

Re: Pre-encrypt IV in CBC mode

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-02/msg00829.html>

- *From:* daw@xxxxxxxxxxxxxxxxxxxxxxxxxxxx (David Wagner)
 - *Date:* Mon, 27 Feb 2006 19:21:22 +0000 (UTC)
-

Ben Pfaff wrote:

For the first block of plaintext, though, the IV takes the place of the previous block of ciphertext. If the IV doesn't differ much from the previous IV, and the actual plaintext block doesn't differ much from the previous packet's, then the effective plaintext won't differ much, either. This means that you have pairs of ciphertext blocks combined with plaintext blocks that differ in just a few bit positions. This can be a wedge for assorted cryptanalytic attacks."

I love Bellovin's work dearly, but in this case I happen to think this argument is weak. If the block cipher is any good, it shouldn't matter whether its inputs are close or not.

The real problem with using a counter as the IV in CBC mode is such a scheme is not IND-CPA secure.

.