

Re: The importance of IVs

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-08/1776.html>

From: mobius30 (mobius30_at_hushmail.com)

Date: 08/30/05

Date: 29 Aug 2005 15:12:21 -0700

Paul Rubin wrote:

>The 64 bit blocksize is in fact a security weakness for some
>types of use.

Agreed, for SOME uses. But for simple plain text encryption, there is nothing wrong with its use in Blowfish.

>I'm not trying to slam Blowfish. It was a good contribution back in
>the DES era but we've had a lot of progress since then. The new
>knowledge lets us do stuff better than we could before. Let's not
>throw away that opportunity.

Also agreed, and I'm not "slamming" AES. Lord knows it was a brilliant idea! But, the fact that AES can now be broken by reducing the number of rounds by just a handful does not make me feel safe about using it. Why? Well it may be safe now, but that's not what AES was created for. It was designed with the purpose of protecting information WELL into the future. That's why we had the whole AES competition in the first place. We needed an algorithm that could replace DES and LAST for a long long long long time. All I've been saying is that other symmetric block ciphers, Blowfish in particular, require much more round reduction to see cryptanalysis results. As the years go by, no doubt we will see the reduced round variants of AES that can be broken inching closer and closer to the number of rounds specified. I agree "the new knowledge lets us do stuff better than we could before." So, I'm just saying, for now, I like Blowfish better, at least for the purposes of plain-text encryption. It requires much more round reduction to see analysis results. Also, I'm just looking to the future, for the next so-called AES. We may need it in 10 years; maybe less, maybe more. A lot of breakthroughs are in store for us and some of them could involve weakening or even compromising AES. Example: I archive an AES encrypted file with privacy information on a secure server. It's critical that this info remain private for say the next 75 years. If that server is broken into TODAY and the AES encrypted files are copied to an outside source and held onto by a clandestine party, I want to feel confident that in 10 or 15 years they won't be able to read the files. The crypto lifespan of this exercist was supposed to be 75 years and I may only be getting less than half that.

sci.crypt: Re: The importance of IVs

That's why it is important to take note that AES has its weaknesses too and someday soon we will find a way to compromise the entire system. You may say, well when a better algorithm emerges, we can just re-encrypt all those files. Huh? Y2K what? Didn't we learn anything about planning ahead? About doing it right the first time? Or have we become a bunch of disposable cellphone using simpletons that can't build houses that last more than 20 years anymore? AES was supposed to be THE SOLUTION. Unbreakable for the rest of our lives! I just think the AES competition didn't get the job done right. Maybe we didn't have enough knowledge then. Maybe if we had the competition again today, we would see better candidates and a better encryption standard that will last for the next 100+ years. But I'm just saying that AES, although newer and more elegant than the more old-fashioned block ciphers, isn't the answer to our prayers.