Application for the 2011
University of California Larry L. Sautter Award
for Innovation in Information Technology

PROJECT TITLE

Kerberos KDC and Passphrase Upgrade Project

CONTACT

Robert Ono

PROJECT TEAM

Blaise Camp	Programmer
Chris Callahan	Technical Architect
Brian Donnelly	Programmer
John Harris	System Administrator
Joyce Johnstone	Co-Project Manager
Bram Lewis	Programmer
Julie McCall	Communication Analyst
Tim Metz	System Administrator
Doreen Meyer	Technical Architect and Co-Chair
Robert Ono	Sponsor and Co-Chair
Jatinder Singh	Manager
Sandra Stewart	Co-Project Manager
Josh Van Horn	System Administrator
Jed Whitten	Programmer
Omen Wild	Programmer
Dan Wright	IT Express Computing Services Help Desk Manager

SUMMARY OF PROJECT SIGNIFICANCE

Universities must have secure and robust authentication services to ensure individuals are who they claim to be when accessing automated systems. At UC Davis, we have recently employed innovative approaches to upgrade and enhance the university Kerberos system, the core technology supporting centralized authentication services for campus and UC Davis Health System community members. As a result of this project, UC Davis has dramatically improved the reliability and security of its central authentication system, based on a Kerberos KDC, as well as the account and password[1] infrastructure. As plans for replacing the KDC were developing, so were new federal minimum password strength requirements. These requirements, and the campus's 20-year-old password standards, were the impetus for undertaking the upgrade to passphrases.

The Kerberos KDC and Passphrase Upgrade Project used innovative approaches that contributed to the project's success. These concepts can be used by other UC institutions as they plan authentication service

[1] A password-based authentication system uses a shared secret between two parties. The use of "passphrase" in this document refers to a shared secret format that is based on the new UC Davis standards for authentication. Passphrases allow the use of a combination of dictionary words and phrases, unlike typical passwords which are based on highly restrictive character selection rules.

changes to meet new UCTrust requirements aligned with InCommon Silver specifications. The innovative approaches included:

- Developing and implementing a creative and effective communication strategy for the 'Upgrade to a Passphrase' campaign (described in more detail below).
- Designing and deploying a new login dialog form displayed during Web authentication to inform account holders about the real-time status of their password change actions during the later part of the campaign.
- Identifying and meeting key granular project deliverables that permitted the project to demonstrate and build on the success of distinct project phases. An example of this approach is the timing of the migration of the account database to the new KDC ahead of the 'Upgrade to a Passphrase' campaign.
- Integrating the measurement of password entropy into the new passphrase selection process for end users. Password entropy is a function of the passphrase length and keyspace (the total number of possible characters represented by the character classes in the passphrase), and follows NIST 800-63 guidelines.
- Visually and numerically presenting the entropy of user selected passphrases through the use of new tools to assist the change process. These tools included a passphrase strength meter that automatically calculated the passphrase entropy and visually reported a moving number and bar graph as the passphrase was being typed by the user.

In addition to the use of innovative technology measures, the improved Kerberos KDC architecture and upgraded passphrases enhanced support of business and administrative effectiveness by:

- Eliminating system downtime by abandoning dated middleware hardware and software.
- Increasing system availability by implementing a remote server at the UC Davis School of Medicine and a disaster recovery site.
- Ensuring uninterrupted access to federal resources by meeting new federal password security guidelines.
- Increasing the number of departments using the campus Kerberos KDC for departmental Windows pass-through authentication by improving interoperability using MIT Kerberos KDC and Microsoft Windows Vista (and subsequent Microsoft operating systems).
- Simplifying criteria for creating an acceptable, strong passphrase.
- Improving the data feeds that push passwords to the Kerberos KDC.
- Enhancing passphrase usability and security by implementing the ability for passphrases to accept all ACSII characters.
- Enabling all hosts running infrastructure services to support passwords greater than 8 characters.

UC Davis was able to achieve these efficiencies through broad collaboration and timely communication with:

- All owners of services using Kerberos, who helped select and tested password infrastructure.
- All IT service owners who operated legacy operating systems, who assisted in development of new standards and supported the decision to upgrade to passphrases.
- Campus advisory boards including the Technical Infrastructure Forum (TIF), TIF-Security subcommittee, Campus Council For Information Technology (CCFIT), and Information and

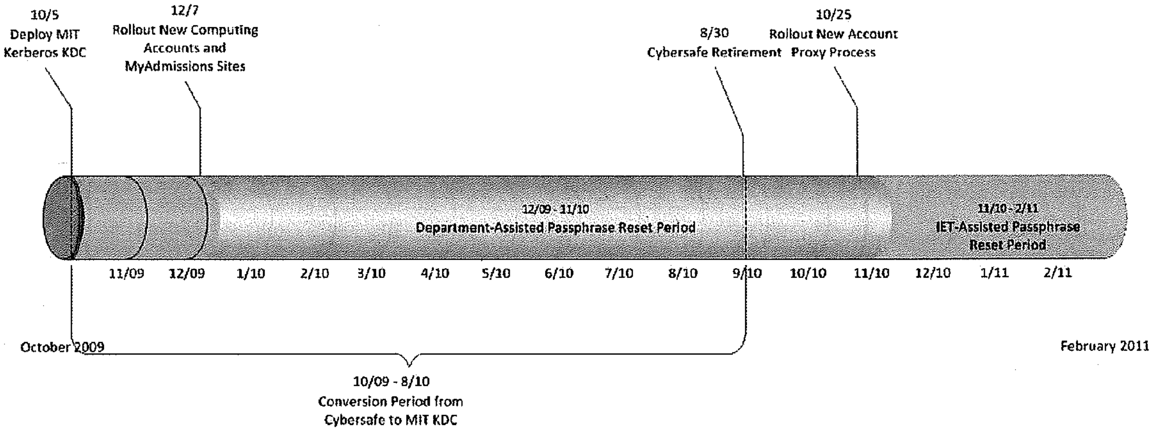
Educational Technology Leadership Council (IETLC), who provided input regarding the new standards.

- IT Express computing services help desk manager and staff, who provided guidance on password expiration strategy and managed the upgrade-related calls for assistance without increasing staff or hours.

Today, 97% of faculty, staff and student accounts meet the federal requirements. Campus account holders' credentials are more secure and the campus technical staff has begun to adapt the campus standards for their departmental passwords. The oversight committees that reviewed our work have a strong sense of participation in this project. Other campuses can benefit from our successes and lessons learned as they tackle authentication service upgrades and/or campus password improvements to meet UCTrust and InCommon Silver specifications.

PROJECT TIMELINE

The timeline below reflects the period of time during which the Kerberos KDC was replaced and campus Kerberos account passwords were upgraded to passphrases. The timeline does not include the initial project implementation, starting in October 2007, when we upgraded the underlying infrastructure.


10/5
Deploy MIT Kerberos KDC
12/7
Rollout New Computing Accounts and MyAdmissions Sites
8/30
Cybersafe Retirement
10/25
Rollout New Account Proxy Process
12/09 - 11/10
Department-Assisted Passphrase Reset Period
11/10 - 2/11
IET-Assisted Passphrase Reset Period
11/09
12/09
1/10
2/10
3/10
4/10
5/10
6/10
7/10
8/10
9/10
10/10
11/10
12/10
1/11
2/11
October 2009
February 2011
10/09 - 8/10
Conversion Period from Cybersafe to MIT KDC

PROJECT DESCRIPTION

Kerberos, a key component of UC Davis's Web single sign-on CAS service, is the most widely deployed system for authentication and authorization in modern computer networks, and the KDC is the enterprise workhorse for Kerberos transactions. At UC Davis, the Kerberos KDC currently serves up to 160,000 authentication transactions per day on average, and 1,400 per 10-minute interval during peak usage. Account holders include faculty, staff, students, and applicants.

In October 2007, a project formed to recommend a replacement for the Cybersafe software that powered the campus Kerberos KDC. Kerberos touches most components of our password infrastructure, so this change motivated a series of password infrastructure improvements and, ultimately, a password change for or expiration of all campus accounts.

The first part of this project, upgrading the KDC, focused on the technical work and collaboration with department and IT administrators who managed services that contacted the Kerberos KDC. The second part, upgrading the passphrase guidelines, focused on the development of new campus passphrase guidelines and involved many advisory groups. The third part, "upgrade to a passphrase" change campaign, focused on a campaign to change all Kerberos passwords, enforcing the new passphrase guidelines and re-encrypting the passphrases using federally recommended encryption standards.

Upgrading the Kerberos KDC

The UC Davis proprietary legacy Cybersafe Kerberos KDC did not meet current security standards for encryption and did not support modern Microsoft operating systems, and a project was formed to provide a recommendation and, ultimately, upgrade the KDC. In this section, we describe the two main parts of this work.

Selecting, Testing, and Determining the Architecture of the new KDC

We followed the standard project methodology for selecting and testing new Kerberos KDC software. We developed objectives, included campus technical staff on the decision team, and evaluated both commercial and open source options. Ultimately, we selected the MIT Kerberos software, now promoted by the MIT Kerberos Consortium and sponsored by key operating system vendors. Our architecture includes separating the account administration functions from the authentication functions. We also now support a remote server for authentication (ticket granting) and disaster recovery. Advantages include no service downtime for maintenance, regular security patch updates, timely feature improvements, and Microsoft and Unix compatibility.

KDC Transition – How to Move More Than 100,000 Accounts With No Client Impact

After selecting the MIT KDC, we worked with service owners who ran services that used the Kerberos KDC and selected encryption types (RC4, AES) and default account attributes (pre-authentication) to increase password security. We first anticipated setting up the Kerberos KDC and populating both the old and new KDCs during password changes. However, we wanted to retire the Cybersafe KDC as quickly as possible and tackled the move of the proprietary Cybersafe database to MIT database format with the assistance of an outside vendor. As soon as the database was moved and the MIT Kerberos KDC rolled out, service owners could point their services to the new KDC, and the Cybersafe KDC could be retired.

Improving the Password Management Infrastructure

Since our passwords are fed to a number of services, we worked with the administrators of the password feeds to enhance which ASCII characters could be included, removed the constraint of 7-8 characters, and improved the security of the feed transfer. We retired or upgraded systems running legacy operating systems that did not support more than 8 character passwords and designed tools to assist the 'Upgrade to a Passphrase' campaign. We developed a tool for technical staff to be able to know more about the status of account changes (when asked by an account holder) and a tool for staff who are authorized to assist with account changes, streamlining the assisted password reset process. We wrote scripts that informed the technical community about the status of accounts in their department. Most importantly, we integrated a look up of the password expiration status with CAS Web authentication logins so that account holders could know in a direct manner that they needed to change their password by a certain date.

Strengthening Password Security Guidelines – Balancing Convenience and Security

The major changes that we made to the password security included the mandatory setting of security questions, the calculation of password entropy (a function of password length and number of character classes) to determine password strength, and the option to use all ASCII characters (except one, no '$' at the beginning of a password due to MacOS limitation). A list of changes to our password security guidelines can be found in the section, Password Guideline Table. The average time to crack a campus password has increased from less than a year to thousands of years, and we now have a well-established method for expiring passwords. There was a lengthy consultation process for both developing the guidelines and seeking endorsements for them. Also, once the new service was deployed, we revised our entropy minimum and eliminated many of the password penalty rules.

Upgrade to a Passphrase Awareness Campaign

Early in the project, the team determined that the campaign could not rely on direct email messaging to raise awareness and encourage campus account holders to upgrade. In recent years, the campus has put a great deal of effort into raising awareness about phishing scams. Sending email messages stating that their passwords would expire by a specific date and a need for users to visit a Web site to upgrade to a passphrase would likely raise many questions in respect to message legitimacy and cause confusion in light of our anti-phishing efforts. Rather than rely on email, the project team developed the creative strategic marketing awareness program described below.

Campaign Web Site

A key communication component was the Passphrase Change Campaign Web site (http://security.ucdavis.edu/passphrase.cfm). This site outlines the purpose of the campaign and provides access to resources designed for specific audiences. Resources included links to:

- The Computing Accounts Web site (https://accounts.ucdavis.edu), where all users upgraded to passphrases
- A self-help article (http://xbase.ucdavis.edu/2019), which describes in lay terms how to create a strong passphrase
- The list of account proxies (http://email.ucdavis.edu/email/proxies.php) who can assist users with upgrades in the event that the user forgot their password
- Links to a password expiration calendar, PDF versions of fliers and posters, suggested email messaging, and other tools for technical support staff and proxies described in more detail below

Partnership with IT Express Computing Services Help Desk

The project team established and maintained open, bi-directional communication with our campus computing services help desk, IT Express, throughout this project. The project team kept help desk staff apprised of upcoming milestones and assessed expected user impact through informal group discussions and email. Meanwhile, help desk staff developed self-help documentation for users, tracked all calls related to this project and kept the project team apprised of the actual user impact of various components of this project (e.g., implementation of passphrase reset service for applicants, implementation of passphrase and security question requirement on central computing accounts Web site, password expirations) were having on their workload.

While the help desk prepared for an influx of calls at these project milestones, the flood never happened. In fact, as a result of the new self-help passphrase reset tool for applicants, the help desk received 70% fewer calls requesting passphrase reset assistance during the student applicant notification period in 2011 than in 2010.

Collaboration with Medical Center, Campus Technical Support Staff and Proxies

Nearly all campus departments have designated one or more technical support coordinator (TSC) and/or an account proxy. These groups provided critical support to the project team and users throughout the campaign as they provided front line support to faculty and staff. To assist these groups, the project team provided the following:

- A password expiration calendar, which showed which letter(s) expired on each day of the campaign; passwords expired by the first letter in the users login ID, beginning with Zs in October and ending with As in February
- A link from the campaign Web site to proxy resources, including information about becoming a proxy, how to request a password change token on behalf of a user, and who to contact for assistance
- A newly-developed Account Detective tool, which enables authorized staff to see if a particular user has upgraded to a passphrase
- Weekly status reports stating who within their designated department has/has not upgraded

Partnership with Design Program

IET communications staff partnered with faculty and students in the UC Davis Design program to develop student-focused visuals to assist with the campaign. Students were given the campaign slogan, *Upgrade to a Passphrase*, and asked to design materials to support this slogan. The partnership lasted one quarter, and students received independent study credits for participating. The resulting designs were used to create large-format posters, computer wallpaper, fliers and icons for campaign-related Web sites.

Piggy-backing on Re-carding Event

In fall 2010, all students were required to get new student identification cards. To facilitate this change, the campus organized a "re-carding event" from September 20 to October 8. The project team arranged with the re-carding event coordinators to have a table outside the event to share *Upgrade to a Passphrase* information with students. The project team hired two enthusiastic students, trained them to answer questions about the campaign and passphrase standards, and provided them with fliers and toothbrushes inscribed with the campaign slogan and URL to distribute.[2]

Major Campus Communication Outlets

In addition to the above, the project team partnered with established communication outlets to get the word out about the *Upgrade to a Passphrase* campaign. This included a campus directive in April 2010 and periodic items in *Dateline,* news for faculty and staff; *The California Aggie,* the daily student newspaper*; Friday Update;* and *Staff Voice*.

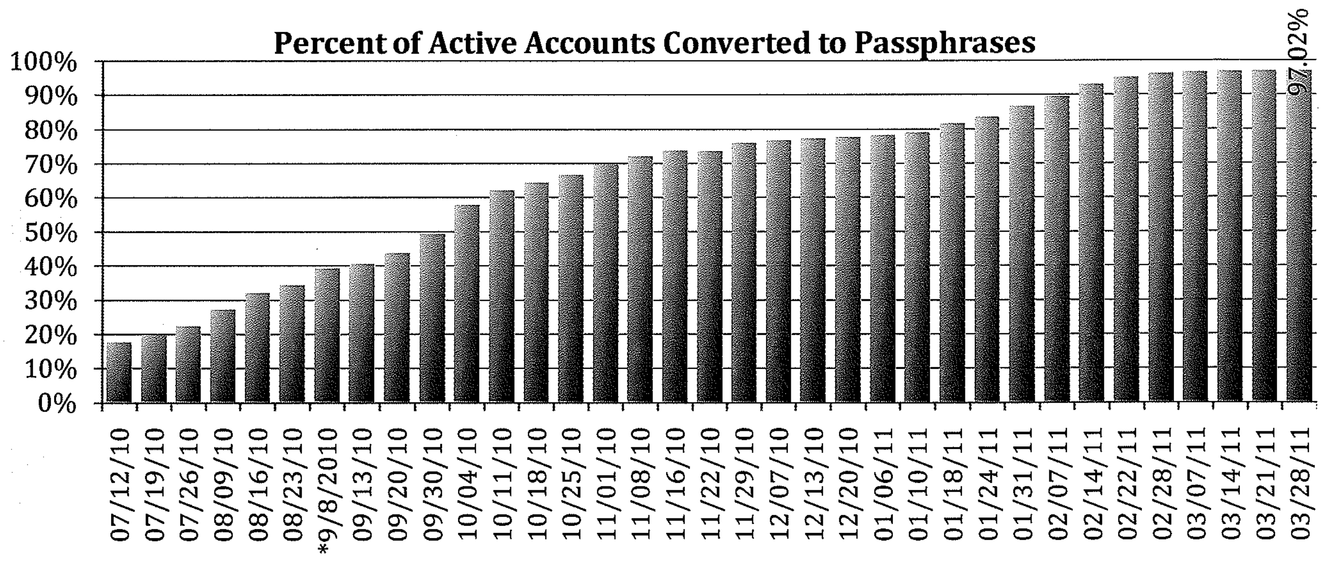
Central Authentication Service (CAS) Messaging

Old passwords were methodically expired by the first letter of the user's login ID beginning in October 2010 and ending in February 2011. To notify all campus account holders of their expiration date, a message was included on the CAS screen each time the user logged in stating

[2] 800 toothbrushes were distributed to students with the slogan, "Don't Brush off Security. Upgrade to a Passphrase." Note that this communication approach was adopted by another UC campus based on the project's success

their expiration date and where to go to upgrade. Messaging began two weeks prior to the assigned expiration date and continued until the user upgraded to a passphrase.

Upgrade Progress



- First date that student data is included in statistics. Prior to 09/08/10, only faculty and staff data was collected.

Password Guideline Table

We used this table structure to clearly show the differences between existing and proposed password standards during discussions with stakeholders across campus. The table has now been updated to reflect the deployed set of standards.

		OLD STANDARDS/PRACTICES	DEPLOYED STANDARDS/PRACTICES
Strengthh	Character Count	7 – 8 characters	• 12-64 characters. Minimum length based on entropy. The formula for entropy is log2 (keyspace) * length and is currently set to 72.3. If a passphrase uses 4 character classes, then the passphrase can be as short as 12 characters.
	Character Classes	All character classes required. Upper- and lower case letters, numbers, keyboard symbols except backslash (\); double quote ("); ampersand (&); semi-colon (;); single quote ('); and back quote (`)	• Allow but do not require all character classes. Minimum number of character classes is based on passphrase entropy. • Symbol character class expanded to include all symbols except $ at beginning and space at end.
	Dictionary Checks & Personal Data Rule	• Prohibits use of dictionary words. • Prohibits use of 3 or more consecutive letters from account name.	• No dictionary checks. • Continue to prohibit use of 3 or more consecutive letters from account name. • Prohibit birth date, first name, and last name.
	Strength Indicator	None	Implement
Reset	Pass Phrase History	No pass phrase history	• No passphrase history will be stored, but new passphrase will be compared with existing passphrase and use of the same will be disallowed.
	Confirmation	None	• Confirm successful or unsuccessful passphrase change via email.
	Setting Pass Phrase Questions During Reset	Optional	• Required. If opt-out, no self-service options will be available.
	Web Interface	• Existing interface is clunky. • Instructions are confusing. • No explanation provided when pass phrases are rejected.	• Interface improved. Added passphrase strength indicator. • Clarified instructions (including "anatomy" of a strong passphrase. • Stated reason(s) passphrases are rejected.
	Expiration Interval	• No expiration.	• Expiration to be evaluated annually and implemented if need identified (e.g., standards are not sufficient given existing conditions).

		OLD STANDARDS/PRACTICES	DEPLOYED STANDARDS/PRACTICES
Change Authorization	• 24/7 self-service on-line authorization • Authorization by Account Proxy • Authorization by IT computer lab staff • Authorization by IT Help Desk via phone/fax	Password change questions	• Online self service using password change questions and account attributes. • On-line self-service for undergraduate applicants.
		Proxy confirms user's identity, fax form to ITX, ITX issues token and informs proxy.	• Deployed a self service web application, allowing the Account Proxy to obtain a token for the account holder.
		IT computer lab staff confirms user's identity and issues a token to the user.	• Continued current process. A drop in use is anticipated due to self service option.
		ITX staff confirm user's identity via phone/fax process and issue a token to the user.	• Continued current process. A drop in use is anticipated due to self service option.

LESSONS LEARNED

- New federal guidelines provided a target standard for the UC Davis authentication infrastructure, and a timely and defensible rationale for forcing campus-wide passphrase upgrades.
- The campus technical and IT security community participated in the development of the campus standards and therefore accepted them and assisted in promoting them across campus.
- Close work with campus technical support staff over several months enabled them to work with individuals and groups within their departments slowly and steadily.
- Tools created for campus technical support staff enabled them to monitor progress and provide support within their departments as needed.
- No arbitrary deadline for completing passphrase changes was set and this flexibility proved critical as expiration dates were set around the academic schedule, midterms, finals, holidays and minor glitches.
- An extended "voluntary" passphrase upgrade period enabled account holders to set a passphrase at their convenience over the course of about 9 months. By the time expirations began – effectively forcing upgrades - over 50% of account holders already had passphrases. This helped manage central help desk and departmental technical support workloads.
- The extended timeline also enabled the project team to evaluate and refine the passphrase change web interface and self-help documentation prior to expirations.

Appendix A: Letters of Support for Sautter Award

UNIVERSITY OF CALIFORNIA, DAVIS

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO | SANTA BARBARA • SANTA CRUZ

RALPH J. HEXTER
Provost and Executive Vice Chancellor

OFFICE OF THE PROVOST AND EXECUTIVE VICE CHANCELLOR
ONE SHIELDS AVENUE
DAVIS, CA 95616
TEL: (530) 752-4964
FAX: (530) 752-2400
INTERNET: http://provost.ucdavis.edu

May 19, 2011

Larry L. Sautter Award Committee:

It has become essential for universities to offer secure and robust authentication services to ensure individuals are who they claim to be when accessing automated systems. At UC Davis, we have recently developed and implemented progressive approaches to upgrade and enhance the university Kerberos system, the core authentication technology for campus and UC Davis Health System community members.

While the Kerberos and Passphrase Upgrade project began before my arrival at UC Davis, I have come to value the overall security program as a proactive investment in our campus community and this initiative as an integral part. With this in mind, I was so pleased to learn of this project and how the project permitted the campus to continue its excellent progress in the area of IT security through innovative technology use.

Protecting our computing resources is critical to maintaining a strong and trustworthy presence in research, teaching and public service. I am proud that UC Davis is a leader within the University of California campuses when it comes to information technology security programs. With the Kerberos and Passphrase Upgrade Project, we not only enhanced security, but we also achieved a high level of compliance with new Federal password management guidelines, an accomplishment that helps ensure that faculty and staff have continued access to federal electronic resources. In fact, with this project, UC Davis is among the very first universities to reach this level of compliance for passphrase strength.

This project is yet another way that UC Davis is leading the way in computer and network security. I recommend that the project be considered for system-wide recognition as a recipient of the Larry L. Sautter award for innovative use of technology.

Sincerely,

Ralph J Hexter

Ralph J. Hexter
Provost and Executive Vice Chancellor

UNIVERSITY OF CALIFORNIA, DAVIS

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

ONE SHIELDS AVENUE
DAVIS, CALIFORNIA 95616-8558
(530) 752-4998
FAX: (530) 754-6550

May 19, 2011

Larry L. Sautter Award Committee:

Security is critical to the University mission, and Kerberos is a core element of UC Davis's authentication infrastructure. Accomplishing the challenging task of upgrading nearly 60,000 accounts to passphrases is not only a testament to the quality of our security program, but also to the security commitment of every student and faculty and staff member at UC Davis.

Few campus projects require action from every community member, and making such a project successful depends upon a high level of awareness and understanding as well as a quick and easy-to-complete process. The creative, innovative and highly collaborative approach the project team developed – from the online self-help resources and applications to the email-free awareness campaign that touched the entire campus community – can easily serve as a model for other campuses undertaking similar endeavors.

I am pleased with the outcome of this project and with all those who contributed to its success. The Larry L. Sautter Award would be an excellent way to acknowledge this accomplishment.

Sincerely,

Peter M. Siegel
Chief Information Officer and Vice Provost
Information and Educational Technology

UNIVERSITY OF CALIFORNIA, DAVIS

BERKELEY • DAVIS • IRVINE • LOS ANGELES • MERCED • RIVERSIDE • SAN DIEGO • SAN FRANCISCO   SANTA BARBARA • SANTA CRUZ

ONE SHIELDS AVENUE
DAVIS, CALIFORNIA 95616-8558
(530) 754-6857

May 19, 2011

Larry L. Sautter Award Committee:

Over the course of this ambitious project, the project team worked closely with the campus technical community, including the Technical Infrastructure Forum-Security Subcommittee. TIF-Security formed a working group that met with the project team on several occasions to help determine the impact the new passphrase standards would have on systems across campus. The working relationship that developed as a result of the working group led to a mutual understanding of challenges both sides faced, and I believe that gaining that understanding contributed to the success of this project.

The best thing, from the technical support position, about this whole project is that we now have an automated way to handle proxy reset requests. Until this project, assisting a client who had forgotten their password and security questions with a passphrase change required that we make a copy of the client's photo ID, fax it to the help desk, call the help desk to see if the fax arrived, then request a passphrase change token. And, this was impossible to do after business hours. Now, we complete a simple online form and receive the token within a few seconds. Finally! A fast and secure proxy reset process.

I applaud the project team for going the extra mile to engage the technical community in a meaningful way and appreciate that the project team has credited the technical community for their critical role in the success of this project.

Sincerely,

Ken Jones

Ken Jones
TIF-Security Subcommittee Chair