The ways people mess up IUnknown::QueryInterface, episode 3

devblogs.microsoft.com/oldnewthing/20091007-00

October 7, 2009

Raymond Chen

Today we'll combine information you already know, some of which I covered in The ways people mess up IUnknown::QueryInterface with additional clues from The layout of a COM object. There's still not enough information for you to solve the problem entirely on your own, but maybe you can demonstrate your nascent psychic debugging powers and solve the problem.

A customer contacted the shell team because their shell extension was causing the shell to crash. Perhaps they were doing something wrong, but they couldn't see what. The crash looked like this:

```
eax=cccccccc ebx=02b31798 ecx=0008db64 edx=02b26348 esi=001ea7fc edi=02b26348
eip=76381427 esp=0008db28 ebp=0008db30 iopl=0         nv up ei pl nz na pe nc
cs=001b  ss=0023  ds=0023  es=0023  fs=003b  gs=0000             efl=00000206
76381427 8b08            mov     ecx,dword ptr [eax]  ds:0023:cccccccc=????????
```

Your next hint is that the crash takes place while the shell is trying to invoke a COM method.

What you should recognize is that this is either at the fetch of a COM object's vtable or at the fetch of the pointer to the `IUnknown::QueryInterface` method (which is the first function in the vtable of any COM object).

Either way, we obviously have a bad COM object pointer. The next hint is that the pointer was the result of a call to `IUnknown::QueryInterface`:

```
ISomeInterface* psi;
punkObj->QueryInterface(IID_ISomeInterface, (void**)&psi);
...
```

If you prefer to speak ATL, it would be something like

```
CComQIPtr<ISomeInterface> spsi(punkObj);
...
```

Either way, the problem is that the `punkObj` responded to `IUnknown::QueryInterface` by putting the special debugging value `0xCCCCCCCC` into the output pointer rather than following the rules for `IUnknown::QueryInterface` which require you either to succeed and produce a valid object pointer or to fail and set the output pointer to `NULL`.

The object in question came from the customer's shell extension. After we pointed out to the customer that their `IUnknown::QueryInterface` implementation did not adhere to the interface contract, all further communication ceased. We never did get any acknowledgement or even a word of thanks. Maybe they were too embarrassed.

Raymond Chen

Follow