Sunday, May 25. 2014

Changes to Openssl in Solaris 11.2

This blog entry wasn't on my radar somehow, nevertheless it reports about an important change to OpenSSL on Solaris 11.2. The most important change from my point of view is the inlining of T4/T5 crypto to Solaris 11.2 openssl:
Years and years ago, I worked on the SPARC T2/T3 crypto drivers. On the SPARC T2/T3 processors, the crypto instructions are privileged; and therefore, the drivers are needed to access those instructions. Thus, to make use of T2/T3 crypto hardware, OpenSSL had to use pkcs11 engine which adds lots of cycles going through the thick PKCS#11 session/object management layer, Solaris kernel layer, hypervisor layer to the hardware, and all the way back.
However, on SPARC T4/T4+ processors, crypto instructions are no longer privileged; and therefore, you can access them directly without drivers. [...]
What does that means to you? Much improved performance! No more PKCS#11 layer, no more copy-in/copy-out of the data from the userland to the kernel space, no more scheduling, no more hypervisor, NADA! [...]

Posted by Joerg Moellenkamp in English, Solaris at 12:44

https://blogs.oracle.com/observatory/entry/openssl_on_solaris_11_2

"However, be sure to leave the pkcs11 engine disabled on T4/T4+ if you want max performance."

How would I do that?
Anonymous on May 25 2014, 23:13