

IO/Storage and protection/security Tutorial - 6

1. Give an example of a device where functionality has been moved into the controller. What are the advantages/disadvantages of doing this?
2. What registers does a typical IO port consists of? What different approaches are used to access these registers from the processor?
3. What is the difference between security and protection?
4. Explain how passwords are stored and authenticated within UNIX systems.
5. [Review Q15.14 from Stallings] Explain the difference between conventional encryption and public-key encryption.

6. [Problems 15.11 from Stallings] Suppose that someone suggests the following way to confirm that the two of you are both in possession of the same secret key. You create a random bit string the length of the key, XOR it with the key, and send the result over the channel. Your partner XORs the incoming block with the key, and send the result over the channel. Your partner sends it back. You check and if what you receive is your original random string, you have verified that your partner has the same secret key, yet neither of you has ever transmitted the key. Is there a flaw in the scheme?