

## Re: What's the bottom line on RC4??

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-02/2155.html>

---

**From:** Scott Fluhrer ([sfluhrer@ix.netcom.com](mailto:sfluhrer@ix.netcom.com))

**Date:** 02/09/03

From: "Scott Fluhrer" <[sfluhrer@ix.netcom.com](mailto:sfluhrer@ix.netcom.com)>

Date: Sat, 8 Feb 2003 23:54:15 -0800

Yama <[Yama@yomama.com](mailto:Yama@yomama.com)> wrote in message

news:bbgb4v8h00e5cgiut5iq6mms11reeo50pn@4ax.com...

> On Sun, 9 Feb 2003 02:01:21 +0000 (UTC), [daw@mozart.cs.berkeley.edu](mailto:daw@mozart.cs.berkeley.edu)

> (David Wagner) wrote:

>

> >Yama wrote:

> >>David Hopwood <[david.hopwood@zetnet.co.uk](mailto:david.hopwood@zetnet.co.uk)> wrote:

> >>>Yama wrote:

> >>>> RC4 is strong if you use proper current RC4 hygiene:

> >>>>

> >>>> 1. You provide between 80-bits and 128-bits of non-repeating (not

> >>>> non-predictable) data (a nonce), you merely append that to your  
master

> >>>> key to create the session key and then prepend those same bytes to  
the

> >>>> data.

> >>>

> >>>>No! This is (almost) precisely the mode of usage that was broken in the

> >>>>attack on WEP.

> >>>

> >>>Wrong! 80 to 128 bits of a NON-REPEATING (loud enough?) nonce is fine

> >>>when coupled with the rest of the hygiene.

> >

> >

> >>I believe David Hopwood is entirely correct. See the

> >>Fluhrer-Mantin-Shamir attack, which breaks a mode of operation very

> >>similar to (if not in fact identical to) your proposed "hygiene", even

> >>when nonces never repeat. IMHO, it would be the height of foolishness

> >>to use RC4 in the way you've proposed, after the WEP disaster.

>

> >I did read the WEP attack information, and viewed diagrams of the

> >information contained in the signal. It appeared broken compared to

> >what I suggested. The amount of bits that were given to the nonce was

> >paltry, and the method of generating the nonce appeared broken.

>

> >Isn't the problem with the WEP disaster due to a \*much\* smaller pool

sci.crypt: Re: What's the bottom line on RC4??

> *of numbers that \*do\* repeat if enough samples are taken, due to a  
> broken implementation of the above? I think it was.*

There are lots of problems with WEP. However, both Davids are correct — the referenced attack does not rely on repeated nonces, and increasing the length of the nonce does nothing to stop it. It may be useful to reference Ciphersaber-1, which does follow your recommendation (1) (using a 80 bit random value as the nonce). I note that Ciphersaber-1 is vulnerable to the attack.

Now, your recommendation (2) does foil that particular attack, in that the attack assumes that the attacker can get access to the first byte of the keystream. However, I would find it quite uncomfortable to drop only 16 bytes. In addition, Ilya Mironov's analysis suggests that dropping 512 bytes or more may be more prudent (<http://crypto.stanford.edu/~mironov/papers/rc4full.pdf> ). In addition, since we know that there exists a related key attack against RC4, it may be prudent to use a strong hash to combine the long term key and nonce together anyways, in order to make any stronger related key attack inapplicable.

>  
> *Was not their method of generating PRNG/RNG shameful, and not working  
> properly, based on what is known? I think it was.*

That is not correct — there is no specified method within the WEP protocol specification to generate nonces, and different implementations use different algorithms. One common method is to use a counter (and so those implementations would never repeat until  $2^{24}$  packets had been sent).

>  
> *IOW, if you capture/take enough of the samples, you end up with  
> samples of CT that are effectively encrypted with the same key, or  
> even worse? I think you do.*

Yes, but WEP is vulnerable before you get to that point.

>  
> *I believe the WEP implementation was a broken example of what I  
> proposed, using too few bits on nonce and not making sure it did not  
> repeat, and therefore does not deserve to be painted with the same  
> brush.*

>  
> *After all, what I proposed is just a regurgitation of known hygiene  
> for RC4.*

I didn't see where you recommended any data integrity checks (such as a MAC applied to the ciphertext) — RC4, like all additive stream ciphers, is quite malleable, making it fun and easy to generate a desired change in the decrypted plaintext by flipping bits in the ciphertext.

>  
> *Not the broken WEP implementation of RC4. Right?*  
>  
> *With respect to David Hopwood, and a lot of respect to you, I'm  
> finding it hard to accept the vague comparisons.*

Re: What's the bottom line on RC4??

sci.crypt: Re: What's the bottom line on RC4??

And with respect to you, I suggest you review the recent literature before making recommendations.

--

poncho