

Sponsored by:

## NETWORKWORLD

This story appeared on Network World at  
<http://www.networkworld.com/news/2009/082709-new-attack-cracks-common-wi-fi.html>

# New attack cracks common Wi-Fi encryption in a minute

Attack works on older WPA systems that use the TKIP algorithm  
By [Robert McMillan](#), IDG News Service, 08/27/2009

Computer scientists in Japan say they've developed a way to break the WPA encryption system used in wireless routers in about one minute. Sponsored by:

The attack gives hackers a way to read encrypted traffic sent between computers and certain types of routers that use the WPA (Wi-Fi Protected Access) encryption system. The attack was developed by Toshihiro Ohigashi of Hiroshima University and Masakatu Morii of Kobe University, who plan to discuss further details at a [technical conference](#) set for Sept. 25 in Hiroshima.

Last November, security researchers first showed how WPA could be broken, but the Japanese researchers have taken the attack to a new level, according to Dragos Ruiu, organizer of the PacSec security conference where the first WPA hack was demonstrated.

"They took this stuff which was fairly theoretical and they've made it much more practical," he said.

They Japanese researchers discuss their attack in a [paper](#) presented at the [Joint Workshop on Information Security](#), held in Kaohsiung, Taiwan earlier this month.

The [earlier attack](#), developed by researchers Martin Beck and Erik Tews, worked on a smaller range of WPA devices and took between 12 and 15 minutes to work. Both attacks work only on WPA systems that use the Temporal Key Integrity Protocol (TKIP) algorithm. They do not work on newer WPA 2 devices or on WPA systems that use the stronger Advanced Encryption Standard (AES) algorithm.

The encryption systems used by wireless routers have a long history of security problems. The Wired

Equivalent Privacy (WEP) system, introduced in 1997, was cracked just a few years later and is now considered to be completely insecure by security experts.

WPA with TKIP "was developed as kind of an interim encryption method as Wi-Fi security was evolving several years ago," said Kelly Davis-Felner, marketing director with the Wi-Fi Alliance, the industry group that certifies Wi-Fi devices. People should now use WPA 2, she said.

Wi-Fi-certified products have had to support WPA 2 since March 2006. "There's certainly a decent amount of WPA with TKIP out in the installed base today, but a better alternative has been out for a long time," Davis-Felner said.

Enterprise Wi-Fi networks typically include security software that would detect the type of man-in-the-middle attack described by the Japanese researchers, said Robert Graham, CEO of Errata Security. But the development of the first really practical attack against WPA should give people a reason to dump WPA with TKIP, he said. "It's not as bad as WEP, but it's also certainly bad."

Users can change from TKIP to AES encryption using the administrative interface on many WPA routers.

*The IDG News Service is a Network World affiliate.*

All contents copyright 1995-2009 Network World, Inc. <http://www.networkworld.com>