

Re: The importance of IVs

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-08/1677.html>

From: Paul Rubin (//phr.cx_at_NOSPAM.invalid)

Date: 08/27/05

Date: 27 Aug 2005 13:50:34 -0700

"mobius30" <mobius30@hushmail.com> writes:

- > *I'm by no means neither a professional programmer NOR an accomplished*
- > *cryptographer. I'm an amateur programmer, with most of my experience in*
- > *VB .NET. I am looking for BOTH off-the-shelf symmetric software and*
- > *the libraries necessary to build my own. The end goal is to gain*
- > *enough reference and knowledge to:*
- > *Build a good solid TRUE Blowfish crypto app in VB.NET. Nothing*
- > *spectacular, just a simple plain-text app that is secure (i.e. doesn't*
- > *write to swap, uses the correct algorithm, does the full 16-rounds, etc).*

The biggest problem here is avoiding writing to swap. I'd be surprise if vb.net gives you any control over that.

- > *Almost every app I've found (freeware at least) uses C or C++.*
- > *So, yes, your help would be greatly appreciated. Do you know of any*
- > *off-the-shelf free (or low-cost) apps that implement TRUE 16-round*
- > *64-bit block Blowfish (you know, what Schneier actually intended a*
- > *decade ago!)?*

I've never heard of anyone implementing "false" 16-round Blowfish. Blowfish has been implemented many times, though maybe not in VB.

Blowfish is sort of old-school these days though. Is there some reason you don't want to use AES? I'd say you should use AES in EAX mode, if you want to be up with the times.

Actually, there may be a Windows CAPI function that does AES, in which case you should use it.