as you begin considering how to strengthen identity and authentication in your security strategy, remember to evaluate how a particular biometric implementation views itself. Proper biometrics are identity only and will be accompanied, like all good identifiers, by a secret of some kind -- a PIN, a private key on a smart card, or even a password, (OASIS, 2006), (Oxford Group, 2006) and (Abagnale, 2006).

Consider biometrics, given the definitions and characteristics of identity and authentication, which is biometrics: identity or authentication?

Before answering the question, think about the attributes of biometrics. Is it public or private? Public, of course. You leave various biometrics everywhere you go -- your fingerprints remain on anything you touch, your face is stored in countless surveillance systems, your retina patterns are known at least by your optometrist, perhaps. And it's believed, although there is no actual evidence to support the claim, that biometrics are unique. Given this, it follows that biometrics are identity, not authentication.

Problems arise when systems begin using biometrics for authentication. Say that all you need to do is swipe your finger to log on, with no additional factors. Your fingerprint is now serving both to identify you and to prove that you are you. How

can such a system be compromised? Very easily, it turns out, without a secret accompanying your fingerprint. Numerous research reports have shown that biometric systems can be spoofed (the most notorious of which involves the assistance of a Gummi Bear; (Putte, 2002) and (Schneider, 2002).

Another sobering example: "Police in Malaysia are hunting for the members of a violent gang who chopped off a car owner's finger to get round the vehicle's hi-tech security system", (Kent, 2005).

Again, because no secret accompanies the finger, all you need is the finger and you can possess the car. Here the security countermeasure moves the risk from the car to the driver! This is when security becomes unsafe. Revocation presents another challenge. If a system relies only on a biometric for both identity and authentication, how do you revoke that factor? Forgotten passwords can be changed; lost smartcards can be revoked and replaced. How do you revoke a finger?

4. Federated Identity Management (FIM)

Federated Identity Management is the result of Identity Management Systems cooperating amongst multiple organizational boundaries. When Identity management implementation encompasses multiple organization boundaries, it is considered as Federated Identity Management. Identity related data are also likely to cross dissimilar Identity Management Systems, which adds further technical complications beside the usual Trust & Security stronghold in this area of discussions.

Other obstacles include how two companies that want to federate will merge their information. The question that arises is that; what can Identity Federation do for you?, (Kirk, 2005).

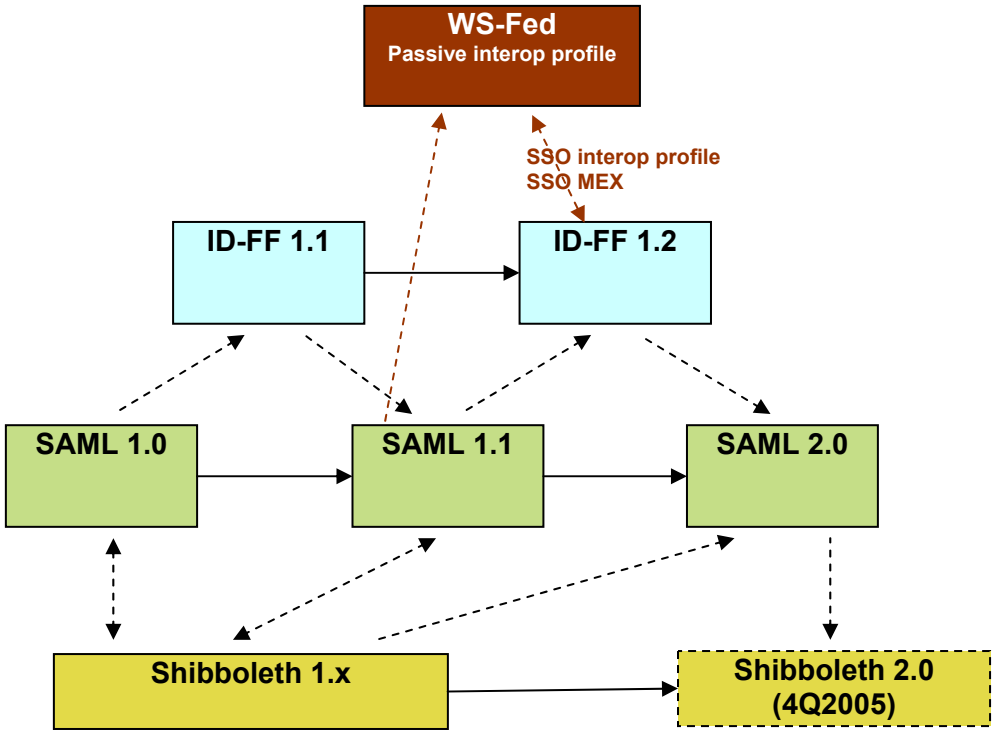
- Provide your customers, citizens, employees, and business partners more control over identity information
- Supply superior security, control, and privacy-improving trust
- Mitigate against breaches and identity theft with no single point-of-failure
- Provision accounts and securely provide access to designated resources both within and outside corporate borders
- Build identity into the foundation of all transactions and personal data services activities
- Eliminate excess passwords and securely implement single sign-on
- Offer a far more satisfactory online experience, and new levels of personalization
- Create seamless and secure business relationships
- Improve authentication with existing internal resources
- Improve shareholder value and compliance procedures by offering a means for better reporting accuracy
- Reduce risk through a more balanced authentication process

The relationships between the existing standards of FIM and the dynamism of the FIM environment are highlighted below:

- Federation continues to be a growing segment of the identity management market
  - Many different use cases are appropriate for federation
- The market is providing a wide range of products that support federation standards

- Web access management (WAM)and standalone federation products lead the way
- Interoperability, conformance, and coexistence of the various protocols is a potential issue for enterprises
- Vendors attempt to address this in product implementations

The diagram below shows the compatibility between different standards as well as any backward compatibility, (Gebel, 2005).



Federation standards family tree and interoperability, Source, (Gebel, 2005)

Twelve vendors plus Internet2 demonstrated how federated identity implementations could interoperate in a mixed environment that included Security Assertions Markup Language (SAML), Liberty Alliance Identity Federation Framework (ID-FF), Shibboleth, WS-Federation, WS-Security, and WS-Trust protocols. Although the participants demonstrated interoperability for basic functions like single sign-on (SSO), there are limitations because functionality differs between protocols or even between different versions of the same protocol.

The Federated Identity Management is still evolving and the standards and applications are yet to mature.

Conclusions

Preparation is the Key for successful IdM implementation. Segregation of duties could be a key. It is not a one-man task and it's not for the faint of heart. Collective decisions must be made at very high level by CXO's and stakeholders.

It is very easy to fall in the trap of coming across just another Technology, Platform, Approach, Standard, Protocol, additional Tool, Compliance, Governance, Industry

Regulation or Best Practices or Ethical issue that would impact your Technical Architecture, Implementation Plan, Compliance or Morals.
Therefore a collective and very calculated decision must be made to avoid having to go back to the drawing board in the middle of a very long project or ending up with massive expenditure that results in liability rather than a success at the end of it all.

References

Abagnale, F., 2006, Abagnale & Associates Available from: http://www.abagnale.com/aboutfrank.htm

Gartner, 2003, "Identity and Access Management Defined," Gartner Group Research Note 4 November 2003 http://web.gc.cuny.edu/banner2000/SCT_Summit_2004/bw/Luminis/bw291.pdf

Gebel, G. (2005) 'Recent Developments in Federation' - Burton Group [online] Available from: www.burtongroup.com/events/downloads/ppt/1032.ppt (23-10-06)

Kent, J. (2005) Malaysia car thieves steal finger [online] Available from: http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm

Kirk, J. (2005) 'Identity federation: Is it time to move now?' IDG News Service Available from: http://ww6.infoworld.Com/products/print_friendly.jsp?link=/article/05/09/15/ HNidfederation_1.html

OASIS, 2006, Organization for the Advancement of Structured Information Standards Available from: http://whatis.techtarget.com/wsearchResults/1,290214,sid9,00.html?query=oasis and Security Services Charter Available from: http://www.oasis-open.org/committees/security/charter.php and Security Services (SAML) TC Available from: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security and Security Services Technical Committee Available from: http://www.oasis-open.org/committees/security/ and Web Services Security (WSS) TC Available from: http://www.oasis-open.org/ committees/tc_home.php?wg_abbrev=wss

Oxford Group, 2006, 'Benefits - Identity and Access Management (IAM)' Oxford Group [online] Available from: http://www.oxfordcomputergroup.com/ocg.aspx?nav=submenu/56EMTPWMAA

Putte, T. V.D. & Keuning, J. (2002). Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned [online] Available from: http://cryptome.org/gummy.htm

Riley, S. (2006) 'It's Me, and Here's My Proof: Why Identity and Authentication Must Remain Distinct' Security Management - Security Technology Unit - Microsoft Corporation [online] Available from: http://www.microsoft.com/technet/community/columns/secmgmt/sm0206.mspx

Schneider, B. (2002). Fun with Fingerprint Readers [online] Available from: http://www.schneier.com/crypto-gram-0205.html#5).