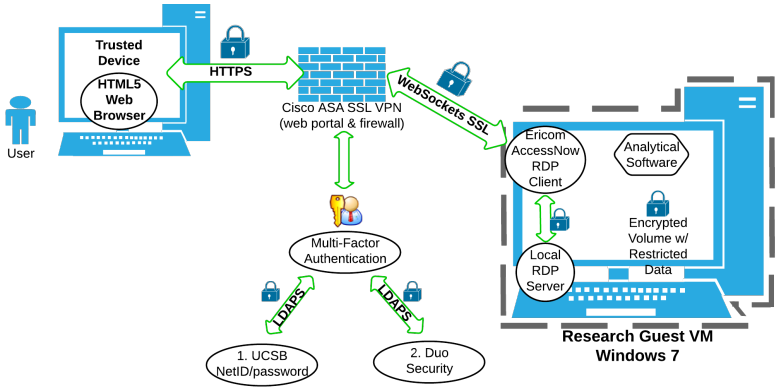
Secure Compute Research Environment
Data Security Plan (DSP)

Overview

The Secure Compute Research Environment (SCRE) is a private, secured virtual environment designed for University of California, Santa Barbara researchers to securely store, access and analyze restricted data in a remote desktop session, without storing data on local computers.

The user experience is similar to a Remote Desktop session, but additional significant security controls are in place around and within the environment, while still remaining to be simple and straightforward for the researcher to use.

Secure Compute Research Environment - User Workflow



Access to the SCRE is protected by strong, multi-factor authentication, and can be accessed from any HTML5 web browser from multiple platforms (Mac, Windows, Linux, tablets etc.) Industry-standard security protocols are used for end-to-end encryption and encryption at rest. All network traffic is encrypted between the user desktop all the way to the research Virtual Machine (VM) guest. Restricted data resides on the research VM guest on a separate virtual disk image, also protected by strong encryption. All services and network access controls within the SCRE operate on the "minimum services, "minimum permissions" and "default deny" principles, with specific exceptions made in firewalls and access control lists to allow only for hosts/services needed for secure operation of the service.

The SCRE was designed using the "defense-in-depth" security principle, in which security controls are put in place at multiple layers of the environment. Additionally, a checklist based on the Top 20 Critical Security Controls was created for initial deployment as well as regular review of this service and environment. These controls are intended to meet and exceed the data security plan requirements for the majority of secure data providers/agencies.

The remainder of this Data Security Plan will outline the security controls in place in the SCRE, and address specifically which objectives are met and how.

Physical Access

The SCRE is hosted on servers on a private, dedicated, secure non-routed network. The VM server host hardware, VPN hardware and network hardware are located in locked racks in North Hall Data Center (North Hall 1201A) on the UCSB campus. The North Hall Data Center is staffed during standard university business hours (5 days a week, 8am-5pm). UCSB Personnel accessing the NHDC must present a UCSB-issued Access Control/ID KeyCard. The NHDC has video surveillance systems that record all activity in NHDC.

Host Security

Each researcher and enrolled research project is assigned a unique and dedicated VM guest image on a VM server, referred to in customer communication as a "SCRE Virtual Research Desktop." Each VM guest has an up-to-date Windows 7 Enterprise operating system installed with a package of standard research software. Each VM guest is "hardened"- only necessary services are installed, running and listening on each VM guest and the Microsoft Enhanced Mitigation Experience Toolkit is installed for additional security. Enrolled researchers are assigned a standard (non-administrative) account on the VM guest with a unique strong password (14 characters: mixture of numbers, lowercase, uppercase letters and special characters, no dictionary words). Researchers can not install software or modify the VM guest system in any way.

Network Security

There are 5 segmented networks within the SCRE, differentiated by traffic type and scope:

- Private non-routable Networks
  - Admin VM Guests – Internal Services (Authentication, DNS, DHCP, Proxy, HIDS, Logging, Proxy)
  - End-User VM Guests - Research Virtual Desktops (RDP, Software License Checkout, Proxy)
- Public Internet routed Networks
  - VM Host Management - Lights-Out (filtered by ACL – Default deny - Allow in from Operator subnet only)
  - VM Host and VPN Management – SSH, HTTPS (filtered by ACL – Default deny - Allow in from Operator subnet only)
  - Admin Hosts – (filtered by ACL – Default deny – Allow in/out defined services/protocols between trusted hosts/networks):
    - VM Admin Guests - Management services: HTTPS, SSH
    - Campus services: DNS, NTP, LDAPS (Authentication), SMTP (outgoing HIDS notifications)
    - External Service Providers: HTTP proxy to whitelisted trusted software update providers, LDAPS to Duo Security

- All systems within the SCRE have network interfaces connected to **only** the necessary networks, and services are limited to running only the appropriate network interface(s).
- All systems within the SCRE have software firewalls installed, running in *default deny* mode, with specific ingress/egress exceptions made for above-defined services/protocols required for operation of the SCRE.

- Access Control Lists (ACLs) exist on all networks that communicate with the public Internet, in *default deny mode*, with specific ingress/egress exceptions made for above-defined services/protocols required for operation of the SCRE.

"Research Virtual Desktop" VM guests, which sit on a private, non-routable VLAN, do **not** have direct access to the public Internet. VM guest firewalls allow specific exceptions only for the following services *to and from specific hosts on the 2 private SCRE networks:*

- Ingress
  - IP address assignment from DHCP server to VM Guest
  - Ericom AccessNow server running on VM Guest (provides clientless RDP view session in HTML5 web browser) from VPN Proxy
- Egress
  - IP address assignment from DHCP server to VM Guest
  - Name resolution to local DNS server
  - License checkout with local license server (research software)
  - HTTP Proxy server (provides limited access out to obtain authorized and whitelisted operating system, application and antivirus updates to VM Guest)
  - Secure logging over TLS from VM Guest to local syslog server
  - Host Intrusion Detection System (HIDS) logs to local HIDS server

Network Access Controls

Researcher authentication/authorization
Researcher access to the SCRE is controlled by a dedicated VPN web portal which allows remote access from any device running an HTML5 browser on the public internet. Portal access is protected by multi-factor authentication. The research must complete ***all*** of these authentication methods to login to the web portal:

- Local RADIUS server – username must be defined as enrolled SCRE user
- UCSBNetID and password (campus Identity service) authentication
- Duo Security authentication (Duo Mobile App on smartphone, SMS codes or Duo Phone Callback)

Remote Desktop access (Ericom AccessNow) to the VM guests on the private network is restricted to authenticated connections originating from the VPN proxy only. VPN access control lists (ACLs) permit communication only between authenticated users and SCRE VM guests. The RADIUS server assigns unique access controls to each user's Ericom AccessNow RDP client settings to permit communication only between an authenticated user and his/her assigned VM guest. Network ACLs restrict egress communication from the VPN proxy to necessary services - domain name service (DNS) and network time protocol (NTP) - on the campus network, and to Duo Security over HTTPS (for multi-factor authentication) on the public Internet.

The following controls have been enabled to limit potential for unauthorized access during remote access sessions:

- Custom Login Warning Text displayed upon Windows session login – "restricted data"
- Windows Screensaver on Guest VM – 3 minute timeout
- Ericom AccessNow Remote Desktop session timeout – 25 minutes
- VPN web portal session timeout - 30 minutes

Management authentication/authorization
Management access to SCRE admin systems is controlled by unique username/strong passwords:

- IPMI (Lights Out Management)
- SSH (admin VM host servers, VM guests and VPN)
- VPN Java client
- HTTPS servers: Log Analysis, Wiki

Encryption in Transit

- End-User Traffic
    - Authentication to VPN web portal/Login to File Transfer Gateway:
        - Authentication traffic to/from local RADIUS server occurs on private network
        - Authentication traffic to/from campus LDAP server is encrypted using TLS/SSL using public key infrastructure (PKI) with a 128-bit RSA SSL certificate
        - Authentication traffic to/from Duo Security service over LDAPS and HTTPS is encrypted using TLS/SSL using PKI with a 128-bit RSA SSL certificate
    - Remote Desktop activity:
        - HTTP traffic between the end-user's web browser and VPN portal is encrypted using TLS/SSL using using PKI with a 256-bit RSA SSL certificate issued by InCommon Server CA
        - From the VPN, proxied WebSockets/HTML5 access to each VM Guest is encrypted using TLS/SSL, using PKI with a self-signed 128-bit RSA SSL certificate, to the Ericom AccessNow server on the VM Guest, which connects to RDP on VM Guest localhost
- Admin Management Traffic
    - VPN management Java client - encrypted using TLS/SSL using PKI with a 256-bit RSA SSL certificate issued by InCommon Server CA
    - IPMI host management – SSL – using PKI with a 256-bit RSA SSL certificate issued by InCommon Server CA
    - SSH host management – encrypted using 256-bit RSA keys
    - HTTPS management – (log analysis, wiki) - using PKI with a 256-bit RSA SSL certificate issued by InCommon Server CA
    - Outgoing syslog traffic to log server – signed and trusted keys self-signed CA
    - Outgoing HIDS agent to server notifications – encrypted using agent encryption/authentication keys and sent over private network

Encryption at Rest

Restricted data and interim research data on each VM guest are stored on a separate virtual hard drive (VHD) image containing a BitLocker password-protected fixed volume, encrypted with AES 256-bit cryptographic keys (no diffuser). Each encrypted volume is assigned a unique, strong password (14 characters, mixture of numbers, lowercase, uppercase letters and special characters, no dictionary words), which must be provided when mounting the volume. Restricted data volume BitLocker passwords are **not** saved or escrowed in any

fashion, and are the sole responsibility of the user/researcher. At time of BitLocker encryption of the restricted data volume, **no BitLocker recovery key is saved, printed or escrowed**. These controls provide *FIPS 140-2, level 1 compliance for the restricted data volume*.

User system variables are set so that all application temporary/scratch files are also stored on this encrypted volume. No restricted data shall be stored on unencrypted or system volumes at any time.

The VHD/BitLocker encrypted volume will automatically detach/re-lock upon user's Windows session logout.

Data Security/Integrity

After login to the VPN web portal, researchers are presented with unique bookmark links that provide access to only the researcher's dedicated VM guest. Upon Remote Desktop login to the VM Guest, researchers are presented with the following warning dialog:

> *"WARNING - You are attempting to access a computer system with restricted access data, operated by the University of California, Santa Barbara (UCSB). If you do no have the appropriate permissions, you should not proceed. Unauthorized use of these data is subject to penalties imposed by UCSB and by 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. "*

No removable media (USB flash drives, optical media) are accessible from the VM Guest. Printing and copy/paste are also disabled on the VM Guest. There is *no access to outside Internet sites* and *no access to email providers* from the VM Guest. An antivirus program is installed and active on the VM Guest, and receives signature updates daily from a trusted provider, through the HTTP proxy server.

Researchers are permitted to access the SCRE File Transfer Gateway through the proxy server. The File Transfer Gateway is a custom internal HTTPS web application (also protected by multi-factor authentication and end-to-end encryption) that provides a mechanism for researchers to securely transfer files in to their Research Virtual Desktop for further analysis.

Files uploaded into the File Transfer Gateway are viewable only from a Research Virtual Desktop, and by the user that uploaded them. Files are scanned for viruses upon upload and infected files are logged and discarded. Files that have not been downloaded from a user's directory on the File Transfer Gateway are automatically deleted when they reach 7 days age.

Where permitted by the restricted data provider, researchers may request the ability to export files from their VM Guest using a secure File Transfer Gateway. In this situation, as well as at the end of any research project, a disclosure review by the PI on each file will be required before any files are exported.

Credential Review/Access to Data

Only users who have signed the appropriate license documents from the restricted data provider will be assigned accounts within the SCRE. The Operator of the SCRE shall sign all appropriate license and non-disclosure documents.

The Operator of the SCRE will perform initial secure intake of the restricted data set, labeling physical media with an assigned project ID number, date, etc. and will perform secure upload of data set from a secured SCRE Operator Workstation to the researcher's assigned VM Guest/Research Virtual Desktop.

The Restricted Data provider or Principal Investigator of an enrolled research project may request termination of a user's access at any time. The Operator will terminate a user's access within 24 hours of notification by authorized personnel and will notify the Principal Investigator of such activity.

Operator will maintain confidentiality of passwords for all accounts. Passwords will be changed if they are suspected of having been, or are known to have been, disclosed.

All active projects utilizing restricted data within the SCRE will be reviewed on an annual basis to ensure that the project is still active and that are no personnel changes on the license that will require revocation of credentials.

Any stored temporary/scratch files in the encrypted volume in the Z:\USERTMP directory will be secure erased by a scheduled job running on the 1st of every month, using the Eraser program with US DoD 5220.22-ME standard.

At scheduled end of project, all VM Guest images will be secure erased by the Operator using the secure-delete Linux packages (srm) command. All physical media will be returned or destroyed, per restricted data provider license agreement.

Logging/Auditing

All systems within the SCRE have operating system and application level logging enabled, forwarded in real-time over a TLS-encrypted TCP connection to an internal syslog server for central storage and analysis. System logs are reviewed on a daily basis by the Operator. Log timestamps on all VM guests are synchronized from the VM host, which synchronizes time via Network Time Protocol (NTP) to the UCSB campus timeservers.

Additionally, a host-based intrusion detection (HIDS) agent is installed on each administrative system within the SCRE, to ensure integrity of the operating system, application software and configuration files. HIDS notifications are sent in real-time from the HIDS server to an email address reviewed on a daily basis by the Operator.

Quarterly network vulnerability scans will be performed on all SCRE networks and compared with baseline scan results to provide a report of listening services and application patch levels, where possible.

Updates/Maintenance

All systems (both administrative VM guests and end-user Research Virtual Desktops) are kept up-to-date with Operating System and Application updates/patches and anti-virus signature updates through the proxy. End-user research VM guests check for and install OS updates daily. Admin VM guests check for and install updates OS daily. Additionally, a monthly maintenance window is defined for any significant update activities that may require a service outage.

Backups/Disaster Recovery

Where permitted by restricted data provider, and requested by the researcher, backups of encrypted volumes (where restricted datasets are stored) are performed. Such backups will be performed weekly, encrypted (encryption key only in Operator possession) and stored in a physically secure location (NHDC listed above).

Roles/Responsibilities/Personnel

Security & Policy

- Review and approval of Data Security Plan
- Sign-off, as required, on Restricted Data License applications
- Electronic Security and Policy

Samuel Horowitz
Chief Information Security Officer
University of California, Santa Barbara
803-893-5005
samh@ucsb.edu

Technical Implementation

- Systems and Network Architecture
- Systems and Network Administration
- Systems and Network Security
- Development of Data Security Plan

Jennifer Mehl
Information Security Analyst
University of California, Santa Barbara
(805) 893-5080
jennifer.mehl@ucsb.edu

Technical Support

- Provides limited technical support to end-users/researchers

- Provides limited technical support to departmental IT personnel

Jennifer Mehl
Information Security Analyst
University of California, Santa Barbara
(805) 893-5080
jennifer.mehl@ucsb.edu

Operator

- Intake and Physical Security of restricted dataset
- Manages Credentials to SCRE
- Creates VM Guests/Research Virtual Desktops
- Communicates with Principal Investigator for credential and restricted dataset management
- Performs Backups
- Performs Regular Log Analysis

Jennifer Mehl
Information Security Analyst
University of California, Santa Barbara
(805) 893-5080
jennifer.mehl@ucsb.edu

Data Center

- Maintains physical security of SCRE servers & network hardware

North Hall Data Center
University of California, Santa Barbara

Principal Investigator

- Reviews qualifications, criteria and approves all project personnel
- Maintains list and qualifications of project personnel/end-users
- Communicates with SCRE Operator for credential and restricted dataset management
- Maintains list of restricted data files and acts as data custodian
- Responsible for reporting to restricted data provider/agency

Requester/User

- Requests use of SCRE Service/Research Virtual Desktop
- End-User of SCRE Service/Research Virtual Desktop