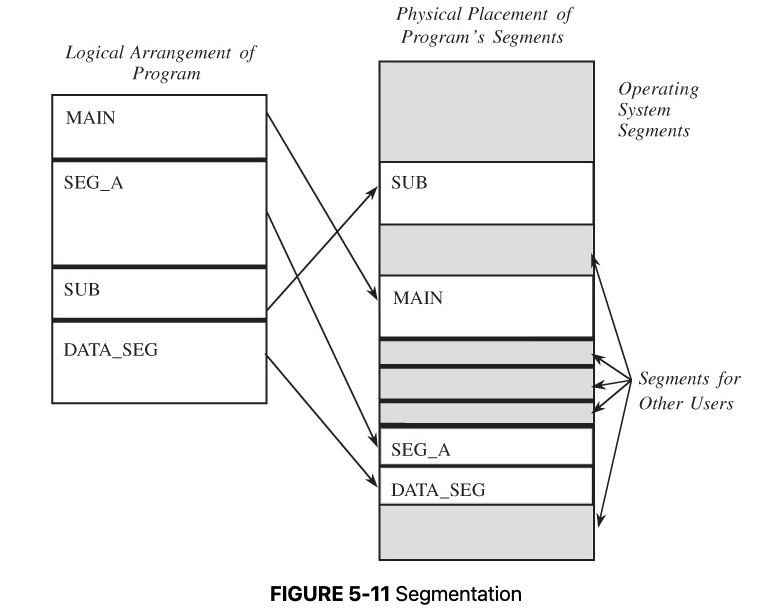
Here’s what the following terms mean in the context of an operating system

* Enforced resource sharing is a memory protection measure that prevents a process from accessing unallocated memory in the OS. For example, it may prevent malware from accessing memory programs that are never intended to be accessed.
* Guaranteed fair service is a scheduling strategy that distributes CPU resources evenly among users.
* Memory protection is a hardware protection mechanism that separates different parts of memory to ensure that each process or program only has access to its allocated memory space.

These are the developments in memory management, the rationale behind each idea, and why the following concept was developed.

* Fence is the simplest form of memory protection. It prevents a faulty user program from destroying part of the resident portion of the OS. It is a method to contain users to one side of a boundary.
* Boundary registers are a second register apart from fence registers and are an upper address limit. In this sense, a program’s addresses are neatly confined to the space between the base and the bounds registers.
* Tagged memory allows a compiler to rearrange a program so that all code sections are adjacent and all data sections are adjacent. Every word of machine memory has one or more extra bits to identify the access rights to that word. This can make the data in addresses execute only.
* Segmentation divides a program into separate pieces, with each piece having different access rights.



* Paging is an alternative to segmentation. This divides a program into equal-sized pieces, and memory is divided into equal-sized units called page frames. This allows a program to be allocated to any place in memory where space is available.

The following operating system features are used to enhance security.

* Layered privilege processes enhance the security of an operating system by ensuring that security problems only affect less sensitive layers. This confines security risks to certain levels of an operating system.
* Virtualization is a great way to increase the security of an entire system. By working directly from a virtual machine, all assets and resources are blocked off the machine’s valuable resources that it utilizes to function. Say that malware is present in a virtual machine; the malware can't seep into the data that the machine itself uses. This is an excellent example of sandboxing.

1. A rootkit is a malicious code that gets beneath the operating system itself. It can control the operating system and pose a severe threat to any system if infected. A rootkit can evade detection by initiating itself before the operating system does. This makes it incredibly difficult for antivirus software to detect a rootkit. Additionally, antivirus tools do not contain code to query disks, determine disk format, identify files and where they are stored, find the file names and properties from an index table, or structure the results for use and display.
2. Instead, antivirus software calls built-in functions that load a number into a register to represent the specific system function to perform and execute a call instruction to the kernel. Information is then presented in a high-level format.