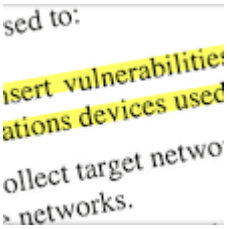
Theodore Ts'o ▸ Public Sep 5, 2013

I am so glad I resisted pressure from Intel engineers to let /dev/random rely only on the RDRAND instruction. To quote from the article below:

"By this year, the Sigint Enabling Project had found ways inside some of the encryption chips that scramble information for businesses and governments, either by working with chipmakers to insert back doors...."

Relying solely on the hardware random number generator which is using an implementation sealed inside a chip which is impossible to audit is a **BAD** idea.



N.S.A. Foils Much Internet Encryption

nytimes.com

243 +1 617 264

Shared publicly • View activity

View 237 previous comments

Mirko Zlojić Dec 17, 2013

+Theodore Ts'o so , after this whole story , can I be confident that my linux box is safe ? are we using HWRNG or not ?

Theodore Ts'o +3 Dec 17, 2013

+Mirko Zlojić We are using RDRAND, but it is being mixed in with other entropy being gathered from the system. That way, it can't do any harm, and if it is in fact an honest RNG, it will help.

SIGN IN

question which you already answered :D

Mirko Zlojić Dec 22, 2013

I still do not believe RSA compromised itself in such a manner ??

कुरूकुल्ले शेर्प Jan 1, 2014

Same for AMD as Intel? Time for NXP / Lenovo Taiwan (via China mainland) to come out with a new NSA proof IC set and take some market share in the USA!

Mojito skurt +2 Aug 30, 2014

+Will Drewry

They can... well indirectly.. Intel rather (if speaking of Intel chips now), were shown to contain a 2048 bit signed/encrypted key in the firmware. Game over... long time. Now you can barely get an Intel chip without VPro etc. Ever wondered how come the i7 series were so cheap w.r.t. to former technology? i.e. 2x00 series say vs. 8XX chips or similar and so on.... Theodore et al. are being necessarily moderated "one chip manufacturer"... It has been revealed that NSA/US intend to subvert any and/or all IT companies they can, including from other countries. This is the largest attack on freedom ever actually. Ironically, Theodore here sits and uses a Haswell or what they are called now intel chip on his laptop.

Add a comment...