Un primo kernel di prova

`kernel.h` 4481 `kernel_boot.s` 4481 `kernel_memory.c` 4481 `_Exit.s` 4488

Avviando il sistema con GRUB 1 o con un altro programma conforme alle specifiche *multiboot*, il kernel dovrebbe trovarsi già in un contesto funzionante in modalità protetta, utilizzando tutta la memoria in modo lineare (ovvero senza suddivisione in segmenti). Pertanto, per visualizzare qualcosa sullo schermo non è indispensabile il passare subito alla preparazione della tabella GDT, cosa che consente di verificare se i file già preparati sono corretti.

In queste sezioni vengono descritti altri file del sistema in fase di sviluppo, ma in particolare '`kernel_main.c`' non è ancora nella sua impostazione definitiva, per consentire una verifica provvisoria del lavoro.

File «kernel.h»

Il file di intestazione '`kernel.h`' viene usato soprattutto per definire le funzioni principali del kernel, ma si possono notare, in coda, delle funzioni che in realtà non esistono, corrispondenti a simboli generati attraverso il «collegatore» (il *linker*). Queste funzioni fantasma servono solo per consentire l'individuazione degli indirizzi rispettivi, così da sapere come è disposto in memoria il kernel.

Listato u168.1. '`./05/include/kernel/kernel.h`'

```
#ifndef _KERNEL_H
#define _KERNEL_H       1

#include <restrict.h>
#include <kernel/multiboot.h>
#include <kernel/os.h>
//
// Funzioni principali da cui inizia l'esecuzione del kernel.
//
void kernel_boot        (void);
void kernel_main        (unsigned long magic, multiboot_t *info);
void kernel_memory      (multiboot_t *info);
void kernel_memory_show (void);
//
// Simboli di riferimento inseriti dallo script di LD (linker script).
// Vengono dichiarate qui come funzioni, solo per comodità, ma servono
// solo per individuare le posizioni utilizzate dal kernel nella memoria
// fisica, così da poter costruire poi una tabella GDT decente.
//
void k_mem_total_s  (void);
void k_mem_text_s   (void);
void k_mem_text_e   (void);
void k_mem_rodata_s (void);
void k_mem_rodata_e (void);
void k_mem_data_s   (void);
void k_mem_data_e   (void);
void k_mem_bss_s    (void);
void k_mem_bss_e    (void);
void k_mem_total_e  (void);

#endif
```

La funzione ***kernel_boot()*** è quella responsabile dell'avvio ed è scritta necessariamente in linguaggio assemblatore. Si trova contenuta nel file '`kernel_boot.s`', assieme alla dichiarazione dell'impronta di riconoscimento *multiboot* e alla collocazione dello spa-

zio usato per la pila dei dati (l'unica pila che questo piccolo sistema utilizzi). È attraverso la configurazione del collegatore, nel file '`linker.ld`', che viene specificato di partire con la funzione ***kernel_boot()***.

Listato u168.2. '`./05/kernel/kernel_boot.s`'

```
.extern kernel_main
#
.globl  kernel_boot
#
# Dimensione della pila interna al kernel. Qui vengono previsti
# 32768 byte (0x8000 byte).
#
.equ STACK_SIZE,  0x8000
#
# Si inizia subito con il codice che si mescola con i dati;
# pertanto si deve saltare alla procedura che deve predisporre
# la pila e avviare il kernel scritto in C.
#
kernel_boot:
    jmp start
#
# Per collocare correttamente i dati che si trovano dopo l'istruzione
# di salto, si fa in modo di riempire lo spazio mancante al
# completamento di un blocco di 4 byte.
#
.align 4
#
# Intestazione «multiboot» che deve apparire poco dopo l'inizio
# del file-immagine.
#
multiboot_header:
    .int 0x1BADB002                     # magic
    .int 0x00000003                     # flags
    .int -(0x1BADB002 + 0x00000003)     # checksum
#
# Inizia il codice di avvio.
#
start:
    #
```

```
    # Regola ESP alla base della pila.
    #
    movl $(stack_max + STACK_SIZE), %esp
    #
    # Azzera gli indicatori contenuti in EFLAGS, ma per questo deve
    # usare la pila appena sistemata.
    #
    pushl $0
    popf
    #
    # Chiama la funzione principale scritta in C, passandogli le
    # informazioni ottenute dal sistema di avvio.
    #
    # void kernel_main (unsigned int magic, void *multiboot_info)
    #
    pushl %ebx          # Puntatore alla struttura contenente le
                        # informazioni passate dal sistema di avvio.
    pushl %eax          # Codice di riconoscimento del sistema di avvio.
    #
    call kernel_main    # Chiama la funzione kernel().
#
# Procedura di arresto.
#
halt:
    hlt                 # Se il kernel termina, ferma il microprocessore.
    jmp halt            # Se il microprocessore viene sbloccato, si
                        # ripete il comando HLT.
#
# Alla fine viene collocato lo spazio per la pila dei dati,
# senza inizializzarlo. Per scrupolo si allinea ai 4 byte (32 bit).
#
.align 4
.comm stack_max, STACK_SIZE
```

La funzione ***kernel_main()*** (avviata da ***kernel_boot()***) che viene mostrata nel listato successivo, non è ancora nella sua forma definitiva: per il momento si limita alla visualizzazione delle informazioni ***multiboot*** e allo stato della memoria utilizzata.

Listato u168.3. Prima versione del file `./05/kernel/kernel_main.c`

```
#include <kernel/kernel.h>
#include <kernel/build.h>
#include <stdio.h>
void
kernel_main (unsigned long magic, multiboot_t *info)
{
    //
    // Inizializza i dati relativi alla gestione dello
    // schermo VGA, quindi ripulisce lo schermo.
    //
    vga_init ();
    clear ();
    //
    // Data e orario di compilazione.
    //
    printf ("05 %s\n", BUILD_DATE);
    //
    // Cerca le informazioni «multiboot».
    //
    if (magic == 0x2BADB002)
      {
        //
        // Salva e mostra le informazioni multiboot.
        //
        mboot_info (info);
        mboot_show ();
        //
        // Raccoglie i dati sulla memoria fisica.
        //
        kernel_memory (info);
        //
        // Omissis.
```

```
        //
      }
    else
      {
        printf ("[%s] no \"multiboot\" header!\n",
                __func__);
      }
    //
    printf ("[%s] system halted\n", __func__);
    _Exit (0);
}
```

I listati successivi, relativi alle funzioni ***kernel_memory()*** e ***kernel_memory_show()***, sono nel loro stato definitivo.

Listato u168.4. '`./05/kernel/kernel_memory.c`'

```
#include <kernel/kernel.h>
#include <stdio.h>
void
kernel_memory (multiboot_t *info)
{
    //
    // Imposta valori conosciuti o predefiniti.
    //
    os.mem_ph.total_s     = (uint32_t) &k_mem_total_s;
    os.mem_ph.total_e     = (uint32_t) &k_mem_total_e;
    os.mem_ph.available_s = (uint32_t) &k_mem_total_e;
    os.mem_ph.available_e
     = (uint32_t) &k_mem_total_e+0x0FFFFF; // 1 Mibyte.
    //
    os.mem_ph.k_text_s   = (uint32_t) &k_mem_text_s;
    os.mem_ph.k_text_e   = (uint32_t) &k_mem_text_e;
    os.mem_ph.k_rodata_s = (uint32_t) &k_mem_rodata_s;
    os.mem_ph.k_rodata_e = (uint32_t) &k_mem_rodata_e;
```

```
    os.mem_ph.k_data_s   = (uint32_t) &k_mem_data_s;
    os.mem_ph.k_data_e   = (uint32_t) &k_mem_data_e;
    os.mem_ph.k_bss_s    = (uint32_t) &k_mem_bss_s;
    os.mem_ph.k_bss_e    = (uint32_t) &k_mem_bss_e;
    //
    if ((info->flags & 1) > 0)
      {
        os.mem_ph.available_e = 1024 * info->mem_upper;
      }
    //
    os.mem_ph.total_l = os.mem_ph.available_e / 0x1000;
    //
    kernel_memory_show ();
}
```

Listato u168.5. ‘./05/kernel/kernel_memory_show.c’

```
#include <kernel/kernel.h>
#include <stdio.h>
void
kernel_memory_show (void)
{
    //
    printf ("[%s] kernel %08" PRIX32 "..%08" PRIX32
            "  avail. %08" PRIX32 "..%08" PRIX32 "\n",
                    __func__,
                    os.mem_ph.total_s,
                    os.mem_ph.total_e,
                    os.mem_ph.available_s,
                    os.mem_ph.available_e);
    //
    printf ("[%s] text   %08" PRIX32 "..%08" PRIX32
            "  rodata %08" PRIX32 "..%08" PRIX32 "\n",
                    __func__,
                    os.mem_ph.k_text_s,
```

```
                        os.mem_ph.k_text_e,
                        os.mem_ph.k_rodata_s,
                        os.mem_ph.k_rodata_e);
    //
    printf ("[%s] data   %08" PRIX32 "..%08" PRIX32
                "  bss    %08" PRIX32 "..%08" PRIX32 "\n",
                        __func__,
                        os.mem_ph.k_data_s,
                        os.mem_ph.k_data_e,
                        os.mem_ph.k_bss_s,
                        os.mem_ph.k_bss_e);
    //
    printf ("[%s] limit  %08" PRIX32 "\n",
                        __func__,
                        os.mem_ph.total_l);
}
```

Altri file mancanti

«

Nella descrizione della libreria che fa capo al file di intestazione ‘`stdlib.h`’, è stata omessa la funzione ***_Exit()*** che ora è indispensabile precisare, essendo usata dalla funzione ***kernel_main()***. In pratica si esegue semplicemente un ciclo senza fine, cercando però di sospendere il funzionamento del microprocessore, fino a quando si verifica un’interruzione.

Listato u168.6. ‘./05/lib/_Exit.s’

```
.globl _Exit
#
_Exit:
    enter $0, $0
    .equ status,  8          # Primo argomento.
    mov  status(%ebp), %eax # Copia il valore da restituire
                             # in EAX, anche se poi non se ne
                             # fa nulla.
    leave
    #
halt:
    hlt         # Ferma il microprocessore.
    jmp halt    # Se il microprocessore viene sbloccato, si
                # ripete il comando HLT.
```

Compilazione e prova di funzionamento

Prima di procedere alla compilazione con lo script ‘**compile**’ (o direttamente con ‘**makeit**’), occorre verificare che la variabile di ambiente ‘**TAB**’ sia dichiarata correttamente nello script ‘**makeit**’, in modo da contenere esattamente un carattere di tabulazione orizzontale (diversamente i file-make non verrebbero creati nel modo giusto). Inoltre occorre avere preparato il file-immagine del dischetto e averlo innestato nella directory ‘/mnt/fd0/’ (diversamente occorre modificare sempre lo script ‘**makeit**’). Quando tutto sembra pronto, basta avviare lo script ‘**bochs**’ (da una finestra di terminale, durante una sessione grafica di lavoro con X) per far partire il sistema giocattolo in prova. Se tutto va bene, viene visualizzato il testo seguente e poi tutto si ferma; se invece si presenta un errore, il simulatore Bochs riavvia e si riparte con GRUB 1.

```
05 20070818140007
[mboot_show] flags: 00000000000000000000011111100111 mlow: 027F mhigh: 00007BC0
[mboot_show] bootdev: 00FFFFFF cmdline: "(fd0)/kernel"
[kernel_memory_show] kernel 00100000..0010BAFC  avail. 0010BAFC..01EF0000
[kernel_memory_show] text   00100000..00102FEC  rodata 00102FEC..00103144
[kernel_memory_show] data   00103144..00103144  bss    00103160..0010BAFC
[kernel_memory_show] limit  00001EF0
[kernel_main] system halted
```

Dall'esempio mostrato si può determinare quanto segue: la memoria bassa arriva fino a $27F_{16}$ Kibyte (639 Kibyte); la memoria alta arriva fino a $7BC0_{16}$ Kibyte (31680 Kibyte); il kernel utilizza la memoria da 100000_{16} byte (1024 Kibyte) a $10BAFC_{16}$ byte (1070 Kibyte circa); pertanto la parte rimanente è tutta memoria libera.

Con questi dati, nel prossimo gruppo di sezioni viene preparata una tabella GDT minima, con la quale si definisce solo la memoria esistente effettivamente.