Tutorial 6

Aims

- To illustrate the different operating system protection needs and principles
- To show the difference between protecting internal and external resources

Questions

1. An operating system has to protect both internal hardware resources (such as main memory) and external ones (such as a printer).

   (a) Can user-oriented and data-oriented security methods be used in both cases? Explain the two methods and the reason why they are/are not suitable in the two cases.

   User-oriented: user ID determines access to resources. Applicable in both cases, as the system should authenticate users and so knows the identity.
   Data-oriented: data and user ID to decide whether to grant access. Requires information about data and its content; which the OS not necessarily has.

   (b) Can physical/logical/temporal/cryptographic separation be used in both cases? Explain the methods and the reason why they are/are not suitable in the two cases.

   Physical separation: Processes exclusively own resources. It reduces resource sharing. Not suitable for internal resources, but external resources can be "owned" by processes.
   Logical separation: "sandboxing", often used in both cases.
   Temporal separation: Only one process can use a resource at a time. Most commonly used in both cases.
   Cryptographic separation: Different data is encrypted with different keys. Data access (both read & write) has additional computational costs. Can be used in both cases.

2. Nowadays many external resources are controlled by embedded computers with their own software. Do you need to build some protection between the main computer software and the external resource's software? If yes why, if not why not? Discuss.

   We cannot rely on third party software / hardware alone for providing security. Even worse, there were cases when the virus was built into microchip itself. The malware is then present in all the hardware sold; once the virus is built in the hardware it is impossible to get rid of it. Also, "security has to be provided at each level" within OS itself, hence if one level of security fails, we still have protection at the next level.

3. Virtual memory extends the memory space available for internal use. How does it increase the risk of external interference? What additional security requirements and protection does it necessitate?

   Virtual memory: The whole address space is stored on disk in a swap file, only a segment is mapped into memory.
   External interference: (i) The hard disk is easily accessible by processes, no physical, logical or temporal separation is provided. Cryptographic separation is not applicable for performance reasons. (ii) Mechanical devices have higher failure rates than electronic devices.
   Additional security requirements: (i) Protection of swap files by the OS from other processes (ii) improved reliability of hard disks (e.g. RAID)

4. Storage in the cloud is becoming increasingly popular. What are the security implications of using cloud storage?

   Confidentiality: The cloud service provider has full access to data. (E.g. Google mail is data mined for advertising, and possibly for other purposes.)
   Reliability: Storage providers usually invest in reliable storage (e.g. by using replication), but network issues can affect reliability. Networks are less reliable (e.g. may lose packets due to congestion), but at the same time resilient.
   Performance: Network communication is slower, which affects the whole system. Hence, certain protection, e.g. via encryption may be prohibitively slow.