Agenda

Secure Compute Research Environment

1. Problem Definition
2. Project Goals
3. Architecture Goals and Solutions
4. Admin Process Goals
5. Security Controls - Policy
6. Security Controls
7. Screen Shots
8. Future Growth of Service
9. Questions
What’s a data security plan?

<table>
<thead>
<tr>
<th>Why is a data security plan needed?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Most restricted data providers require a data security plan before access to sensitive data is authorized.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>What’s included?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• What data will be used?</td>
</tr>
<tr>
<td>• How will data be used?</td>
</tr>
<tr>
<td>• Who will work with the data?</td>
</tr>
<tr>
<td>• What are the plans for notifying authorities in case of a real or suspected breach of security?</td>
</tr>
<tr>
<td>• How will data be accessed, stored, and destroyed?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Typical Minimum Standards:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• A standalone computer in a uniquely-keyed physical location</td>
</tr>
<tr>
<td>• A standard user account with a strong password</td>
</tr>
<tr>
<td>• No internet connection</td>
</tr>
<tr>
<td>• USB/optical media disabled</td>
</tr>
<tr>
<td>• Printing disabled</td>
</tr>
<tr>
<td>• Antivirus installation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Who approves data security plans?</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Chief Information Security Officer (CISO)</td>
</tr>
<tr>
<td>• Data provider</td>
</tr>
</tbody>
</table>
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.
Administrative Process Goals

1. Create a “pre-approved by CISO” Data Security Plan “template” documenting technical details of this service that can be provided to majority of granting agencies.

2. Develop administrative process in which SCRE research virtual desktop “request” form is initiated as part of grant proposal w/ Secured Data Set.

3. Intake of Secure Data Set/physical media custody.

4. Provide end-user documentation for use of the system.

5. Create documentation for final “operator” of service.
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 - Policy

Develop crosswalk documents mapping controls with other third-party restricted data provider requirements, as required by researchers.

Third-party data providers/Agencies in progress:

- Department of Education (Institute of Education Sciences)
- University of Michigan AddHealth
- University of Michigan Panel Study of Income Dynamics
- CA Health and Human Services Agency
## Security Controls

<table>
<thead>
<tr>
<th>Security 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

Secure Compute Research Environment Portal

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

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

Power 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

Duo Mobile now
Login request: Secure Research Computing Portal
slide to view

UCSB
ETS SCRE File Transfer Gateway

john_doe
128.111.12.64
Santa Barbara, CA, US
3:11 PM PST
January 21, 2015

Approve
Deny
Portal Bookmarks

Web Bookmarks

- **Login to my SCRE Research Virtual Desktop**
- Login to your default SCRE Research Virtual Desktop
- **SCRE File Transfer Gateway**
- Transfer files in/out of your SCRE Research Virtual Desktop
- SCRE Service Info
- SCRE Service Info - Support, Request Forms
Login/Remote Desktop
Login/Remote Desktop
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 4:26 AM
CPU: Dual 2.6 GHz Intel Xeon E312xx (Sandy Bridge)
Memory: 8192 MB

OS Version: Windows 7
Service Pack: Service Pack 1
# Future Growth of the Service

## v.1.x

- Promote service availability to other department/ORU MSOs
- Develop Crosswalk document mapping DSP against requirements in CSC, NIST 800-53 and DFARS clause
- Determine costs for future pricing as “Service” offered to campus
- Develop internal SCRE service monitoring systems

## v. 2.0

- Linux virtual research desktops (VM guests)
- VM resource management (auto-start VM upon user login)
- Transition operation of service from SOC to data center/VDI group within ETS
- Windows expertise - Active Directory - scale group policies/users
- VDI expertise - scale service
QUESTIONS

Website: ets.ucsb.edu/services/secure-compute-research-environment

Email: scre-support@lists.ets.ucsb.edu