Subject: Re: .full_reset_session causing a seg fault
Posted by Karl Schultz on Fri, 10 Feb 2006 17:59:48 GMT
View Forum Message <> Reply to Message

On Fri, 10 Feb 2006 08:25:14 -0800, Ed Wright wrote:

```
>  To: IDL users
>
>  I developed a large dlm (335 routines to interface IDL to the NAIF
>  CSPICE library) which seems to run correctly on Solaris, OSX, Linux, and
>  Windows.
>
>  This morning while testing an addition to the interface set, I
>  discovered the .full_reset_session command causes a seg fault on OS X,
>  Linux and Windows, e.g.:
>
>  IDL> print, cspice_j2000()
>  % Loaded DLM: ICY.
>         2451545.0
>  IDL> .full_reset_session
>  Segmentation fault
>  skynet 20:
>
>  I used this command quite often during initial development. Can anyone
>  provide advice as to what mechanism might cause this event?
```

One thing that I can suggest is that your DLM is allocating memory someplace and the DLM code is overwriting memory outside the bounds of the allocation, damaging the memory allocator data structures. When IDL frees memory it allocated as part of the reset session process, it may try to free a block whose associated memory control block got damaged, which leads to a crash.

Memory control blocks often reside close to the actual memory that was allocated, so it is pretty easy to whack one. Also, sometimes a block can get damaged at a certain point in time and the damage may never be noticed because the process terminates in a way that frees the entire heap at once. Or the damage may not be noticed until much later because the memory block is long-lived and does not get freed until something drastic like reset session happens.

One way to verify this assumption is to run under a debugger and look at the resulting stack trace. If the stack frame at the top of the call stack indicates that the program was in one of the memory allocation or free routines (malloc or free), then that's the problem. If the top of the call stack indicates the crash happened someplace else, like in IDL, it is possible that a pointer important to IDL got whacked by the DLM and IDL gets lost because of that.

This isn't necessarily a bug in CSPICE. It is possible that the IDL layer isn't checking for the right data types passed to the DLM and may be doing the wrong thing based on the data passed in, etc. Lots of possibilities. But I think a memory control block overwrite is a likely cause. Good luck.

Karl