

Case Study: Rice University

BACKGROUND

Support of authentication services at Rice University is a mix of centralized and distributed services: the core IT services support Kerberos and IMAP and administrative systems use their own service, but leverage the NetID that the core IT services provides. The bulk of authentication transactions support email and desktop login, because these services are centrally managed.

POLICIES

We have an appropriate use policy at <http://www.rice.edu/it/vpit/aup.html>. We do not have a policy requiring the use of a consolidated authentication service for most applications; however an identity management advisory committee has been tasked to consider it.

Policy is being developed to eliminate or restrict the use of clear text passwords in applications. We have an IT Security Officer that manages the security issues related to authentication.

PRACTICES

Level of Assurance - We do support two levels of assurance and two factor authentication, although it's not widespread. We have a private PKI that requires in person vetting for issuance of an X509 certificate on a USB token. These credentials are required for administration of our Microsoft Active Directory Domain. To achieve the higher level of assurance, we require in-person identity vetting and, in some instances, a separate account is issued. We also issue digital certificates on a USB Token that is unlocked by a password.

The departments that perform id proofing include:

HR – identity proofing for Staff and Faculty

Registrar – identity proofing for Students

Campus Police provide identity proofing for ID badges

Guests – System has not yet been completed and only asserted Rice Member identity proofing is required.

Identifiers and Credentialing - A NetID credential is assigned to all new faculty, staff and students. We assign a persistent, not-reassigned, opaque identifier (NetID) for login (such as {brr1234}): It is somewhat identifiable because the NetID contains the person's initials. We have to refer to the directory for name mapping. To create our electronic identifiers and passwords/tokens, we use a Nexus that runs via dynamic triggers from information in our Banner system.

We do not have a system of record for affiliates at this time but are currently developing a self service assertion based guest account process. Currently official guest are created in the HR system as unpaid employees.

For new users, the institution requires that they enter information that is distributed via US mail or in person and that this, along with additional information that the person knows, allows them to set an initial password on a secure web site. We do not distribute an initial password

Login credentials are then issued to new users and linked to all applications that we deliver. The NetID portion of the credential is persistent, opaque and currently never recycled.

Password Management – The passwords choices are programmatically checked for compliance with the following rules:

- Password MUST be 8 characters or longer and are not reset.
- Password MUST not be the same as your account name, forward or reversed

- Password MUST contain at least two characters from any two of the characters types below. None of the elements can make up more than 80% of the password:
 - Upper case characters
 - Lower case characters
 - Digit characters
 - Special characters
- Password MUST not be or contain a dictionary word IF IT IS LESS THAN 12 CHARACTERS IN LENGTH. If the password is greater than 12 characters, then it may contain dictionary words. (We do not have systems that enforce a maximum password length, but there are some Unix crypt systems that will only recognize the first 8 characters.)
- Password MUST not use 'simple' character substitutions that would otherwise make a dictionary word; For example, using '5' for 's', '3' for 'e', '1' for 'l'

Rice does not keep a password history, but we do pre-crack passwords and encourage the use of pass phrases. We also require that no clear text passwords be transmitted to insure the credential's integrity is maintained. To re-link a person credentials if they are compromised, we have a help-desk password mechanism and will be implementing a self-service password reset in the future. Mobile users can cache passwords and store them locally for reuse. CAS and Kerberos do not require caching due to their short shelf life.

Single Sign-on - For our Single Sign-on system, we are migrating from IMAP to Kerberos 5, with tickets being active for 12 hours. We currently store passwords in our person registry and are planning to house them only in the Kerberos system. We also use Yale's CAS for WebSSO and will be implementing Shibboleth in the fall. Our LDAP does not store passwords but uses Kerberos for authentication.

Currently applications that use our SSO system, include email, Active Directory, Unix login, Portal, Sakai, file services, dialup, VPN, 801.11, 802.1X. We are currently only integrating systems into the Kerberos KDC that have similar security requirements. Systems that require higher LOA require separate credentials and vetting processes. These systems include financials, alumni and other higher risk services that are distributed to a small set of the campus.