Simplifying Secure Access and Analysis of Restricted-Use Data
Secure Compute Research Environment

SUBMITTED BY

Jennifer Mehl
Information Security Analyst
Enterprise Technology Services
University of California, Santa Barbara
jennifer.mehl@ucsb.edu

UCSB PROJECT TEAM

- Jennifer Mehl, Information Security Analyst, Enterprise Technology Services
- Kevin Schmidt, Director of Networking, Communications and Security Services, Enterprise Technology Services
- Brendy Lim, System Administrator, Institute for Social, Behavioral and Economic Research
- Nicholas Brown, Developer, Engineering Computing Infrastructure & Letters & Science Information Technology
- Dr. Stuart Sweeney, Director of the Institute for Social, Behavioral and Economic Research and Professor, Department of Geography
- UCSB Office of Research

PROBLEM DESCRIPTION

Restricted-use Data providers/agencies often require a minimum set of security controls in a Data Security Plan in order to approve usage of restricted data containing personally identifiable information (PII). These security controls are burdensome for an individual researcher to set up and maintain, and often include things like: standalone computer in a uniquely-keyed physical location, a standard user account with a strong password, no internet connection, USB/optical media disabled, and an antivirus installation.

Additionally, these requirements create issues with campus space allocations, significant financial commitments to researchers, and burdens on the local IT support staff, who are often charged with deploying and supporting these standalone computers.

SOLUTION

The Secure Research Compute Environment (SCRE) is a private, secured virtual environment in which researchers may remotely analyze sensitive data, create research results and output their research results and analysis. This environment is described in detail in a Data Security Plan that has been pre-approved by the UCSB CISO for use with selected agency/data provider data security plans. Researchers may provide this DSP document along with application to various agencies/data providers for restricted dataset licenses.

The SCRE is an alternative to the creation of an individual solution each time a researcher needs to analyze restricted datasets. The SCRE minimizes the security control and implementation burden for researchers who can not easily construct their own data security plan. Software and security updates are applied centrally within the SCRE, with no user intervention.

The environment was designed with the Critical Security Controls for Effective Cyber Defense as a guideline, reaching above and beyond the initial security controls required by many restricted data providers. Additional controls required by government data providers, such as the NIST 800-53 “Minimum Security Controls for Safeguarding Controlled Technical Information” and the subset of controls used in the DoD DFARS clause 252.204-7012 - “Safekeeping of Unclassified Controlled Technical Information” were also applied in the environment.

Each enrolled research project is assigned a unique virtual machine guest instance (the “Research Virtual Desktop”) on a secured private network, in which the researcher can perform his/her research activities and analysis. A set of commonly-used research applications are installed in each Research Virtual Desktop. An encrypted, password-protected disk image is provided for storage of the restricted dataset, interim research results and applications’ temporary file storage.

Researchers use a web browser to connect to the secure VPN web portal, which provides a secured connection to the RDP server running on their unique remote Research Virtual Desktop. The environment can be accessed from any internet-connected device, using any HTML5-compliant web browser (Internet Explorer 10/11, Mozilla Firefox, Google Chrome, Apple Safari) as well as most mobile devices. No additional plug-ins (i.e. Java, ActiveX) or software clients need to be installed on the researcher’s local device.

The SCRE uses a multi-factor authentication service (MFA) for login to the VPN web portal as well as the File Transfer Gateway secure web application. The MFA service is simple to use - first the researcher authenticates with his/her UCSB NetID and password, and then is required to provide a second token (either by interacting with the Duo Security app on his/her mobile devices, entering a code from the app or from an SMS message, or by responding to a phone call to his/her enrolled phone number). After the second authentication factor is provided, the user is logged in.

The overall user experience in the SCRE is very similar to use of other traditional Remote Desktop-type clients, but with substantial security controls in place, and the ability to use almost any modern hardware to connect.

Technical Components / Security Controls

- Private/Segmented Networks, protected by web-based VPN Portal
    - Network Access Control Lists
    - Web VPN Access Control Lists
    - Session Timeouts
- Secure Physical Media storage for Restricted Data Sets
- Multi-Factor Authentication (MFA)
    - UCSB NetID/Password
    - Duo Security service (Push app, SMS codes, OTP or phone authentication)
- Virtual Desktop Infrastructure:

- End-User VM guests - “Research Virtual Desktops”
  - Windows 7 Professional w/ HTML5 RDP server (Ericom Access Now) over encrypted WebSockets/HTML5
  - Session Timeouts on RDP
  - Standard user accounts - can not install software or modify hosts
  - Host-based firewalls on inbound/outbound traffic
  - No internet access, proxy access to whitelisted sites for regular software, OS and antivirus updates
  - Anti-virus software installed, daily updates
  - Common research and administrative software packages installed (Microsoft Office, Acrobat Professional, Mathematica, R, Stata, SPSS, SAS)
  - Encrypted Disk Image - Microsoft BitLocker, password protected encrypted data volume, for storage of restricted data files, interim research results and application temporary storage
- Administrative VM guests
  - DNS & DHCP
  - RADIUS - authentication, authorization and accounting for VPN & File Transfer Gateway
  - Proxy - internal proxy allows limited access outbound to whitelisted sites for software, OS and anti-virus updates
  - Syslog - central syslog of all SCRE hosts, HIDS and network devices
  - HIDS - host-based intrusion detection on admin guest VMs
  - License Manager - provides licensing to end-user software applications
  - File Transfer Gateway - custom written web application used to securely transmit files in/out of the SCRE

COLLABORATION

Architecture of the SCRE was primarily developed by Enterprise Technology Services, in partnership with the Institute for Social, Behavioral and Economic Research (ISBER). Faculty and graduate students from ISBER and the Department of Economics provided feedback on usability, software usage and support documentation.

The Engineering Computing Infrastructure and Letters and Science Information Technology groups provided vital development support for the custom SCRE File Transfer Gateway web application.

Funding for this project was provided by the Office of Research, the Institute for Social, Behavioral, and Economic Research and Enterprise Technology Services.

Although the SCRE is a service developed at UCSB, and initial customers are UCSB faculty and researchers, the service is easily extended to customers from other UC campuses. We are currently in discussion with representatives from two UC campuses to determine how the service may be suitable for use by their researchers. We encourage any interested parties from other UC campuses to contact us to discuss our solution further.

TIMELINE

- Research, Planning and Development - October 2013 - January 2014
- Architecture of Beta - January - March 2014
- Beta - June 2014 - April 2015
- Production - April 2015

OUTCOMES & IMPACT

Streamlined Secure Remote Access to Research

Researchers can now work on restricted datasets from any location where they have access to an HTML5-compliant web browser and an enrolled MFA device. This supports and advances the University's mission to research.

Improved Security Posture

UCSB has an improved security posture as a result of the SCRE implementation. Researchers do not need to worry about OS and application patching, updates etc. Restricted data is protected by multi-factor authentication, isolated and segmented networks, and access control lists. The VPN and RDP server provide encryption in transit and the BitLocker data disk provides encryption at rest.

Use of a common secured environment eliminates the redundancy of multiple systems, and decreases the likelihood of human error when deploying and maintaining these systems.

Flexible Deployment

Use of a Virtual Desktop Environment (VDE) allows dynamic resource allocation. If a researcher needs more RAM or more CPU for analysis, it is simple and straightforward to change the allocation to an individual Research Virtual Desktop (VM guest) to accommodate those needs.

Cost and Time Savings

Because the SCRE is scalable to many users at a time, it has realized hardware & software savings for local departments, as well as labor savings for local IT staff support time.

Real Estate Savings

The SCRE has eased space allocation issues on campus, because individual researchers no longer need to dedicate individual rooms/offices for standalone computers dedicated to research using restricted data.

Scalability to Other UC Campuses

The SCRE has been designed to accommodate customers from other UC campuses, thereby increasing the security posture across the UC system.

Streamlined Restricted Data Application Approval Process

Several restricted data providers have "pre-approved" the SCRE Data Security Plan, which speeds up the application process for researchers wishing to license use of restricted data. This equates to more time dedicated to research. These providers include: UNC Carolina Population Center National Longitudinal Study of Adolescent to Adult Health (AddHealth), California Health and Human Services Agency, Committee for the Protection of Human Subjects, U.S. Bureau of Labor Statistics - National Longitudinal Survey of Youth Geocode Files, and California Employment Development Department.

TESTIMONIALS

"Before SCRE, I had to maintain my own standalone computer in my office. This amounted to backing up files and keeping the software up to date (which is increasingly hard now, given that software updates require internet access). Now the difficulty has been taken out of my hands. I don't have to spend time doing these things, and, moreover, I have found new space in my office without the need for a standalone computer. I believe the SCRE will be a nice recruiting tool for faculty and students, as more and more researchers use restricted data."

--Dr. Heather Royer, Professor, Department of Economics, UCSB

"The SCRE service excels in giving me easy access to restricted versions of the Add Health data necessary for the first piece of my dissertation. It seemed a daunting task as a first time researcher to have a secure set-up required, as there is generally a large set of rigid requirements for accessing these datasets, but I was able to access the dataset through the SCRE's Research Virtual Desktop without much difficulty. One of the best parts of the SCRE is the convenience it provides in generating results from the data stored "inside" and transferring those unrestricted results to my desktop system."

--Chang Lee, Graduate Researcher, Department of Economics, UCSB

"The SCRE has been a terrific resource for me, enabling my graduate students to have effective access to vital restricted-use data in a secure environment."

--Dr. Shelly Lundberg, Professor, Department of Economics, UCSB

"Working with ETS to put and use secure data on SCRE has been extremely easy and useful. Access to the SCRE has made it easier to get access to, and to work with the restricted data. The SCRE is an extremely important resource for UCSB researchers working with restricted data."

--Dr. Kelly Bedard, Professor, Department of Economics, UCSB

FOLLOW-UP

For more information about the Secure Compute Research Environment, or to contact us to become a customer, please see our web pages at http://www.ets.ucsb.edu/services/secure-compute-research-environment