Realtime publishers

"Leading the Conversation"

The Essentials Series

IT Compliance Volume II

sponsored by

SECURE COMPUTING

by Rebecca Herold

Addressing Government Agency Access and Authentication Challenges

by Rebecca Herold, CISSP, CISM, CISA, FLMI ***February 2007***

The Importance of Authentication and Access Control

Authenticating users to access enterprise information resources is a critical component of enterprise information security. Creating technologies that authenticate users with a high degree of confidence has always been a challenge not only because of the typical complexity of the systems but also because of the amount of confidence that must be placed within the end user to appropriately secure his or her own user authentication information, most commonly the user ID and password. This challenge increased exponentially as computing moved from the solely centralized mainframe to decentralized enterprise business processing on multiple, business unit managed servers, and then expanded beyond the perimeter into the Internet and systems owned and managed by business partners.

> Why is authentication important? Significant protection of enterprise information resources depends upon knowing the identity of a user of the network and associated systems.

Access control is another critical component for securing enterprise information resources. Access controls must be established to preserve the confidentiality and integrity of information. Confidentiality requires that only authorized users can read information, and integrity requires that only authorized users can alter information in authorized ways. Authorization and authentication are fundamental components of access control.

> Authentication is a process of determining who you are. Authorization determines what you are allowed to do.

Significant Concerns for Government Information

Over the past several years, the U.S. Government Accountability Office (GAO) has identified the historically poor authentication and access control practices as barriers for successful information sharing not only between government entities but also with the private sector. Since 1997, the GAO has recommended the development of a comprehensive plan for information sharing to support critical infrastructure protection efforts. It continues to be a concern. All government agencies must act to address the significant information security weaknesses within their systems and applications. Authentication and access control practices are two key areas to resolve.

> 🕮 From the GAO's 2007 "High-Risk Series: An Update" which was released on January 31, 2007 (http://www.gao.gov/htext/d07310.html): "To improve existing technology protection programs, agencies need to implement the many GAO recommendations that remain unaddressed. In addition, further action is needed. The legislative and executive branches should strategically examine existing programs, evaluate alternative approaches, and develop a comprehensive framework with clear responsibilities and accountability for identifying and protecting critical technologies."

The concerns are validated through numerous incidents that have recently occurred within federal agencies. Just a sampling of them shows how authorization and/or access controls were vulnerable:

- October 12, 2006—Hackers broke into the Congressional Budget Office's mailing list and sent a phishing email message that appeared to come from the CBO.
- August 20 - 22, 2006—A security breach in the William D. Ford Federal Direct Loan Program within U.S. Department of Education and Federal Student Aid exposed private information of student loan borrowers during a computer software upgrade. Users of the Direct Loans Web site were able to view personal information, including Social Security numbers, of others.
- August 23, 2006—A faulty Web site software upgrade resulted in the exposure of personal information of 21,000 student loan holders on the U.S. Dept. of Education Direct Loan Servicing Online Web site. Information included names, birthdates, Social Security numbers, addresses, phone numbers, and in some cases, account information.

There are also significant concerns with state and local level government agencies. According to a paper released December 21, 2004 by the National Association of State Chief Information Officers (NASCIO), "Who Are You? I Really Wanna Know: E-Authentication and its Privacy Implications," some of the most critical factors impacting information security within the government are authentication and access controls.

> 🕮 E-authentication within the NASCIO report refers to the process of establishing the identity of individuals involved in transactions over the Internet. Get the report from http://www.nascio.org/publications/documents/NASCIO-WhoAreYouEAuthBrief122104.pdf.

The report stresses the need to address authentication risks involved with putting applications and systems on the Internet, raising the awareness of the people authenticated, limiting the amount of personal information used for authentication purposes, and understanding the benefits and risks of identifiers. The concerns are well-founded, as the following examples demonstrate.

At the state level:

- July 16, 2006—The Mississippi Secretary of State's Web site listed more than two million Uniform Commercial Code (UCC) filings in which thousands of individuals' Social Security numbers were exposed.
- June 29, 2006—A hacker broke into a Nebraska Treasurer's Office child-support computer system containing names, Social Security numbers, and other information such as tax identification numbers for 9000 businesses.

At the local level:

- November 16, 2006—The Carson City, Nevada Sheriff's Department reported that at least 50 residents had their credit card information stolen from the department's systems by employees of local businesses.
- November 7, 2006—Hackers broke into the City of Lubbock, Texas' Web site and compromised the online job application database, which included Social Security numbers.
- October 23, 2006—An official from the Illinois Ballot Integrity Project says his organization gained unauthorized access into Chicago's voter database containing the names, Social Security numbers, and birth dates of 1.35 million residents.
- September 20, 2006—The City of Savannah, Georgia's Web site exposed personal information, including name, address, driver's license number, vehicle identification number, and Social Security number, online for 7 months because of improperly configured access controls on the firewall.

Government Initiatives

Over the past few years, there have been various laws and executive orders specifying the actions necessary to improve information sharing for government agencies, particularly since September 11, 2001. Just a few of these include:

- The Homeland Security Act of 2002 required procedures for facilitating homeland security information sharing and established authorities to share different types of information, such as grand jury information; electronic, wire, and oral interception information; and foreign intelligence information.
- The Critical Infrastructure Information Act of 2002 required the establishment of uniform procedures for the receipt, care, and storage of critical infrastructure information that is voluntarily submitted to the federal government.
- The Electronic Government (E-Government) Act of 2002 was designed to enhance the management and promotion of electronic government services and processes and to increase the electronic availability of information to the public. It established the Office of E-Government within the Office of Management and Budget, authorized the use of nearly $350 million over 4 years to fund e-government initiatives, expanded the use of share-in-savings contracts for information technology, and created a statutory chief information officers council.

> 🕮 The E-Government Act of 2002 is located at http://thomas.loc.gov/cgi-bin/query/D?c107:5:./temp/~c107F0ctv1.

- Federal Information Security Management Act (FISMA) of 2002 was passed into law as part of the E-Government Act. Its goals include development of a comprehensive framework to protect the government's information, operations, and assets. FISMA assigns specific responsibilities to federal agencies, the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB), in order to strengthen information system security. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce information technology security risks to an acceptable level. To ensure the adequacy and effectiveness of information security controls, FISMA requires agency program officials, Chief Information Officers, and Inspectors General (IGs) to conduct annual reviews of the agency's information security program and report the results to OMB.

> 🕮 The Federal Information Security Management Act of 2002 is located at http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3844.

- The Homeland Security Presidential Directive 12 (HSPD-12) of 2004 requires a common identification standard using two-factor authentication for federal employees and contractors for gaining physical access to controlled facilities as well as logical access to controlled information systems.

> 🕮 HSPD-12 is located at http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html.

International initiatives, data sharing, and associated requirements have also heightened the need for better security and strengthened authentication and access controls. For example, the U.S. and other members of the Financial Action Task Force (FATF), an inter-governmental policy-making body created to develop and promote national and international policies to combat money laundering and terrorist financing, have attempted to address these issues in a global context by adopting international standards. FATF Special Recommendation VII requires countries to mandate that cross-border funds transfers of more than a specified amount contain accurate and meaningful information about the person originating the transfer. This information must include:

- Name of the originator
- Location of the account
- Account number, if one exists, or a unique reference number
- Address of the originator, or national identity number, customer identification number, or date or place of birth if the country permits

Authentication and Access Control Challenges

Implementation of effective authentication and access controls to meet the requirements of these various laws and directives will be challenging to all government agencies. The challenges must be met with thorough and careful planning.

Certification and Accreditation

Government agencies must have their information security programs certified and accredited. The National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 1000, National Information Assurance Certification and Accreditation Process (NIACAP), establishes the minimum national standards for certifying and accrediting government agency security systems. This process provides a standard set of activities, general tasks, and a management structure to certify and accredit systems that will maintain the Information Assurance (IA) and security posture of a system or site. Security test and evaluation validates the correct implementation of identification and authentication, audit capabilities, access controls, object reuse, trusted recovery, and network connection rule compliance. Individual tests evaluate system conformance with the requirements, mission, environment, and architecture as defined in the System Security Authorization Agreement (SSAA).

> 🕮 The National Information Assurance Certification and Accreditation Process (NIACAP) is located at http://www.cnss.gov/Assets/pdf/nstissi_1000.pdf.

Unique Requirements

Some laws that government agencies must follow have very specific and unique information security requirements. Consider HSPD-12 in particular. The NIST Computer Security Division developed Federal Information Processing Standard (FIPS) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors to satisfy the requirements of HSPD-12.

> 🕮 FIPS 201 is located at http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf.

At a high level, FIPS 201 standards require agencies to:

- Properly protect the personal privacy of all subscribers of the PIV system
- Authenticate identity source documents to obtain the correct legal name of the person applying for a PIV card
- Electronically obtain and store appropriate biometric data, such as fingerprints and facial images, from the PIV system subscriber
- Create a PIV card that is personalized with data needed to grant access to the subscriber to federal facilities and information systems
- Assure appropriate levels of security for applications and access to information
- Provide interoperability among federal organizations

There are many issues involved with implementation of the standards. Just a few of the issues CIOs must consider include:

- HSPD-12 and FIPS 201 compliance activities are unfunded mandates. Costs may be significant.
- Background checks must likely be performed on most, if not all, existing employees and contractors, along with the ongoing costs for these activities.
- Replacement IDs must likely be issued for most, if not all, existing employees and contractors, along with the ongoing costs for issuing new IDs.
- Badge scanners for buildings and individual computers will need to be chosen, purchased, and implemented. It is likely most agencies will need to upgrade systems and modify applications to handle the cards.

Compliance Challenges

Implementing Two Factor Authentication

There will be challenges to meeting the authentication requirements of these standards. Historically, the most common method of authentication was using a password or personal identification number (PIN). This typically was the only component necessary in conjunction with the ID to authenticate; called "single factor authentication." This was the "something you know" component of authentication.

Other components of authentication can include either "something you have," such as a driver's license or smart card, or "something you are," such as a type of biometrics. Using two of these three components is commonly called two-factor authentication. HSPD-12 requires two-factor authentication in addition to using "secure and reliable identification."

The standard single factor username/password or PIN authentication method can no longer provide adequately secured authentication. The availability of sniffers and password/PIN cracking tools used to defeat single-factor authentication has removed accountability for the activities that occur through the ID. In addition to these tools, bad habits, such as users choosing easy-to-guess passwords or writing down and leaving passwords in conspicuous places, also put secure authentication of the actual individual at risk.

Using two-factor authentication significantly enhances security by ensuring that all authentication must be carried out using this additional component that only the user is supposed to possess, making the user accountable for the actions on the system and removing the ability for freely available tools to be used to defeat the authentication system.

Don't Overlook Important Components

Organizations must remember that authentication issues go beyond the network perimeter:

- Organizations will need to implement additional components, such as PKI readers, fingerprint readers, or other mechanisms, on mobile computers and mobile media devices to meet the two-factor authentication requirement.
- Remote access components will need to be changed to incorporate two-factor authentication.
- Business continuity plans and tools must account for supporting two-factor authentication and strong access controls.
- Reporting, logging, and audit capabilities must exist to indisputably document all access attempts into the network as well as resources that were accessed upon successful authentication.

Identity Verification

Typically birth certificates, passports, and visa applications were used to verify the identities of individuals when authorizing them to access government systems and applications. The September 11, 2001 attacks raised concerns about the integrity of identity documents such as passports and visa applications because the terrorists responsible for the attacks reportedly used such documents to board the planes that were hijacked. HSPD-12 requires secure and reliable identification that:

- "Is issued based on sound criteria for verifying an individual employee's identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically
- Is issued only by providers whose reliability has been established by an official accreditation process."

Implement a PIV Management Strategy

Agencies need to establish a sound PIV management strategy. They need to create an effective user ID enrollment procedure as well as well-defined and documented issuance and management procedures. This is not just an electronic information logical access issue. Agencies must also implement procedures to control physical access to areas where information on the network is accessed and where physical information processing resources, such as servers, are located. These procedures must include how to terminate these logical and physical access authorizations.

Implementing Appropriate Access Controls

To be most effective and cost efficient, the chosen access control system should have components able to integrate each authorized individuals' access to physical and logical resources. The system should

- Be compatible with the physical facility security devices, such as parking gates, building entrances, and so on
- Control logical access to all types of network resources, such as databases, workstations, applications, and so on
- Be able to restrict access to only the resources necessary to perform job responsibilities; this will typically consist of being able to establish access privileges through such mechanisms as Access Control Lists (ACLs)

Meeting Compliance Requirements Is Possible

Meeting compliance requirements with all the many laws and regulations can seem overwhelming, and sometimes impossible. However, it can be helpful to look at an organization that has succeeded in meeting this compliance challenge. Orange County, California is a good case in point.

Orange County's network delivers a wide range of services to public agencies throughout the county. Each county agency is responsible for managing their own user IDs and associated access controls but they each need access to certain services and resources on the core network, such as mainframe data, terminal services, and other custom applications.

A challenge for Orange County network administrators was the inability to restrict and track access of additional connections once outside agencies had made the initial connection with the core terminal server. Synchronization with the scattered agency systems was critical to ensure that user data was properly shared between agencies, minimizing redundant data, and reducing the cost and resources necessary to maintain data across several systems.

After careful consideration and risk analysis, Orange County established several key requirements:

- Create a single portal entry point into the network.
- Deploy and enforce a centralized information resource access policy from users in outside agencies.
- Establish and implement a centralized user domain in Microsoft Active Directory (AD) that leverages data from each outside agency's existing AD systems.
- Implement a single sign-on (SSO) capability to reduce the number of logins needed throughout the network for users from outside agencies.

Orange County implemented SafeWord SecureWire from Secure Computing (http://www.securecomputing.com) to

- Connect the outside agencies to the centralized network through a single portal
- Create an enterprise-wide, policy-driven access control system with SSO for applications
- Standardize the authentication protocols, utilizing tokens for the two-factor authentication
- Create audit trails to track and enforce access policies for each individual within the central outside agencies
- Manage the existing infrastructure using AD tools

Successful Compliance Will Result in Improved Security and Privacy

The old information security practices typically used within most government agencies are not only inadequate for today's new security threats, as a review of recent incidents demonstrates, they also will not meet the many new legal requirements. It is time to strengthen security and better protect information security and privacy within government agencies.

When implementing authentication and access control compliance solutions, it will be important to:

- Understand the information security and privacy risks associated with different methods of authentication.
- Choose authentication methods to minimize information security and privacy risks consistent with the need for security in a transaction, due to the flow of personal information in the process of authentication.
- Conduct risk assessments to establish appropriate levels of authentication for different transactions.
- Understand the importance of cross-boundary cooperation when different jurisdictions are involved in authentication.
- Involve IT specialists, information security specialists, and privacy specialists in designing authentication systems.