



[讨论]Windows是如何得知硬件信息的 如显卡网卡



机械瞑衍



大侠

2016-11-25 13:24

8831

都知道CPU型号和详细信息可以通过cpuid命令来获取 那么网卡,显卡硬盘等硬件 在最底层是如何获取信息的呢 是通过什么命令获取的 还是其他的什么方式？

【公告】欢迎大家踊跃尝试高研班11月试题，挑战自己的极限！



收藏 · 3



点赞



打赏



分享

最新回复 (24)



hzqst



3

2016-11-25 16:55

2 楼

0

给对应的设备驱动发请求呗。如果你说设备驱动是如何识别硬件的。。那你得问厂商

大牛



机械瞑衍



2

2016-11-27 11:22

3 楼

0

这些请求有没有规定好的协议呢 或者windows是不是封装了API?

大侠



ugvjewxf



5

2016-11-27 14:04

4 楼

0

每个硬件出厂之前都会把，硬件信息固化在ROM里的，程序直接去取就可以了，操作系统也是到硬件ROM里面取的。windows一般都会取出来放注册表里面的，我们编程一般去注册表去就可以了。

大侠



老伙计



6

2016-11-27 16:50

5 楼

0

通过Windows系统提供的WMI服务，可以查到几乎你能想到的任何硬件、软件的状态和信息。

极客



机械瞑衍



2

2016-11-28 08:46

6 楼

0

请问ROM中的信息要如何去读 去获取呢

大侠



机械瞑衍



2

2016-11-28 16:54

7 楼

0

WMI是通过注册表实现的 想要越过注册表并不难 所以我想在最底层实现信息的修改

大侠



叁毛



1

2016-11-28 17:33

8 楼

0

cpu是cpuid指令。

大佬

硬盘是用ioctl 比如可以读取厂商信息 磁盘序列号等 这个是工业用的ATA/ADAP标准

最新回复 (24)

```
HANDLE hPhysicalDrive = NULL;
WCHAR wszDriveName[MAX_PATH]={0};
(void)StringCchPrintfW(wszDriveName,
                        _countof(wszDriveName),
                        L"\\\\.\\PhysicalDrive%d",
                        uDiskNumber);

hPhysicalDrive = CreateFileW(wszDriveName,
                              GENERIC_READ | GENERIC_WRITE,
                              FILE_SHARE_READ | FILE_SHARE_WRITE,
                              NULL,
                              OPEN_EXISTING,
                              0,
                              NULL);

if (hPhysicalDrive == INVALID_HANDLE_VALUE)
{
}

DWORD dwBytesReturned = 0;

// Get SMART version information
GETVERSIONINPARAMS VersionParams;
ZeroMemory(&VersionParams, sizeof(VersionParams));
if (!DeviceIoControl(hPhysicalDrive,
                     SMART_GET_VERSION,
                     NULL,
                     0,
                     (LPVOID)&VersionParams,
                     (DWORD)sizeof(VersionParams),
                     &dwBytesReturned,
                     NULL))
{
}

if (VersionParams.bIDEDeviceMap > 0)
{
    BYTE bIdOutCmd[sizeof(SENDCMDOUTPARAMS) + IDENTIFY_BUFFER_SIZE
- 1] = {0};

    // Setup SMART request
    SENDCMDINPARAMS InParams;
    ZeroMemory(&InParams, sizeof(InParams));
    InParams.cBufferSize = IDENTIFY_BUFFER_SIZE;
    InParams.irDriveRegs.bFeaturesReg = 0;
    InParams.irDriveRegs.bSectorCountReg = 1;
    InParams.irDriveRegs.bSectorNumberReg = 1;
    InParams.irDriveRegs.bCylLowReg = 0;
    InParams.irDriveRegs.bCylHighReg = 0;
    InParams.irDriveRegs.bDriveHeadReg = (BYTE)(SMART_BASE_DRIVE_HEAD |
((uDiskNumber % 2) << 4));
    InParams.irDriveRegs.bCommandReg = ID_CMD;
    InParams.bDriveNumber = (BYTE)uDiskNumber;

    // Get SMART information
```

最新回复 (24)

```
SMART_RCV_DRIVE_DATA,
(LPVOID)&InParams,
sizeof(SENDCMDINPARAMS) - 1,
(LPVOID)&btIdOutCmd,
sizeof(SENDCMDOUTPARAMS) + IDENTIFY_BUFFER_
SIZE - 1,

&dwBytesReturned,
NULL) != FALSE)

{
}

}

CloseHandle(hPhysicalDrive);
```

网卡没搞过



**Rookietp** 2016-12-1 12:00 9 楼 0

极客

网卡也可以通过上述驱动设备来读取!



**MistHill** 2016-12-1 12:36 10 楼 0

大牛

- 应用层用API比较方便。
1. CPU, cpuid(8楼)
  2. 硬盘, kernel32.CreateFile/kernel32.DeviceIoControl(8楼)
  3. 显卡, 读注册表
  4. 网卡, iphlapi.GetAdaptersInfo

底层驱动级的请楼下回答。



**机械限衍** 2016-12-1 22:10 11 楼 0

大侠

显卡只能读注册表吗 用DeviceIoControl不行吗



**dmxc** 2016-12-12 16:08 12 楼 0

极客

有两种方法：一种是搜索物理内存 0x000F0000-0x000FFFFFF，找到EPS表之后，再通过它读取SMBIOS的数据结构表就行；另外一种是直接去注册表中的Local machine中去读取。两种方法读取的值可能会不一样。使用第一种方法要注意，在使用最新的win10纪念版时，检测出来的主板ID可能会发生变化，第二种方法则不会存在这种情况。



**yy虫子yy** 2016-12-12 16:13 13 楼 0

极客

注册表读取，设备请求读取



**dmxc** 2016-12-12 16:14 14 楼 0

极客

额。。。我好想理解错了，@MistHill说的对



**ecrious** 2016-12-13 17:46 15 楼 0

极客

显卡可以用CUDA来获取信息

最新回复 (24)



**shopinng** 2016-12-14 12:47

16 楼 0

底层驱动级的表示原理是一样，只不过是底层的API和调用汇编更方便点。。。

极客

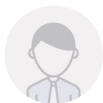


**wangfengge** 2017-1-23 14:27

17 楼 0

简洁明了。

极客



**aisht** 2017-1-29 11:55

18 楼 0

同问 驱动应该要在哪个环节下.

修改硬件信息好呢.

当然.不hook ssdt不触发pg 最好...

v校前段时间成提到说可以做到.

然而还没找出这种哪改好...

极客



**陶宝plus雪** 2017-1-30 15:54

19 楼 0

我觉得应该读ROM吧

极客



**bamboogj** 2017-1-30 18:32

20 楼 0

默默的觉得wmi 最方便。。不过 跟你需求不太相关。。

大侠



**机械阉衍** 2017-2-3 08:41

21 楼 0

就是HOOK硬件通讯的捏个XXXIOXXX的捏个API就好了

大侠



**aisht** 2017-2-7 11:34

22 楼 0

问题就是这个点..

这个api是属于ssdt的...

驱动下hook这个api.会触发pg..

所以...好头疼.

极客



**机械阉衍** 2017-2-7 16:30

23 楼 0

用VT 或者老外貌似有一个过掉PG的东西 不过怎么说呢 都不是特别好的解决方案🙄

大侠



**aisht** 2017-2-7 19:30

24 楼 0

vt兼容性又是个问题.(好吧,其实是不会)

过pg的更是...

可不想写出只对某个系统能用的东西..这不符合也不是编程爱好者的想法.

要说"达到目的就行"这种话..

那硬编码多好.~缺点大家也都知道

极客



**机械阉衍** 2017-2-8 09:05

25 楼 0

据说老外的捏个可以过掉WIN7-WIN10 具体如何实现就不知道了 在破解这块就不要把代

码想的太美好了 因为没有代码没有框架 实施也是比较随意一些吧 总之不管什么方法 可以

达到目的就算成功了嘛 能够过掉PG的并且很稳定那就算成功了

大侠

最新回复 (24)



游客

登录 | 注册 方可回帖

回帖

表情

高级回复

返回