Identity Management and Access Control
By Ed Tittel and Justin Korelc

Introduction
This paper is meant to provide an introduction to and a broad overview of the related subjects of identity management and access control. In a computerized accounting environment, identity management and access control are the means by which segregation of duties is implemented and enforced. Individual identities are associated to access rights to specific information and resources within an environment, system or network, and application, based job descriptions and roles. In order to access a given system, application or function, the user must establish their identity, and that identity must be affiliated with rights or permissions to the system, application or function with the system, application or function the user is attempting to access.

As an introduction and overview, the material presented here is probably most useful to those with little or no familiarity with these topics, or those seeking a refresher. Readers who fall into these categories would be well served by reading this document from start to finish. At the very least, financial professionals, even those familiar with these subjects, should read the next section, “Opportunities for Financial Professionals,” the sections entitled “Special … considerations for accountants,” and the annotated reading and resource list created to accompany this paper. This information should be of definite interest, and can lead them to other, more detailed resources.

Here’s a roadmap to this document’s contents:
- Introduction (what you’re reading right now)
- Opportunities for Financial Professionals
- What is Identity Management?
  - Identification and Authentication Techniques
    - Passwords
    - Biometrics
    - Tokens
    - Tickets
    - Single Sign-on (SSO)
    - Multiple Authentication Factors
  - Special considerations on identity management for accountants
- What is Access Management
  - Why are access controls important?
  - Types of access control
  - Layered access controls and "defense in depth"
  - The Process of Accountability
- Access Control Techniques
  - Discretionary Access Controls (DAC)
  - Nondiscretionary Access Controls (NAC)
  - Mandatory Access Controls (MAC)
  - Role-Based Access Controls (RBAC), Task Based Access Controls (TBAC)
- Lattice-Based Access Controls
- Access Control Methodologies and Implementations
  - Access Control Administration
  - Account Administration
  - Account, Log, and Journal Monitoring/Audits
  - Access Rights and Permissions
Opportunities for Financial Professionals

Financial professionals who review and advise clients regarding identity management and access controls as part of their service engagements are well-advised to review the security related materials that make up a key component of the AICPA’s Trust Services Principles and Criteria, information about which is readily available through the Trust Services home page (you can also find a detailed overview and roadmap into these materials as part of the reading that proceeds this document). Given that access controls are important to an entity’s implementation and enforcement of segregation of duties, embodying the “need to know” and proper roles or tasks where financial systems and information are concerned, there should be ample opportunities to consult information related to these topics in the context of designing and maintaining of IT infrastructures, but also during the auditing of such systems, regardless of whether the assessment is being undertaken as part of internal effort, an IT or security engagement, or a financial statement audit.

What is Identity Management?

*Identity management* is meant to support the identification of authorized users. It is a lifecycle activity that involves the establishment, management, and retention (or deletion) of identity information, as well as user enrollment in a system defined by individual and group memberships that assign various levels of access to resources based on business roles and responsibilities. Identity management is an integrated system of business processes, policies, and technologies that facilitates business-critical control activities related to physical and logical access.

Identity management systems are the machinery and mechanisms involved in identifying individuals within an access-controlled environment. Users are labeled as *subjects* and all available applications, data, files and resources are called *objects*. Subjects are defined by the object-relates access permissions, rights, or privileges assigned to them.

Conceptually speaking, identity management is an umbrella of techniques and technologies that includes processes, protocols, and procedures to implement, maintain—and when necessary to monitor or audit—user accountability. Although this is the ultimate goal for any protected user-based system, there are several other distinct advantages and benefits. These are described in further detail in the sections that follow.

Identification and Authentication Techniques

Identity is a crucial aspect in any computerized security system. Computer systems identify users in the best way they can—through credentials that are presumably supplied only by authorized parties. Unlike the simple facial or voice recognition that most humans utilize to identify authorized and unauthorized subjects perceptually, computers generally rely upon a trust model based on the face value of whatever credentials users present to assert their identities.

Usernames and passwords are the basis for many authentication systems, but many employ credentials specific to each person. Each distinct type of identification—password or passphrase, physical token or device, biological measurement, and so forth—counts as a separate identification factor. Employing combinations of individual factors and increasing the complexity of the individual factors used to assert or establish identity increases the security value of a given system. Multiple factors are more secure than
single factors, and more complex factors are generally more secure than those involving less detail. That said, each type of identity factor has its relative strengths and weaknesses.

There are three primary types of authentication factors. A Type 1 factor is something you know (such as a password, a PIN, or numeric combination). A Type 2 factor is something you have (which might be a smart card, a token or a physical key). A Type 3 factor is something you are (this could mean sensing or measuring some part of your body or your physical behavior, such as a thumb- or fingerprint, or a retinal or voice pattern). Individual elements are examined below.

**Passwords**

Clearly the most common and obvious form of authentication factor is the password. By the same token, a password is also generally the most weakly chosen and poorly implemented form of authentication and security. The reasons for this are many and varied.

The largest contributors to weak passwords are the users themselves. Humans are creatures of habit, and the easier something is to repeat or remember the more habit-forming it is likely to become. Simple passwords that are easy to recall, such as special dates, child or pet names, favorite colors, music preferences, and other personal preferences often serve as the basis for user-determined passwords. On the other hand, complex passwords that are easily forgotten are often written down making it easy for others to obtain them. Recording passwords and storing them in insecure locations is an ill-advised practice perpetrated out of habit. None-the-less, it occurs with surprising frequency in many companies and organizations, admonitions and cautions to the contrary notwithstanding.

Apart from casual observation, weakly-chosen passwords can also be intercepted, stolen, or guessed using automated brute force applications that can cycle through tens of thousands of attempts in a matter of seconds. Passwords may be transmitted in the clear using some common but insecure Internet protocols, used in publicly-accessible terminals (Internet cafes), or sent to unwanted third parties (such as fraudulent online banking sites). Accordingly, some secure systems enforce password expiration, minimum password lengths, minimum complexity, and maximum authentication requirements. Unfortunately there is little any secure system can do, regardless of its inherent complexity, to protect against weak passwords or ineffective password policies.

**Biometrics**

A biometric authentication factor (Type 3) invariably draws upon some behavioral or physiological aspect unique to individual subjects. Fingerprints, facial identification, hand geography, keystroke analysis, palm topography, retinal or iris scans, signature dynamics and voice recognition are all recognized Type 3 factors. All of them proffer unique properties that depend on certain physical characteristics of the individuals who supply them for authentication.

Biometric device successes and failures are rated according to false negative and false positive authentication results. Many systems utilize sensitivity adjustment controls to fine-tune these results. Systems can fail by denying authentication to valid users or by accepting authentication from invalid users. The ratio of inappropriate rejections to valid authentications is known as the False Rejection Rate (FRR) and the ratio of erroneous authentications to valid authentications is the False Acceptance Rate (FAR). For the various Type 3 authentication factors mentioned in the preceding paragraph those that are most popular seek to minimize FRR and FAR. The most widely used Type 3 factors today include iris scans, voice recognition, and palm topography.
**Tokens**

Hardware and software *security tokens* are Type 2 factors that generate passwords for subjects that possess them and present them for authentication purposes. Token devices can rely on static information (such as a debit card), synchronous or asynchronous (one-time) passwords (as with RSA SecurID cards), or utilize challenge-response software in which an authentication server queries the device with a challenge, and the device responds with appropriate data.

Static tokens are the most common token devices in use today—they may take the form of plastic cards, flash or magnetic storage drives, or physical locks—and are readily available. Static tokens usually require at least one additional authentication factor (a 4-digit PIN, or password) and many provide access to a cryptographic private key, digital signature, or encrypted credentials stored securely on the devices themselves. Asynchronous dynamic password tokens generate event-based passwords (which may use proprietary random value generators or timing values for network packet arrivals or keypress intervals) whereas synchronous dynamic password tokens generate passwords at fixed periodic intervals. Finally, challenge-response systems are based on interactions instructed by the authentication host, and use built-in circuitry or a collection of stored values to produce responses to challenges presented.

**Tickets**

*Ticket authentication* mechanisms employ third-party entities to verify user identities and validate user authentications. A security *ticket* is a unique number or packet of information that corresponds to a client on a network server. This ticket can be delivered locally or remotely as proof of authentication or authorization. Tickets are deliberately constructed to be sufficiently long and complex that they cannot be easily faked or forged.

Tickets are electronic credentials that verify users and vouch for their identities on secured computer systems. A ticket may utilize an encrypted protocol message to provide that authentication or may itself be an access key conveyed across the network through messaging to permit subjects to access objects. Once a ticket expires, its authentication becomes invalid and the subject must request a new one. The Kerberos system originally developed as part of MIT’s Project Athena is probably the best-known ticket-based authentication system in wide use today.

**Single Sign-on**

*Single sign-on (SSO)* mechanisms authenticate subjects once in a single place and provide unrestricted access to multiple networks and systems (based on the users rights and permissions) thereafter. Once authenticated on an SSO system, users may freely utilize broader network resources without repeatedly authenticating across system and network boundaries. SSO is a double-edged sword: it provides unrestricted access for both legitimate users and also malefactors who manage to jump the system’s authentication hurdles.

The term *enterprise reduced sign-on (RSO)* refers to the same process, with the distinction that SSO is impractical without a homogenous IT infrastructure. SSO is a visible benefit wherever a single-entity authentication scheme exists or where centralized user databases are in ubiquitous use. All information processing systems can leverage a single database or central repository for account sign-on and user identity information for organized-wide authorization and access purposes. RSO lowers the bar somewhat, but requires multiple authentication systems to exchange data correctly and transparently in the background.
Multiple Authentication Factors

Strong authentication techniques require two or more methods of identification to be presented before authenticating any subjects. For example, a two-factor authentication scheme requires two distinct and disjoint pieces of information to be presented to establish an identity, which may or may not be different factors. For example, a user must supply a logon name and two passwords (similar factors) or an identity card and a fingerprint (different factors). Security for two-factor authentication systems is considerably stronger where different authentication factors are utilized.

Several competing types of authentication factor apply here: security tokens, biometric properties, mobile phones, smart cards and various others. Using multiple authentication factors significantly raises the bar for those who challenge the system even where one or more factors can be faked, forged or fooled (including fingerprints and retinal scans). Despite the apparent security advantages of multi-factor authentication, its adoption and usage is not yet widespread.

Special considerations on identity management for accountants

Given the importance and sensitivity of financial information, and of managing access to the systems, applications and functions that support the execution of financial transactions and management of accounting information and processes, financial professionals are wise to consider carefully how identity management is practiced in a given IT environment and what kind(s) of hurdles their users must surmount before access is permitted. Just as it is typical to require additional approvals for transactions that exceed certain thresholds, it also makes sense to require authorized users to present additional (and additionally secure) credentials as the systems and information to which they have access presents a greater risk for losses, errors and theft to occur, and then again as the potential materiality of such errors, losses and thefts escalate.

Thus, for example, users with access to payroll system may be required to present a valid account and a strong password to initiate check runs, but then required to present a SmartCard or other token device to update salary amounts for raises, bonuses, or other changes to payment amounts. Likewise, individuals who can issue expense checks or make routine petty cash payments may only need to present a valid account and a strong password to process such payments, but those same (or other) individuals may then be required to provide a valid voiceprint or hand scan before being allowed to issue checks in excess of $10,000.

Accountants, CFOs, and financial analysts should be aware of the risks associated with authentication schemes currently in use to protect financial information and activity within their organizations. Where current implementations appear to pose potential risks of loss or misuse, it is their responsibility to recommend stronger authentication technologies, and perhaps to lobby for implementations where the number and strength of authentication factors increases in proportion to the potential losses that could occur because of fraud or misuse.

What is Access Management?

Simply put, Access management is the control exerted over the user’s ability to see, use, change, or delete applications or resources, or to access system or application functionality within a computer network. Access control involves the regulation and restriction of user access to controlled information and functionality.

Managing access to sensitive network and application resources is a far-reaching problem with roots in a diverse range of applications and services that need to be secured. Managers of network resources and
repositories and those responsible for monitoring and testing access controls must understand the importance of clear, well-documented and well-defined access policies that correspond to its confidentiality or sensitivity level, or to the level of harm or loss that unwanted or unauthorized access (or loss) could produce, and take appropriate segregation of duties into consideration.

**Why are access controls important?**

Access controls are instrumental to managing user access to system resources and maintaining the extent of that relationship. Authentication allows subjects to identify themselves on a network or within an application, while access controls permit them to access and utilize protected resources appropriate to their established identity. As noted above, access controls not only apply to information and data repositories, but also to applications and processes. This makes access controls extremely important for the functional security of any information system or environment, since applications and processes are subject to manipulation only by those users with adequate security clearance or permission.

Access carries the implication of risk. Confining user access to select elements helps to minimize this risk by restraining the user’s ability to execute erroneous or fraudulent activities, confining their authorization to specific thresholds, and supporting a strong system of checks and balances that helps to limit their ability to disguise or cover-up errors and fraud.

**Types of Access Control**

Access controls preserve the availability, protect the confidentiality and support the integrity of the objects (information, processes and resources) residing on a given system. Under this conceptual umbrella is a diversity of multidisciplinary platforms, procedures, processes and protocols.

Access controls are divided into several categories according to their functional purposes, showing visible overlap in some cases. Brief descriptions for each categorical entry are as follows:

- **Preventive** access controls stop unwanted or unauthorized activity from occurring. They include biometrics, fences and locks; data classification, job rotation and separation of duties; and auditing, cryptography and monitoring.

- **Deterrent** access controls discourage the violation of security policies, often filling the gap left by preventive controls. They include gates, keyed-access and security guards; badges, cameras and intrusion alarms; or awareness training, separation of duties and security clearances.

- **Detective** access controls discover unwanted or unauthorized activity but often take effect after an incident has occurred as opposed to before or during its occurrence. Examples include: guard dogs, security patrols and security badges; security cameras, motion detectors and sound alarms; or incident investigations, supervisory review, audits, and violation or exception reports.

- **Corrective** access controls restore systems to a known-good state following a security-related breach or incident. Examples include: access termination, service restarting or system rebooting; the implementation of intrusion detection systems, antivirus programs and malware scanners; or business continuity planning, disaster recovery planning and security policies.

- **Recovery** access control is used to repair and restore critically-damaged capabilities, functions and resources following a security violation. These are more complex in scale and scope than corrective controls and include: backups, rollbacks and restorations; fault-tolerance, redundancy and clustering; or antivirus scanners, database shadowing and data replication.
• Compensation access control provides aid to various other existing controls in the enforcement of system-wide security policies. Examples include: security policies, operational requirements or utilization criteria; or personnel supervision, monitoring and work procedures.

• Directive access control confines and controls the actions of subjects to enforce and encourage strict security policy compliance. Examples include: security guards, guard dogs and security cameras; policy requirements, security criteria and posted notifications; or escape routes, employee supervision and awareness training.

• Administrative access control encompasses the organizationally-defined policies and procedures that govern overall access, focusing on personnel and business practices. Such examples include: workplace policies, procedures and hiring practices; background checks, data classification and security training; or work reviews, employee supervision and personnel controls.

• Logical or technical access controls are hardware and software mechanisms that manage access to and provide protection for shared computer and network resources. Examples include: encryption, passwords and smartcards; access control lists, biometrics and constrained interfaces; or cryptographic protocols, firewall appliances and network routers.

• Physical access controls are structural barriers emplaced to prevent direct access to components of a facility, network or system. Examples include: security guards, guard dogs and fences; alarm systems, motion detectors and security windows; or security lights, security locks and video cameras.

**Layered Access Controls and “Defense in Depth”**

Access controls in and of themselves are insufficient to individually protect entire network infrastructures and system resources. Most environments utilize several forms of access control in a more comprehensive manner to provide greater security coverage. All this comes as part of a defense in depth strategy that perceives individual security elements as smaller components within a much larger, more functional security framework.

Several concentric circles of protection envelop assets and resources within logical rings of security processes, protocols, or procedures. Would-be attackers must then penetrate several differing aspects and different layers of the security framework to make unauthorized use of a protected system or network resources.

**The Process of Accountability**

A principle tenet and primary function of access control systems is to manage and allow for monitoring and accountability. The individual activities and actions that users perform on systems, the resources they access and the connections they establish are all part of their accountability factor. Identification, authentication, authorization and auditing are several components in maintaining user accountability.

• Identification refers to the processes and procedures through which specific subjects are proven authentic, accredited with permissions and held accountable for individual actions and activities. In the context of computerized systems, authentication generally requires that users supply identities (logon names, ID cards) and credentials (passwords, PINs) to prove credibility and maintain accountability.
Authentication is the process of verifying that a given identity is valid by requiring that subjects provide private information that corresponds to and is known only to the identity in question. It is also used to establish validity of messages, transmissions and originators of activities on protected systems.

Authorization is the process of determining the types and extent of activities that are permissible to established users or groups on a protected system. This determines whether clients may utilize services, applications may make connections, or users may utilize resources or perform network and application functions.

Auditing is the process of formally examining and reviewing activities, applications and processes initiated by users (or other applications and processes) on a system. This systematic monitoring of activity can be used to detect malicious activity and investigate non-compliance issues.

Accordingly, there are several different types of access control techniques used to facilitate these accountability-based methodologies.

**Access Control Techniques**

Access control techniques are the deployment mechanisms and component implementations that facilitate authorized access to protected resources. These are the elements that enforce the logical control techniques that define how subjects can access objects and to what extent.

There are several methods of limiting access to authorized persons and personnel, based on roles, rules or responsibilities. Other controls are based on individual identities and membership within various predefined groups. These techniques provide control coverage to network and application resources including databases, directories, repositories and activities.

**Discretionary Access Controls (DAC)**

Systems using Discretionary Access Controls (DAC) control and define object permissions at the discretion of the originator or owner. Object access is granted or denied to other users in a coarse-grain manner using primitive control values (e.g., read, write, execute) and rudimentary identities (e.g., user, group, other). DACs are usually implemented through Access Control Lists (ACLs) that define the permissions granted and denied to individuals and group subjects. Thus, DAC is account-driven.

DAC does not provide centrally-controlled management because object owners specify object access. However, DAC can include and implement time-based controls, transaction controls and other basic forms of identity-based control (i.e., device or host name, network protocol or address). User privileges can be suspended, resumed or revoked with relative ease under DAC-based systems.

**Nondiscretionary Access Controls (NAC)**

In a system where Nondiscretionary Access Controls (NAC) applies, sets of rules or restrictions control object access. Therefore, access permissions are not specified by originator or owner—NAC does not observe user identities like DAC. Static permissions govern the encompassing environment in a completely centralized manner. Sweeping changes are effected throughout such environments without modifying permissions for individual objects. Thus, NAC is action-driven.

Generally, established NAC rules remain constant throughout their lifetime. Firewall rules are administratively-defined network traffic filters that govern port and protocol transactions. Individual
end-users aren’t taken into account; instead, interactions between endpoints are allowed and denied based on source and destination addresses or ports and permissible (or impermissible) protocol transactions.

**Mandatory Access Controls**

Finally, Mandatory Access Control (MAC) utilizes security classification labels that represent security domains. These security domains are governed by a trust model based on subject labels defined in clearance levels and object levels based on classification. In an indirect way, MAC conceptually combines the account-driven controls of DAC and the action-driven controls of NAC. Technical implementations are completely different.

Under MAC, a subject can access objects of equal or lower classification—operating on a *need to know* basis. Subjects with high clearance levels are granted access to sensitive resources only as their job tasks require. Even with sufficient security clearance, there are instances where a subject is denied access to lowly-classified objects. By design, MAC systems are prohibitive rather than permissive: permission is expressly forbidden unless explicitly allowed.

**Role Based Access Controls (RBAC), Task Based Access Controls (TBAC)**

In a Role-Based Access Control (RBAC) environment, subject access to objects is defined according to job descriptions. On the other hand, Task-Based Access Controls (TBAC) define subject permissions according to job functions. Application controls supporting segregation of duties within an accounting application are an example of TBAC.

Contrasted against previous control methods, RBAC is best utilized in highly volatile environments with frequent personnel changes, rotations or turnovers. Under RBAC, a subject occupying a management position has greater access to organizational resources than a subject performing rudimentary low-level tasks. RBAC isn’t bound to individual or group permissions so subjects with several memberships will be governed by whatever capacities and functions those roles possess. RBAC maps administratively-defined, site-specific security policies directly into an organizations hierarchical and management structures.

**Lattice-Based Access Controls**

Some non-discretionary controls are also considered *lattice-based access controls* where they define upper and lower boundaries of access corresponding to every relationship between subject and object. Boundaries can be arbitrary but they typically adhere to security level labels. Subjects with lattice permissions between *sensitive* and *private* classifications can access resources between those label-based bounds but nothing beyond and outside of them (e.g., confidential, proprietary, public).

Accordingly, subjects are assigned a *least upper bound* and *greatest upper bound* to lattice-based object labels. This form of access control is designed to address the flow of information through computer systems with an emphasis toward maintaining confidentiality where applicable. Lattice-based permissions are a hierarchy of least-to-most privileged security classification labels.
Access Control Methodologies and Implementations

All access control methodologies are divided into two primary categories: centralized and decentralized or distributed. In centralized systems, all authorizations are performed by a single entity within the system. In decentralized systems, authorizations are performed by various entities throughout a system.

Centralized access control methodologies are easily managed by an individual or small workgroup, carry lower administrative overhead and single changes to the system have widespread results. It is also its own single point of failure in that subject and object interactions are compromised when the singular access control system is inaccessible. A Centralized Access Control structure is also easier to audit because the number of access control points is significantly less than in the Decentralized model.

Decentralized access control methodologies generally require medium to large workgroups of individuals and carry higher administrative overhead accordingly. In a decentralized environment, maintaining a homogeneity of equipment and services scales in increasing difficulty with proportion to the number of access control points. Changes effected on individual systems are spread locally, instead of having the wide-reaching consequences and effects of a singular centralized system.

Access Control Administration

The collection of duties, responsibilities and tasks assigned to administrators to manage user accounts, access and accountability is collectively known as access control administration. Access relies upon four principles (identification, authentication, authorization and accountability) related to access control administration to perform three primary responsibilities: account management, activity tracking and access rights.

Account Administration

Lifecycle user management requires establishing, maintaining and terminating user accounts when necessary. Though mundane and routine, this lifecycle process is vital to system access control capabilities without which there would be no accountability.

Account, Log, and Journal Monitoring/Audits

Account auditing, activity tracking and application access are provided through monitoring and logging facilities within access control management. Accountability is also maintained through the inspection and investigation of audit logs and monitoring reports following policy violations and security incidents.

Alert logs, event reports and system journals are accessory elements that correlate to define the context of events as they happened when they occurred. These electronic trails yield clues that are smaller pieces of a much larger puzzle that merge to create a picture of events to support conclusions drawn about an incident.

Access Rights and Permissions

Assigning subject access to objects is an ongoing process that shifts and transitions with time but remains a constant fixture of the business infrastructure. Clients and employees come and go, shift status within the organization or transition to different priority or clearance levels. Their job duties and responsibilities also change with time, bringing new and different permission levels into play. These dynamic values must remain flexible across a constant access control framework.
Rights and permissions are often compartmentalized across departments depending upon user and group memberships. Accountants in payroll have little reason to access network administrator resources and vice versa. A CEO might have direct access to marketing data but marketing employees are expressly prohibited from accessing CEO documents, and so forth. Rights and permissions are varied and change over time.

**Special Considerations on Access Controls for Accountants**

Access controls are of greatest interest to financial professionals of any stripe primarily as they pertain to financial information and systems. The principle of least access, which states that individuals and groups should obtain no more access to information than is necessary for them to do their jobs, and not a whit more, applies nowhere else as clearly as it does to financial data and systems.

Application-based access controls are the means by which segregation of duties are enabled and enforced. Here, conventional separation of duties applies. An A/P accountant responsible for approving invoices for payment should not be authorized to sign checks, etc. Individuals granted permission to disburse or manage funds should be carefully instructed about proper and acceptable behavior. They must also be made aware that formal auditing applies to all such activities not just as a matter of prudence and fiscal responsibility, but also as a matter of law or regulations that govern most forms of corporate and organizational financial activity. This information should be incorporated into Human Resource’s employee handbooks, and made part of the employment agreement that all financial professionals who work for the company or organization must sign.

Among other things, proper management of and accounting for access controls means that periodic financial audits should also include comprehensive investigation into and analysis of the assignment of the controls over financial information and systems. Auditors should consult the appropriate audit standards for clarification. IT is also important to ensure that security and financial policy dictate granting and cancellation of access rights as part of job changes that move individuals into and out of positions with financial involvements within specific time periods following such changes. Recent incidents, such as the rogue trading at Société Générale may have been prevented if proper procedure regarding the removal of access right had been followed and monitored more carefully. Any internal or external penetration testing should include determined attacks on financial systems and information, if only because they are likely to attract the same kind of attention and focus from genuine malefactors.
Reading List: Digital Identity Management and Access Controls

Professional Articles, Websites, and Publications


“Customer Focus Through Identity Management,” Light Reading, 9/11/2007. An overview of identity management, particularly as it pertains to e-business, but with good general coverage of related standards and best practices (see the great list of pointers on page 2), as well as fundamental principles.

“Identity Management Architectures and Digital Identity,” by Phillip Windley, O'Reilly Media. A synopsis of Windley’s Digital Identity book, this article digs into what’s involved in choosing and implementing digital identity infrastructures for various situations and circumstances. Windley’s “Understanding Digital Identity Management” is also a pretty good place to start digging into this subject matter.

“Identity Management,” Dark Reading. A collection of articles from 2008 back to 2006 that touch on various aspects of identity management, and related security concerns or implications.

“Global Technology Audit Guide 9: Identity and Access Management,” Published by the Institute of Internal Auditors, the purpose of this GTAG is to provide insight into what Identity and Access Management (IAM) means to an organization and to suggest internal audit areas for investigation. It can assist CAEs and other internal auditors to understand, analyze, and monitor their organization's IAM processes. A checklist for IAM review is also included in this guide.

DigitalIDWorld is available in both print and digital editions, and its entire focus is on the subject of identity management. Its Identity Related White Papers section includes numerous items under the following headings: Identity Management, Identity Federation, Access Management, Identity Security, and more, plus Standards and Tutorials. Very helpful, but also very vendor/solution oriented.

The Digital Identity Forum is a UK-based professional organization that specializes in research, discussion, and education on the subject of digital identity. In addition to managing an annual and well-attended conference on this subject matter (most recently in November, 2007), the Website makes content (mostly speaker presentations) freely available on its Web pages. The 2006 conference also produced proceedings that have been published in book form as Digital Identity Management, by David G. Birch, Gower/Ashgate, May 23, 2007, ISBN: 0655086794.

Books

access control mechanisms, including role-based access control (RBAC), along with coverage of identity management, trust models, and governing theory behind access control models.

*Digital Identity*, by Phillip Windley, O’Reilly Media, August 1, 2005, ISBN: 0596008783. A concise but compelling and accurate look at how corporations and organizations can provide and deliver security to customers, employees, partners, and suppliers. Founded on the concept of “identity management architecture,” a method for providing protection while also permitting access to authorized users, the book describe what is involved in constructing, protecting, and managing digital identity. Windley’s experience in industry (VP product development at excite@home.com) and government (CIO for the State of Utah under Governor Micheal Leavitt) informs his discussion with detailed, real-world examples and illustrations.


*Mechanics of User Identification and Authentication: Fundamentals of Identity Management*, by Dobromir Todorov, Auerbach, June 18, 2007, ISBN: 1420052195. (Note: Most Auerbach books are best described as massive compilations of expert-authored articles, rather than coherent books; this one is apparently all Todorov’s work). This book provides detailed and comprehensive coverage of the so-called Triple-A (Authentication, Authorization, Accounting/Auditing) topics in information security, though some of the material presented is somewhat out of date (for example, coverage of Windows predates Windows Server 2003).

*Role-Based Access Control*, by David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli, Artech House Publishers, second edition, January 31, 2007, ISBN: 1596931132. A revised and expanded volume on the role-based access control model, including comparison and contrast with other access control models, new RBAC standards, updated case studies and coverage of role engineering and design of role-based systems, as well as tools and frameworks used to administer RBAC environments.