

Cyber Security Design Write Up 2

Due

April 20 at class.

Goal

Create a network design to implement a set of security constraints.

Scenario

YoYoDyne was pleased with your content server design. They decided to go with an implementation that leverages the SE Linux type enforcement MAC controls. The designs are labeled with specific types and the customers are placed in domains at login such that the SE Linux rules only allow access to the type labeled designs that they have paid for.

Now they need to deploy the content server in a networked environment. They have several concerns:

- The confidentiality of the designs should be preserved from observers or man-in-the-middle attackers between the customer and the content server.
- In addition to the content server, a much broader audience of potential future customers should be able to access general information about YoYoDyne's services from the outside world.
- A paying customer may intentionally or accidentally share information about how to access to the subscribed designs. Ideally, the design should "automatically" detect such anomalies. At a minimum the system should gather information to prove what accesses were made to the content to prove suspected breaches.

In addition to customer accesses, YoYoDyne needs to consider employee accesses. How should the system be designed to limit impact of employee write accesses? What are the implications of allowing employees to work from home? There are two classes of employees: engineers, who should have edit access to the designs, and administrators, who should have access to system configurations.

In addition to the content server, YoYoDyne needs to provide a standard network infrastructure including mail, web, and DNS. For web, some content is really for internal use only. They also want to add wireless support in the office. Currently YoYoDyne uses a simple two interface firewall that does basic packet filtering. It does not allow any employee access from the outside.

Your tasks

You will need to present your design in 3 pages (or 4 pages for graduate students taking the course for 4 credits) with sensible formatting. In addition you will need to create a diagram showing the layout of your network design. This diagram can be hand drawn.

Your design needs to satisfy the security constraints and explain why you made particular decisions. Specific items you should consider include:

- What protocols need to be passed in order to support the designed network experience?
- What network separation is needed?
- What information needs to be audited?
- What are the tradeoffs between security and flexibility?