

# WPA safety and/versus WPA2 – just thinking...

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2005-06/2074.html>

---

**From:** Markus Jansson (*seemyhomepage\_at\_katsokotisivuulta.ni*)

**Date:** 06/29/05

Date: Wed, 29 Jun 2005 03:17:19 GMT

Short summary

[http://www.ezlan.net/wpa\\_wep.html](http://www.ezlan.net/wpa_wep.html)

[http://www.draytek.co.uk/support/wlan\\_wepwpa.html](http://www.draytek.co.uk/support/wlan_wepwpa.html)

And the questions/comments of mine:

- 1) WPA only has 64bit auth key size, so its not safe against brute force...why not 128bit?
- 2) WPA only has 64bit encryption key size, so its not safe against brute force...why not 128bit?
- 3) In WPA, Michael is not well-researched and analysed algorithm, and there propably are yet-unknown-but-soon-to-be-discovered-vulnerabilities in it...why not use SHA-2 etc?
- 4) In WPA, IV is only 48, so its not safe against brute forcing etc...why not use 128bit?
- 5) Why isnt the key schedule set up to change keys even faster?
- 6) WPA2 is not that clever either. Encryption key size and authentication key size might be better at 256bits, and IV ofcourse 128bits. CCM seems ok for the time being however.  
) Why didnt they pick "better ones" to the WPA/WPA2? Yes, I know, compatibility issues, power issue, computing power issue, support issue, blahblahblah. Yeah. Why not choose just some lame XOR encryption while you are at it then?
- 7) Are we going to see anything that uses other than "home-grown-algorithms" (except the AES ofcourse, and yes some TLS implications inside the authentications etc. etc.) and protocols to secure Wi-Fi in the near future or "is this as good as it gets"?
- 8) How can securing Wi-Fi be so hard that they couldnt get it right at the first try and not very well at the second try either (and not perfect in third attempt either)? It cant be just hardware/performance issue can it, I mean dedicated hw can perform miracles...

## sci.crypt: WPA safety and/versus WPA2 – just thinking...

--

i»¿My computer security & privacy related homepage  
<http://www.markusjansson.net>  
Use HushTools or GnuPG/PGP to encrypt any email  
before sending it to me to protect our privacy.