

7 November 2008

By: Lucian Constantin, Web News Editor



WPA wireless
encryption protocol
partially cracked
TARINGA!

[WPA Encryption No Longer Secure](#)

Two researchers successfully cracked the TKIP key used by the WPA protocol

Security researchers Erik Tews and Martin Beck have succeeded in partially cracking the WPA (Wi-Fi Protected Access) encryption, which until now had been considered safe. The two hackers will demonstrate their feat at the upcoming [PacSec](#) security conference in Tokyo, Japan.

WPA is a protocol that has been widely adopted as a replacement for WEP (Wired Equivalent Privacy), which has been known to be insecure since as far back as 2001. The initial attack on WEP was actually a dictionary attack, thus requiring great computational resources. This meant that attack scenarios on a large scale were highly unlikely.

The uncertainty ended at the beginning of 2007, when Erik Tews, along with two student colleagues from the Darmstadt University of Technology in Germany, developed a new technique which allowed them to break WEP security in only two minutes. Their method, which became known as the PTW attack, prompted all security professionals to declare WEP a high security risk. In fact, the use of WEP as encryption protocol is what allowed hackers to steal millions of credit card details in the [T.J. Maxx hit](#).

[NetworkWorld](#) reports that, according to Dragos Ruiu, the PacSec organizer, in order to crack the TKIP (Temporal Key Integrity Protocol) key, the researchers found a way to trick the router into sending them large amounts of encrypted data. Combining this with what Ruiu calls a "mathematical breakthrough", the attack time was reduced to a matter of minutes, between 12 and 15.

This is even more impressive as it is not a dictionary attack, because just as in the case of WEP, the idea that WPA might be vulnerable to a dictionary attack has always been voiced by researchers. However, considering the amount of resources, computational and time-related, needed to pull off such an attack, this has never been considered a big threat to WPA security.

The two researchers only succeeded in cracking WPA's TKIP key, but they haven't been able to actually decrypt the individual keys generated by the TKIP, which are used to encrypt the data packets sent between a computer and the router. Even so, this is "just the starting point," Dragos Ruiu pointed out. "Erik and Martin have just opened the box on a whole new hacker playground," he explained.

Mr. Ruiu also outlines the problems raised by this achievement, mainly the fact that WPA is now a requirement for security standards compliance almost everywhere. As a result, WPA has been adopted and is being used by many organizations and not just by individuals. "Everybody has been saying, 'Go to WPA because WEP is broken'. This is a break in WPA," concluded Ruiu.

[Robert Graham](#), of Errata Security, begs to differ. According to him, WPA or WPA-RC4-TKIP as it is technically known, has been designed from the start as just a temporary fix to WEP and everybody should have known that. The entire reason for WPA-RC4-TKIP's existence was to reduce adoption costs by accommodating older WEP hardware, which wasn't able to support WPA2 (WPA2-AES-CCMP) at that time. The WPA2,

which uses the AES "block cypher" and not the RC4 "stream cypher" implemented in both WPA and WEP is not affected by this new attack and, according to Mr. Graham, will continue to be secure for a long time to come.

"There are no weakness in AES or the WPA2 standard based upon it. It's going to last for the next 20 years," claims Robert Graham. He adds that since WPA and WPA2 have been basically standardized at the same time, but one as a temporal fix and the other as a long term one, "you should always have been planning WPA2-AES-CCMP eventually, and been planning to rely upon that for many years. If you planned to only do WPA-RC4-TKIP, then you were wrong".

Regardless of whether you considered or were even aware of the temporal nature of WPA or not, you should immediately start planning for full WPA2 implementation, as it's likely that not much time will pass until it is completely compromised. If you are a home user, check if your router has WPA2 support, which is the case for newer ones, and switch to it.

In addition, Erik Tews plans on publishing the findings in an academic journal in the near future, while Martin Beck has released parts of the attack code as [tkiptun-ng](#), a tool incorporated in the popular and freely available [Aircrack-ng](#) suite, a collection of applications aimed at cracking wireless encryption.