SUBSCRIBE

Computerworld is New Zealand's only specialised information systems fortnightly.

Subscribe now for $97.50 (24 issues) and save more than 37% off the cover price!

TOP 10 WEBSITE
hitwise
JAN – JUN 2009

SIGN UP

Air is 'thick' with wireless networks — many crackable

Finding an open wireless network in Wellington proves to be a simple affair

BY STEPHEN BELL | WELLINGTON | WEDNESDAY, 9 FEBRUARY, 2005

✉ EMAIL   🖨 PRINT

The air in any central business district nowadays is thick with wireless signals and "wardriving" expeditions prove that a discouraging proportion of them are still unencrypted, says Nick von Dadlszen of Auckland's Security-Assessment.com.

Speaking to the Computer Society in Wellington, von Dadelszen notes that security laxness is more of an issue not only because of the easy access to a wireless signal as opposed to a physical link, but because wireless has generated so much enthusiasm among users.

"Security is an issue because [your staff] want wireless now," he said. If you take your time about implementing it securely, they will implement it insecurely and outside your control, he says.

The problem is becoming more acute as an increasing population of devices, down to the scale of personal digital assistants, acquire wireless capability.

In a practical demonstration, Dadelszen found eight networks accessible from the ceantral Wellington company meeting room where the talk was held – though about half were CafeNet links, necessarily unencrypted to allow new users to log on. But of the remaining four, only one was guarded by any encryption.

He used two common tools, Netstumbler and Kismet, to find a considerable amount of detail about the links. SSIDs, identifying the network, are routinely broadcast and give a starting point for spoofing by generating a fake ID from an intruder's own access point.

Users often attempt a kind of "security through obscurity" by turning off SSID broadcasting or filtering on MAC addresses to ensure they only communicate with users known to them. The latter is a measure of doubtful value, Dadelszen says, since MAC addresses can be "sniffed" and one's own address can then be easily changed to mimic a trusted party.

The first generation of encryption, WEP, is flawed — through problems with its initialisation have allegedly been fixed. But even if this upgrade is effective, it is likely that some users will still be using an old version. Software called WEPcracker is available online and, like all the other aids to attacking wireless connections, it's free. "That's open source for you," Dadelszen says.

There is a new generation of WEPcracker, known as Aircrack, and a "brute-force" cracker for the newer encrypted protocol, WPA. Here a would-be intruder would capture a number of packets — even inducing more traffic by prompting with packets of their own — then store the packets for decryption at leisure.

Strong schemes of authentication such as Radius are available particularly to corporate users and should be used where possible, Dadelszen says. But if you are forced to rely on WEP or WPA encryption without strong authentication "change your key often".

One of the most disturbing vulnerabilities he described is the ability to send out packets instructing a computer to disconnect from its local radio access point, and to have a hidden access point run by the intruder. The disconnected machine is likely to reconnect to the fake AP, letting the intruder in — a kind of wireless equivalent of the "phishing" scheme worked with fake websites.

"Check regularly for rogue APs", he says, and keep an eye on the telltale locks and similar symbols on the screen that will indicate that a connection is properly secured.

SHARE THIS STORY WITH:

MOST POPULAR

READ   COMMENTED   EMAILED   SHARED

- Netbook failure rate disappoints major user
- Google Wave code to live on
- Govt plans hinder FX Network sales
- File-sharing bill could extend surveillance culture - Bott
- Surveillance Bill amendments reassure telcos
- HP researcher cracks conundrum

WHITE PAPERS

On Common Ground: Where Compliance and Data Protection Overlap

Automation Makes Perfect: Taking the Time Crunch Out of IT Compliance with Automation

POPULAR EVENTS

Excellence in the Use of ICT in Government Award 2010 Award
Click here for more details

The Sustainable 60 Awards
Entries open now.
Click here for more details

The Sustainable 60 Workshops
Dates confirmed
Click here for more details

SPONSORED LINKS