

Wi-Fi code cracked in minute

Contributed by Bogdan V
Monday, 07 September 2009

The second generation of Wi-Fi security systems has now been broken as badly as its notoriously insecure predecessor: Japanese researchers say they can crack WPA (Wi-Fi Protected Access), the successor to the old-school WEP, inside of a minute's time spent eavesdropping on a wireless network.

Details on the mechanics of the attack are set to be announced next month at a computer conference, but it's tentatively described as taking to "a new level" the previous method by which WPA had been roughly compromised, adapting previously theoretical holes in the WPA system and turning them into practical attack techniques.

The previous method of attacking WPA devices took up to 15 minutes to be successful, and didn't always work. The new method is said to work on far more devices and, obviously, much more quickly. However, as with the old attack, the new one only works on WPA devices that use the TKIP (Temporal Key Integrity Protocol) algorithm, which is a setting in your router and device setup.

WPA devices that use the newer AES (Advanced Encryption Standard) algorithm, plus devices that use WPA2 -- the third generation of wireless security standards -- are still safe for now.

{mosgoogle}

However, this does mean that it won't be long before this attack technique trickles out into software that malicious hackers can use to invade WPA networks. With access to your wireless network, a hacker can potentially eavesdrop on any traffic sent, access shared folders on computers attached to the network, and of course send and receive data (like illegal file sharing or even child pornography) which could then be blamed on you.

To protect yourself, upgrade the security settings on your devices to WPA2 if they all support the standard. Alternately, you can upgrade any WPA device from TKIP security to AES. Check in your router administration console and on your computer for and where how to do this.