

## Re: FreeBSD Security Advisory FreeBSD-SA-05:09.htt [REVISED]

*Source:* <http://www.derkeiler.com/Mailing-Lists/FreeBSD-Security/2005-05/0064.html>

---

*From:* Colin Percival ([cperciva\\_at\\_freebsd.org](mailto:cperciva_at_freebsd.org))

*Date:* 05/18/05

Date: Tue, 17 May 2005 16:18:32 -0700

To: David Schultz <[das@freebsd.org](mailto:das@freebsd.org)>

David Schultz wrote:

> *Some colleagues and I have a paper in submission that addresses*  
> *the issue of key-dependent control flow, much as you describe.*

Care to send me a pre-print?

> *If you're willing to wait a day or two, you don't even need to*  
> *have a local account:*  
>  
> <http://crypto.stanford.edu/~dabo/abstracts/ssl-timing.html>

1. The Boneh-Brumley attack is specific to a particular method of performing large integer arithmetic (and thus only applies to RSA, DH, and DSS). My attack applies to essentially all code -- both crypto and non-crypto -- although I picked RSA/OpenSSL as a good demonstration platform.

2. The Boneh-Brumley attack was fixed two years ago.

> *I'm just reading Colin's paper now---so as you say, it sounds like*  
> *the punchline is that having a local account buys you a few orders*  
> *of magnitude in attack time. Kewl.*

No. On hyperthreaded systems which don't run FreeBSD or SCO, having a local account buys you an attack which would otherwise be impossible. (Unless you're running a really old version of OpenSSL.)

Colin Percival

---

[freebsd-security@freebsd.org](mailto:freebsd-security@freebsd.org) mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-security>

To unsubscribe, send any mail to "[freebsd-security-unsubscribe@freebsd.org](mailto:freebsd-security-unsubscribe@freebsd.org)"