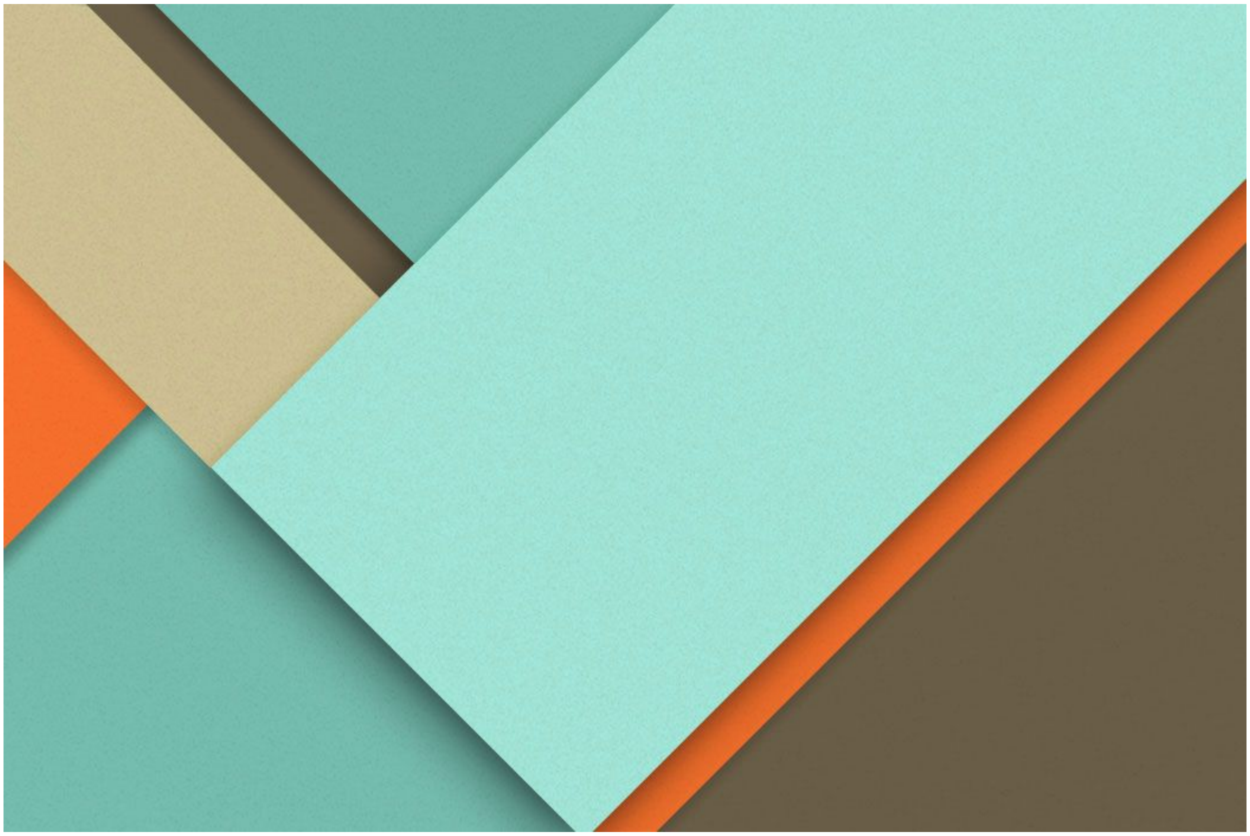

FERPA Server

CS 4450 - Spring 2019

Brucelee Nguyen
Taylen Wanner
Matt DeBoer
Weber State University

Overview

This project is to have a server that is certified to store FERPA-related data and projects that may require access to FERPA-related data. The server will be able to host Weber State University Computer Science student projects. The server will be in compliance with FERPA requirements in order for student projects to access data that may be sensitive to FERPA regulations.

The scope of this project also includes a user interface available to WSU CS students to request their project to be hosted on this server. The user interface allows the student to authenticate through CAS, request the desired disk space, and view approved or denied requests.

Goals

1. Build a server(s) for students to utilize and host school projects -- must be FERPA-compliant
2. Research what it means to be FERPA-compliant
3. Build a user interface allowing students to request their project to be hosted

Milestones

1. Came to an agreement with Weber State University IT department; they would provide two servers, a Linux server and a Windows server, they would maintain both of these servers, as well as maintain FERPA compliance
2. We were able to find detailed FERPA regulations, as well as receive confirmation from WSU IT on how they govern their compliance regulations
3. Built mock-up designs for our vision of the user interface

Requirements

Like many other government regulations, there's no formal compliance auditing or certification process. It's left to the schools and universities to ensure that their IT systems and practices are FERPA-compliant. The documentation, webinars, and videos to help schools get familiar with FERPA and inform education IT professionals on security best practices and FERPA compliance.

- **Policy and governance:** Develop a comprehensive data governance plan that outlines organizational policies and standards regarding data security and individual privacy protection.
- **Personnel security:** Create an Acceptable Use Policy that outlines appropriate and inappropriate uses of internet, intranet, and extranet systems.
- **Physical security:** Make computing resources physically unavailable to unauthorized users. This includes securing access to any areas where sensitive data are stored and processed, such as buildings and server rooms.
- **Network mapping:** Network mapping provides critical understanding of the enterprise (servers, routers, etc.) and its connections.
- **Inventory of assets:** The inventory should include both authorized and unauthorized devices used in your computing environment. Usually checked by an automated system monitoring device.
- **Authentication:** The ways in which someone may be authenticated fall into three categories: something you know, something you have, or something you are. Two-factor authentication (TFA) combines two of these elements and is more costly, but provides more security.
- **Provide a layered defense:** Employ a "Defense in Depth" architecture that uses a wide spectrum of tools arrayed in a complementary fashion.
- **Secure configurations:** It is a best practice not to put any hardware or software onto your network until it has been security tested and configured to optimize its security.
- **Access control:** Securing data access includes requiring strong passwords and multiple levels of user authentication, setting limits on the length of data access, limiting logical access to sensitive data and resources, and limiting administrative privileges.
- **Firewalls and Intrusion Detection/Prevention Systems (IDPS):** A firewall is a device designed to permit or deny network transmissions based upon a set of rules.
- **Automated vulnerability scanning:** When new vulnerabilities (to hardware, operating systems, applications, and other network devices) are discovered, hackers immediately scan networks for these vulnerabilities.

- **Patch management:** Patch management is the process of using a strategy and plan for the testing and roll out of software updates and patches on a regular basis.
- **Shut down unnecessary services:** Each port, protocol, or service is a potential avenue for ingress into your enterprise.
- **Mobile devices:** When sensitive data are stored on servers or on mobile devices, such as laptops or smartphones, the data should be encrypted.
- **Emailing confidential data:** Consider the sensitivity level of the data to be sent over the email.
- **Incident handling:** When an incident does occur it is critical to have a process in place to both contain and fix the problem.
- **Audit and compliance monitoring:** Audits are used to provide an independent assessment of your data protection capabilities and procedures.

This list of FERPA requirements is the minimum requirements needed in order for a system to be in compliance. However, it is stated by FERPA that the governing institution reserves the right to make the judgement on what is considered “FERPA sensitive” and therefore “FERPA compliant.” In our discussions with Weber State IT, Florian Stellet mentioned what WSU IT requires for a system to meet FERPA compliance. The three main regulations Stellet and Information Security, as well as WSU IT, will expect to be met are:

1. All data stored on the server must be encrypted. If the data needs to be in a printed form, the data needs to be stored and locked in a secure room when at rest.
2. All persons requiring access to the data must be FERPA certified. Certificates must be renewed every three years.
3. There must be a justified reason for access to the data.

All other security controls and best practices are being handled by WSU IT based off of their standard work, thus are outside of this project’s scope and need-to-know.

Expectations and Agreements

The expectations of this group were frequently changing. The goal was to receive two servers: a Linux distribution and a Windows distribution. At first, it was unclear which party would build these servers and meet FERPA compliance. After a meeting with WSU IT, expectations were agreed upon between WSU IT and WSU CS. They were as follows:

- IT will create two VMs for CS one Linux one Windows.
    - CS will need to provide specs. Reminder that in most cases the specs can be changed over time.
    - CS will need to provide IT with class names or CRNs to create groups to allow access to said servers.
    - CS will need to provide needed firewall rules. General rule of thumb is if its not needed by the general public use the VPN for access off campus.
- CS will have regular meeting with the IT team to discuss needs.
- CS will provide the user interface allowing students to request disk space for their project to be hosted

Many of these items that CS is meant to provide will be handled at the Department level, per Tate Taylor. At this point in time, it is unclear who will manage the incoming requests (IT or CS), it was suggested to be decided later on during the implementation phase.

Contacts

Below is a list of Weber State faculty that we were in contact with throughout our requirements gathering.

- Brad Peterson, Client - bradleypeterson@weber.edu
- Jonathan Karras, Networking and firewall - jonathankarras@weber.edu
- Mark Buxton, Servers - markbuxton@weber.edu
- Floriann Stellet, Security - florianstellet@weber.edu
- Peter Waite, Director of Application Development - pwaite@weber.edu
- Shelly Belflower, Director of Academic Technology - sbelflower@weber.edu