Infrastructure Software Development & Architecture

Identity Management: Provisioning and De-Provisioning Authentication IDs & Authorization Privileges

Current State of the Union

Paul Hill

Sep 11 2006

Information Services & Technology

Identification / Authentication / Authorization

- MIT ID provides you an *identification* number
- MIT ID Card provides you with a physical identifier
- Kerberos and X.509 certificates allow your identify to be *authenticated*
- Roles, Moira, and other systems, define and manage *authorization* to access certain resources

MIT ID Number

- The MIT ID number is a unique identifier for people in MIT Information Technology (I/T) systems. Having an MIT ID number does not in itself provide any status, relationship, access, responsibility, or privileges. These are conferred and defined by the Institute business processes for which I/T systems exist. Thus who has an MIT ID number is defined by the MIT businesses. The system of record of all MIT ID numbers is the MIT ID server operated by IS&T.
- Who can get an MIT ID number?
  - Faculty
  - Students
  - Staff
  - Family members (spouses and dependants)
  - People that buy services such as access to athletic facilities or library patronage
  - Sponsored guests
  - Contractors
  - Visiting scholars
  - Others

Who can get an MIT Kerberos ID and X.509 certificate?

- All MIT community members (faculty, students, and staff)
- "A sponsored guest account is required for voucher or temp staff, former students or staff who are no longer eligible but need continuing access to their account, as well as visitors who need an MIT electronic identity"
  - Account can be sponsored by any current member of the MIT faculty or staff, but not students
  - Guest accounts are valid for up to 2 years and easily renewed

Authentication Demographics

	Current (MIT Fact Book '05)	Number with authentication credentials
Faculty	983	2473
Staff	9780	11156
Undergrad	4136	4697
Grad	6184	6777
Guest	--	2415
Other*	--	988

* Other includes vouchers/temp (308), system accounts (245), pre-frosh (142), random project staff (214), etc.

Total of 28,506 IDs as of 2/13/2005

Kerberos ID activation

- Self service registration
- Separate provisioning processes for:
  - Employees (faculty and staff)
    - Should be gated on HR business process of hiring and establishing MIT ID number
  - Undergraduate and Graduate Students
    - MIT ID number generated at time of application.
    - Ability to activate account provided in acceptance package
  - Guests
    - IS&T accounts group and online sponsorship form

Kerberos ID deactivation

- Automatically in January after the graduation of a student in the prior year.
- Manually when notice is received from HR that an employee has been terminated.
- Manually when a guest’s sponsor does not respond to a renewal request.
- Almost never for faculty.
- ***Note that if a person remains affiliated with MIT, although the relationship changes, the Kerberos ID will not, and it will not be deactivated.***

X.509 certificate deactivation

- MIT X.509 certificates cannot be obtained once the Kerberos ID has been deactivated.
- Existing MIT X.509 certificates will normally have a useful lifetime up to July 31st of the period just preceding Kerberos ID deactivation.

Authorization is distinct from authentication

- ***Systems that need to restrict access MUST implement some form of authorization.***
- Client/Server applications must not rely solely on client based authorization, since this makes the application server and/or database vulnerable to an attacker who can easily bypass the client-enforced authorization checks. Such security attacks are possible via commercially available SQL tools and by modifying and replacing client software.
- Simply authenticating a user via Kerberos or a user certificate is rarely provides sufficient information needed to make an authorization decision because of the broad range of people that can legitimately obtain such credentials. Authorization decisions can be implemented in many ways.
- ***Access control SHOULD NOT be based on IP address.***
  - Proxy systems and IP tunnels may exist on campus which enable an off campus user to appear to be originating from a net 18 address.
  - MIT users may be working from anywhere in the world. They may be on campus, or in a Starbucks just down the street. They may be on a research ship at sea connecting via a satellite link or visiting a research station in the Antarctic. Typically the location of the user should not determine their level of access. Access should typically be determined by the user's privileges.

IS&T provides authorization management systems

- ROLES
  - groups business functions and authorizations into Function Categories
  - Function Category may apply to more than one application; for example, financial reporting authorizations in the SAP category apply both to SAP R3 and the Data Warehouse
- MOIRA
  - Simple list management that may be provisioning into other systems as access control lists (AFS PTS, WIN security descriptors, Stellar, …)
- LDAP
  - May use OU placement as an attribute value (e.g. is an employee or is a student)

Our Responsibilities

- If you are assigning privileges it is also your responsibility to remove privileges when appropriate.
- You must not assume that another person’s ability to authenticate to your system will be removed in a timely or appropriate manner.

We need your assistance

- As an IT Leader you should document
  - The business process that determine who should have access to your system and with what level of privilege
  - The technologies used to implement and enforce your business processes
- ***Please send the information to pbh@mit.edu (Paul B. Hill)***

Obstacles to proper privilege management

- There are too many disparate privilege management systems in use today.
- Not all systems (even from IS&T) use the recommended privilege management systems.
- This hinders the responsible people from knowing what privileges have been granted and what needs to be revoked.

Some tasks to improve the situation

- MIT Roles DB
- MIT Card Office
- Multipart names and context aware authentication
- Guest Accounts
- Provisioning process improvement for employees

Improvements to Roles DB

- Short term – new API to enable application developers better integrate Roles data into their systems
- Longer term
  - improved admin interface to Roles
  - Retire Powerbuilder application and replace it with rich web interface
- Future
  - Integration with other authorization systems
  - Improved reporting to make overall privilege management more consistent

MIT Card Office

- Working with IS&T to manage door access via MIT Roles
    - Able to delegate management to responsible individuals within departments
    - Provide responsible individuals with better reporting about who has physical access

Multi-part names and context aware authentication and authorization

- Kerberos provides the ability to create multi-part IDs and assign distinct passwords (joe, joe/root, joe/test, joe/dialup,…)
  - Improve management and reporting of these IDs
  - Publicize the ability to request and use these IDs
  - Support these in all of our authorization systems

Guest Accounts

- Market the current ability to create guest accounts
- Provide web interface to determine who a sponsor is, or what accounts have been sponsored by a user
- Possibly new class of guest accounts that do not receive an MIT email address or other services by default

Provisioning process improvement for employees

- Make it easier for new hires to initialize their account before their first day of work
- Document and advertise the processes to be used when people cease to be employees.
- Provide improved reporting regarding employee terminations so that privileges can be easily reviewed and acted upon.