

---

Subject: Re: Examine "Saved" IDL procedures now too!  
Posted by [Randall Skelton](#) on Tue, 26 Mar 2002 18:21:01 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

On Tue, 26 Mar 2002, Paul van Delst wrote:

[snip]

- > As for the sad folk that have a predisposition to ignore software license agreements, it seems
- > to me they are always going to be around - both the sophisticated and the brain-dead. If a
- > software developer makes it easy for people to hack code, then of course more people will do
- > it. If one is really serious about distributing and protecting proprietary code, I would think
- > a not insignificant amount of time and resources would need to be dedicated to this end - and
- > that would more than likely involve legal resources. Anything less would seem to be the
- > equivalent of finger-crossing and hoping for the best.
- >
- > All the above is purely my badly informed personal opinion. :o)

I agree. The only way for this to be resolved is for RSI to step up and define a system whereby IDL code can be massaged into a somewhat tamper-resistant form. What about using some sort of key-generated encryption scheme that developers need to buy into? This way, every registered 'IDL developer' would get a a strong encryption tool and a set of keys to encrypt their source. RSI would be responsible for the maintenance and security of both the encryption tool and keys. When a user gets one of these encrypted files from a developer, they simply place it in the IDL path like any other .pro file and when needed IDL would auto-magically decrypt the code into a compiled procedure, function or object set. Assuming that RSI uses a modern, strong encryption scheme, the chances of the source file being decoded would be small. Alas, depending on how RSI represents the compiled functions, procedures and objects in IDL's working memory, it may still be possible to recover the the source...

Comments?  
Randall

---