Hacker program threatens wireless security

By The Associated Press
Special to CNET News.com
August 23, 2001, 10:20 p.m. PT
http://news.cnet.com/news/0-1004-200-6958805.html?tag=prntfr

Airports, schools and hotels might want to look closer at the wireless Internet networks they have been installing as a convenience for the must-stay-connected crowd.

A new program called AirSnort, released on the Internet this week, lets enterprising hackers easily grab sensitive data as it is transmitted through the air--unless certain precautions are taken.

"There's going to be some major events that will occur, some takedowns, things like that," said Les Owens, a Vienna, Va.-based expert on wireless security. "I would be cautious (on a wireless network in a public place), a lot more cautious than I would be at home."

Because wireless networks broadcast signals over the public airwaves like radios and cell phones, security experts have known for a long time that they are vulnerable to snoops.

But not until AirSnort--and a less-complete tool called WEPCrack that was released earlier--were the means to carry out such an attack made so easily available to anyone anywhere.

The programs exploit flaws in a commonly used encryption scheme for securing traffic on a certain kind of wireless network--the one based on a popular standard known as Wi-Fi, or 802.11b. Computers linked with a competing standard, known as Bluetooth, are not susceptible to AirSnort or WEPCrack, but Bluetooth also is considered more vulnerable to spies than hard-wired networks.

AirSnort's programmers believe too many wireless network users have shrugged off or couldn't understand recent research describing flaws in the popular Wi-Fi encryption system, which is known as Wired-Equivalent Privacy, or WEP.

The AirSnort designers said they wanted to make it clear that businesses should be careful about letting important data get out on wireless networks and that many networks need security upgrades.

"It is my firm belief that a false sense of security is worse than no security at all," said AirSnort co-programmer Jeremy Bruestle, who runs a small computer security firm called Cypher42 in St. Cloud, Minn. "In order to stay ahead of the hackers, people need to make informed decisions."

Critics have told Bruestle, 23, and co-author Blake Hegerle, 20, that giving hackers a tool to crack wireless networks doesn't do much to advance the their cause.

"But the truth is the security flaw exists regardless of AirSnort, and it is not a difficult flaw to exploit," Bruestle said.

A similar program was developed this summer by researchers at AT&T Labs, who chose not to release their code "for a combination of moral and legal reasons," said team member Adam Stubblefield.

There are ways to make wireless networks more secure, such as installing virtual private networks, or VPNs. Those methods increase the systems' cost and complexity, but could become more popular.

"If I had to guess, I'd say we'll see a lot of better-protected networks in the very near future," Stubblefield said.

Owens said companies that make wireless Internet equipment must work together on developing more advanced security standards, but it's unlikely to happen until consumers begin insisting on them.

He compared the situation with the rampant cell phone cloning by criminals a decade ago before the industry came up with better protections and the government cracked down on the practice.

"This has the potential to be similar in that you may see the same kind of things," Owens said, pointing out that many companies expect to begin using wireless data networks for voice transmissions. "It's a repeat of history."