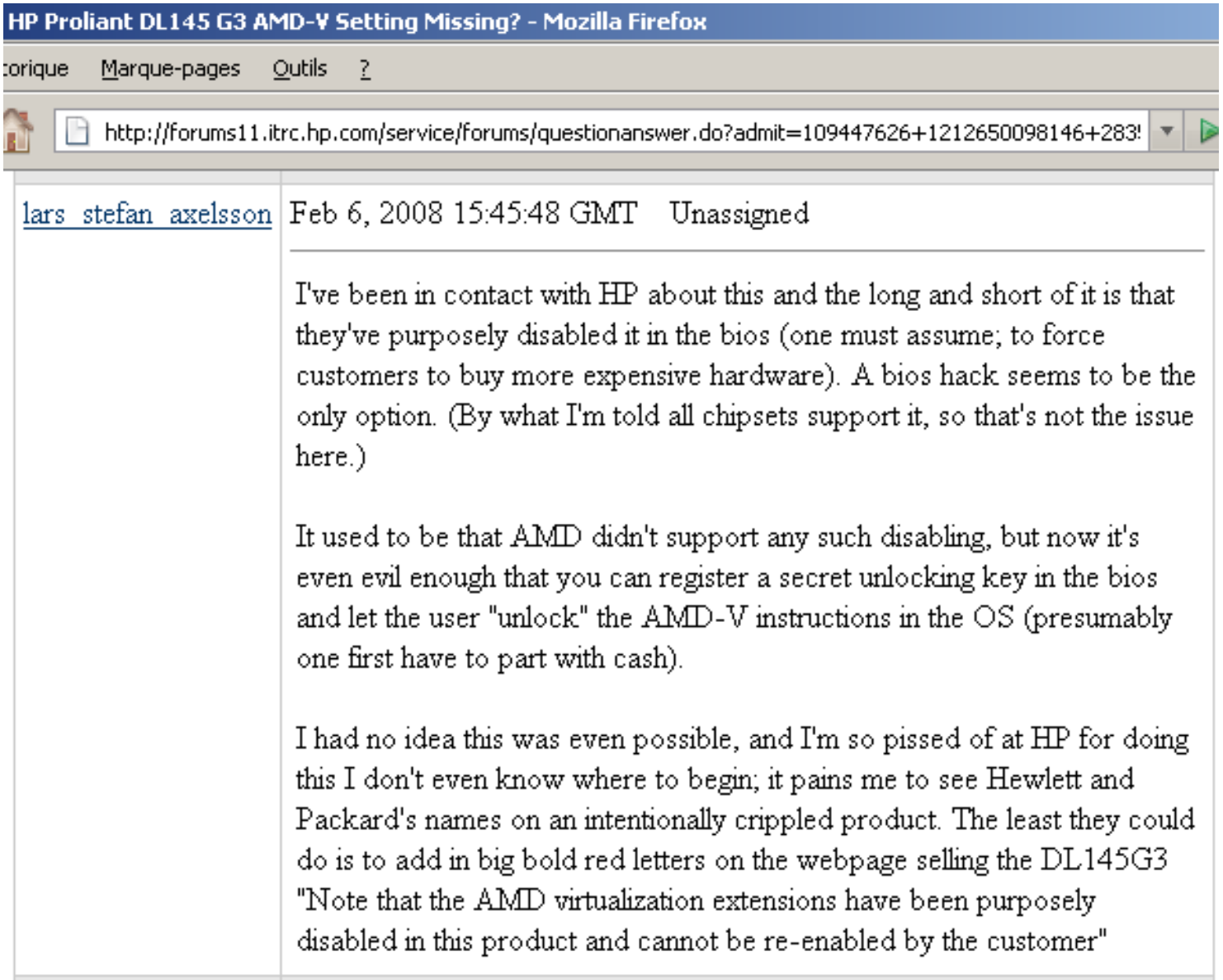
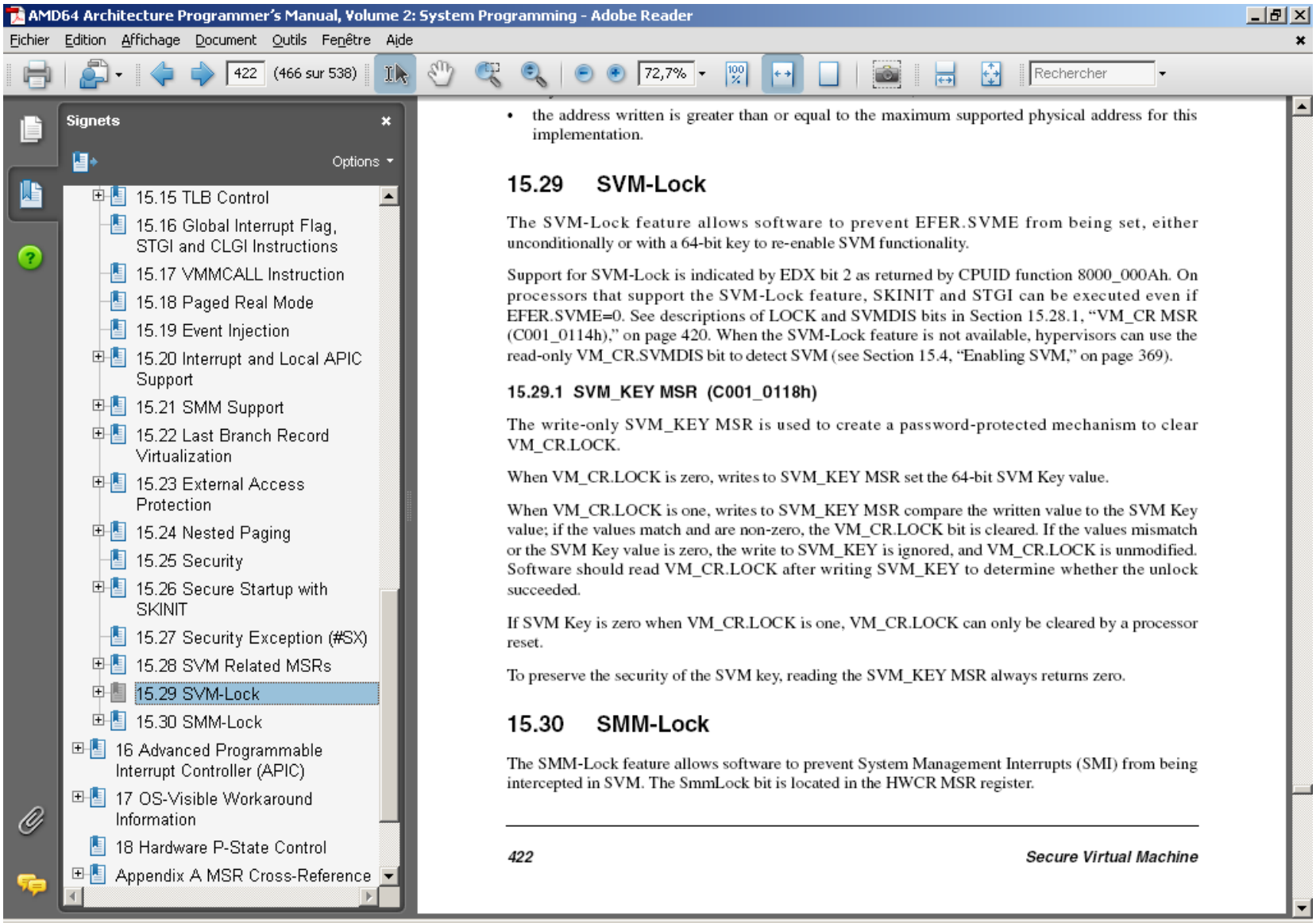
HP m'a tuer

Le coupable

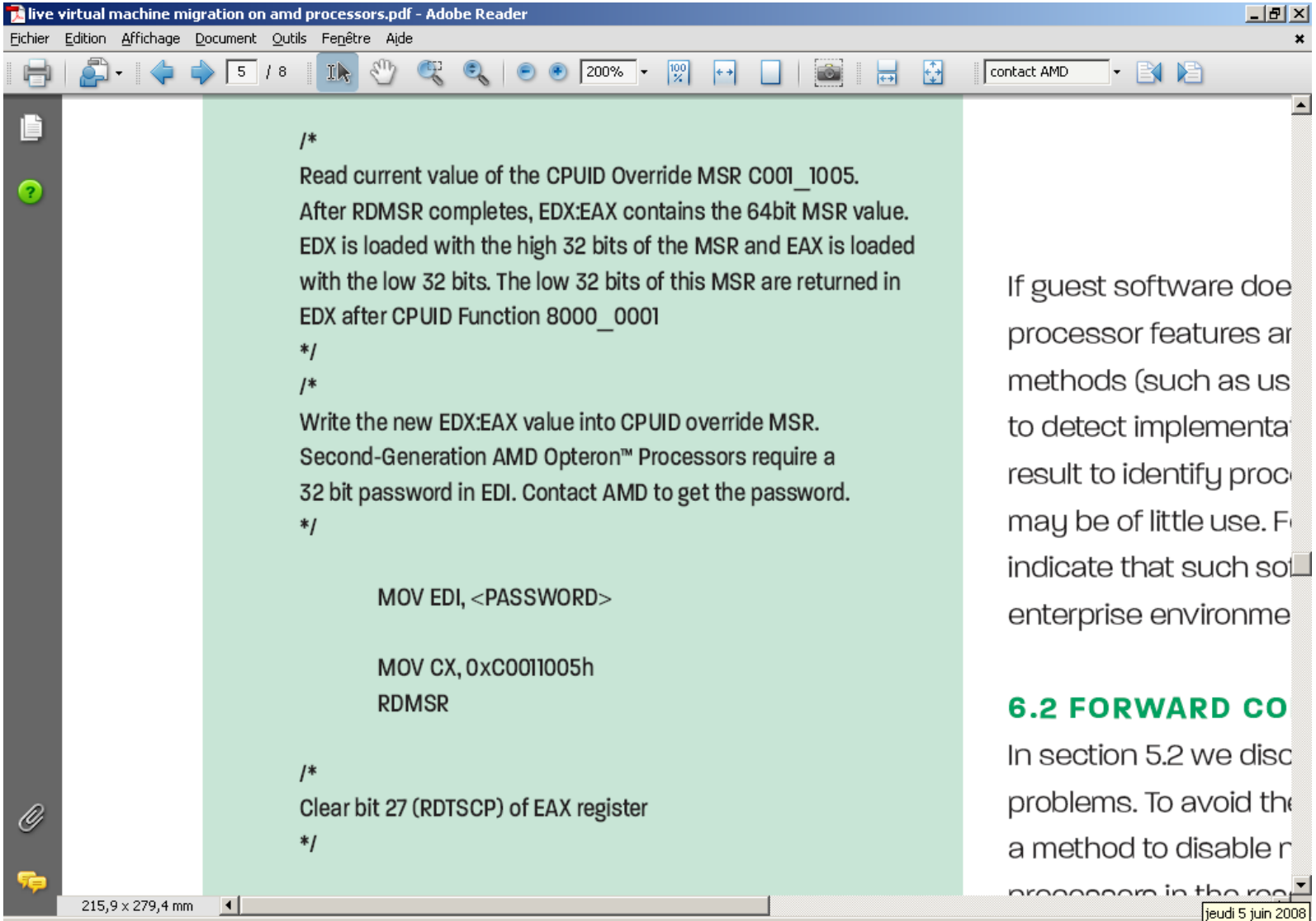
Le problème


HP Proliant DL145 G3 AMD-V Setting Missing? - Mozilla Firefox
orique Marque-pages Outils ?
http://forums11.itrc.hp.com/service/forums/questionanswer.do?admit=109447626+1212650098146+283
lars_stefan_axelsson
Feb 6, 2008 15:45:48 GMT Unassigned
I've been in contact with HP about this and the long and short of it is that they've purposely disabled it in the bios (one must assume; to force customers to buy more expensive hardware). A bios hack seems to be the only option. (By what I'm told all chipsets support it, so that's not the issue here.)
It used to be that AMD didn't support any such disabling, but now it's even evil enough that you can register a secret unlocking key in the bios and let the user "unlock" the AMD-V instructions in the OS (presumably one first have to part with cash).
I had no idea this was even possible, and I'm so pissed of at HP for doing this I don't even know where to begin; it pains me to see Hewlett and Packard's names on an intentionally crippled product. The least they could do is to add in big bold red letters on the webpage selling the DL145G3 "Note that the AMD virtualization extensions have been purposely disabled in this product and cannot be re-enabled by the customer"

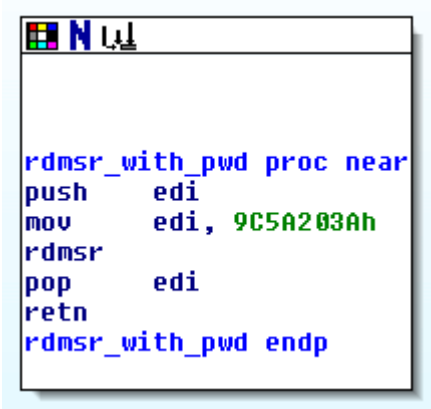
Le complice


AMD64 Architecture Programmer's Manual, Volume 2: System Programming - Adobe Reader
Fichier Edition Affichage Document Outils Fenêtre Aide
422 (466 sur 538)
72,7%
Rechercher
Signets
Options
15.15 TLB Control
15.16 Global Interrupt Flag, STGI and CLGI Instructions
15.17 VMMCALL Instruction
15.18 Paged Real Mode
15.19 Event Injection
15.20 Interrupt and Local APIC Support
15.21 SMM Support
15.22 Last Branch Record Virtualization
15.23 External Access Protection
15.24 Nested Paging
15.25 Security
15.26 Secure Startup with SKINIT
15.27 Security Exception (#SX)
15.28 SVM Related MSRs
15.29 SVM-Lock
15.30 SMM-Lock
16 Advanced Programmable Interrupt Controller (APIC)
17 OS-Visible Workaround Information
18 Hardware P-State Control
Appendix A MSR Cross-Reference
• the address written is greater than or equal to the maximum supported physical address for this implementation.
15.29 SVM-Lock
The SVM-Lock feature allows software to prevent EFER.SVME from being set, either unconditionally or with a 64-bit key to re-enable SVM functionality.
Support for SVM-Lock is indicated by EDX bit 2 as returned by CPUID function 8000_000Ah. On processors that support the SVM-Lock feature, SKINIT and STGI can be executed even if EFER.SVME=0. See descriptions of LOCK and SVMDIS bits in Section 15.28.1, "VM_CR MSR (C001_0114h)," on page 420. When the SVM-Lock feature is not available, hypervisors can use the read-only VM_CR.SVMDIS bit to detect SVM (see Section 15.4, "Enabling SVM," on page 369).
15.29.1 SVM_KEY MSR (C001_0118h)
The write-only SVM_KEY MSR is used to create a password-protected mechanism to clear VM_CR.LOCK.
When VM_CR.LOCK is zero, writes to SVM_KEY MSR set the 64-bit SVM Key value.
When VM_CR.LOCK is one, writes to SVM_KEY MSR compare the written value to the SVM Key value; if the values match and are non-zero, the VM_CR.LOCK bit is cleared. If the values mismatch or the SVM Key value is zero, the write to SVM_KEY is ignored, and VM_CR.LOCK is unmodified. Software should read VM_CR.LOCK after writing SVM_KEY to determine whether the unlock succeeded.
If SVM Key is zero when VM_CR.LOCK is one, VM_CR.LOCK can only be cleared by a processor reset.
To preserve the security of the SVM key, reading the SVM_KEY MSR always returns zero.
15.30 SMM-Lock
The SMM-Lock feature allows software to prevent System Management Interrupts (SMI) from being intercepted in SVM. The SmmLock bit is located in the HWCR MSR register.
422
Secure Virtual Machine

Une backdoor ?

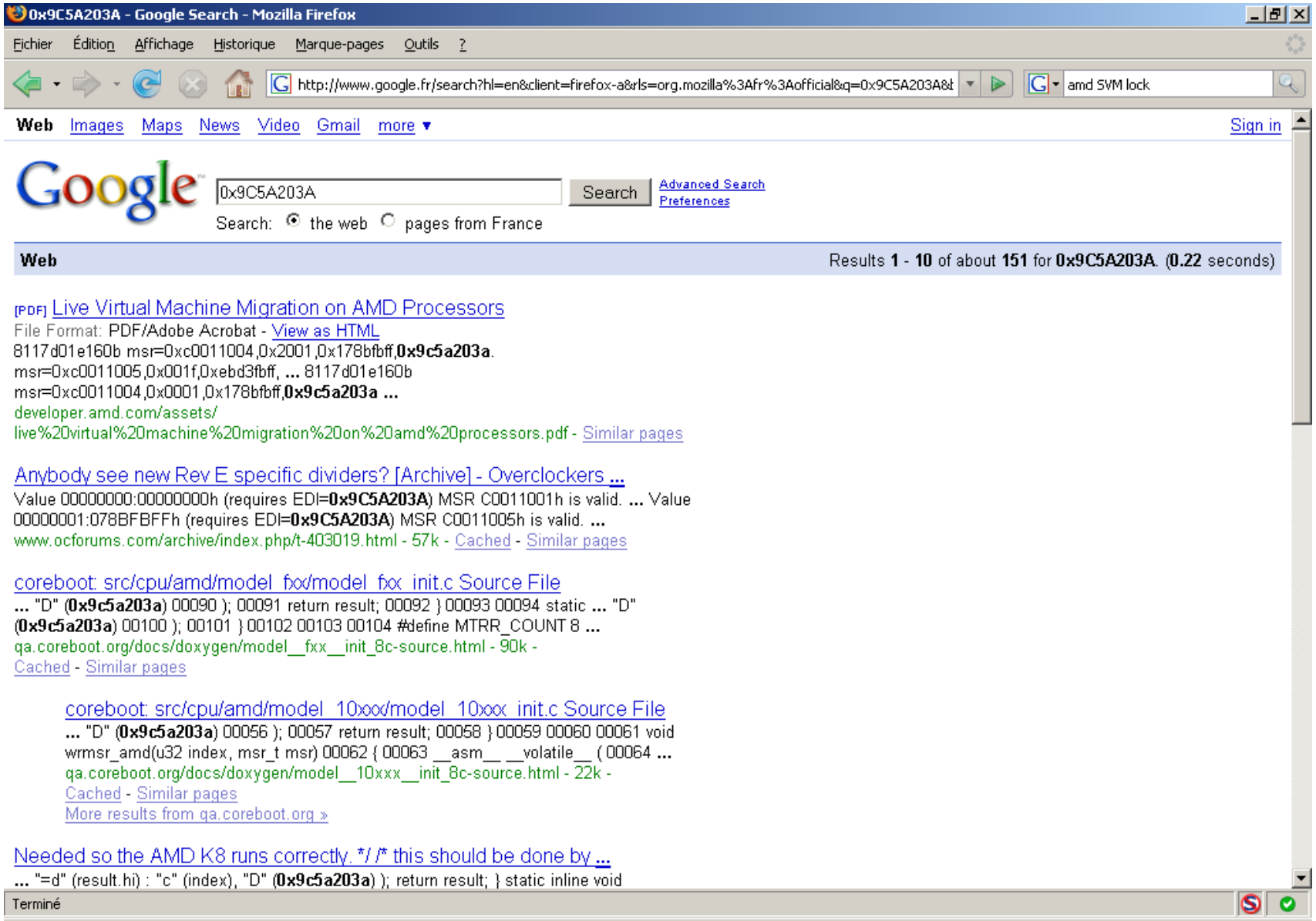


Trop facile



```
rdmsr_with_pwd proc near
push    edi
mov     edi, 9C5A203Ah
rdmsr
pop     edi
retn
rdmsr_with_pwd endp
```

Old news ?


0x9C5A203A - Google Search - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils ?
http://www.google.fr/search?hl=en&client=firefox-a&rls=org.mozilla%3Afr%3Aofficial&q=0x9C5A203A&t
amd SVM lock
Web Images Maps News Video Gmail more ▾
Sign in
Google
0x9C5A203A
Search
Advanced Search
Preferences
Search: the web pages from France
Web
Results 1 - 10 of about 151 for 0x9C5A203A. (0.22 seconds)
[PDF] Live Virtual Machine Migration on AMD Processors
File Format: PDF/Adobe Acrobat - View as HTML
8117d01e160b msr=0xc0011004,0x2001,0x178bfbff,0x9c5a203a.
msr=0xc0011005,0x001f,0xebd3fbff, ... 8117d01e160b
msr=0xc0011004,0x0001,0x178bfbff,0x9c5a203a ...
developer.amd.com/assets/
live%20virtual%20machine%20migration%20on%20amd%20processors.pdf - Similar pages
Anybody see new Rev E specific dividers? [Archive] - Overclockers ...
Value 00000000:00000000h (requires EDI=0x9C5A203A) MSR C0011001h is valid. ... Value
00000001:078BFBFFh (requires EDI=0x9C5A203A) MSR C0011005h is valid. ...
www.ocforums.com/archive/index.php/t-403019.html - 57k - Cached - Similar pages
coreboot: src/cpu/amd/model_fxx/model_fxx_init.c Source File
... "D" (0x9c5a203a) 00090); 00091 return result; 00092 } 00093 00094 static ... "D"
(0x9c5a203a) 00100); 00101 } 00102 00103 00104 #define MTRR_COUNT 8 ...
qa.coreboot.org/docs/doxygen/model__fxx__init_8c-source.html - 90k -
Cached - Similar pages
coreboot: src/cpu/amd/model_10xxx/model_10xxx_init.c Source File
... "D" (0x9c5a203a) 00056); 00057 return result; 00058 } 00059 00060 00061 void
wrmsr_amd(u32 index, msr_t msr) 00062 { 00063 __asm__ __volatile__ (00064 ...
qa.coreboot.org/docs/doxygen/model__10xxx__init_8c-source.html - 22k -
Cached - Similar pages
More results from qa.coreboot.org »
Needed so the AMD K8 runs correctly. */ /* this should be done by ...
... "=d" (result.hi) : "c" (index), "D" (0x9c5a203a)); return result; } static inline void
Terminé

Conclusion

- Plusieurs "features" processeur ont été mises en évidence
  - Accès à des MSRs "cachés" par un mot de passe 32 bits "en dur"
  - Activation/désactivation sélective de la virtualisation par un mot de passe 64 bits "choisi par le BIOS"
- Est-ce robuste ?
  - RDV à SSTIC > 2008