

Cyber Security Design Write Up 1 - Comments

In this assignment you were asked to sketch out a security design to satisfy YoYoDyne's new data server. In particular, I asked for information on four points.

Operating System

Most people went with a Unix/SELinux solution, but several folks adequately defended a Windows solution. I think a good argument could be made for either choice. The one problem with a Windows solution is the lack of a mandatory access control, but in this constrained scenario I think you could create an adequately locked down access control system for non-privileged users.

Access Control Systems

Many people just mapped the YoYoDyne access control requirements into Windows ACLs, SE Linux type enforcement, or SE Linux MLS.

A fair number of people though were not going to use the file system access controls. Instead they were going to implement a custom solution with their own embedded access controls. This is also a reasonable solution, although I personally would be leery of rewriting everything from scratch. One can make the qmail argument that a completely rewritten small and modular system will be smaller, simpler, and less buggy than leveraging existing code. Many of these design through did not go into much detail of how the YoYoDyne access control requirements would be implemented.

Several people tried to address the very hard problem of limiting access to the designs once they are revealed to the subscribing client. The idea is to protect YoYoDyne from customers with subscriptions who get a digital copy and share it with their friends. One person suggested a hardware solution with TPM or a dongle. Another person just suggested using digital watermarks, so you can track the leaker if the information is found with a competitor or non-paying customer. This is probably the most pragmatic approach at this point. If you can create an evidence trail of wrong doing then you can rely on the legal system to punish those that broke the contract with YoYoDyne.

Administration

Several folks pointed out that the administrative interface should be limited. Ideally, you would not have any networked administrative interface. Folks also pointed out that the system should be hardened and extraneous services removed.

I was looking for a discussion here of the actions that must be performed by an administrator on a day to day basis to add or remove customers from the system and add documents to the system.

Threat Model

With the threat model, I wanted you to identify several threats to the system, e.g., natural disaster, bad customer, or insider threat.

Several folks suggested using an encrypting file system. This raises many interesting issues of how the master password is stored. Must a user be present to enter the password on boot? How is key escrow performed?