

The Final 'Final' Nail in WEP's Coffin?

April 6 2007

Wireless security protocol, WEP, is everywhere in Wi-Fi networks and just got quicker and easier for hackers to break into.

Researchers have discovered a new way of attacking Wired Equivalent Privacy that requires an amount of data "more than an order of magnitude" less than the best known key-recovery attacks. In effect, the cracking can be done within a minute, as the title of the paper suggests: [Breaking 104 bit WEP in less than 60 seconds](#).

Specifically, only 40,000 data packets are needed for a 50 percent chance of success, while 85,000 packets give a 95 percent chance of success, according to the paper's authors: Erik Tews, Ralf-Philipp Weinmann and Andrei Pyshkin, all researchers in the computer science department at Darmstadt University of Technology in Darmstadt, Germany.

The ease of cracking WEP is nothing new; cryptanalysts showed six years ago that any WEP key can be cracked with readily available software in one minute or less. The protocol, which is part of the IEEE 802.11 wireless networking standard, was superseded by WPA (Wi-Fi Protected Access) in 2003, then by WPA2, another name for the full IEEE 802.11i standard.

What's new that has been missing from WEP cracking until now is that a Wi-Fi attacker no longer needs long periods of time nor much smarts, according to Wi-Fi security experts.

"...To crack WEP - up until now - it 1) required a knowledgeable attacker - and - 2) took a long time," said Andrea Bittau, in an e-mail exchange. Bittau is a research fellow at the University College London and a co-author of [a paper](#) describing what had been the most effective WEP cracking technique prior to the Germans' research.

"In the past, the wait time could have been hours, whereas now, it seems to be only a few minutes," Battau said. "Thus, WEP cracking has finally made it into the 'general public' at a reasonable cost - only a few minutes - ."

Thanks to this new discovery, we can expect the arrival of tools that can break WEP in 10 minutes or less by pressing a single button, Battau said. In other words, tools that can allow for walk-through hackings, whether in Wi-Fi-networked conference rooms or in the local coffee shop.

Battau's Web cracking paper, published with Mark Handley of University College London and Netgear's Joshua Lackey, was titled "The Final Nail in WEP's Coffin."

When published in May 2005, the paper presented a breakthrough in WEP cracking: a novel vulnerability that allows an attacker to send arbitrary data on a WEP network after having eavesdropped only a single data packet, along with techniques for real-time decryption of data packets that can be used under common circumstances.

If that "final nail" wasn't the final nail, will this new research be the one that really puts WEP into its grave?

David Wagner, co-author of a paper on the insecurity of 802.11, said he'd like to think it's the last nail for WEP, but we're probably not going to see the end of it soon.

"Ironically, last May, when Bittau, Handley and Lackey released their research showing new flaws in WEP, I remember calling that the final nail in the coffin and the end of the road for WEP," he said in an e-mail exchange. "But it seems that no matter how bad we think WEP is, the news can always be worse than we imagined."

And still, WEP enjoys wide deployment.

In Battau's May 2006 paper, the researchers detail their survey of 400 wireless networks in London and 2,539 networks in the Seattle area. Although more secure protocols exist - WPA and 802.11i - the researchers found that few networks use them.

"In both cases, about half of the networks used encryption," according to the paper. "In London, 76 percent of the encrypted networks in our sample used WEP, and in Seattle 85 percent of them used WEP. Although vendors recommend upgrading to WPA or 802.11i, only a minority of users seem to use these solutions."

But as Wi-Fi networking equipment vendors will tell you, there's no way to walk away from WEP with all the legacy laptops and network cards still around that use the encryption scheme.

Som Pal Choudhury, Netgear's product line manager, advanced wireless, said in an interview that, like many, WPA and WPA2 are default encryption schemes in the company's routers and that Netgear's reference and setup manuals all explain the dangers of WEP.

In fact, the Wi-Fi Alliance as of March 2006 mandated WPA2 for all new devices in order to be Wi-Fi Alliance certified.

Still, Pal Choudhury said, there are "Legacy drivers, legacy devices out there ... you buy a laptop for three to five years. If you bought in 2002,

2003, it used to only support WEP. Now, with the second generation of laptops you're going to buy, these are all going to be WPA, WPA2."

In the meantime, Wi-Fi security experts agree that the new WEP cracking techniques should be a wake-up call for equipment manufacturers to make defaults more secure and to make the security features easier to use.

"Perhaps this will lead people to totally abandon WEP and switch to something else," Battau said. "Frankly, however, I think that WEP will still be around for a while due to ignorance. It has received much publicity in academic papers, but there was no response. We will now see what the response will be when a one-click tool for breaking WEP in 10 minutes becomes available."

A one-button WEP-breaking tool would certainly get Wi-Fi users' attention and thus hasten WEP's demise. Wi-Fi security experts have the Germans to thank for that. After all, Battau said, "Yes, - the Germans' research - was the missing nail."

Copyright 2007 by Ziff Davis Media, Distributed by United Press International

Citation: The Final 'Final' Nail in WEP's Coffin? (2007, April 6) retrieved 9 April 2024 from <https://phys.org/news/2007-04-wep-coffin.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--