



Date: Tuesday, 29 November 2005  
Page Number: 39  
Edition: First  
Supplement: Information Technology

Market: WA  
Circulation: 236,467  
Published: MON TO SAT  
Editorial: [email the editor](#)  
Item No: P8468163

Size: 246.02 sq. cm.

# Hot spots prone to attack

## Security found to be lacking in CBD wireless access points

NEALE PRIOR

Corporate security groups yesterday warned that companies operating in the Perth central business district were virtually advertising themselves as being open for attack by hackers through their security practices for wireless computer access.

US network technology group Altiris and Australian wireless consultancy group Spectrotech yesterday released the results of a study that showed that 67 per cent of the wireless access points detected in the Perth CBD were employing a low form of wireless encryption security known as Wireless Equivalent Privacy (WEP).

The survey also found that just 4 per cent of the networks in the Perth CBD were using the higher level wireless access security system known as Temporal Key Integrity Protocol, compared with about 13 per cent nationally.

Spectrotech managing director Mark Morgan said the WEP technology had proven to be highly vulnerable to attack and there were a range of programs available over the internet that could allow a hacker to read material that was being transmitted wirelessly using WEP encryption.

Mr Morgan said the poor security

also meant that hackers could potentially gain access wirelessly to a computer network or to the internet, but that would be dependent on whether other security systems were in place to control access to the network.

He said the study, carried out last month, did not go beyond detecting the wireless signal and seeing what type of encryption technology was being used because it would have been illegal and unethical to hack any further into a network.

Wireless technology, much of which can be bought over the counter and plugged into computers, allows users of a network to gain access to the network away from their desk and in areas surrounding the office.

It is also increasingly being used in homes, with many broadband modems having multiple wireless access points as standard fixtures.

Public access wireless points such as internet hot spots usually do not use encryption technology when sending out signals because they are trying to attract the attention of potential subscribers, but have other means of controlling access.

The Altiris-Spectrotech study found 230 of the 798 wireless access

points detected in Perth had their encryption systems disabled, which indicated they were either public access hot spots or were owned by people who did not have security as a high priority.

Laura Chappell, a US wireless security consultant who assisted with the Altiris-Spectrotech study, said the use of the low-grade WEP encryption technology sent a signal to hackers that the access point operator had something to hide and could be worth attacking.

"A hacker would look at WEP enabled sites as being more juicy," she said.

Ms Chappell said the network operators using WEP was a pointer to there being a range of other problems with the system they ran, including virus detection mechanisms being out of date, defective firewalls and unauthorised software being on the network.

She said she had noticed in numerous companies that staff had attached wireless devices to their desktop computers without network operators knowing, completely compromising network security because they gave hackers an access point within firewalls.