Subject: Re: Encrypted storage with streaming (OpenSSL, AES)
Posted by koldo on Fri, 18 Sep 2009 11:23:27 GMT
View Forum Message <> Reply to Message

Hello Mindtraveller

About rdtsc, in fact it compiles in gcc as it has an ifdef so that:

- If MSC, it takes a value from rdtsc (time stamp counter 64-bit register)
- Else it takes Random()

It seems that to get a random number our Random() implementation is better than the clock (MT19937 algorithm), so perhaps rdtsc() would have to be changed with Random()

I have tried to compile in MinGW, but I get linking errors, in summary:

Openssl\out32\libeay32.lib(tmp32/ui_openssl.obj),(.text[_rea d_string_inner]+0xb): undefined reference to `__security_cookie'
Openssl\out32\libeay32.lib(tmp32/ui_openssl.obj),(.text[_rea d_string_inner]+0x149): undefined reference to `@__security_check_cookie@4'
Openssl\out32\libeay32.lib(tmp32/ecp_smpl.obj),(.text[_ec_GF p_simple_group_set_curve]+0x6): undefined reference to `_chkstk'

Does anybody know how to solve these problems with chkstk and security_cookie ?

Best regards
Koldo