Identity and Access Management

Table of Contents

Getting Started

Inter-institutional collaboration, cloud computing, online/distance education, teleworking and portable computing, federation, access from anywhere at anytime, and many other business needs are challenging institutions of higher education to adapt or rebuild their Identity and Access Management (IAM) infrastructures to enable new and secure ways to further their missions as well as meet requirements from Federal and State government, industry standards, and an increasing number of business associates and partners. To get started with IAM projects, big or small:

1. **Define** the challenge and the approach to meet it.
    - Clearly understand and articulate the institution's IAM desired state, target services, target users, and impacted functions (e.g. single-sign on, two-factor, federation, automation of IAM processes, etc.).
    - Define the approach needed to meet the challenge (i.e., high-level description of policies, technology, business processes that need to be addressed).
2. **Define** the business and regulatory drivers and their importance to the institution's missions. Examples include:
    - Federal and State regulations.
    - New constituencies (e.g., online students, student apps and parents, alumni sand retirees, contractors and service providers, patients, peers and collaborators, etc.).
    - Centralization of distributed services including authentication.
    - Improve information security, confidentiality, and user privacy by minimizing the collection, maintenance, and use of identity information.
    - Improved user experience (e.g., reduced sign-on, self-services, remote access and telecommuting, etc.).
3. **Define and document** the Institution's current IAM posture.
    - Does the institution have policies for identity and access management, information technology, and information security in place?
    - What is the institution's IAM and policy governance approach?
    - What is the degree of centralization? Are authentication decisions made by system, by application, by department or centralized (e.g., LDAP)?
    - How are users affiliated to the institution? Can they have multiple types of affiliations?
    - How are identifiers and credentials issued to users? Is the provisioning process consistent throughout the institution? In-person vetting? Is self-service capability available for password resets?
    - Are authentication requirements for applications and services risk-based?
    - Does the institution have an information technology roadmap? (e.g., EDUCAUSE Identity and Access Management (IAM) Tools and Effective Practices, NMI-EDIT Enterprise Directory Implementation Roadmap, or NMI-EDIT Enterprise Authentication Implementation Roadmap)
4. **Determine** the gaps between the Institutions current IAM posture and the desired state, target services, and target users.
    - Map a matrix of the target users and target services and determine the required policies, processes, and technology considering the risk and the business and regulatory requirements.
5. **Identify** project stakeholders and determine who should be involved and the level and timing of their involvement. Training and communication early and often are critical.
6. **Develop** the policy framework.
    - Roles and responsibilities.
    - What is required to identify users?
    - What criteria is used to determine the types of credentials used?
    - What criteria is used to determine the level of access to applications and services?
    - What is required from identity providers and from service providers?
7. **Develop** the required business processes. What steps are required to:
    - Identify and register a user?
    - To provision and de-provision credentials?
    - To provide support and training?
    - To request, grant, and modify access to applications and services?
8. **Develop** the technology framework.
    - Source of Authority systems.
    - Authentication protocols and technologies.
    - Approaches and products.
    - Staff and skill sets.

Top of page

Overview

Access control is the use of administrative, physical, or technical security features to manage how users and systems communicate and interact with other information resources.

Access is the flow of information between an entity requesting access to a resource or data and the resource. The entity can be a device, process, or a user. Access control is any mechanism by which a system grants or revokes the right to access some data, or perform an action. Normally, an entity must first login to the resource using some authentication system. If the entity provides proper credentials, they are allowed to login. Next, the Access Control mechanism controls what operations the entity may or may not make by comparing the credentials provided to an access control list.

Examples of access control:

- When a user is prompted to provide a username and password to be able to access EDUCAUSE resources (e.g., this guide).
- Upon logging in, the user attempts to Edit a resource (e.g., this guide section) and the user is denied since that user does not have the access to edit an EDUCAUSE resource.
- Since the user was denied access, the user requests to be given rights to edit the resource. Upon verification of membership in an EDUCAUSE Working Group and establishing the business need, the user is added to the list of users that have the right to edit the resource.

Top of page

Business Requirements of Identity Management and Access Control

Objective: To describe what institutions must consider when establishing and documenting the rules that control access, authorization, and dissemination of information and restricting the access to institutional networks.

As depicted below, *the business requirements that drive access control needs, practices, and scope are often diverse.*

blocked URL

1. Access Control Decisions

Institutions of higher education create, collect, and makes available information in support of their educational, healthcare, and research missions. This information must be administered and protected in accordance to its value, and in conformance with government, and institutional rules and regulations.

Institutional staff, faculty, students, retirees, alumni, prospective students, student's parents, and members of the community access and utilize different types of information stored on and accessible via institutional systems. Examples include:

- Students
  - Learning resources such as course management systems or online access to the library
  - Online student systems such as class schedules and bill payment
- Staff
  - Employee directory, webmail
  - Online human resources systems such as timesheets, payroll, and benefits
- Faculty and Researchers
  - Online course materials and library resources
  - Federal research agencies, funding, and data resources
- Alumni and Donors
  - Email for life
  - Alumni directories and services
- Parents
  - Tuition Payments
- All
  - Student/Employee directory
  - Emergency notification systems

University data governance policies and standards should define roles that can evaluate, approve and assign the level of access to systems and data based on the responsibilities, job functions, reporting or outreach requirements of users. The level of access will be based on the confidentiality of the data and the restrictions imposed by government and institutional rules and regulations. Effectively managing this access requires clear methods for documenting who has access to systems at any given time and mechanisms for periodic audit reviews of the users to ensure that access is given only to appropriate individuals.

Related links and additional information:

- For a list of common business situations in higher education that call for access management solutions see Access Management Use Cases Organized by Area of Interest.
- The Aegis Identity Survey White Paper - Trends in Identity & Access Management Solutions in Institutions of Higher Education - 2012 contains a detailed analysis of identity and access management technologies as they relate to university business drivers, challenges; strategic approaches towards related technology; and the effects of emerging technologies on identity and access management infrastructure.
- See Electronic Identity: The Foundation of the Connected Age, for an analysis of the increasing importance of trusted electronic identities in higher education.
- See Information Security or Identity and Access Management? for an overview of the overlap that exist between information security and IAM and what the University of Massachusetts and the University of Chicago are doing to bridge the gaps that may exist between the two practices.
- Watch a recording of the ECAR Working Group's Data Stewardship and Governance in Higher Education for an overview of effective practices in establishing institutional data stewards and data governance.

1a. Centralized Access Control

Rather than maintaining separate accounts on each system, some institutions use a central account database that all systems can authenticate against. In many environments, a Windows domain controller functions as the central authentication system. Other institutions use Kerberos because it supports a broader range of applications and operating systems. However, because Windows systems work best in a Windows domain, even institutions that use Kerberos generally maintain a Windows domain controller that is synchronized with the accounts in their Kerberos domain. Lightweight Directory Access Protocol also known as LDAP is another approach to centralized authentication and authorization that is increasingly used in higher education institutions.

1b. Decentralized Access Control

It is not uncommon to find institutions opting for decentralized or distributed user account databases where the verification of authorization is performed by various entities located throughout the campus. Common disadvantages of decentralized access control are that they can be duplicative, require coordinated work of several teams, and administrative overhead is high since changes may need to be implemented by numerous locations. One drawback is that each location may be maintained by local administrators without the input / coordination of the other teams. Decentralized access control implementations do have benefits. A well implemented and coordinated distributed system does not have single point of failure. If one access control point fails, others can balance the load until the problem is resolved.

2. Access Control Policy

Access control policies should clearly communicate the institution's business requirements regarding identification of users, access to institutional information, user access rights, and special access privileges and restrictions. Institutions should ensure that their policies comply with any applicable regulatory requirements such as those currently affecting access to student financial aid information and Controlled Unclassified Information (CUI). Many in the higher education community demonstrate compliance by applying the access control requirements in NIST 800-171. The following could comprise the core of an institutional access control policy framework.

- Roles and responsibilities
    - Need-to-Know: Access only to information needed to perform assigned tasks.
    - Need-to-Use: Access only to information resources needed to perform assigned tasks
    - Access levels and privileges by role
    - Periodic review and removal of access levels and privileges
    - Segregation of duties for requesting, authorizing, and reviewing access levels and privileges
- What is required to identify users?
    - Requirement for vetting users in person
    - Requirement to archive records concerning user identification and credentialing
- What criteria is used to determine the types of credentials used?
- What criteria is used to determine the level of access to applications and services?
    - Identification of roles with privileged access
    - Contractual obligations for limiting access granted to vendors and partners
- What is required from identity providers and from service providers?
    - Requirement to identify the security requirements of applications - both, purchased and developed internally
    - Requirement to determine the Level of Authentication (LOA) required to access a service based on risk

The EDUCAUSE Access Control page contains publications, presentations, policies, podcasts, and blogs regarding mechanisms by which a system grants or revokes the right to access some data, or perform some action.

3. Access Control Program

As data, access, and networks continue to expand, institutions have an increasing need to manage identities and access. The optimum solution for this function may be a well-planned and institution-wide Identity and Access Management (IAM) program. In its simplest form, IAM ensures that only the right people can access the right services at the right time.

Identity and access management refers to the policies, processes, and technologies that establish user identities and enforce rules about access to digital resources. In a campus setting, many information systems–such as e-mail, learning management systems, library databases, and grid computing applications–require users to authenticate themselves (typically with a username and password). An authorization process then determines which systems an authenticated user is permitted to access. With an enterprise identity management system, rather than having separate credentials for each system, a user can employ a single digital identity to access all resources to which the user is entitled.

However, within a complex organization, establishing an IAM program is not an easy task. Many stakeholders, technology areas, policies and processes must work together for a scalable and robust IAM Program. In addition, governance plays a key role in the success of any IAM Program and implementation.

blocked URL

IAM Programs Seek To Securely Manage Digital Identities Through Their LifeCycle

Note: It is important to remember that the identity life-cycle applies for each type of relationship or affiliation that an individual may have with institution. They may have multiple simultaneous roles (e.g., faculty & staff members, students, and full-time employee).

It is important to keep in mind that the current model for managing identity becomes more problematic when relationship complexity is added. IAM systems in the future will need to transition to entity relationship management that includes users (people), devices, and services.

Top of page

User Access Management

Objective: To cover of the stages of user access life-cycle - from determining the types and affiliation of institutional users and their corresponding privileges to procedures to revoke and disable their access.

1. User Types and Affiliations

Institutions of higher education have a broad user base with varying degrees of affiliation. One thing in common among all members of an institution's constituency is that all require access to some type of institutional information for a determined amount of time - they all become users.

At a high level, institutions can divide Users into two groups based on their type of affiliation to the institution:

- Formal Affiliation: These are users whose affiliation to the institution is established by formal contract, employment, or enrollment. Users in this group include staff members, employee, faculty, researchers, and students.
- Casual Affiliation: These are users whose affiliation to the institution is transitory, periodic, mostly informational and not established by a contract or enrollment. Users in this group include guests, retirees, donors, parents, library patrons, alumni, and external vendors.

Furthermore, a considerable number of Users have multiple affiliations depending on the number of "hats" an individual wears while affiliated to an institution. Examples:

- Administrators with Faculty appointments
- Student Staff
- Staff or Faculty and Parent of Applicant or Student
- Staff and Alumni
- Staff and Employees who are also Students pursuing a degree
- Emeriti Faculty

Lastly, it is important to understand the affiliation life-cycles and User transitions that should inform an institution's User Access Management process. Examples:

- Student Student/Worker Employee/Staff/Faculty Retiree
- Student Alumni/Donor
- Applicant Employee/Staff/Faculty Former employee
- Prospective/Expected User Active User Deactivated User Deleted User

The examples above are one-dimensional and serial. As stated above, many times these can be multi-dimensional and cyclical.

2. User Registration

Identification is the process of ensuring that a user, program, or device is the entity it claims to be.

The User registration process generally has four steps:

1. Identity Vetting: the collection and validation of identity information. This information may include full name as it appears in identity documents, date of birth, current address, existing relationship with institution (e.g, hired employee, enrolled student, etc.)
2. Identity Proofing – aligning collected data and matching an actual person to it. This can be done either:
    - By leveraging a pre-existing relationship with an individual (e.g., individual was a former student or a former employee)
    - In-person. The individual is required to go to the institutional office charged with User registration and produce a valid current government photo ID that contains the individual's picture (e.g., driver's license or passport) and an address. The office compares the picture to the person, verifies the information with its records and, if everything checks, records the sources of proof and approves the issue of a credential.
    - Remotely. If the individual is unable to fulfill the proofing requirements in-person (e.g., staff in a small satellite campus, researcher in the field in a different country/continent), they can utilize approved University secure file exchange services to send electronic imprints of identity materials along with supporting documentation. The office contacts the corresponding agencies and verifies the information provided with their records, and, if everything checks, records the sources of proof and approves the issue of a credential.
3. Creation of a master identity record
4. Issuance of credentials - each credential issued shall include a unique identifier (e.g., UserId) that distinguishes it from all other credentials issued to the individual and shall clearly associate the credential unique identifier to the individual's master identity record. Credentials are usually issued as an UserId / Password pair but they can also be embedded in other devices such as Id Cards, second factor tokens (See Two-Factor Authentication topic below)

Related links and additional information:

- See UM Community System: Expanding Identity Boundaries for the University of Maryland's approach to establishing UM identities to users outside the traditional campus user base such as volunteers, visiting students, or contractors.
- See Provisioning Remote Users for a discussion of the general challenges of provisioning remote users and the specific impact of HEOA regulatory requirements that ask accrediting organizations to evaluate college identity procedures for distance education students.
- See Identity Verification for the University of Indiana's approach to verify the identity of affiliated individuals including alternatives for verifying an identity when in-person vetting is not an option.
- See CommIT: Simplifying Admissions Identity Management for Georgetown University's way to leverage federated identity management to match electronic records for college applicants and institutions using a single set of user credentials that can be used across various services.

3. Privilege Management

Privilege management is the set of processes for managing user attributes and policies that determine a user's access rights to an information resource. In other words, the user attributes, job functions, and organizational affiliations can serve as the basis for access authorization decisions. Users should be granted access based on least privilege - the most restrictive set of permissions or access rights - needed to perform assigned work tasks.

Some data may be restricted from general access by users and may require additional levels of approval before being made available. Users are granted access to this data on a need-to-know basis - when there are justified work-related reasons for access or the need to know. An important characteristic of need-to-know access is that access is granted for a limited period of time. When the reasons for access are no longer valid, access to the data is (or should be) revoked.

Two common problems related to privilege management are excessive privilege and creeping privilege. The former happens when a user has more access or permissions than the assigned work tasks and/or role requires. The latter happens when a user account accumulates privileges over time as roles and assigned work tasks change. Both problems are addressed by periodic review of user access rights.

Management of Administrative privileges is important since common cyberattack techniques take advantage of unmanaged administrative privileges. An attacker can trick a user into downloading an application from a malicious website or opening a malicious email attachment which contains executable code that installs and runs on the user's device. In cases where users have administrative rights to their devices, the attacker can take over the device and install keystroke loggers, sniffers, etc. to find administrator passwords and other confidential data. Another common attack involves domain admin privileges in Windows environments potentially giving an attacker significant control over numerous devices and access to the data they contain.

See Privilege Management Recipe for best practices and processes for establishing a privilege management system.

4. Password Management

Good Password Practices

- Use strong passwords or long passphrases
- Do NOT write passwords down
- Do NOT share passwords
- Use different passwords for different applications (e.g., work vs personal; shopping, and banking vs casual email and Facebook; applications that contain confidential information vs those that do not, etc.)

What is a Strong Password?

The strength of a password is determined by several factors such as password length, password age, case usage, numeral usage, use of special characters, and reuse restrictions. These factors help to reduce the average number of guesses an attacker must try to guess the password and ease with which the attacker can test the validity of the guessed password.

Password entropy is a mathematical way to measure the difficulty of guessing or determining a password. As applied to passwords, guessing entropy is the estimate of the average amount of work needed to guess a password. Min-entropy is the measure of difficulty of guessing the easiest single password to guess in the population. Password entropy is expressed in bits.

See the following InCommon Assurance link for helpful Password Entropy Calculators. Most Institutions who are pursuing InCommon Silver are using the the University of Wisconsin calculator.

In recent years, there has been a significant shift in perspective and guidance on effective password composition requirements. These changes have been brought forth by research on how users actually use highly predictable strategies to achieve mixed-character set passwords and unique passwords. In 2017, NIST published a significant number of revisions to their Guidance on Management of Digital Identities series (NIST 800-63-3). This publication certainly warrants consideration and review as you review or revisit password requirements for your institution. Some significant elements of this guidance include:

- Emphasis On Password Length vs Mixed-Case or Varied Character Set Constructions
    - Passwords That Are Least 8 Characters
- No Need For Periodic Password Resets
    - Users regularly defeat this control by using predictable passwords
- Disallowing Dictionary Terms
    - Ensuring inclusion of Dictionary Checks For Password Creation
- Don’t use Password Hints or Knowledge Based
    - These measures are often easy to defeat with poor hint selection or use of information that can be found.
- Effective Deployment of Multi-Factor Authentication Solutions

The important take away here is that determining effective password strength requirements must also take into consideration the context of the security risks you are trying to manage, the inevitable predictable workarounds your users will employ, and the overall effectiveness and cost of associated password management activities.

Password Sharing Policy

It is important to realize that people will share or reuse their passwords on multiple accounts unless you provide them with some other method of allowing specific individuals to access information in their accounts. For instance, individuals in upper management often ask an administrative assistant to check their e-mail. Also, when people go on vacation, they may need to give someone temporary access to data on their computers, in e-mail, and on other systems. Password sharing policies should be put in place along with solutions that provide needed functionality with accountability for the shared resource.

To Change or Not to Change? How Often?

How often should passwords be updated? The reason for changing passwords regularly is that the longer a password remains the same and the more often the same password is used, then it is more likely that the password will be discovered or compromised. Also, the benefit of an "expiration date" on a password is that it limits the amount of time a lost or compromised password can be used by an unauthorized party. The more secure or sensitive the information resource, the more frequently passwords should be changed.

Conversely, the argument against changing passwords regularly is that strong passwords are reasonably secure and they take longer time and more effort to guess thus making them less likely to be discovered or compromised. Also, it may not be as easy to come up with easy to remember strong password very 30 or 60 days.

Even though there is no "right"or "perfect" answer, the following points are worth considering:

- Password policy should be based on risk, vulnerabilities, and deployed safeguards
- The amount of time between changes should be determined by the required strength of the passwords being used
- Password changes makes it harder for users to use the same password for multiple services (i.e., forces password "diversity")

- Periodic password changes, especially when done as a routine, could limit successful phishing attempts since users would know when it is time to change passwords and when it is not.

Password Management Problems

- Need (and failure) to remember multiple passwords
- Need (and failure) to remember strong passwords
- Frequency of password change
- Coming up with easy to remember but difficult to hack passwords multiple times per year
- Need to replicate password change to multiple devices or applications
- Sophistication of social engineering and "phishing" attacks

See Passwords, a presentation by Joe St Sauver PhD, Security Programs Manager - Internet2 for a broad discussion on Passwords and related trend, problems, alternatives, and available technologies.

Solutions to Password Management Problems

Passphrases

A passphrase is a different way of thinking about a "secret" or "something you know". The main difference is that a passphrase is longer. While a usual password is 8 to 10 characters long, a passphrase can be twice as long. Compared to passwords, a passphrase is generally stronger because it is more memorable than passwords thus reducing the need to write them down, they make some types of brute force attacks more difficult since they are much longer than passwords, and they make phrase or dictionary attacks harder if the passphrase is well constructed. See how the Indiana University is using passphrases to enhance information security.

Password Managers

Users may have to remember multiple passwords for different systems, especially if Single Sign-On is not in use for all institutional systems. To prevent reuse of passwords and assist users with remembering multiple passwords, a password manager can be used. By using a password manager, the user will only need to remember one strong password or passphrase. There are several free and enterprise level products available for use.

Learn more about Password Manager Tools, including the benefits and risks to consider.

Two-Factor Authentication: Is a Username and Password Enough?

Information security professionals are continuing to make the case that passwords and password practices are bad and getting worse. Specifically, usernames and passwords are no longer sufficient or completely secure to authenticate to information resources containing confidential information.

Two-Factor Authentication is the use of an additional factor to minimize the probability of fraudulent authentication. Two-factor adds an extra layer of security by not only requiring “something you know”, such as a password, but also an added factor which could be “something you have” such as a smartcard or your smartphone, “something you are” such as a fingerprint or a retinal scan, or even “someplace you are” such as only being able to sign-in from a specific location. This is helpful in that, if a username and password are compromised, it requires an additional authentication factor before full authentication will occur.

See this guide's Two-Factor Authentication page for an overview and technology available. This document describes the use of a second factor in addition to the traditional User ID/password pair to minimize the probability of fraudulent authentication. It touches on the business reasons for using an additional factor, technology available, and a discussion of biometrics.

5. Review of Access Rights

Least privilege and need-to-know access underscore the importance of the periodic review of user accounts and their corresponding access rights. Dormant user accounts - active user accounts which show no activity for very long periods of time - poses an unnecessary risk for unauthorized access to confidential data. The periodic review of user accounts and corresponding access rights with system owners, disabling user accounts after a preset period of inactivity, purging them after a longer period of inactivity are all good practices to ensure that a system does not contain old, unused user accounts and to mitigate risk.

Top of page

User Responsibilities

Objective: To underscore the importance of the active participation of users in safeguarding the access privileges, credentials, privileges provided to them and practices needed to prevent the unauthorized user access and disclosure of privileged information.

Users should be made aware of their responsibilities towards protecting their issued credentials, choosing strong passwords and keeping them confidential, as well as preventing unauthorized disclosure of sensitive information under their care. The following can be included in the institution's Acceptable Use or Information Security Policy. Systems should be locked when left unattended.

Users shall

- Access data and comply with the duties of their role or job duties on a need to know basis.
- Not attempt to access data or programs contained on systems for which they do not have authorization.
- Not share their computer/network username, password, personal identification number (PIN), digital certificate, security token (i.e. Smartcard), or any other device used for identification and authorization purposes.
- Not share passwords used for digital signatures.
- Not circumvent password entry through use of auto logon, application "remember password" features, embedded scripts or hard-coded passwords in client software.
- Password-protect and lock their desktops/laptops when left unattended

Top of page

Operating System and Applications Access Controls

Objective: To cover the mechanisms that an institution can use to ensure that only authorized users have access to institutional computing devices.

1. Operating System Access Control

1a. Authentication

Authentication is the process to confirm the identity of an entity requesting access to an information resource. To be properly authenticated, the entity is required to provide credentials - a unique identifier such as a username and a password, passphrase or token. The credentials are compared to the identifying information previously stored on the entity and if the credentials match the stored information, the entity is authenticated.

Most institutions of higher education require all members of their communities to have their own unique username and password to access certain resources. In addition, institutions authenticate these individuals before allowing them to connect to the campus network or Internet. This approach not only enables institutions to attribute network activities to individual accounts, it also gives institutions the opportunity to scan systems for vulnerabilities before they connect to the network.

The Enterprise Authentication Implementation Roadmap, from the NMI-EDIT consortium, is a recommended approach that can be used by institutes of higher education to build enterprise authentication services to enable appropriate interoperability with peer institutions, the Federal Government, industry, and other partners.

1b. Single Sign-On

Single Sign-On, also known as SSO, is an authentication process that allows a user to access multiple applications with one set of login credentials. In other words, a user's username and password associated with the institution, would allow access to many or all institution systems that the user is authorized to access. Single Sign-on makes signing in to multiple services easier for the end user since they are not required to remember multiple passwords for use with institution resources.

Although having a central authentication system makes account management easier, the exposure of one stolen account is greater when it gives the attacker access to multiple systems on the network. Therefore, single sign-on is not necessarily desirable in higher education environments where password theft is a common risk. Less sign-on is ideal - using centralized authentication for most systems but maintaining separate accounts on computer systems that contain particularly sensitive data and require added protection and overall maintenance.

See CommIT: Simplifying Admissions Identity Management for Georgetown University's way to leverage federated single sign-on to match electronic records for college applicants and institutions using a single set of user credentials that can be used across various services.

2. Application and Information Access Control

2a. Information Access Restriction

The EDUCAUSE Access Control page contains presentations, policies, and articles regarding mechanisms by which a system grants or revokes the right to access some data, or perform some action.

2b. Sensitive System Isolation

Information resources that are critical to the institution's mission performance, resources that contain confidential information, or information that is otherwise considered sensitive should be segregated into its own environment based on sensitivity and risk. The segregation of information resources can be accomplished by:

- Creating network domains – a collection of devices and subjects that share a common security policy. Also by creating domain trusts - a security bridge between network domains to enable users of one domain to access resources from another. Domains are defined based on risk and the specific security requirements of the domain.
- Implementing virtual local area networks (VLAN) and/or virtual private networks (VPN) for specific user / application groups. Example, students may be placed on a separate VLAN from faculty and staff.
- Controlling network data flows using network routing and switching capabilities – e.g., access control lists (ACLs)

2c. Federation

A federation is an association of organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions (InCommon.org).

Drivers

- Increasingly, people must easily and securely exchange information across the internet, among known individuals and be trusted to access restricted resources, without having to struggle with numerous and onerous security processes.
- Ideally, individuals would each like a single digital credential that can be securely used to authenticate his or her identity anytime authentication of identity is required to secure any transaction. (William Weems, Ph.D. UT Health Science Center at Houston: Sharing Restricted Resources Across Organizational Boundaries)
- Traditional forms of authentication and authorization are no longer sufficient or the level of assurance needed by modern internet-based applications
    - Increase security
    - Compliance with federal and state rules
- Application security is becoming increasingly onerous (multiple applications, multiple enterprises, and multiple user roles in multiple contexts)
    - Inter-institutional collaboration
    - Operational efficiencies and cost control

- Examples:
    - Institution wants to offer services to their constituents but doesn't want to host them.
    - Vendor wants to offer a service to institutions but doesn't want the burden of managing user credentials and authentication.
    - User wants seamless access to services. "Single Sign-On".
    - Security officer wants to protect University assets, user identity information, and passwords.

Traditional Approach

blocked URL

Federated Approach

blocked URL

First Steps

Technically speaking, it involves:

- new policies
- new processes
- new trust relationships
- new authentication and authorization mechanisms
- new enterprise directories
- new applications and much more

Participating organization ***must agree*** on:

- Technical specifications: data attributes to exchange, the software to interoperate with
- Policy specifications: privacy, establish trust and trustworthy data

Must provide two sets of services:

- Metadata management: aggregate, distribute, and maintain members' attribute data, syntax, and semantics
- Trust management:
    - federation and member operation practices and control
    - privacy and security policies

Things to Think About

- Policy work is very slow, but critical - start work on this early
- Do not underestimate the difficulty of application integration with new or legacy infrastructure
- Authorization can be quite a challenge (e.g., how to identify subsets of people)
- Consider new support models
- Communication and coordination are key
- Keeping all stakeholders motivated and involved can be a challenge

Policy Issues

- Which services reside where?
- How is vetting / credentialing performed?
- How do application owners determine required Level of Assurance (LOA) for their applications?
- How do Identity providers comply with applications' LOA requirements?
- Who supports the end users and applications?
- Who audits identity providers' practices and what standards are used?
- What is the role of Information Security Governance?

Federation Technology Standards

- Security Assertion Markup Language (SAML):
    - Standard developed and ratified by OASIS, an international non-profit standards organization, and managed by the OASIS Security Services Technical Committee
    - Has broad vendor and industry acceptance
- Shibboleth:
    - Open source software package for web single sign-on across or within organizational boundaries
    - SAML-based software managed by Internet2. See other Internet2 middleware initiatives in higher education, including OpenSAML
    - Higher-education and increasing vendor acceptance
    - Provides extended privacy functionality
- Open ID: a user-centric distributed web-SSO technology perceived as being lighter-weight and less focused on communities of trust than SAML
- OAuth: an open standard for access delegation, provides to clients a “secure delegated access” to server resources on behalf of a resource owner commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords.

Benefits of Federation

- Sharing of Resources between institutions
- Collaboration between institutions and users.
- Increase security (fewer usernames and passwords to manage)
- Lower support costs (no application-based identity management)

- Improved user experience (fewer usernames and passwords to remember)

Challenges of Federation

- Deploying new infrastructure is hard. The infrastructure must be there before gains can be realized, which makes justification a challenge.
- Policy development can take considerable time.
- Trust can be difficult to achieve. Good policy and governance helps ("trust but verify")
- Making it ubiquitous across entities of varying size is a challenge. Many times, the smaller organizations will benefit most.

The InCommon Assurance Program awards certifications to qualifying institutions of higher education and research organizations that support InCommon requirements for consistent management of digital credentials.

Good security and identity practices help ensure that an individual using an electronic credential is the person you think it is. For Service Providers in an identity federation, having Identity Provider Operators support a standard practice set (or profile) can mitigate the risk of service compromise. For Identity Providers, it is a way to provide single sign-on access to applications requiring an increased level of confidence in a credential.

See CommIT: Simplifying Admissions Identity Management for Georgetown University's way to leverage federated single sign-on to match electronic records for college applicants and institutions using a single set of user credentials that can be used across various services.

2d. Cloud Computing and Software as a Service (SaaS)

Cloud Computing is the use of a network of remote servers hosted on the Internet to store, manage, and process data, rather than a local server or local computer.

Software as a Service (SaaS) is the capability provided to a user by a third party, to use a provider's applications running on a cloud infrastructure, which is accessible from client devices through a web browser or other means of remote connection such as a thin client.

For a comprehensive discussion of major identity and access management functions in the cloud, see: Identity and the Cloud - Preparing Your Campus.

Managing security and privacy is an ongoing challenge, compounded by the expanding interest in software as a service (SaaS) and cloud computing. Specifically, the concept and benefits of participating in InCommon, campus policy requirements, preparing institution identity management infrastructure, choosing and installing the appropriate standards-based software, and collaborating with other institutions of higher education and with resource providers.

Challenges

- The decision to procure cloud computing services or SaaS may be driven mostly by individual departments instead of institutional IT strategy.
- Integrating separately developed applications into an integrated approach.
    - How to manage access?
    - How to manage provisioning?
    - How to integrate these applications into institutional web services?
- How to reduce the number of credentials

An Alternative Solution

- Focus on four activities:
    - Develop an institutional Identity Management System
    - Create a standard set of attributes for each person (eduPerson)
    - Use a federation to enable external access
    - Require institutional developers and in RFPs that service providers support SAML and InCommon
- InCommon provides an easy to use framework for customers and service providers that will work across higher education.

See Supporting High-Value, High-Risk Cloud Services with Federated Identity Management to see how campuses are using federated identity management to meet the security standards needed to provide access to services containing sensitive data in the cloud.

The EDUCAUSE Cloud Computing Security page contains security, privacy, identity, and other compliance implications of moving data into the cloud as well numerous higher education and industry resources on the topic.

2e. Mobile Computing and Teleworking

Teleworking (i.e., telecommuting), e-commerce, online education, and the increased use of portable computing devices such as laptops, tablets, and smartphones are driving the need for access to information resources from any place at any time.

Today's mobile work force and mobile users are no longer just staff, faculty, and students trying to check e-mail from home, they are telecommuters, business partners, students. and patients who rely on access to institutional networks to accomplish day-to-day business, attend classes, and follow-up on medical treatments. Information security controls specifically targeting mobile computing and remote access to information resources are becoming an increasingly critical component of any institution information security program ensuring the protection of the integrity of the institutional networks while allowing remote access to it.

Challenges of Mobile Computing

- User Authentication
- Protection of Transmitted Data
- Protection of the Institutional Network

To enable remote access to institutional information resources, institutions of higher education are implementing Virtual Private Networks (VPN) technology to provide a secure connection to the institutional network from remote locations such hotels and airports. VPNs send data securely through a shared network. VPNs can be established between remote users and a network or between two or more networks thus using the Internet as the medium for transmitting information securely over and between networks via a process called tunneling.

The EDUCAUSE Mobile Internet Device Security Guidelines page contains helpful advice to develop mobile Internet device security policy, standards, guidelines and procedures.

Top of page

Resources

EDUCAUSE Resources

EDUCAUSE Resource Center Pages

- Access Control, Publications, presentations, policies, podcasts, and blogs regarding mechanisms by which a system grants or revokes the right to access some data, or perform some action.
- Two-Factor Authentication Resource, a document that describes the use of a second factor in addition to the traditional UserId/password pair to minimize the probability of fraudulent authentication. It touches on the business reasons for using an additional factor, technology available, and a discussion of biometrics.
- Identity and Access Management (IAM) Tools and Effective Practices
- Encryption, Publications, presentations, policies, and blogs regarding the mechanisms to convert data into a form, called a ciphertext, that cannot be easily understood by unauthorized people.
- Identity and Access Management, Publications, presentations, podcasts, and blogs regarding the mechanisms to create a trusted authority for digital identities across multiple organizations and employ a single digital identity to access all resources to which a user is entitled.
- Mobile Internet Device Security Guidelines page contains helpful advice to develop mobile Internet device security policy, standards, guidelines and procedures.
- Electronic Identity: The Foundation of the Connected Age, an article from the EDUCAUSE Review online, Oct. 2013

Corporate and Campus Solutions

- Multi-Factor Authentication: All in This Together, an IAM Online presentation
- CommIT: Simplifying Admissions Identity Management, an IAM Online presentation
- Identity and the Cloud - Preparing Your Campus, Preconference seminar at the EDUCAUSE Conference, 2010
- Implementing True Identity Management On Your Campus And Planning For Success (And Avoiding Critical Mistakes), Presentation at the EDUCAUSE Conference 2012.
- UM Community System: Expanding Identity Boundaries, University of Maryland, Presentation at the EDUCAUSE Mid-Atlantic Regional Conference, 2013
- Supporting High-Value, High-Risk Cloud Services with Federated Identity Management, Presentation at the EDUCAUSE Information Security Professionals Conference, 2013
- Finally, A Two-Factor Solution for the Rest of Us, Presentation at the EDUCAUSE Security Professionals Conference, 2013
- Information Security or Identity and Access Management?, Presentation at the EDUCAUSE Security Professionals Conference, 2013
- Social-to-SAML: Accepting Social Identities for InCommon Federated Services, an IAM Online Presentation. Presentation slides.

Technology Concepts

- Access Management Use Cases Organized by Area of Interest, EDUCAUSE and Internet2 CAMP(Campus Architecture and Middleware Planning)
- Identity Management for Security Professionals: Leveraging Federations , Postconference seminar at the Security Professionals Conference, 2010
- The Enterprise Authentication Implementation Roadmap (NMI-EDIT), a recommended approach that institutes of higher education can use in building enterprise authentication services to enable appropriate interoperability with peer institutions, the Federal Government, industry, and other partners.

Initiatives, Collaborations, & Other Resources

- IAM Online webinars
- Privilege Management Recipe, A set of best practices and processes for establishing a privilege management system.
- Internet2 Middleware Initiative
- Shibboleth® Federated Single Sign-On Software, A Project of the Internet2 Middleware Initiative
- Middleware Architecture Committee for Education (MACE)
- The NSF Middleware Initiative - Enterprise and Desktop Integration Technologies(NMI-EDIT)
  - NMI-EDIT Enterprise Directory Implementation Roadmap
  - NMI-EDIT Enterprise Authentication Implementation Roadmap
- OpenSAML, A set of open-source libraries to support the Security Assertion Markup Language (SAML)
- InCommon Federation, A common framework for trustworthy shared management of access to on-line resources in support of education and research in the United States
  - InCommon Grows Up (Flash Video) (PDF), Presentation at the Internet2 Member Meeting, Spring 2010
  - InCommon Certificate Service
  - InCommon Assurance Program
  - InCommon Assurance Password Entropy Calculators
- Aegis Identity Survey White Paper - Trends in Identity & Access Management Solutions in Institutions of Higher Education - 2012, Detailed analysis of identity and access management technologies as they relate to college and university business drivers and challenges; strategic approaches towards related technology; and the effects of emerging technologies on identity and access management infrastructure.

Top of page

Standards

ISO	NIST	COBIT	PCI DSS	2014 Cybersecurity Framework	HIPAA Security
27002:2013 Information Security Management **Chapter 9**: Access Control **ISO/IEC 9798-1:2010**	**800-100**: Information Security Handbook: A Guide for Managers **800-53**: Recommended Security Controls for Federal Information Systems and Organizations **800-12**: An Introduction to Computer Security - The NIST Handbook **800-14**: Generally Accepted Principles and Practices for Securing Information Technology Systems	**APO01.06** **BAI02.01** **BAI06.01** **DSS05.02** **DSS05.04** **DSS06.03** **DSS06.06**	**Req 6** **Req 7** **Req 9** **Req 10**	**PR.AC-1** **PR.AC-4** **PR.DS-5** **PR.PT-3**	**45 CFR 164.308(a)(4)** **45 CFR 164.312(a)(1)**

Top of page
