

Anti-VM with ACPI tables

@gsuberland

whois

- Graham Sutherland
- Twitter: @gsuberland (partyhat)
- IRC: gsuberland on freenode
- Email: contact@fisting.horse

disclaimer

This talk does not reflect, refract, absorb, ionise, engage in quantum superposition with, or otherwise associate with the views of my employer, their clients, or their clients' clients.

I like where I work. Please don't fire me.

Research done in 3 hours. Slides written in an hour.

I borrowed this laptop from @dominicgs, don't judge me for any donkey porn popups or other sketchy business.

This may or may not be original research. Who knows. The internet is a pretty big place.

how this came about

- Looking into WPBT at lunch today
- Discovered ACPI tables are A Thing(TM)
- A thought occurs (a rarity, I know)
- Looked into it, vague mentions from places
- I now know that AV knows about this trick

dafuq is an ACPI table?

- Bunch of data tables from hardware
- Used to expose hardware config to OS
- Contains stuff like:
 - SMBIOS data
 - APIC data
 - PCI data
 - HPET data
 - SLIC licenses
 - Trusted Computing evil
 - WPBT evil

so what?

- Tables have names
- Tables have OEM IDs
- Tables have OEM Table IDs
- Tables have Creator IDs
- Tables contain system-specific data
- This stuff isn't (usually) faked by VMs
- It's accessible from ring3, non-admin!
 - (on Windows)

what you talkin bout willis?

picture > 1000 WORDS

The screenshot shows the FirmwareTableView application window. The main area displays a table of BIOS tables with the following columns: Signature, Firmware Provider, Length, Revision, Checksum, OEM ID, OEM Table ID, OEM Revision, Creator ID, Creator Revision, and Description. The APIC table is selected and highlighted in blue.

| Signature | Firmware Provider | Length | Revision | Checksum | OEM ID | OEM Table ID | OEM Revision | Creator ID | Creator Revision | Description |
|-----------|-------------------|---------|----------|----------|--------|--------------|--------------|------------|------------------|--|
| Raw | Raw | 131,072 | | | | | | | | |
| Raw | Raw | 131,072 | | | | | | | | |
| SMBIOS | SMBIOS | 1,284 | | | | | | | | |
| SMBIOS | SMBIOS | 1,284 | | | | | | | | |
| APIC | ACPI | 188 | 1 | 64 | HPQOEM | 161E | 0x00000001 | 0x20205048 | 0x00000001 | Advanced Programmable Interrupt Controller |
| ASFI | ACPI | 165 | 32 | 197 | HPQOEM | 161E | 0x00000001 | 0x20205048 | 0x00000001 | |
| DMAR | ACPI | 176 | 1 | 95 | INTEL | SNB | 0x00000001 | 0x4c544e49 | 0x00000001 | DMA Remapping Table |
| DSDT | ACPI | 152,193 | 2 | 243 | HPQOEM | 161E | 0x00000001 | 0x4c544e49 | 0x20060912 | Differentiated System Description Table |
| FACP | ACPI | 244 | 3 | 125 | HPQOEM | 161E | 0x0000000f | 0x20205048 | 0x00000001 | |
| FACS | ACPI | 64 | 0 | 0 | | | | | 0x00000001 | |
| HPET | ACPI | 56 | 1 | 158 | HPQOEM | 161E | 0x00000001 | 0x20205048 | 0x00000001 | IA-PC High Precision Event Timer Table |
| MCFG | ACPI | 60 | 1 | 198 | HPQOEM | 161E | 0x00000001 | 0x20205048 | 0x00000001 | PCI SIG |
| SLIC | ACPI | 374 | 1 | 220 | HPQOEM | SLIC-MPC | 0x00000001 | 0x20205048 | 0x00000001 | Microsoft Software Licensing Tables |
| SSDT | ACPI | 614 | 1 | 165 | HPQOEM | SataAhci | 0x00001000 | 0x4c544e49 | 0x20060912 | Secondary System Description Table |
| TCPA | ACPI | 50 | 2 | 163 | HPQOEM | 161E | | 0x20205048 | 0x00000001 | Trusted Computing Platform Alliance Capabilities Table |
| XSDT | ACPI | 132 | 1 | 221 | HPQOEM | SLIC-MPC | 0x0000000f | 0x20202020 | 0x01000013 | |

Below the table, a hex dump of the selected APIC table is shown:

```
00000000 41 50 49 43 BC 00 00 00 01 40 48 50 51 4F 45 4D APIC.....@HPQOEM
00000010 31 36 31 45 20 20 20 20 01 00 00 00 48 50 20 20 161E .....HP
00000020 01 00 00 00 00 00 E0 FE 01 00 00 00 00 08 00 00 .....
00000030 01 00 00 00 00 08 01 01 01 00 00 00 00 08 02 02 .....
00000040 01 00 00 00 00 08 03 03 01 00 00 00 00 08 04 00 .....
00000050 00 00 00 00 00 08 05 00 00 00 00 00 00 08 06 00 .....
00000060 00 00 00 00 00 08 07 00 00 00 00 00 01 0C 00 00 .....
00000070 00 00 C0 FE 00 00 00 02 0A 00 00 02 0A 00 00 00 .....
00000080 00 00 02 0A 00 09 09 00 00 00 0D 00 04 06 00 05 .....
00000090 00 01 04 06 01 05 00 01 04 06 02 05 00 01 04 06 .....
000000A0 03 05 00 01 04 06 04 05 00 01 04 06 05 05 00 01 .....
000000B0 04 06 06 05 00 01 04 06 07 05 00 01 .....

```

The status bar at the bottom indicates "16 item(s), 1 Selected" and "NirSoft Freeware. <http://www.nirsoft.net>".

virtually undetectable differences

2008R2 x64, VirtualBox

The screenshot shows the FirmwareTableView application window. The title bar reads 'FirmwareTableView'. The menu bar includes 'File', 'Edit', 'View', 'Options', and 'Help'. Below the menu bar is a toolbar with icons for file operations. The main area contains a table with the following columns: Signature, Firmware Provider, Length, Revision, Checksum, OEM ID, OEM Table..., OEM Revision, Creator ID, Creator Revision, and Description. The table lists several firmware tables, with the SMBIOS table selected. Below the table, the raw data for the selected SMBIOS table is shown in hexadecimal and ASCII format.

| Signature | Firmware Provider | Length | Revision | Checksum | OEM ID | OEM Table... | OEM Revision | Creator ID | Creator Revision | Description |
|-----------|-------------------|---------|----------|----------|--------|--------------|--------------|------------|------------------|--|
| Raw | | 131,072 | | | | | | | | |
| Raw | | 131,072 | | | | | | | | |
| SMBIOS | | 458 | | | | | | | | |
| SMBIOS | | 458 | | | | | | | | |
| FACS | ACPI | 64 | 0 | 0 | | | | | 0x00000001 | |
| XSDT | ACPI | 60 | 1 | 191 | VBOX | VBOXXSDT | 0x00000001 | 0x204c5341 | 0x00000061 | |
| SSDT | ACPI | 460 | 1 | 225 | VBOX | VBOXCPUT | 0x00000002 | 0x4c544e49 | 0x20100528 | Secondary System Description Table |
| FACP | ACPI | 244 | 4 | 64 | VBOX | VBOXFACP | 0x00000001 | 0x204c5341 | 0x00000061 | |
| APIC | ACPI | 92 | 2 | 79 | VBOX | VBOXAPIC | 0x00000001 | 0x204c5341 | 0x00000061 | Advanced Programmable Interrupt Controller |
| DSDT | ACPI | 7,403 | 1 | 85 | VBOX | VBOXBIOS | 0x00000002 | 0x4c544e49 | 0x20100528 | Differentiated System Description Table |

| Hex | ASCII |
|--|------------------|
| 00000000 00 02 05 25 C2 01 00 00 00 14 00 00 01 02 00 E0 | ...%. |
| 00000010 03 01 90 80 01 48 00 00 00 01 00 69 6E 6E 6F |H.....inno |
| 00000020 74 65 68 20 47 6D 62 48 00 56 69 72 74 75 61 6C | tek GmbH.Virtual |
| 00000030 42 6F 78 00 31 32 2F 30 31 2F 32 30 30 36 00 00 | Box.12/01/2006.. |
| 00000040 01 1B 01 00 01 02 03 04 52 29 94 47 AC 7C 46 3A |R).G. F: |
| 00000050 8B 17 53 05 DE C4 03 0C 06 00 05 69 6E 6E 6F 74 | ..S.....innot |
| 00000060 65 6B 20 47 6D 62 48 00 56 69 72 74 75 61 6C 42 | ek GmbH.VirtualB |
| 00000070 6F 78 00 31 2E 32 00 30 00 56 69 72 74 75 61 6C | ox.1.2.0.Virtual |
| 00000080 20 4D 61 63 68 69 6E 65 00 00 02 0F 08 00 01 02 | Machine..... |

10 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

and on vmware?

2008R2 x64, VMware Workstation

FirmwareTablesView

File Edit View Options Help

| Signature | Firmware Provider | Length | Revision | Checksum | OEM ID | OEM Table ID | OEM Revision | Creator ID | Creator Revision | Description |
|---------------|-------------------|---------------|----------|----------|--------|--------------|--------------|------------|------------------|--|
| Raw | | 131,072 | | | | | | | | |
| Raw | | 131,072 | | | | | | | | |
| SMBIOS | | 14,158 | | | | | | | | |
| SMBIOS | | 14,158 | | | | | | | | |
| APIC | ACPI | 962 | 1 | 52 | PTLTD | APIC | 0x06040000 | 0x50544c20 | | Advanced Programmable Interrupt Controller |
| BOOT | ACPI | 40 | 1 | 165 | PTLTD | \$SBFTBL\$ | 0x06040000 | 0x50544c20 | 0x00000001 | Simple Boot Flag Table |
| DSDT | ACPI | 116,897 | 1 | 21 | PTLTD | Custom | 0x06040000 | 0x5446534d | 0x03000001 | Differentiated System Description Table |
| FACP | ACPI | 244 | 4 | 102 | INTEL | 440BX | 0x06040000 | 0x204c5450 | 0x000f4240 | |
| FACS | ACPI | 64 | 0 | 0 | | | | | | |
| HPET | ACPI | 56 | 1 | 170 | VMWARE | VMW HPET | 0x06040000 | 0x20574d56 | 0x00000001 | IA-PC High Precision Event Timer Table |
| MCFG | ACPI | 60 | 1 | 254 | PTLTD | \$PCITBL\$ | 0x06040000 | 0x50544c20 | 0x00000001 | PCI SIG |
| SRAT | ACPI | 1,232 | 2 | 100 | VMWARE | MEMPLUG | 0x06040000 | 0x20574d56 | 0x00000001 | Static Resource Affinity Table |
| WAET | ACPI | 40 | 1 | 98 | VMWARE | VMW WAET | 0x06040000 | 0x20574d56 | 0x00000001 | Windows ACPI Emulated Devices Table |
| XSDT | ACPI | 92 | 1 | 73 | INTEL | 440BX | 0x06040000 | 0x20574d56 | 0x01324272 | |

| | | |
|----------|---|------------------|
| 00000000 | 00 02 04 00 46 37 00 00 00 18 00 00 01 02 0C EA |F7..... |
| 00000010 | 03 00 90 DF 09 7C 00 00 00 00 81 07 04 06 00 00 | |
| 00000020 | 50 68 6F 65 6E 69 78 20 54 65 63 68 6E 6F 6C 6F | Phoenix Technolo |
| 00000030 | 67 69 65 73 20 4C 54 44 00 36 2E 30 30 00 30 37 | gies LTD.6.00.07 |
| 00000040 | 2F 30 32 2F 32 30 31 32 00 00 01 1B 01 00 01 02 | /02/2012..... |
| 00000050 | 03 04 56 4D BC 2D DA C4 7D 1D 94 64 F1 4A DD 2D | ..VM.-...}.d.J.- |
| 00000060 | 81 B8 06 00 00 56 4D 77 61 72 65 2C 20 49 6E 63 |VMware, Inc |
| 00000070 | 2E 00 56 4D 77 61 72 65 20 56 69 72 74 75 61 6C | ..VMware Virtual |
| 00000080 | 20 50 6C 61 74 66 6F 72 6D 00 4E 6F 6E 65 00 56 | Platform.None.V |
| 00000090 | 4D 77 61 72 65 2D 35 36 20 34 64 20 62 63 20 32 | Mware-56 4d bc 2 |

14 item(s), 1 Selected

NirSoft Freeware. <http://www.nirsoft.net>

teh code?

- Kernel32.dll
 - EnumSystemFirmwareTables
 - GetSystemFirmwareTable
- Fully documented on MSDN
- Trivial to use, even a Lemon could do it
- Probably comparable APIs on Linux/BSD
 - (I am a Windows monkey, don't ask me.)

approach

- Enumerate ACPI, FIRM, RSMB system tables
- Get info & contents for each table
- Check for known VM values
- Exit if found

countermeasures

- VboxAntiVMDetectHardened (kernelmode.info)
 - Replaces some ACPI tables
 - Fixes lots of hardware descriptors
 - Doesn't fix everything!
 - Only for VirtualBox.
- AV
 - Some AV detects code that enumerates firmware tables, via heuristic magics.
- Only run Windows XP
 - XP doesn't support dumping FIRM and RSMB
 - This is not a solution ever :-\
- ???
 - Anyone know something I don't?

future research

- Results from ESXi, QEMU, KVM, etc.
- Results from other guest operating systems.
- Deeper analysis of table contents for variances.
- A public PoC that's actually worth a damn.
- ????

kthxbai

any questions?