Proyecto 1

Jose Andrey Sequeira Ruiz
2016109087

Agosto 2021

II Semestre

Índice

1. Modos de funcionamiento **2**
1.1. Modo Real 2
1.2. Modo Protegido 2
1.2.1. Anillos de protección 2

2. Bootloader: Multiboot **3**

1. Modos de funcionamiento

El procesador x86 tiene diferentes modos de funcionamientos que impactan de diferentes maneras en el procesador, pero para este caso se investiga el modo real y el modo protegido. Estos modos de funcionamiento también se denominan **modos heredados**.

1.1. Modo Real

La mayoría de los sistemas operativos utilizaban este modo antes del surgimiento del modo protegido, este modo proporciona un entorno de programación del intel 8086. El modo real es un modo de 16 bits y por motivo de compatibilidad (programa que se hizo en decadas anteriores es capaz de correr en un procesador actual) todos los procesadores x86 arrancan en este modo, es decir justo después del arranque el código predeterminado es de 16 bits. Este modo presenta algunas características:

- Posee 20 bits de espacio de direccionamiento segmentado, es decir, solo puede acceder a 1MB de memoria, lo cual es un contra de este modo debido a que es poco en comparación con otros métodos.
- Se tiene acceso directo del software a las rutinas del BIOS y el hardware periférico.
- No posee protección de memoria a nivel de hardware. El SO no es capaz de resguardar la seguridad, es decir, una aplicación A puede impactar negativamente una aplicación B.

En este modo es posible utilizar registros de 32 bits con la implementación de un "Prefijo de anulación de tamaño del operando"(0x66) al inicio de cada instrucción. Es probable que al utilizar registros de 32 bits el ensamblador haga uso por defecto de este prefijo.

1.2. Modo Protegido

En los procesadores Intel modernos(80286 y posteriores) este es el modo de funcionamiento principal. Ahora se tiene un modo protegido de 32 bits que permite el trabajo con varios espacios de direccionamientos virtuales, cada uno con un espacio máximo de 4 GB de memoria direccionable. Se soluciona el problema de seguridad presentado por el modo real ya que se permite que el sistema aplique protección de E/S de hardware y memoria.

A partir del procesador 80386 y procesadores de 32 bits posteriores se agrega un sistema de paginación que forma parte de este modo.

Este modo con el uso de **anillos de protección** anillos de protección restringe el conjunto de instrucciones disponibles.

1.2.1. Anillos de protección

El sistema operativo es el encargado de velar no solo por la seguridad contra amenazas externas como virus si no también de amenazas internas como que un proceso no acceda a la memoria fuera de su espacio de direcciones. Hay dos tipos de seguridad en el SO, seguridad de alto y bajo nivel. Los anillos de protección del modo protegido forman parte de la seguridad de bajo nivel.

Como ya se mencionó anteriormente los anillos de protección restringen el conjunto de instrucciones disponibles, esto según en que anillo se encuentre. Existen cuatro anillos de protección entre los que se reparten los permisos a ciertos niveles de acceso a los recursos del proceso.

- **Anillo 0:** En este anillo se le conoce como modo kernel o modo supervisor, en este nivel se tiene la menor protección y el mayor manejo de los recursos. También se encuentran aquí los manejadores de interrupciones.
- **Anillo 1 y 2:** Este nivel es utilizado normalmente para controladores de dispositivos.
- **Anillo 3:** Este nivel es el que la mayoría de SO utiliza para las aplicaciones, en este nivel se tiene la mayor protección y menor acceso a los recursos. Este espacio se le conoce como espacio de usuario, y para acceder a recursos que puede brindar el kernel se hace a través de Syscall.

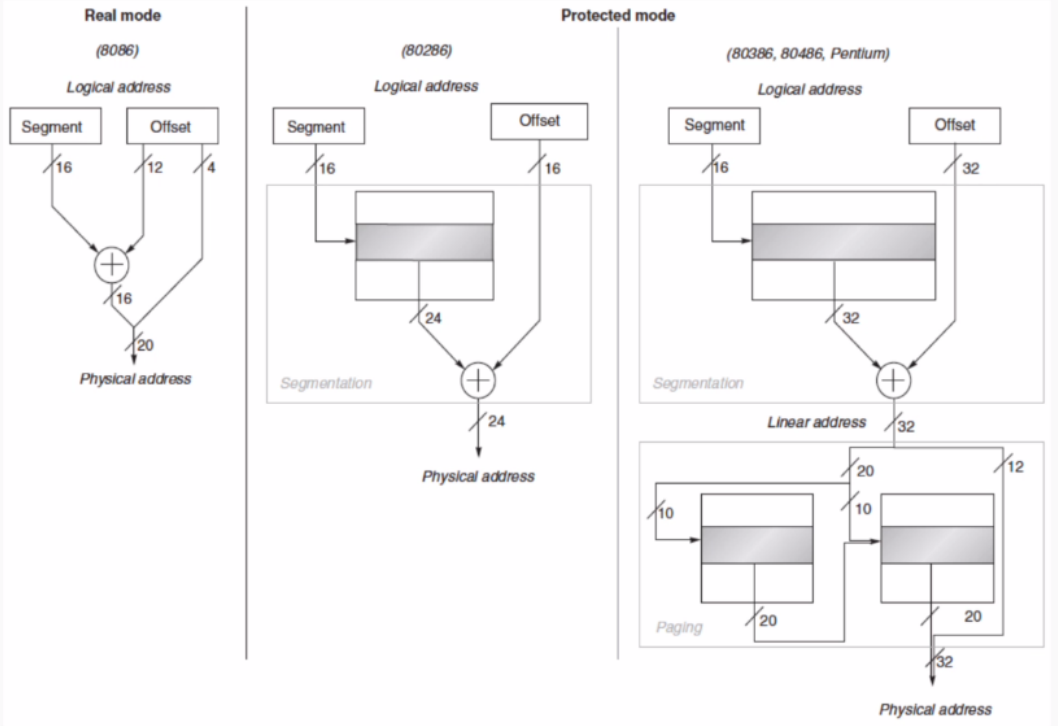

Figura 1: Modos de funcionamiento.

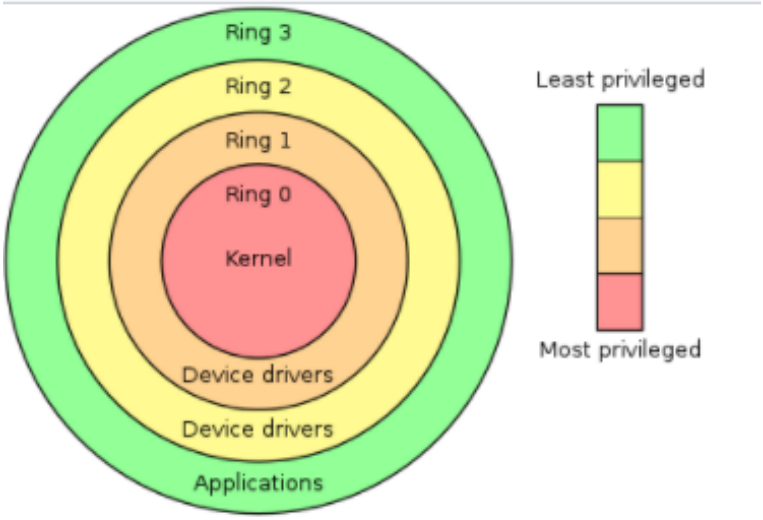

Figura 2: Anillos de protección.

2. Bootloader: Multiboot

El estándar multiboot, creado por GRUB, permite que cualquier implementación de cargador de arranque compatible arranque cualquier núcleo de un sistema operativo, por lo que permite que varios sistemas operativos y sus bootloader trabajen juntos e interoperen. Con esto se pueden tener múltiples sistemas operativos en una computadora.

Para el multiboot se define un encabezado que estará presente en el archivo de imagen. El encabezado debe de estar en los primeros 8192 bytes de la imagen del SO, el cargador busca este encabezado a través de un número mágico(0x1BADB002).

El bootloader busca esta secuencia e interpreta un kernel multiboot. La configuración del multiboot se puede encontrar en el archivo boot.s del proyecto 1.

Con un multiboot se puede seleccionar con cual SO se quiere iniciar, lo cual es perfecto para la implementación del proyecto 1.