

# Wireless security

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-05/2273.html>

---

**From:** Paul Crowley ([paul\\_at\\_JUNGCATCHER.ciphergoth.org](mailto:paul_at_JUNGCATCHER.ciphergoth.org))

**Date:** 05/29/03

Date: Thu, 29 May 2003 18:25:06 GMT

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.

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)?

Thanks in advance,

--

\_\_\_ Paul Crowley  
\\ / o\ [sig@paul.ciphergoth.org](mailto:sig@paul.ciphergoth.org)  
/\\_\_\_/ <http://www.ciphergoth.org/>