When you crash on a mov ebx, eax instruction, there aren't too many obvious explanations, so just try what you can

devblogs.microsoft.com/oldnewthing/20120511-00

May 11, 2012

Raymond Chen

A computer running some tests encountered a mysterious crash:

```
eax=ffffffff ebx=00000000 ecx=038ef548 edx=17b060b4 esi=00000000 edi=038ef6f0
eip=14ae1b77 esp=038ef56c ebp=038ef574 iopl=0         nv up ei pl nz na po nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00010202
FOO!CFrameWnd::GetAssociatedWidget+0x47:
14ae1b77 8bd8            mov     ebx,eax
```

A colleague of mine quickly diagnosed the proximate cause.

> *Something* marked the code page PAGE_READWRITE, instead of PAGE_EXECUTE_READ. I suspect a bug in a driver. FOO is just a victim here.
>
> ```
> 0:002> !vprot 14ae1b77
> BaseAddress:       14ae1000
> AllocationBase:    14ae0000
> AllocationProtect: 00000080  PAGE_EXECUTE_WRITECOPY
> RegionSize:        00001000
> State:             00001000  MEM_COMMIT
> Protect:           00000004  PAGE_READWRITE
> Type:              01000000  MEM_IMAGE
> ```

This diagnosis was met with astonishment. “Wow! What made you think to check the protection on the code page?”

Well, let’s see. We’re crashing on a `mov ebx, eax` instruction. This does not access memory; it’s a register-to-register operation. There’s no way a properly functioning CPU can raise an exception on this instruction.

At this point, what possibilities remain?

- NX, which prevents the CPU from executing data.
- Overclocking, which will cause all sorts of “impossible” things.

- A root kit.

(Note that the second and third options involve rejecting the assumption that the CPU is behaving properly.)

These are in increasing order of paranoia, so you naturally start with the least paranoid possibility.

Then, of course, there's the non-psychic solution: Ask the debugger for the exception record.

```
EXCEPTION_RECORD:  ffffffff -- (.exr 0xffffffffffffffff)
ExceptionAddress: 14ae1b77 (FOO!CFrameWnd::GetAssociatedWidget+0x00000047)
   ExceptionCode: c0000005 (Access violation)
  ExceptionFlags: 00000000
NumberParameters: 2
   Parameter[0]: 00000008
   Parameter[1]: 14ae1b77
Attempt to execute non-executable address 14ae1b77
```

That last line pretty much hands it to you on a silver platter.

Raymond Chen

Follow