

Writing patch in IAR and using elf2vkp?

Writing patch in IAR and using elf2vkp?

by [mc_kibel](#) on 29 Jun 2009 21:03

Hello!

I've got A2 phone now. As we know, it's not possible to run elfpack. So I was wondering about something like creating patch in C.

For example there is a SysGfx v2.0 by VertexBZ written in C in IAR. I know that the elf is changed into patch by elf2vkp (and .xcl file is needed). All unnecessary stuff, which is connected with elf, should be removed too. So what can I do when I've got something like this and I want to create the same patch as elf?

```
unsigned short timer = 0;

void InitIntelligenceAutoBacklight ( )
{
    DATETIME dt;
    REQUEST_DATEANDTIME_GET ( 0, &dt );
    int h = dt.time.hour;
    int val = 0;

    if ( h < 8 ) // 00.00 - 07.59
        val = 50;
    else if ( h < 18 ) // 08.00 - 17.59
        val = 80;
    else if ( h < 22 ) // 18.00 - 21.59
        val = 60;
    else // 22.00 - 23.59
        val = 50;

    DISPLAY_SetBrightness ( 0, val );
}

void onTimer (unsigned short timerID , LPARAM n)
{
    BATT Battery;
    GetBatteryState((int const*)1 , &Battery);
    char pc;
    pc = Battery.RemainingCapacityInPercent;

    if ( pc <= 10 )
        DISPLAY_SetBrightness (0, 50);
}
```

```
else
    InitIntelligenceAutoBacklight();

Timer_ReSet(&timer,1000,onTimer,0);
}

int main (void)
{
    timer = Timer_Set ( 1000, onTimer, 0 );
    return 0;
}
```

RE: Writing patch in IAR and using elf2vkp?

by [Mojsa](#) on 29 Jun 2009 21:17

You just need to define addresses along with functions, and create xcl file with hook and patch body 😊

There's one more patch written in IAR too :P

RE: Writing patch in IAR and using elf2vkp?

by [Edgpaetz](#) on 29 Jun 2009 22:04

EP, sysgfx and (as far as I know) some large patches are written in C, compiled in IAR and the converted into VKP with elf2vkp.

unfortunately I don't know how that works... but if you wanna learn something new, learn ARM and create new patches....

I'm guessing you can make a hook in GetBatteryState(...) function, and from then check the needed values and call DISPLAY_SetBrightness() with the needed value, this way brightness control should be called every time GetBatteryState(...) function is called => (that's my idea)

Regards

RE: Writing patch in IAR and using elf2vkp?

by [mc kibel](#) on 29 Jun 2009 23:21

Mojsa wrote:

You just need to define addresses along with functions, and create xcl file with hook and patch body 😊

There's one more patch written in IAR too :P

Yeah, I know that and it sound really easy :grin: But I don't know (and I don't have any idea) how to do

it...

Example: (w760i r3ea037)

REQUEST_DATEANDTIME_GET = 0x1084B014

GetBatteryState = 0x111196C8

DISPLAY_SetBrightness = 0x1108F9D4

And TimerSet and TimerReSet are easy to port :-)

unfortunately I don't know how that works... but if you wanna learn something new, learn ARM and create new patches....

Yup, I don't know how does it work too... I do know nothing about ARM and it will be difficult for me, but maybe I'll try.

Thanks for replies, regards! :hmmm:

RE: Writing patch in IAR and using elf2vvp?

by [Mojsa](#) on 30 Jun 2009 07:06

Example:

Hidden code, Developers Access Only.

This is from one patch, you don't have to define addresses of lib funcs, they'll be read from asm file with functions.

But this will need defining addresses:

Hidden code, Developers Access Only.

:grin:

RE: Writing patch in IAR and using elf2vvp?

by [mc kibel](#) on 30 Jun 2009 10:26

Mojsa, I think that the addresses can be defined in ASM file, right?

```
defadr REQUEST_DATEANDTIME_GET,0x1084B014+1
```

```
defadr GetBatteryState,0x111196C8+1
```

```
defadr DISPLAY_SetBrightness,0x1108F9D4+1
```

```
defadr Timer_Set,0x10E83854+1
defadr Timer_ReSet,0x10E83888+1
```

These addresses are for W760i R3EA037. But I don't know what's next. I just need to know how to connect xcl and asm file with project, and what should I put there... I know, that is a lot of explanation, but patches written in C can be much more advanced.

Regards! :hmmm:

by [Mojsa](#) on 30 Jun 2009 10:49

Yes,I think. :grin:

by [ultrashot](#) on 30 Jun 2009 15:49

look at elfpack's sources. XCL is setted in Project->Options

by [mc kibel](#) on 30 Jun 2009 15:54

Ok. So I know how to add xcl file to project I think. But I don't know what should I put into ASM file (it's needed, right?) and I don't know where I can get any good entry point to .xcl file.

by [ultrashot](#) on 30 Jun 2009 16:34

@mc_kibel,
wait, i am making patch's template for IAR

by [mc kibel](#) on 30 Jun 2009 16:45

It's just great :hmmm: I'm sure it will help me a lot.
So post it here when You finish it.
Regards! :hmmm:

RE: Writing patch in IAR and using elf2vvp?

by [ultrashot](#) on 30 Jun 2009 16:45

ok, wait[hr][hr]

nobody should publish it anywhere else (at the moment)

Hidden code, Developers Access Only.

Open IAR, ->New project->Elf SDK

Attachments

[iar_templates.zip](#)

(116.2 KiB) Downloaded 340 times

RE: Writing patch in IAR and using elf2vvp?

by [mc_kibel](#) on 30 Jun 2009 18:03

Thank you very much, I hope it will help me. Regards! :hmmm:[hr][hr]Hmm... I can't find this "New project -> Elf SDK"

That's all what I see when I run IAR

<http://img188.imageshack.us/img188/6955/17404212.png>

Edit: I found it. Files must be in ARM/Config/Template/Project.[hr][hr]Ok, now I need help. You can download project from attachment. What's next? Any instructions ? :hmmm:

Password is in UltraShot's post.

Attachments

[Patch.rar](#)

(35.05 KiB) Downloaded 282 times

by [ultrashot](#) on 01 Jul 2009 09:12

@mc_kibel, there is an "ElfPatch" template special for you

RE: Writing patch in IAR and using elf2vvp?

by [mc_kibel](#) on 01 Jul 2009 10:20

Ok, I see now.

But what does it mean?

Fatal Error[e72]: Segment INITTAB must be defined in a segment definition option (-Z, -b or -P)

Thanks for replies ! :hmmm:[hr][hr]

Just look into project... I don't know what's wrong. And I do not know what should I put into ASM file (I don't understand it...)

It would be great if someone will fix it...

Attachments

[BCPATCH.rar](#)

(71.82 KiB) Downloaded 373 times

by [ultrashot](#) on 01 Jul 2009 11:22

@mc_kibel, you should learn patch creating:)

to *.asm you should add places where patch would start running

by [jamesbond22](#) on 05 Jul 2009 07:30

I think that this great patch can be easy created by IAR and elf2vkp:

[vkp];W810 SW-R4DB005

;BookManager v1.2 fix

;Đ;Đ¾Đ·Đ´Đ°ĐµĐ¼ Đ¿Đ°Đ¿Đ°Ñf "/usb/other/ini/" (Đ±ĐµĐ· Đ°Đ°Đ²Ñ¿Ñ‡ĐµĐ°)

;Đ´Ñ

...

by [lanceaugust31](#) on 31 Aug 2009 14:28

I guess for the crash problem in elf2vkp specially for k750,w800. download 010 editor.demo ... You need a patch to deactivate it...

by [kirpeace](#) on 02 Sep 2009 01:01

i made tutorial in se-nse for making elfpack for k750/w800

by [Edgpaez](#) on 04 Sep 2009 01:57

@kirpeace

Would you mind posting one here ? :grin:

we can use it to compile from DB2020 (seems A2 isn't available)

Regards

by [kirpeace](#) on 04 Sep 2009 03:32

sorry i meant to compile using iar and svn source along with how to overcome that error in k70/w800.

i made an elfpack for k550 using tut for porting patches

my topic for compiling.its big and i have given other links to other pages too

<http://forums.se-nse.net/index.php?showtopic=28916>

by [juLi0Naru](#) on 23 Nov 2009 18:16

@ultrashot

iar _templates also work with w580?

For make patch :grin:

so?

Code: [Select all](#)

```
#define patch1_addr // ??????? Where does?
```

main.c

Hidden code, Developers Access Only.

Hidden code, Developers Access Only.

Hidden code, Developers Access Only.

by [mc kibel](#) on 28 Nov 2009 22:47

This is entrypoint address - you need to enter address, where patch will start.

RE: Writing patch in IAR and using elf2vvp?

by [mc kibel](#) on 29 Nov 2009 15:37

First and easiest (and only one I know :P) :

Take for example a function: 091C: 00000000 951D3545 ; 247: void GoMusic(void);

951D3545 = 45351D95.

Open main in ida (this is adress for K770 r8ba024). Press alt+B and paste 45351d95. patch1_addr is the result from IDA. Then add in:

in asm:

```
                PUBLIC returnto

returnto        equ returnto_addr //original jump to GoMusic function
```

in Target:

```
#define returnto_addr 0x45351D95 //original jump to GoMusic function
```

and in main.c

```
extern __thumb returnto();  
//...  
__root void fixed_function(void)  
{  
//.....  
    returnto();  
};
```

Now when we use GoMusic function, our patch will start :) So in fixed function you just can put MessageBox and try :p

by [blacklizard](#) on 14 Dec 2009 07:54

I got this error when compiling in IAR

```
Warning[410]: DC or DS directive while in CODE area.
```

What should I do?

by [mc kibel](#) on 14 Dec 2009 13:51

It's not error, it's warning :) Ignore it :D

RE: Writing patch in IAR and using elf2vvp?

by [anarkes](#) on 05 Jan 2010 22:30

Hi devs, i have a problem when i create a vvp patch for my w580. After to installing on my cell phone does not go to screen startup.

```
#include "..\include\Types.h"  
  
/*  
"Patch in C++" template by UltraShot  
*/  
  
#define SID_ANY_LEN 0xFFFF  
#define TEXT(__STR__) L##__STR__  
#define _T(__STR__) L##__STR__  
#define MAXELEMS(x) (sizeof(x)/sizeof(x[0]))  
#define STR(__STR__) Str2ID(_T(__STR__),0,SID_ANY_LEN)  
#define header 0x6fffffff  
  
extern __thumb int strcmp(char *s1, char *s2);  
extern __thumb BOOK* FindBook(IS_NEEDED_BOOK);  
extern __thumb Str2ID(const void * wstr , int flag , int len);
```



```
extern __thumb void MessageBox(int HeaderStrID,int
MessageStrID,wchar_t IconID, int style /*1 or 2*/,int time,BOOK *
unk);

__root void fixed_function(void *unk,int id,int RED,int GREEN,int
BLUE, int delay, int onoff)
{
    MessageBox(header,STR("This is my First Patch -
anarkes"),0,1,5000,0);
};
```

```
#include "Target\W580_R8BE001.h"

                PUBLIC strcmp
strcmp          equ strcmp_addr

                PUBLIC FindBook
FindBook        equ FindBook_addr

                PUBLIC MessageBox
MessageBox      equ MessageBox_addr

                PUBLIC Str2ID
Str2ID          equ Str2ID_addr

dcdaddress      equ patch1_addr

                CODE16
                org dcdaddress
                extern fixed_function
                DCD fixed_function

                END
```

```
#ifdef W580_R8BE001

/*
Target file for patch
Configuration: W580 R8BE001

*/

#define strcmp_addr 0x44557424+1
#define FindBook_addr 0x452ACB08+1
#define MessageBox_addr 0x452B987C+1
```

```
#define Str2ID_addr 0x45347434+1
#define patch1_addr 0x45748B84

#endif
```

The patch is this

```
+44140000
;
01608B84: A9BF2945 E9FBC045
;CODE,DATA_C
01ACFBE8: 0000000000000000 084A094810B50021
01ACFBF0: 00000000000000000000000000000000
00F014F804000748002103B401230648
01ACFC00: 00000000000000000000000000000000
0022210000F00EF81CBDC046FFFF0000
01ACFC10: 00000000000000000000000000000000
34FCC04588130000FFFFFF6F004B1847
01ACFC20: 00000000000000000000000000000000
3574344508B4024B9C4608BC6047C046
01ACFC30: 00000000000000000000000000000000
7D982B45540068006900730020006900
01ACFC40: 00000000000000000000000000000000
730020006D0079002000460069007200
01ACFC50: 00000000000000000000000000000000
73007400200050006100740063006800
01ACFC60: 00000000000000000000000000000000
20002D00200061006E00610072006B00
01ACFC70: 0000000000000000 6500730000000000
```

Please Help me.

Regards. 😊

by [blacklizard](#) on 07 Jan 2010 13:34

Code: [Select all](#)

```
#define patch1_addr 0x45748B84
```

This entry point is from what function?

Its better to try with GoMusic() function and you don't have return address.

Take a look from intelligent brightness controller patch source.

A question to developers.

Does heap shift is used for if else statement?

Thanks xD

RE: Writing patch in IAR and using elf2vvp?

by [mc kibel](#) on 07 Jan 2010 20:32

blacklizard wrote: Does heap shift is used for if else statement?

Heapshift in patches written in IAR is used only for global variables.

by [anarkes](#) on 11 Jan 2010 18:12

blacklizard wrote:

Code: [Select all](#)

```
#define patch1_addr 0x45748B84
```

This entry point is from what function?

Really... I don't know :sick::grin:, When opened a New Project with compatibility to Transform to VKP, this function is added.

Regards.

Sorry for my late reply.

by [blacklizard](#) on 16 Mar 2010 06:26

Hi guy.

I get this error in IAR. What should I do?

Fatal Error[e72]: Segment INITTAB must be defined in a segment definition option (-Z, -b or -P)

Thanks

by [jamesbond22](#) on 14 Apr 2010 16:49

Code: [Select all](#)

```
__thumb functions can only call __swi functions with swi_number  
in range 0-0xFF
```

What does this message?

Re: Writing patch in IAR and using elf2vkp?

by [anarkes](#) on 14 Apr 2010 20:08

you've tried use something as this, right?

Code: [Select all](#)

```
//Example  
#pragma swi_number=0xFFFF
```

I have a same error in this

```
__thumb __swi __arm int ModifyKeyHook( int (*proc)( int, int,  
int ), int mode );
```

and when I change the processor mode, only put this and work :D

```
#pragma swi_number=0x107  
__swi __arm int ModifyKeyHook( int (*proc)( int, int, int ), int  
mode );
```

I had a same error a few days ago, I fix the problem change processor mode to ARM, try and tells me.