

Re: (N)ever (S)ay (A)nything – Any ideas ??

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-06/1981.html>

From: Colin Percival (*cperciva_at_sfu.ca*)

Date: 06/28/05

Date: Tue, 28 Jun 2005 01:43:55 +0000 (UTC)

Galathas <galathas@centrum.cz> wrote:

> *what are Your ideas about NSA development nowadays ??*

Side channel attacks. Two decades ago, they were "encouraging" people to not investigate the possibility of information leakage via memory access patterns; we know that they have a large investment in power consumption and electromagnetic ("TEMPEST") side-channels; and the US export requirements for cryptographic code are exactly what one would expect if the intention was to simplify side-channel attacks ("show us your code, so that when we see a signal we can work out exactly where it is coming from").

Of course, they're also doing things like operating system development for the benefit of other government departments, and all sorts of signal interception... but I'm fairly confident that their major cryptographic focus is side channel attacks.

Colin Percival