Campus IT Forum
Thursday, May 7, 2015
Agenda

1. Welcome
2. Introduce New/Transitioning Staff
3. Announcements
   A. IT Council News
   B. Connect Project Update
   C. Secure Research Computer Environment Overview
   D. Password Wallet Overview
4. Bring Your Own Device Discussion
New Staff

INTRODUCTION
ETS Staff Update

New Staff

- LOREN BROWDY, IT Support Desk Technician
- DARLENE CRAWFORD, Change Management & Training
- SEAN JACKSON, IT Support Desk Technician
- SCOTT LEON, Electronics Technician
- KATIE MANKINS, PMO Director
- VICTORIA MANTHE, Business Relations Analyst
- HANNAH MORAND, Fiscal & Budget Support Specialist
- JOSH PRESTON, Senior Linux & Network Engineer

Transitions

- KIRK GRIER, Infrastructure Director
- SHAJAN KAY, Business Relationship & Services Manager
- CHRIS ROSENSTOCK, Telecommunications Systems Systems Manager
ETS Open Recruitments

- END USER COMPUTING ARCHITECT
- SERVICE & BUSINESS RELATIONSHIP MGR-END USER COMPUTING
- PEOPLESOFT LEAD DEVELOPER
- PEOPLESOFT DEVELOPER
- SENIOR IT ENGINEER
- SOFTWARE ENGINEER
- SUPERCOMPUTING CONSULTANT
- SR. INFORMATION SECURITY FORENSICS AND PEN TESTING LEAD
- SR. CAMPUS INFORMATION SECURITY CONSULTANT
IT Council Roster (January 2015)

Denise Stephens, Interim CIO, Chair
Bruce Bimber, Political Science
Cindy Bumgarner, Summer Sessions
Linda Flegal, College of Letters & Science
Jacob Godfrey, Business & Financial Services
Alan Grosenheider, Library
Carl Guitierrez-Jones, Undergrad Education
Chuck Haines, Budget & Planning
Karen Hanson, Office of Research
Janowicz Krzysztof, Geography
Alan Liu, English Department
Mary Lum, College of Letters & Science

Michael Miller, Financial Aid & Scholarships
Jeffrey Monteleone, Facilities Management
Alex Parraga, News and Communications
Chris Pizzinat, Development
Lisa Sedgwick, Office of EVC
Cynthia Seneriz, Human Resources
Timothy Sherwood, Computer Science
Robert Silsbee, Office of VC for Admin Services
Christian Villasenor, Graduate Division
Kirk Grier, ETS Infrastructure, Ex-Officio
Sam Horowitz, CISO, Ex-Officio
Advisory Groups

- Academic
- Administrative
- Data Center
- Information Security
- Infrastructure
- Research
- Student Support
ETS presented an assessment to the IT Council and IT Board in early 2015.

The assessment included:

- Business needs assessment for email and calendaring services
- Google Apps proof-of-concept
- Testing methodologies used to compare the Office365 and Google Apps platforms
- Analysis of the Google Apps and Office365 service offerings
- Detailed implementation scenarios for Office365, Google Apps, and dual-platform co-existence
Connect Project Status Update

ETS and LSIT are working together on a project proposal for Google Apps.

The proposal is scheduled to be presented to the IT Council on May 21.
Secure Compute Research Environment

OVERVIEW
Problem Definition

Researchers working with restricted data must provide Data Security Plans (DSP) to the granting agency.

Computing environment defined in DSP is usually a stand-alone, offline computer in a secure, locked room.

Researcher must be physically on-site in to interact with computer and perform data analysis.

Significant costs to set up, change door locks, and dedicate space for one computer.

Higher probability of errors due to multiple parties’ involvement.

Each DSP has to be individually signed off on by Campus Information Security Officer.
Project Goals

Meet researchers’ needs for data security, ease of use, and software package availability

Meet data providers’ needs for data security and technical controls

Ease technical burden on local IT staff

Reduce time investment by CISO on approval of DSPs

Achieve widespread usage of the service and improved security posture for the campus
Architecture Goals/Solutions

Develop a secure research computing environment

• Establish a private secure network for research data using a Virtual Desktop Environment (VDE).
• A “Research Virtual Desktop” is an isolated researcher desktop environment.

Provide secure remote access to VDE using a web VPN portal

  • Duo security = push App, SMS code or phone code
Access from any device with an HTML 5-compliant browser.
  • works with iPads/tablets
  • no client software needed
  • works with all modern web browsers (IE 10/11, Firefox, Safari, Chrome); no plug-in installation required

Create software license pool

Provide common software on VM guest systems.
  • R, Stata, SPSS, Mathematica, Matlab, Microsoft Office suite, Adobe Acrobat Pro

Provide secure file transfer capabilities

Bring files into secured environment and scan for malware: File Transfer Gateway web application.
Security Controls - Policy

Defense in Depth principles

Use Critical Security Controls (CSC Top 20) checklist for effective cyber defense

Develop crosswalk documents mapping controls with federal guidelines for controlled unclassified information:

- NIST SP 800-53 rev4 (Security and Privacy Controls in Federal Information Systems and Organizations)
- DoD - all new contracts now require DFARS clause 252.204-7012 (Safeguarding of Unclassified Controlled Technical Information)
  - a minimum subset of controls from NIST SP 800-53 rev4
  - SC-13 requires if cryptographic protection is in use, it must be NIST FIPS 140-2 Level 1 certified - Security requirements for Cryptographic Modules
- NIST 800-171 draft - future - “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations”
## Security Controls

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Host-based firewalls</strong></td>
<td>• Authorized hosts have limited access to provide only necessary services.</td>
</tr>
<tr>
<td><strong>Network level firewalls</strong></td>
<td>• Access control lists are enforced by the VPN.</td>
</tr>
<tr>
<td><strong>Limited access to software updates through proxy</strong></td>
<td>• No direct internet access.</td>
</tr>
<tr>
<td><strong>No administrative privileges</strong></td>
<td>• Users cannot install software or modify host-based firewalls, etc.</td>
</tr>
<tr>
<td><strong>Logging</strong></td>
<td>• All authentications/access/file transfer activity is logged.</td>
</tr>
<tr>
<td><strong>Encryption in Transit</strong></td>
<td>• All network traffic to guest VMs travel over encrypted protocols (TLS/SSL).</td>
</tr>
<tr>
<td><strong>Session Timeouts</strong></td>
<td>• Session timeouts will be enforced on portal login and remote desktop RDP.</td>
</tr>
<tr>
<td><strong>Encryption in Use</strong></td>
<td>• VM hosts hardened and ACLed on private network.</td>
</tr>
<tr>
<td><strong>Encryption at Rest</strong></td>
<td>• Each guest VM has an encrypted data volume where secured &amp; intermediate data resides.</td>
</tr>
<tr>
<td><strong>Where allowed, backups of encrypted data volumes stored in physically secure location</strong></td>
<td>• No other components will regularly be backed up.</td>
</tr>
</tbody>
</table>
Web Portal Login
Portal Login - Duo

[Image of the portal login page]

Secure Compute Research Environment Portal

Developed in cooperation with the Institute for Social, Behavioral and Economic Research, and funding from the Office of Research

Two-Factor Authentication

Powered by Duo Security

Protect Your UCSB Account

Two-factor authentication enhances the security of your account by using your phone to verify your identity. This prevents anyone but you from accessing your account, even if they know your password.

This process will help you set up your account with this added layer of security.

Start Setup
Portal Login - Duo Push
Portal Bookmarks
Login/Remote Desktop
Login/Remote Desktop

WARNING - Restricted Access

You are attempting to access a computer system with restricted access data, operated by the University of California, Santa Barbara (UCSB). If you do not have the appropriate permissions, you should not proceed.

Unauthorized use of these data is subject to penalties imposed by UCSB and/or the providers of the data. Unauthorized Access to Data (Individually Identifiable Information) on this computer is a violation of Federal Law and will result in Prosecution.

By continuing to use this system, you indicate your awareness of and consent to these terms and conditions of use.

OK
Remote Desktop

UCSB ETS
Secure Compute Research Environment

User Name: test
Host Name: RES-GUEST-TMPLT
Login Time: 2/24/2015 8:01AM

IP Address: 192.168.1.65
MAC Address: 52:54:00:EC:75:AC
Boot Time: 2/24/2015 4:28 AM
CPU: Dual 2.6 GHz Intel Xeon E312xx (Sandy Bridge)
Memory: 8192 MB
OS Version: Windows 7
Service Pack: Service Pack 1
Questions?

Website: ets.ucsb.edu/services/secure-compute-research-environment
Email: scre-support@lists.ets.ucsb.edu
Password Wallet

OVERVIEW
Password Management

Problems

• too many passwords
• same password for multiple sites

One Solution

• a password manager

• Password Wallet is a password manager that works on Windows and Macintosh.
• ETS pays the license cost.

More information and links to PW Wallet:
http://www.ets.ucsb.edu/security/password-management
Password Wallet

- Amazon.com
  - URL: www.amazon.com
  - Username: Gjetson
  - Password: jane
- Citibank
- EBAY Login
- My Apple.com
- Online Investments
- Spacecraft Traffic School
- University Library
  - URL: http://www.library.university.edu
    - Username: JetsG
    - Password: read76
- Category: None
- Browser: Default Browser
- Notes:

Modified 2/24/10, accessed 11/3/08
DISCUSSION

Bring Your Own Device
1. How do you define BYOD?

2. What challenges with BYOD are you encountering in your area?

3. What BYOD trends are you noticing?

4. What strategies have you been using to manage BYOD? How are they working?