小華的部落格

將自己踏入BIOS領域中所學習到的知識做一些心得整理，像是Legacy BIOS、EFI BIOS、Windows Driver...etc. ※版權與智慧財產權聲明:保留所有法律權利。我在寫文章時如果有引用到其他人的地方我會盡量說明參考出處，如果有遺漏的地方請告訴我，我會馬上註明! 而轉貼我的文章時也請您註明出處!

星期二, 10月 16, 2007

[我所知道的BIOS]->[VGA init] 10

一般而言,BIOS會在POST時 locate 3 devices:
- Input device(Ex. Keyboard)
- Output device(Ex. Display device)
- IPL(Initial Program Load, Ex. HDD)

這次要提到的是 Display device,即 VGA !

在PCI_SCAN之後,BIOS會在記憶體中建立一個data structure,代表整個系統的 PCI architecture.
Ex. Ponter-> NB->P2P->SB->IDE->AUDIO->LAN->USB 2.0->USB 1.1->...->VGA->...->End

在VGA_init的階段,BIOS會去 go-through this list,一個個的問:"有沒有人需要shadow Option ROM的 ?"

---
*1 在此,先break,並說明一些觀念:
1. Option ROM是 for H/W的 firmware;像BIOS一樣是 for MB.有可能直接在硬體上 ,or 包在BIOS image中
2. 有Option ROM的 H/W可能有: VGA card,Lan card, RAID card,...etc
3. VGA's Option ROM 也就是 VBIOS ! 專門處理 screen I/O operation(主要是int10h)

訂閱電子報

EZMAIL提供

Translate

选择语言 | ▼

網誌存檔

4. VGA "shadow" 即代表: 將 VBIOS copy 到 shadow RAM, Ex. C0000h~C7FFFh處(32K)
5. VGA init這個階段只 consider "VGA device" ! for 其他 device,之後再考慮其 shadow的事宜

(承接前面的 flow):此時,VGA device會舉手說:"我要" !此時,BIOS會去尋找VGA device's Option ROM(即VBIOS)在哪裡;此時,VBIOS有可能在card上 or "當初" 被包在 BIOS image中(*2)

一但找到,則會先 作一些 checks:Ex.
- Option ROM signature is 0xAA55 ?
- 比較 Option ROM內的 Vendor ID/Device ID = H/W's IDs ?
- class code and sub-class code correct ?
- length = 0 ?
...etc...

若都符合,則視它為 VGA Option ROM(VBIOS) ! 之後,利用 memory2memory copy將之 copy到 shadow memory,從 C0000h處開始存放...

複製完後,再 check "checksum"是否正確;if yes then jump to "entry of initialization code",控制權自此轉移至 VGA Option ROM,由它去做 initialize VGA的工作 ! (若是CRT螢幕,user會聽到ㄉㄧㄤ的一聲 ! 即代表 initialize VGA成功 !!!)

<- 此為 VGA_init的工作 !!!

*2 說"當初"的原因是: VGA BIOS若包在BIOS image中,在 BIOS shadow時,也會被一併 copy到記憶體的某處放著;當然,會記住存放處 !

[Note] 一般遇到 VGA init fail的issue時,可以先 check:是否 VGA BIOS已被 copy 至 C0000h處;若有,則check是否已經 jump to VBIOS or NOT;若否,則可以往前 check是否前面所列的一些 "關卡"沒過 (Ex. ID不 match, or checksum 不相等...etc)

VGA 若 ok,電腦就是彩色的 ^_^

- 相關討論 ----------

通常都是板子一來就會去開始Debug VGA...
VBIOS 若壞，螢幕是黑ㄟ
VBIOS若好，螢幕是彩色ㄟ

逛逛不一樣的地方

沒螢幕的情況下要繼續Porting BIOS就比較麻煩一點

[Q]Option ROM是 for H/W的 firmware;像BIOS一樣是 for MB.有可能直接在硬體上 ,or 包在BIOS image中。前者我叫它SW ROM,後者叫legacy ROM，您已經提到sw rom的load方式，那麼legacy rom load方式是否應該有所不同呢? 一但找到OpROM,則BIOS 會先作一些 checks:
Ex.
- Option ROM signature is 0xAA55 ?
- 比較 Option ROM內的 Vendor ID/Device ID = H/W's IDs ?
- class code and sub-class code correct ?
- length = 0 ?
...etc...

兩种rom都是通過這種方式嗎?
Ans: 我所說的都是 rough flow，而這兩種ROM的"處理方式"不同,但"檢查的機制"大同小異...建議去trace BIOS code比較清楚

[補充1]
1.可以查看PCI ROM Spec... 裡面有詳細說明如何Load OpROM 的方式，而檢查項目就各家BIOS不同...

2.可以用HEX編輯器直接開啟ROM File，例如VBIOS.bin or OpROM.dat ...etc 來查看內容(Binary file)，例如某VBIOS.DAT 的內容如下:

00000 55 AA 80 E9 4B ....
00010 30 30 00 22 E9 19 21 5F 40 00
.....
00040 50 43 49 52 86 80 42 2A .....

其中:
a)55AA是這個ROM的Signature <--代表他是符合規範的ROM
b)80 這個ROM的Code size <--需查閱Spec確定一下
c) 接著是EntryPoint Address <--實際上會執行的程式碼進入點的位址，所以一般都是講Jmp OpRomBaseAddr+3 <-- 你如果trace BIOS 程式碼，這就是 +3 的由來
d) 000018h=40 代表另一個PCI Header在Offset 00040h的地方
所以 50 43 49 52 是Signature，如果用ACSII 來看就是"PCIR"
其他更多資訊可以查看PCI ROM Spec說明.....

e) "PCIR"後面緊跟著這個OpRom的VID與DID ...即8086 2A42 <--Intel=8086

3.如果想要改OpRom裡面的Code，可以使用反組譯工具去修改或是用Debug去修改

演算法 (影像處理, 資料結構, 智慧型視訊分析, 人工智慧)
平凡的幸福
相關資訊
流浪小築
旅遊美食~
小君君的祕密花園
繼續閱讀懶人加強版
幸福雅痞~
懷舊系列~

標籤

一些筆記 (10)
分享 (2)
心情分享 (3)
生活運用 (1)
其它 (9)
思念 (1)
音樂分享 (1)
音樂歌詞 (1)
組合語言Assembly (4)
軟體工具 (12)

如果比較簡單的OpROM要做實驗的話我都用Debug.com 把OpROM 載入到Mem，接著利用T /P 指令單步執行去追蹤與修改，修改好之後再查看機器碼，再利用Hex編輯器 or 反組譯工具寫回去OpROM (找Bug時可以嘗試這樣寫啦，不過違反智慧財產權，最好還是叫Vendor幫你改，而且光看懂OpROm的流程就需要一點時間了 ^^!)

如果要用組合語言寫一個Dummy OpRom的做法就像下面範例去模擬一個OpROM...
至於你BIOS端可不可以run 就要看你的檢查機制嚴謹程度或是你自己修改你的BIOS code來達到模擬的目的 :

```
.586p
.code
YourCodeStart:
ORG 0
db 55h, 0AAh
TotalCodeSize db (offset YourCodeEnd) - (offset YourCodeStart)
ORG 3
jmp entrypoint

entrypoint:
.....

YourCodeEnd:
END
```

組譯完之後可以利用微軟工具EXE2BIN.EXE 把他轉成xxx.bin (binary file)然後你就可以包進去BIOS測試。

[補充2]
當VGA init時,那時VGA BIOS的放置處可能有:
case 1: 在 memory中(當初在 shadow stage時被 copy 到 memory)
case 2: 在 card上(Ex. 一般的 external VGA card上都有一顆小rom)

因此,這兩種case的處理方式便不同.
Ex. In case 2 若VGA card在 bridge後面,則還需要 config 該 bridge's resource window使Option(in card)可以被正確的 accessed...<- 所以處理方式有所不同 !

至於檢查機制;因為Option ROM不管放哪裡,其 content都是一樣 ! 因此檢查機制大同小異...還有,不同家BIOS的 "checks" 也未必完全相同 !!!

張貼者： 小華的部落格
標籤： BIOS相關

9 則留言:

匿名 提到...

版主所说的都是PCI环境好后的做法，请问该如何在开机后，BIOS未做任何事的时候来INIT VGA呢？如何配置整个PCI DATA STRUCTURE呢?

8月 08, 2008 2:06 上午

匿名 提到...

跳到C000:0003h需要用到far jump
请问far jump如何回来?

8月 21, 2008 10:16 下午

小華的部落格 提到...

far jmp後一般在OpROM內都是使用RETF返回...

你可以試試看用Debug玩玩看下面的東西:

```
-A100
PUSH CS
MOV AX,10A
PUSH AX
JMP FAR C000:0003
MOV AH,09
MOV DX,113
INT 21
INT 20
DB 'C000:0003 TEST!!!','$'

-G
```

沒意外的話你可以看到顯示一個字串在螢幕上...如果你追進去看的話，會看到他用RETF返回...

8月 25, 2008 12:29 上午

匿名 提到...

I would like to exchange links with your site biosengineer.blogspot.com
Is this possible?

8月 11, 2010 8:36 下午

IPC 提到...

現今市面的NB VBIOS(Nvdia chip)都是存取在CPU裡面的cache嗎???

10月 28, 2010 7:49 上午

IPC 提到...

現今市面的NB VBIOS(Nvdia chip)都是存取在CPU裡面的cache嗎???

VBIOS似乎包在BIOS image裡

10月 28, 2010 7:50 上午

johnson0617 提到...

請問如何測試 vga 的 dram
1. 有沒有一個位址,可以write/read dram of vga?

9月 07, 2011 6:50 下午

CCCCCC 提到...

請問顯卡裡的bios（rom），除了用hex軟體編輯之外，還有其他軟體可反編譯嗎?
因為用hex軟體開了之後，一大堆英文與數字的組合，看不懂。
謝謝。

10月 17, 2011 5:29 上午

Unknown 提到...

How about ultraedit

8月 30, 2016 2:31 上午

張貼留言

較新的文章 首頁 較舊的文章

訂閱： 張貼留言 (Atom)