

MBizCentral

Wireless Data Networks Called 'Inherently Insecure'

By *Robert Lemos, ZDNet, USA Today*

07/13/01, 4:26 PM

A new way to attack wireless networks underscores the lack of security for PC owners using the airwaves to connect their computers, say security experts speaking at the Black Hat Briefings conference. Tim Newsham, a researcher for security firm @Stake, presented the details of weaknesses in the password system of wireless networks that could lead to a break in security in less than 30 seconds. The flaw is the third to be uncovered in the so-called Wired Equivalent Privacy, or WEP, protocol that supposedly secures wireless networks. "WEP is inherently insecure," says Newsham. "So using WEP is essentially just throwing another barrier -- and a small one -- in front of the attacker." That barrier can be overcome in 5 to 30 seconds in certain cases, he says.

Specifically, wireless systems that rely on a 64-bit key -- used in many homes and earlier hardware -- can be broken in less than a minute, letting the attacker see the data beamed across the networks. Newer 128-bit wireless LAN (local area network) cards are fairly strong. But poorly chosen passwords can still be cracked with an old technique known as a dictionary attack: Using a list of common passwords and a dictionary of words, the potential intruder can try various combinations until the password is broken. "Either it works or it doesn't," Newsham says. "If it doesn't, you can try one of the other attacks." Earlier at the Black Hat conference, Ian Goldberg, of private network seller Zero Knowledge Systems, presented details on a variety of techniques for cracking the encryption of wireless networks. "The point of a cryptographics protocol is to be able to communicate securely over an insecure medium," he says.

Using Goldberg's techniques, which he developed while earning a doctorate at the University of California at Berkeley, data on wireless networks can be modified, added or, in some cases, decrypted. In the end, people need to understand that wireless networks are completely insecure. For the security conscious, virtual private network (VPN) technology such as Secure Shell, known as SSH, or other encryption techniques should be used, he says. "People need to treat wireless networks just as they do the Internet," Goldberg says. "That means using encryption technology to secure their data."

Copyright 2001, ZDNet. All rights reserved. Copyright 2001 USA Today a division of Gannett Co. Inc.