Homework5

Misato Morino

Priciple of Least Privilege

It wasn't followed appropriately because any people couldn't maintain the equipment in the engine room, then the engine stopeed. They should have to share the right to maintain and modify it.

Defense-in-Depth

It wasn't followed because the system didin't have immunity against the simple failure such as dividing by zero. They should have implemented the exception processing.

Diversity-in-Defense

It wasn't followed because all computers on Yorktown were designed to shutdown when one of them got bad data and knocked off. The system should had been designed to eliminate the bad data and recover infected computer or values.

Securing the Weakest Link

It wasn't followed because the accident cooured by zero entered by the administrator. Now Navy train people to avoid using bad data and change the values, so the principle is followed today.

Fail-Safe Stance

It wasn't followed because Yorktown didn't have the system backup. What they could have is to try to keep the backup or to have a system to run the engine for a while in an emergency.

Secure By Default

It wasn't followed because the system couldn't avoid the failure because of dividing by zero. As I wrote avobe, the system should have been implemented the immunity against those simple failures.

Simplicity

It wasn't followed appropriately because people couldn't fix the problem about engine. If it worked with no problem, the simplicity was good because people didn't have to maintain it. However, there were no way to fix it in an emergency.

Usability

It was followed because I guessed usually people didn't have to care about their behaviors on the ship.

Security Features Do Not Imply Security

It wasn't followed because it seems there were more vulnerabilities. They should have tried to find security hole by themselves and covered up it.