



Anakam Identity Services

Who Are You? (And What Should You Know?)

by Peter Buxbaum

As the challenges of controlling access and privileges to networks and systems become more complex, interrelated and vital to security, identity and access management is emerging as a key technology for the Department of Defense and other federal agencies.

The importance of identity management was underscored recently by an Obama administration document that emphasized its role in protecting the nation's infrastructure.

Adding to the complexity are the requirements that information be shared across agencies, that different individuals will require different levels of access, and that all of the above is also applicable to outside contractors and their employees. In some cases, as with health systems, for example, spouses and dependents of defense personnel may also need access to DoD systems.

Although they started out as two discreet processes, identity management and access management are increasingly being thought of in tandem. Identity management involves verifying the identity of individuals who need access to an organization's information resources, and issuing credentials that can authenticate the identity in the future. It is focused on activating and deactivating users.

Access management is the process of combining identity data with other attributes to determine a user's authorizations and privileges. Taken together, identity and access management involves managing who has access to what information over time.

A 2008 survey of government IT managers undertaken by Quest Software indicated that more than 80 percent viewed access management as an essential component of identity management. A more recent report from Forrester Research suggested that organizations consider a move from identity management to information and access management as they prepare their 2011 security strategies.

"Security professionals increasingly recognize that access control and information management are key components of data security," the report noted. "This means that onboarding and deactivating users in a reliable, timely fashion is not enough. Organizations have to ensure that users get appropriate access rights, both initially and as they move through an organization."

Taken together, the Quest survey and the Forrester report make clear that identity and access management are probably be best thought of as one integrated process, or at least two highly interrelated processes.

"Systems are heading toward a more holistic approach to security," said John Mauthe, a principal at Booz Allen. "Traditionally, the emphasis has been on keeping unauthorized users out. But now the focus is on granting authorized users the right to get into the right application at the right time. It has become more that just a binary 'yes or no' for access to a system. We are also going beyond traditional security boundaries to provide authorized access to individuals from external organizations."



The importance of proper access, and not merely identity, controls is underscored by the fact that most of the damage from today's cyber-attacks comes from inside an organization. "Eighty percent of the attacks come from outside the organization, but they do only 20 percent of the damage," said Dipto Chakravarty, chief of the cloud security business unit at Novell, a provider of infrastructure software. "Inside attacks, from disgruntled employees or rogue managers, constitute 20 percent of the attacks but cause 80 percent of the damage worldwide."

"The general issue that we are dealing with is that networks are inherently not built for security," said Ron Carpinella, vice president for identity at Equifax. "The problem we have to deal with is that there is no incorruptible or perfect security system. We are always balancing between access and enablement and being able to lock down and control how you get in. If you make these controls very user-unfriendly, then the network isn't the communications channel that it is meant to be."

Another level of complexity has been added with the advent of virtualization and cloud computing, the implications of both being that applications are not necessarily hosted within an organization's premises. "Cloud computing was a very disruptive phenomenon," said Chakravarty. "The advent of the cloud has given rise to ubiquitous utility computing without walls, and in this new world a lot of the old enforcement models become insufficient."

Federated Approach

In the past, entering a user ID and a two-factor authentication was sufficient to establish identity. "Data used to reside inside the perimeter of an organization," said Chakravarty. "With virtualization, we have hardware on- and off-premise. With virtual private networks and mobile devices, we have employees accessing networks from anywhere."

One of the best practices that has emerged in identity and access management "is to implement identity management as a program, not a project," said Idan Shoham, chief technology officer at Hitachi ID Systems. "This involves examining and re-examining priorities and implementing them. It goes on forever because business processes and integrations change all the time. You never run out of stuff to automate. It becomes a new IT function."

As with many military and other information systems, there is a move away from the stovepiped management of identity and access management toward a federated approach that could reach across different systems. "The Defense Manpower Data Center is charged with providing ground truth with regard to all identity attributes of every person within the systems," said Mauthe. "They are now coming up with ways to serve up that information to all identity data consumers inside DoD. The silo systems will no longer be required."

This type of federated identity and authentication management is being mandated across the federal government. A memorandum released by the Office of Management and Budget in February noted that the president's policy "highlighted the importance of identity management in protecting the nation's infrastructure" as previously established in 2004 by Homeland Security Presidential Directive 12. HSPD-12 requires agencies to follow technical standards and business processes for the issuance and use of federal personal identity verification (PIV) smartcard credentials while moving toward "full use of the PIV credentials for access to federal facilities and information systems."

The recent OMB memo mandated that all new systems under development must be PIV-enabled effective immediately and that "existing physical and logical access control systems must be upgraded to use PIV credentials" by the beginning of fiscal year 2012.



While PIV is not directly applicable to military systems, which use the Common Access Card (CAC), a looming issue involves how to allow authorized PIV-equipped personnel access to certain military systems. At this point, the PIV and the CAC are not interoperable.

The technology response to these increasing levels of complexity has been to evolve identity and access management “from a set of tools, to a product, to a suite and to a platform over time,” according to Chakravarty. “Convergence and consolidation of identity management tools under a common framework have resulted in the emergence of platforms to allow you to authenticate, authorize, provision and audit in an automated fashion.”

Hitachi ID Systems’ identity and entitlement management system automates the provisioning process across multiple enterprise systems. “Our tools detect the creation or deletion of a user on one system and matches that process on other systems across the enterprise,” explained Shoham. The Hitachi system is capable of performing this task on more than 100 systems and integrations, including SAP, Microsoft Active Directory, SQL and Oracle databases, and the Unix and Linux operating systems.

“For example, the system might detect someone has been hired by looking at a data feed from the human resources department,” said Shoham. “The system would then automatically provision rights on other systems depending on the organization’s rules and policies. Or the system might detect a termination. In that case, it would look up all access of the individual’s rights and deprovision all of them.”

These automated changes are accomplished through a connector that the Hitachi deploys among the various systems. These automated changes work cost effectively on systems with many users.

“But most organizations have many small applications with only a handful of users,” said Shoham. “Implementing a connector is not cost effective in those cases. So instead we have an automated work flow that chases after the person who needs to make the changes in the systems.”

These changes need not be made by IT personnel, but can be delegated to a manager within the user base. The system also features an automated audit function through which lists of users are sent to managers, who are asked to verify whether the employee still reports to that manager and whether the employee still requires access to the systems.

Up-Front Costs

Implementing automated identity and access management systems is not cheap, however. “One of the big challenges is that there are fairly significant up-front costs in investing in this technology, especially for many smaller organizations,” said Mauthe.

Equifax endeavors to deal with this challenge by providing a flexible platform, known as Anakam, into which tools can be plugged as needed. “We simply want to make the platform as adaptable and flexible as it can be,” said Carpinella. “New layers of security can be applied in response to new threats and risks. Capabilities can be added or disabled depending on the needs of the organization.”

The Anakam.IDP tool solves the problem of expensive, in person verification by providing identity proofing during the user’s initial enrollment on a web portal. “It does not use data that the end-user has pre-registered at the enterprise,” said Carpinella. “Instead, the identity proofing questions and answers are developed from a variety of outside sources to maximize the ability to uniquely identify an individual and to prevent fraud.”



Anakam.IDP works by asking questions related to the applicant's history, such as past residences, motor vehicle registrations, demographic information and credit data. Applicants must answer an enterprise-established percentage of consecutive questions correctly, making it extremely difficult for an impostor to gain access to an organization's web-based applications.

"The number of questions and the required score can be varied based upon the user's role, the risk of the transaction, or the risk that the claimed identity is not authentic, for example in case of a known stolen identity or mismatch," said Carpinella.

Equifax also offers Anakam.ODI, a tool that allows organizations to grant access to outside users. Anakam.ODI develops requirements for ID proofing using on standards issued by the National Institute of Standards and Technology based on a variety of public and private data sources.

"This solution minimizes the costs of identity proofing while maximizing the likelihood that the person conducting the transaction is who they claim to be," said Carpinella. "Using Anakam.ODI means that an organization no longer needs to maintain a user name and password identity management process for those users. This streamlines the business process." Once an identity has been verified by Anakam.ODI, the user is then registered for two-factor authentication and receives a credential that will be used to grant access in the future.

Quest Software seeks to mitigate the financial bite of investing on a full-blown identity and access management system by offering its tools on a modular basis. "Customers can buy an entire identity management framework from us," said Dmitry Kagansky, the company's chief technologist, "but they also can also implement it piecemeal to respond to the current pressure, crisis or need."

An organization might have logical access controls figured out, said Kagansky, but need a single sign-on tool or require components addressed auditing, logging or integration. "There are a lot of options," he said. "Our customers find that we take things slower and are reasonable about what gets implemented next. We don't come in wheeling an entire stack."

One of Quest's tools works within Microsoft Active Directory—a directory service that provides a central location for user access single sign-on to network resources and standardizing access to application data. It speeds up the provisioning process based on job title, location and other factors, so that new users can get up and running more quickly.

"Some customers say that Active Directory is not the center of their universe," said Kagansky. "In that case, we have an identity store or warehouse that can be implemented where they can centralize the process that can be used across different systems. This becomes a hub that stores access information on users and feeds it to systems which rely on that information for access controls."

Novell has taken the approach of developing separate identity and access management suites for physical, virtual, and cloud computing environments. "Today's IT environments are typically 75 percent physical, 20 percent virtual and 5 percent cloud," said Chakravarty, "but that mix is likely to change in the future."

The approach taken by Novell has been to build software for each type of environment from the ground up. "We chose to do that rather than retrofitting our existing software to the cloud environment," he explained. "Taking an enterprise product and retrofitting it to the cloud does not solve the problem, because the footprint must be much smaller. You can't change the basement of a house after you've built the house. We have developed these solutions with the customers, as well as their vendors and hosters, in mind. We believe that our tools make hosters best-of-breed suppliers and make their customers more secure."



Novell offers a service that allows customers to repurpose their policies in the event they switch from one cloud-computing provider to another. “We provide customers a future proofed way of managing identity across the physical, virtual and cloud ecosystems at a significantly reduced cost of ownership,” said Chakravarty.

Context Aware Security

Future developments in identity and access management could include what Chakravarty called “fine grain access control and context aware security.” That means that an individual’s access entitlements could change, for example, depending on the person’s location, as well as “who you are, where you are and what time you are there.”

A manager in one department, for example, might have one set of entitlements when sitting in his or her office, but after taking the elevator two flights up to the finance department, the access privileges may change at that location.

In the federal arena, Kagansky expects that the government PIV initiative will eventually be harmonized with DoD’s CAC regime. “At this point they are not compatible,” he said. “At some point as information sharing continues to become more important, and as contractors might need access to defense and civilian systems, the government will figure a way so that authorized users can get on all systems with the single credential. It’s not a technology issue so much as a policy issue. DoD clearances need to be accepted by civilian agencies and vice versa. They have to learn to play nice together.”

Booz Allen’s Mauthe sees the development of risk-based identity and authentication management systems in the future. “As systems become more evolved and sophisticated, they will have greater forensic and heuristic capabilities,” he said. “Future systems will be able to evolve and make decisions based on historical and observed factors providing a dynamic enforcement point rather than a stagnant security control capability.”

Contact Us Today

Learn why the nation’s leading healthcare, government, banking and commercial organizations have chosen Anakam Identity Services.

For more information, visit www.anakam.equifax.com or call 888-826-2526.