WPA Wi-Fi Encryption Cracked In Sixty Seconds

August 28 2009, by John Messina

(PhysOrg.com) -- Two Japanese computer scientists have developed a way to crack the WPA encryption between wireless routes and devices in 60 seconds.

Using this attack method, hackers can read encrypted data sent between wireless routers and computers. These attacks only work when a router's wireless security is set for WPA using Temporal Key Integrity Protocol (TKIP) algorithm.

About a year ago security researchers explained how WPA could be cracked. The Japanese computer scientists took this theoretical approach and turned it into reality. All this is explained in a paper that was presented at the Joint Workshop on Information Security that was held in Kaohsiung, Taiwan this month.

These attacks can be avoided by using the more recent WPA2 or WPA

encryption systems that use a stronger algorithm, AES (Advanced Encryption Standard).

Wireless routers have a long history of security problems that started back in 1997, when the Wired Equivalent Privacy (WEP) system was first introduced. Two years latter WEP was cracked and rendered useless as an effective security option.

WPA with TKIP was meant to be an interim encryption method for Wi-Fi security until a stronger algorithm was developed. Going forward the use of WPA2 should be the standard method for Wi-Fi security. As of March 2006, WPA2 has been certified in wireless router.

Going forward users today should use either WPA2 or WPA with AES encryption in their wireless router.

Via: TechWatch