

Re: Wireless security

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-05/2284.html>

From: Brian Gladman (*fake_at_nowhere.org*)

Date: 05/29/03

Date: Thu, 29 May 2003 19:55:42 +0100

"Andrew Swallow" <am.swallow@eatspam.btinternet.com> wrote in message news:bb5k9g\$q3v\$1@titan.btinternet.com...

> *"Paul Crowley"* <paul@JUNGCATCHER.ciphergoth.org> wrote in message
> news:87fzmx4nvk.fsf@saltationism.subnet.hedonism.cluefactory.org.uk...

>> *This isn't strictly speaking a sci.crypt question but I hope you'll
>> forgive my asking.*

>>

>> *What do you need to look for on a wireless network product in order to
>> know that it is capable of securely encrypting and authenticating what
>> it carries?*

>>

>> *I know that things like AirSnort and WEPCrack use the Fluhrer, Mantin,
>> Shamir attack to break WEP as originally fielded. I also understand
>> that a new AES based protocol is in the works. There seems to be
>> wireless equipment on the market branded "54g" which implements the
>> forthcoming 802.11g standard.*

>>

>

> *Any links to the proposed standard?*

>

>> *Will these new cards support the new, AES based protocol? If so, is
>> the new protocol secure? If not, is there any practical way of
>> getting link layer encryption for a wireless LAN today, or do I have
>> to rely on encryption in the higher levels (eg IPSec and ssh)?*

An input to the proposed standard is here:

<http://www.hifn.com/support/ccm.htm>

I have provided code for CCM mode for some months now and judging by my emails and downloads I would guess that there is a lot of implementation work going on right now.

Brian Gladman