

Case Study: University of Wisconsin - Madison

BACKGROUND

A number of distributed authentication services are deployed at The University of Wisconsin-Madison.

- A centralized web initial sign-on (Web-ISO) service is provided based on Pubcookie, using LDAP authentication via Sun's LDAP directory server. Faculty, staff and students use this service primarily to access the UW-Madison web portal, which provides access to web-based email, email folders (IMAP), calendaring, payroll data and many other applications.
- A centralized PKI infrastructure is in place, laying the groundwork for the eventual implementation of PKI-based authentication services. However, due to the decentralized nature of our environment, we cannot currently require service providers to use the system. We believe that the benefits of PKI and the availability of a centrally maintained service will drive voluntary adoption and are working to integrate our existing PKI service with Web-ISO to allow applications needing a high level of assurance to take advantage of digital certificate-based authentication.
- Due to the highly decentralized nature of the campus, various local authentication mechanisms exist in various administrative departments, schools and colleges. These mechanisms include local LDAP and Active Directory.

The UW-Madison does not currently provide a central service to authenticate workstations, but is planning to implement a central Kerberos service to support workstation authentication in public labs. Various areas have implemented Active Directory locally in support of workstation authentication.

POLICIES

The UW-Madison has recently implemented a campus-wide password policy.

<http://www.doit.wisc.edu/security/policies/password.asp> .

In addition, the use of clear text password is discouraged, so a strong motivator for connecting to the Web-ISO is its use of SSL to protect passwords during transmission.

The UW-Madison is currently considering the feasibility and implications of a policy requiring the use of the centralized authentication services. Use of the Web-ISO service is strongly encouraged. More information on Web-ISO can be found at

<http://weblogin.services.wisc.edu/docs/>

IDENTIFIERS AND CREDENTIALING

Identifiers and passwords are automatically provisioned for the majority of users via feeds from the human resources and student information system. Various special feeds provision accounts for large user populations affiliated with the university (e.g. hospital employees). Manual account creation is also supported. For the ad hoc addition of a person, a description of the source is documented.

A person registered in the enterprise directory is provisioned with a lucent, publicly visible, identifier (NetID) used for login. These are not reused. Users are also provisioned with a persistent identifier to support identity linking between systems. Furthermore, because there are numerous authentication systems deployed on campus, most users are issued additional (multiple) credentials.

During the vetting process, students or faculty present some form of personal photo identification such as a valid driver's license, passport, or state ID to the Photo ID office. The Photo ID Office issues a photo ID that contains a campus ID. The campus ID can be presented to an online system that creates a NetID.

Users may then choose their NetID, commonly the last name; or first initial and last name; or first and middle initial and last name. Persons may be assigned a new NetID under certain circumstances (e.g. marriage). The UW-Madison has a project underway to define institutional standards around NetID persistence and reusability. In addition, services are provided that allow demographic data to be returned based on NetID as input.

PASSWORD PRACTICES

UW-Madison is currently implementing rules to improve the strength of passwords. The new rules will require a minimum length and structure (letters, numbers, and special characters).

Passwords are now stored in the centrally maintained LDAP directory and in a number of distributed systems (including multiple Active Directories), but are not replicated between stores. They also do not expire. We do provide a web-based mechanism for users to change their password at will, however.