

## **Case Study: University of California, Riverside**

---

### **GENERAL AUTHENTICATION**

The University of California (UC), Riverside uses a mixed authentication model. Our primary credential store is provided by our enterprise directory (OpenLDAP), and is replicated to a handful of other services including Active Directory, password databases on Unix machines, Blackboard, etc.

The majority of our non-web services verify credentials using the LDAP protocol. Some campus units maintain their own password store, set their own policy, etc. For example our student information system accepts a wide array of credentials not supported by our LDAP infrastructure. The largest consumer of credential verification on campus is electronic mail.

UC Riverside does not currently have multi-factor authentication, nor do we have applications that rely on multiple levels of assurance. Implementing these two features is high on our list of priorities. We plan to investigate various technologies, and hope to implement some kind of pilot program over the coming year. We have not yet started investigating the processes and requirements of the Federal eAuthentication initiative, but probably will work toward this process in the next year or so.

However, in practice, we have two levels of assurance. While none of this is enshrined in any database or directory as of yet, we do support multiple levels of assurance. In order to elevate a person from our level 1 to level 2, the user must appear in person with a form of picture ID.

### **POLICY**

We do not have a policy requiring that applications use our authentication infrastructure. Rather, we try to convince developers to use our infrastructure, as it makes their lives easier. We do have policies detailing best practices; this policy document is available on the web at:

<http://www.cnc.ucr.edu/passwords/index.php?content=password/index.html>.

### **ISSUING IDENTIFIERS**

UC Riverside creates digital identities in batch, based on feeds coming from one or more databases of record, e.g., student information system or personnel and payroll system. Users are issued one set of credentials for centralized systems. The association between NetIDs and persons is maintained in our enterprise directory. Those with appropriate access may map NetIDs to student Ids or employee Ids.

Students are provisioned for authentication upon their application to the institution. Once students are accepted and declare their intent to attend, they are assigned e-mail access and are provisioned for the full complement of services. Students are automatically assigned a NetID based on their name. As a matter of policy, we only change NetIDs when our method for generating NetIDs creates a vulgar word, e.g., "Stephanie Hit" would generate "shit001".

Faculty and staff are provisioned for the full complement of services as soon as they are entered in the payroll and personnel system, and a departmental deputy (departmental Telecommunications Coordinator) verifies their identity. Faculty and staff are allowed to choose their NetID.

For the most part, NetIDs are never re-assigned. NetIDs assigned to applicants who do not officially enroll are not reserved.

### **PASSWORD MANAGEMENT**

Students are initially assigned a password based on a registration pin number distributed via the US Postal Service. Students may also discover this number via a self-service kiosk, if they are able to answer five questions based on their personal data in the student information system.

Faculty and staff are assigned a temporary password and are given a URL that allows them to register a permanent password within a timeframe of one week. Failure to register within that time period invalidates the temporary password.

The system of record for affiliates is provided by administrative staff. Credentials are stored in our enterprise directory. Credential management is accomplished via a number of locally developed programs and typical policy statements. Specifically, we use a mixture of Unix hash and MD5 in OpenLDAP. Passwords are replicated to Active Directory.

Policy regarding password use enforces a maximum password length (legacy systems), and password syntax, where passwords must contain at least 2 alphabetical and 1 non-alphabetical characters. Beyond this, passwords do not undergo any pre-crack testing. Some applications consuming authentication information can accept arbitrarily long passwords, though some cannot.

We do not enforce mandatory password changes, unless there is reason to believe that a password has been compromised. However, faculty and staff may reset their passwords through their departmental telecommunications coordinator, which involves the user going through the same temporary/permanent password process described above. Students must go to the student help desk with a picture ID in order to reset their password.

We have a small handful of services that still send passwords over the network in the clear. We are working towards upgrading or eliminating these services or training users to use some secure tunneling method.

### **SINGLE SIGN ON**

As of summer 2005, UC Riverside has been using the CAS, developed by Yale University, as our web sso. CAS validates credentials against our enterprise directory and creates a session that is valid for eight hours. All enterprise financial applications use the CAS, and we are slowly migrating other applications to use it.

All systems which participate in the CAS use the same set of credentials (since CAS does a simple bind over TLS on the backend). We do not allow applications to cache passwords for the purposes of SSO.