UC RIVERSIDE
UNIVERSITY OF CALIFORNIA

Two-Factor Authentication

Integrating Safeword with OpenLDAP

The Problems

- Integrate Secure Computing's Safeword tokens with our CAS Single Sign-on service.
- Require Safeword use depending on affiliations, policies, and job roles.
- Don't break Kerberos support.

First Steps

How can CAS communicate with the Safeword authentication service?

- RADIUS
- HTTP
- Safeword Eassp Protocol

Should CAS do it?

It can, however:

- HTTP seems ugly.
- What is Eassp?

RADIUS works, but introduces the problem of distributing shared secret keys.

Other services?

Modifying authentication front-ends doesn't scale at all.

We haven't yet considered enforcing a Safeword policy and retaining Kerberos support.

What about LDAP?

LDAP is ubiquitous at UCR and a great candidate for Safeword integration.

LDAP supports Simple and SASL authentication, but doesn't directly support RADIUS or Eassp.

OpenLDAP can map Simple binds to SASL binds.

Can SASL do it?

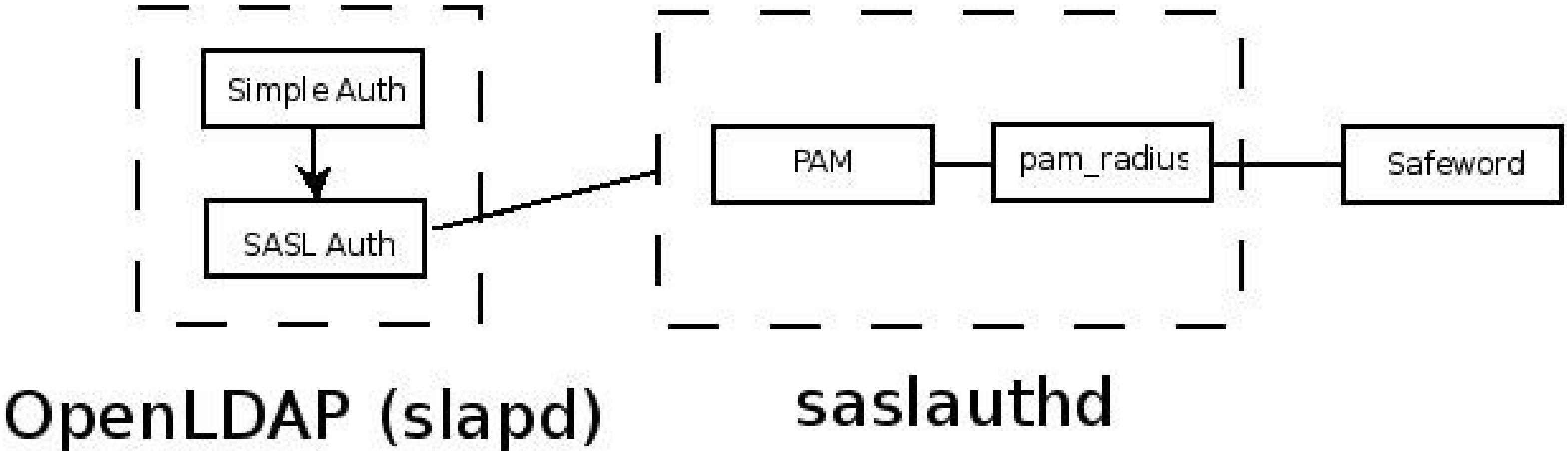
Cyrus-SASL supports several mechanisms. The PLAIN mechanism defers authentication to saslauthd.

Saslauthd

Saslauthd responds to authentication requests over a UNIX domain socket, and supports several back ends.

The PAM backend is the most interesting because of pam_radius, which can use Safeword.

The Big Picture



Deferring to SASL

OpenLDAP examines a user's userPassword during authentication.

A value of {SASL}netid@REALM defers authentication to SASL, passing netid@REALM and the Safeword password to saslauthd.

SASL Mapping

OpenLDAP uses authz-regexp directives to map SASL principals to their corresponding LDAP entries.

The Other Problems

We can use LDAP to enforce Safeword use by placing {SASL}netid@REALM in a user's userPassword attribute.

We can also put pam_krb5 in the PAM stack and allow LDAP to turn Simple binds into Safeword and Kerberos authentications in parallel.

The Future

- Deferring control of Safeword distribution and enforcement to UCR's Enterprise Directory coordinators.
- Seamless MIT/Heimdal Kerberos integration.