Wireless weak spots uncovered

In the last few weeks, Rits Information Security carried out a security review of wireless hotspots in a number of commercial locations across the city of Dublin.

This review, sometimes known as ‘wardriving', was carried out to assess the level of security controls that companies and installers are applying to wireless Lan access points.

Most people getting internet connections today in their home are getting wireless Lan access points included in the router that connects them to the internet. This provides great flexibility for the homeowner, as it means that the wireless Lan (wi-fi) equipped laptop can be used anywhere in the house.

Many small to mediumsized enterprises (SMEs) are getting the same sort of equipment when they connect to the internet and are benefiting from the wi-fi systems in the same way.

However, with this flexibility comes some risk. Wi-fi signals do not honour the physical boundary of your home or premises.

The range of most access points today for connectivity can be up to 1,000 feet with no specialist antennae, but with a small investment, this can run to miles.

Why is this an issue? Surely increased signal strength is good?

The problem lies with the relative ease with which an unauthorised person can get access to the access point and then other computers on the wired or wireless network nearby.

When the first wireless standards were being developed (IEEE 802.11i), the engineering and design teams understood that there would be a need to include security. After all, a company's internal and sensitive information would be flying through the airwaves and easily monitored.

The teams came up with a standard called wired equivalent privacy (Wep).

As the name suggests, it was intended to give the wi-fi user the same level of security as if it was a traditional wired Lan.

Soon, however, it became apparent that there were some issues in the architecture of Wep.

Specifically, theRC4 encryption algorithm was implemented in a flawed manner.

Tools became available that demonstrated how to break the Wep systems and it became discredited.

Recently, researchers have demonstrated further attacks that mean Wep can be cracked in less than a minute. Previously, it would have taken a number of hours and a reasonable amount of gathered data.

Soon after this was discovered, the standards body approved wi-fi protected access

(WPA) and thenWPA2 as the most secure methods for protecting wireless Lan access.

WPA2 is still considered to be a secure method for deploying wireless Lans and should be considered as the entry point. Other appropriate controls must also be deployed in addition to WPA2.

Given that there has been a reasonable amount of awareness of the insecurity of wi-fi, Rits was astounded to see the results of the aforementioned audit.

It identified 30 per cent of all business wireless access points in the main business areas in Dublin as having no form of encryption or access control enabled.

One of the issues with carrying out an audit like this is that there are now a number of wireless access points deployed in places such as hotels, cafes, business centres, etc.

Where possible, Rits identified these and removed them from the report as they will, by nature, be open and unencrypted.

Rits also removed any access points that could clearly be identified as being residential ones.

With this data cleansing complete, the number of access points in the audit was almost 3,000. These were located in the following areas: Dublin 2, IFSC, Parkwest, Citywest and Sandyford.

Other concerning statistics from the audit were that 70 per cent of access points that were broadcasting an identifier (SSID) were using one that was too descriptive (43 per cent) or the default (27 per cent).This information provides a wealth of information to the malicious user and is unnecessary.

Why are these issues so concerning? Where there is no security in place, or flawed technologies, it is trivial for a malicious user to connect to a wireless Lan access point and then attempt to access other resources on the network.

Network security technologies are often deployed on the perimeter of an organisation and in a situation where there is an insecure wireless Lan access point on the Lan, they are about as much use as the Maginot Line in World War I.

It has been suggested recently that the use of an insecure wireless access point on the internal Lan was the initial method used by hackers in the breach of security at retail giant TK Maxx (TJX) that led to the theft of more than 45 million credit card numbers.

It is also a preferred method of carrying out malicious, and sometimes illegal, activity on the internet. If there is an insecure wireless access point available, it could be used by someone to carry out hacking attacks and if any of these potential crimes are investigated, the insecure access point will be identified with virtually no way of determining who used it.

In Britain recently, a number of different people have been arrested and charged with illegally accessing wireless networks for illicit web browsing.

The impacts on the owners of these access points can be very significant. In a

situation where an internet access contract has a charge for data transferred, the owner can be left with a significant bill to be paid. If it is used for illegal activity of any type, the owner risks being prosecuted and equipment seized.

Extreme cases, such as that in the TK Maxx situation, highlight the potential once a malicious user has gained access to the network.

The message here is clear: if you are going to deploy wireless Lan technologies, do so in a secure and controlled manner.

Have the systems regularly reviewed and maintain access logs.

Wireless technologies can be great enablers when deployed correctly, but devastating when not.

Rits Group Head Quarters
Information Security Centre
2052 Castle Drive
Citywest Business Campus
Co. Dublin
Ireland

Tel: +353 (0) 1 6420500
Fax: +353 (0) 1 4660468
Email: info@ritsgroup.com
Web: www.ritsgroup.com