

SASL Pass-Through Authentication with OpenLDAP

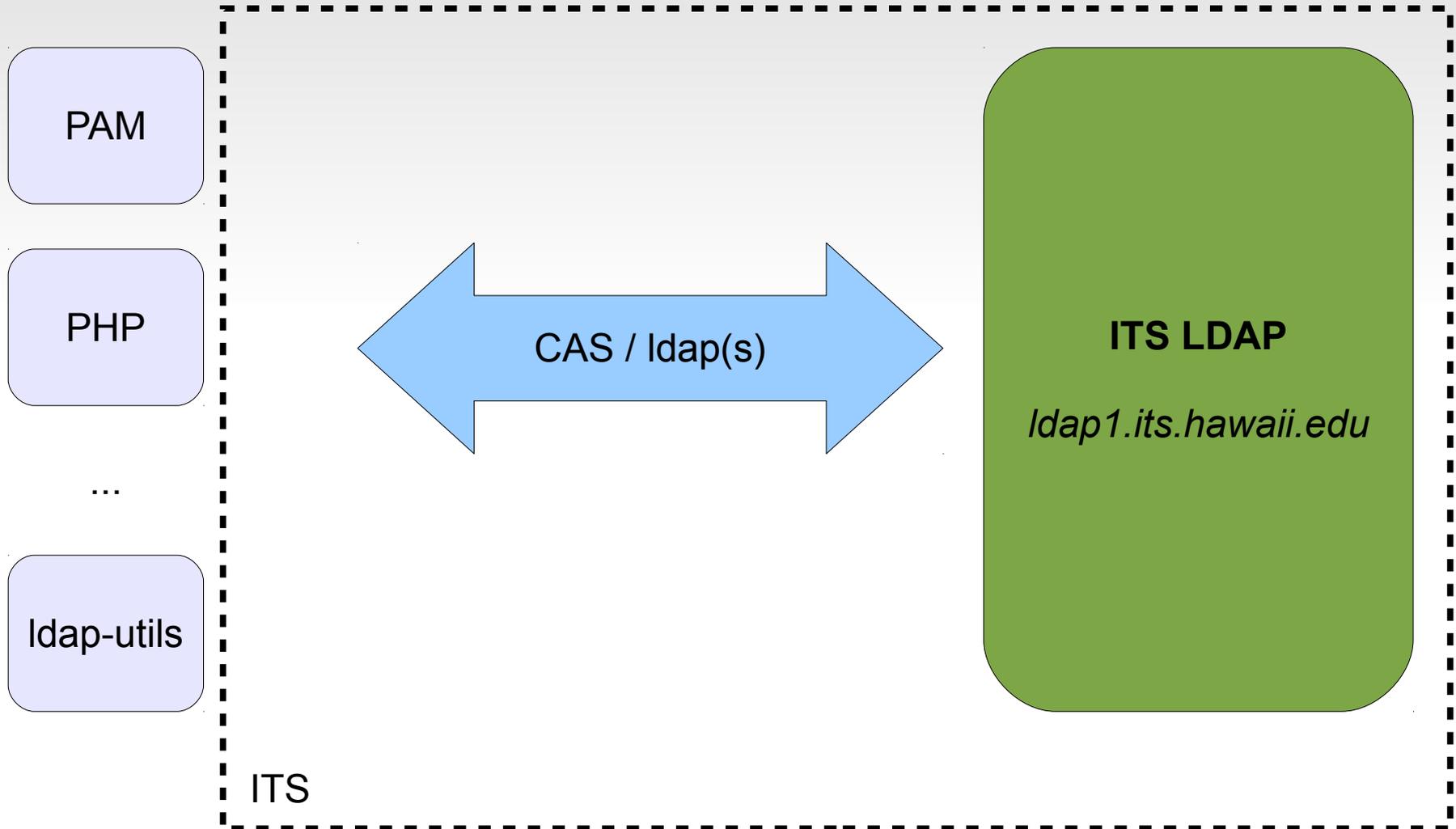
Stephan Fabel
sfabel@hawaii.edu

College of Education
University of Hawaii at Mānoa

Quite a mouthful!

- SASL = Simple Authentication and Security Layer
 - framework for authentication and data security
 - decouples authentication mechanisms from applications
 - IETF Proposed Standard (2010)
- Pass-Through Authentication
 - server hands off authentication part to something else
 - invisible to the client application
- OpenLDAP
 - originally based of Univ of Michigan project
 - free, open source LDAP server implementation
 - can be downloaded from www.openldap.org
 - but is usually included in all Linux and BSDs

Concept



Concept

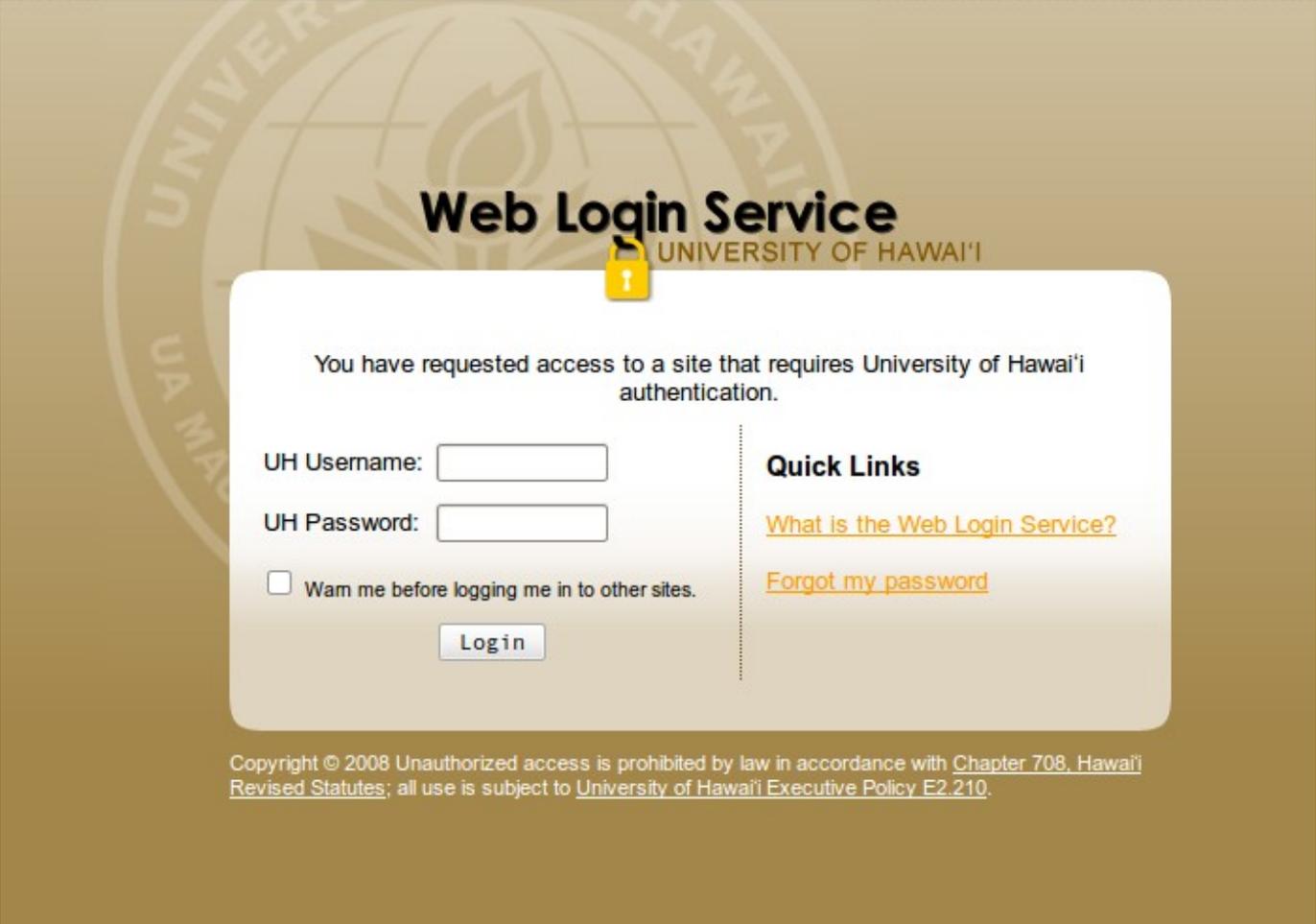
PAM

PHP

...

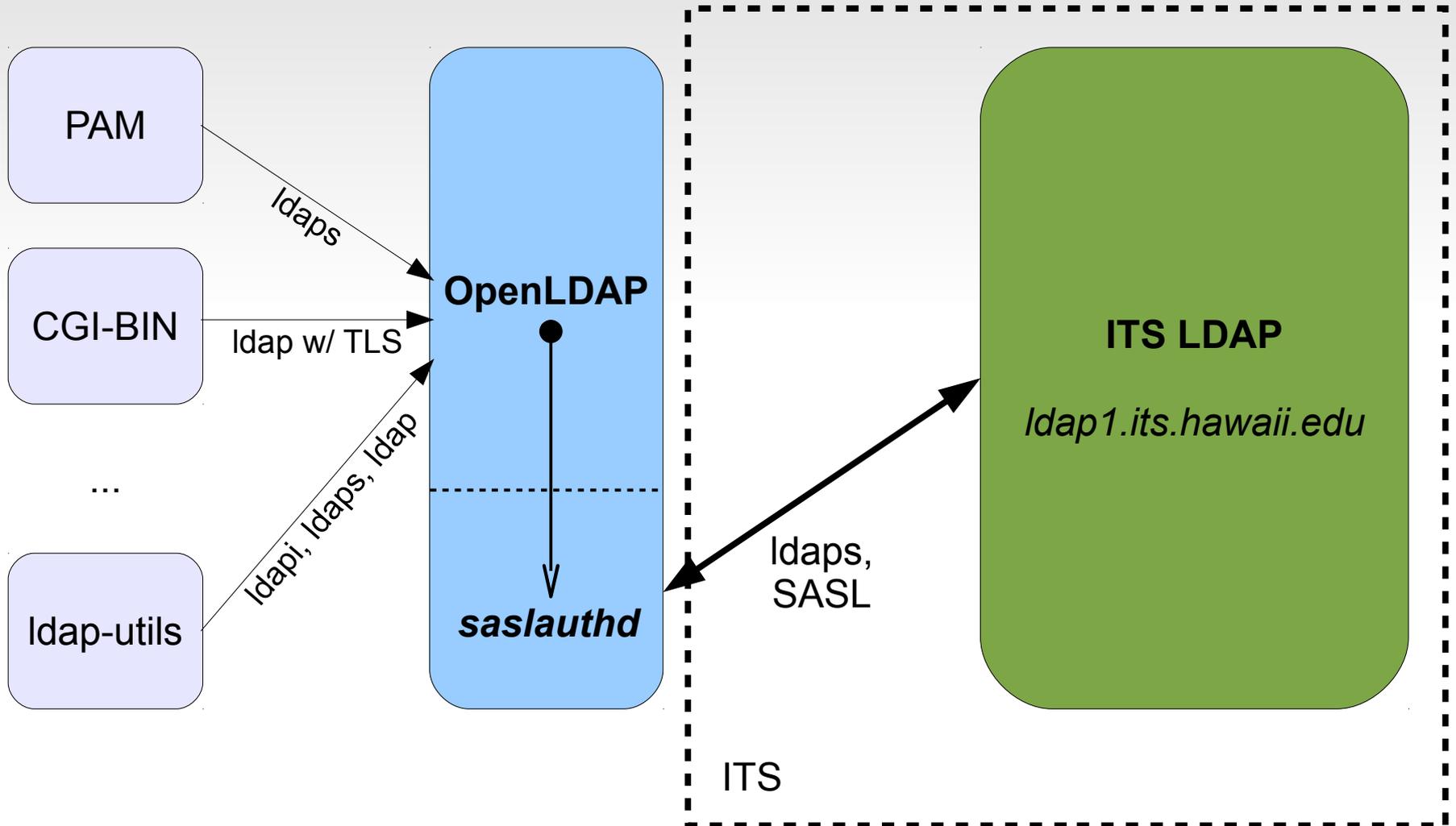
Idap-utils

ITS



The screenshot shows the University of Hawai'i Web Login Service interface. At the top, the text reads "Web Login Service" with a yellow padlock icon and "UNIVERSITY OF HAWAII" below it. The background features the university's seal. The main content area contains a message: "You have requested access to a site that requires University of Hawai'i authentication." Below this are two input fields: "UH Username:" and "UH Password:". A checkbox labeled "Warn me before logging me in to other sites." is present. A "Login" button is located below the password field. To the right, under the heading "Quick Links", there are two links: "What is the Web Login Service?" and "Forgot my password?". At the bottom of the page, a copyright notice states: "Copyright © 2008 Unauthorized access is prohibited by law in accordance with Chapter 708, Hawaii Revised Statutes; all use is subject to University of Hawai'i Executive Policy E2.210."

Concept



Advantages

- interface **not restricted** to http/https applications
- provides **local** attributes, classes and authorization policies
- **flexibility** in user management/lifecycle management
- completely **compatible** with the existing ITS LDAP directory
- no interruption with the CAS login even with web applications
- UH Credentials down to **file system level**
 - POSIX user ids and group membership define access rights
 - **desktop login with UH credentials**
 - no local caching of authorization details, **no “shadow” system**

Limitations

- user lifecycle management still not automated
 - LDAP != PeopleSoft
 - RabbitMQ may help, but not as elegant and requires separate listener
- UH LDAP does not store NTLMv2 hashes
 - no Windows passwords can be “passed-through”, this method works only for LDAP attribute “userPassword”
 - logins possible using pGina, but no Windows shares accessible (using password auth)
 - Mac OS X logins presumably possible, but require extensive adjustment of the OpenLDAP server and unfortunately LDAP schema support not up-to-date

Configuration / More Info

- Instructions can be found on the **UHIMS Wiki**
 - URL <https://www.hawaii.edu/bwiki/x/CJidDQ>
 - Ubuntu Server 10.04 LTS
 - all packages from the default repository
- **OpenLDAP Admin Guide**
 - chapter 14.5
"Pass-through authentication"
- **COE LTSP Lab**
 - UH Credentials Login
 - NFS mounted home directory
 - also based on Ubuntu 10.04

