

Re: Passwords with evolving key/expansion/setup that has flaws some bite leak could be a good thing

Re: Passwords with evolving key/expansion/setup that has flaws some bite leak could be a good thing

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2006-07/msg00522.html>

- *From:* "John E. Hadstate" <jh113355@xxxxxxxxxxxx>
 - *Date:* Sat, 15 Jul 2006 23:14:54 -0400
-

<jt64@xxxxxxxx> wrote in message
news:1153002494.935764.5960@xx

Dabiker! Old buddy! Still collecting cipher designs from wastebaskets at the NSA? ;-)

Well since Tom started writing about byte access i started searching and come to read about permutation based PRNG as base for ciphers.

You mean like RC4? Maybe not such a good example to follow.

However, you should realize that AES in CTR mode could be called a "permutation-based PRNG" and is thought to be an excellent base for ciphers.

I understand you say that the problem with permutation PRNG ciphers like my Streambuddy is that once you know the password there is no challenge to decipher since it never change and you just have to follow the evolution of permutation.

Isn't that true of any cipher? Once you know the password, there is no challenge to decipher. Yes, that is sometimes considered more a strength than a weakness. In many applications it does help to be able to decipher what you've enciphered.

Re: Passwords with evolving key/expansion/setup that has flaws some bite leak could be a good thing

Re: Passwords with evolving key/expansion/setup that has flaws some bite leak could be a good thing

Well maybe this is just an wild idea to try to obfuscate the fact that it is easy to follow a PRNG.

Only if the PRNG is poorly designed or has features that make it predictable (like the linear congruential or LFSR PRNGs). If the PRNG is of cryptographic quality, it is nearly impossible to predict the next value with any probability better than random chance, no matter how much history you have available for modeling.

Once you find *the correct* password, so is it really a bad thing that some keys duplicate permutation PRNG if the password itself is permutating creating different keysetups.

Well that is my question.

I don't understand how that's a question. It seems to me that once the attacker finds the correct password, you are completely hosed until you change the password. If you are saying that it should be difficult for the attacker to find the correct password from studying the ciphertext and known plaintext, well, you're right. In fact, it must be practically impossible or your cipher is worthless.

I think you might be saying that processing the password through a one-way function before it's used will solve a problem with using a PRNG that leaks key bits. On the surface, this is an appealing idea, but if you think about it, it doesn't solve the problem. If the PRNG leaks its key bits, the attacker will simply reconstruct the key as it was fed to the PRNG (the output of the one-way function). He doesn't need to take it all the way back to the original password. He will simply skip the one-way function and apply the reconstructed password directly to the PRNG. The only solution is to use a "permutation-based PRNG" that doesn't leak the key bits (like AES or Twofish or Blowfish or 3DES in counter mode).

Re: Passwords with evolving key/expansion/setup that has flaws some bite leak could be a good thing

Re: Passwords with evolving key/expansion/setup that has flaws some bite leak could be a good thing

JT

Re: Passwords with evolving key/expansion/setup that has flaws some bite leak could be a good thing