

Invisible wireless dangers stalk the unwary

Hackers and criminals are exploiting weak spots in networks, but firms remain alarmingly complacent about taking defensive measures

Reports by **Jon Gordon**

WIRELESS TECHNOLOGY IS a rare innovation that promises to live up to the hype surrounding it.

From allowing internet access to once inaccessible areas to helping enterprises realise their visions of a truly mobile workforce, wireless technology has opened an unprecedented range of opportunities.

But with these opportunities come fresh threats.

The proliferation of wireless devices has opened up vulnerabilities that criminals and hackers are ingeniously exploiting.

Despite such high-profile security breaches at leading companies such as Verizon and Best Buy, most firms are complacent about defending their wireless networks.

A recent study by communications market researcher In-Stat found that most businesses had completed or were considering wireless local area network (LAN) deployment, but the adoption of dedicated wireless security mechanisms remained low. This apparent lack of concern is surprising, considering the dangers wireless LANs can present.

Abby Tang, director of enterprise marketing for Asia-Pacific at networking vendor Juniper Networks, said wireless access could not be physically secured or limited to certain places, making traditional safety measures such as locked doors and thick walls largely useless.

Networks are potentially open to anyone within reach of wireless radio waves.

Intrusions can take the form of unauthorised direct access or eavesdropping, in which invaders steal vital information broadcast between a laptop and a wireless access point.

"These kinds of attacks are especially easy when access points are not properly secured, whether as a result of improper configuration or hardware and software driver vulnerabilities," Ms Tang said.



Users should not leave desktops and laptops continuously connected to any public network. Photo: Bloomberg

Dixon Ho, chief information security officer for Microsoft Hong Kong, said any enterprise investing in wireless infrastructure should also keep a close eye on its own employees, especially those who had free reign over customer files containing credit card information or other sensitive data.

"A knowledgeable employee can easily put a malicious program on the company network," he said.

Wireless users are contending with a new breed of viruses such as MVW-WiFi, which Mr Ho said could bore into any laptop

through a wireless link and multiply by finding and forwarding themselves to adjacent networks.

"MVW-WiFi's destructive capabilities are exponential in nature," he said.

Fortunately, protecting a wireless-enabled enterprise from the most common weaknesses and attacks is a relatively simple affair.

Ms Tang of Juniper Networks said a good first step was to invest in Secure Socket Layer Virtual Private Network (SSL-VPN)

solutions. These secure data transmissions over wireless connections through encryption and user authentication. More advanced SSL-VPN tools can even scan computers attempting to access a network for "malware".

Microsoft's Mr Ho said companies could further shore up their defences by maintaining logs that recorded who accessed confidential records, and by installing and updating anti-virus software.

Wireless security becomes more difficult when people move

outside of the workplace. Many companies are only too happy to have their staff file reports or fire off e-mails when they are on the road, but fail to educate employees on the perils of using public networks. This leaves many mobile devices open to targeted or random assaults.

Hansen Chang, vice-president Asia-Pacific at network security appliance specialist Fortinet, said the most common threat in wireless networks in Asia came from hacking simply "to see if it can be done".

"This is easy to do if the user has turned off his laptop firewall and left some of his folders shared," he said.

This is not to imply that most wireless hazards are superficial or unsophisticated. A slew of clever new traps are out there and they are designed to pinch crucial information from the unwary. Mr Ho cited one of the most popular, known as "WiPhishing".

This involves "rogue" access points that replicate trusted network names in hopes that unsuspecting users would log on and open the door to their data or computer files. Wireless users were also being tempted by "promiscuous clients". Strong signals (beamed randomly or intentionally) from the 802.11 wireless cards contained in many devices have proved a powerful lure.

Laptops may be the most frequent targets, but attackers have moved beyond the computer to devices such as mobile phones and PDAs.

Mr Ho said Bluetooth-enabled wireless devices provided an entry point for hackers and a host of new scams were taking advantage of the Bluetooth-ready handheld boom. These scams included "Bluejacking", in which unauthorised users spammed phones with messages, and "Bluesnarfing", in which mobile phone data was stolen.

"That's only part of the problem," Mr Ho warned. "The more troubling issue is that these actions are often untraceable."

There is no shortage of off-the-shelf solutions to help enterprises and individuals deal with these security challenges.

Wireless "sniffers", such as those bundled with Microsoft's Windows XP, help users monitor and test network airspace. Drive encryption tools can hamper attempts to view or capture information stored on laptops.

Running a good firewall each time you surf the internet with a high-speed connection will stop many intruders in their tracks. And many of the soft spots associated with Bluetooth devices can be

continuously connected to any public network, especially if the computer was not being continuously monitored.

"Many of the hotspots have little or no security, which makes anyone connected to them vulnerable to a virus or wireless attack," he said.

Users should stay off public networks entirely if they wanted to download critical documents, or were handling sensitive

information. Also, they should never be totally dependent on wireless systems.

"One thing to keep in mind is that Wi-Fi can be easily jammed by accidental or intentional interference," Mr Ho said.

"You should never place mission-critical applications on a wireless network as the primary network."

The experts say companies should supplement investments in their security architecture by teaching their staff good habits, such as updating their anti-virus software and not jumping onto free public access points that come their way.

"The biggest wireless security threat, by far, is not a virus or hacker attack," Mr Ho said.

"Awareness is the most critical part of fortification. If users were simply aware of what could take place, of what the true risks were, then everything else could be built on that."



Abby Tang



Dixon Ho

patched up simply by boosting security settings.

Nonetheless, industry experts agree the most important weapons in the wireless security struggle do not come out of a box.

Fortinet's Mr Chang said: "The best way to protect yourself is to be just a little more diligent."

This can be as simple as shutting down your laptop when it is not in use, instead of putting it in hibernate or suspend modes and leaving your files vulnerable.

Mr Ho said users should not leave laptops or desktops

TOP SECURITY TIPS FOR IT MANAGERS

It is virtually impossible to build an impregnable wireless network, but IT managers can minimise the chances of security lapses or data loss by following a few relatively simple steps:

- At the bare minimum, deploy a Secure Socket Layer Virtual Private Network (SSL-VPN) solution to encrypt data and discourage intrusions
- Consider more versatile options such as unified threat management appliances if you have greater security needs
- Ensure all company PCs and laptops are installed with firewall and anti-virus software, and updated regularly
- When employees access critical documents or engage in communications of a confidential nature, make sure they do so via dedicated networks
- Put policies and tools in place to control the use of key documentation or data, and keep a log to verify who is accessing it
- Stage training sessions for key staff members who travel frequently to educate them on the importance of good security practices

Online world faces threat of an elusive, slow-moving foe

BY SOME ACCOUNTS the battle against viruses has already been won.

After all, massive, global-scale attacks such as the "Love Bug" that struck millions of computers worldwide and inflicted billions of dollars worth of damage at the turn of the millennium are now increasingly rare. But experts say this is hardly the time for enterprises to let down their defences.

IT research firm Gartner continues to rank viruses among the top five dangers facing companies today, as they have moved into the realm of a "permanent annoyance".

Any victory against an individual virus or piece of malicious software is fleeting, as more will spring up to take its place, and businesses must strive to contain rather than defeat the problem. The threat, it seems, is as real as ever, but its nature is changing.

"The current threat landscape is populated by lower-profile, more targeted attacks - attacks that propagate at a slower rate in order to avoid detection and thereby increase the likelihood of successful compromise," said Michael Chue, Hong Kong managing director for security vendor Symantec.

Allan Bell, Asia-Pacific marketing director at anti-virus software maker McAfee, said: "As virus outbreaks are less common, users would be forgiven for thinking that they are less likely to be infected by a virus."

"The most recent trend is for viruses to be written to steal money for online criminals, and they would prefer to avoid the publicity of an outbreak which might encourage users to update their virus protection."

Whereas the viruses of the past often required users to take some kind of action, such as opening an e-mail attachment, before they could infiltrate any files, Mr Bell said much of the malicious software floating around today was "self-propagating", needing only a vulnerable computer with an

internet connection to infect a PC and spread.

Mr Chue said Symantec had also noticed a renewed interest in "polymorphic" viruses, which constantly changed their byte pattern when they replicated.

This cloak-and-dagger style of strike is increasingly the norm.

Mr Bell said viruses often targeted specific lists of computers, aiming to recruit more machines into a "botnet", an army of remotely controlled host computers that were often used to disseminate spam or phishing e-mails that trawled for valuable personal information.

"Many users are not even aware that their computer is running as a 'bot' in the background," he said.



Allan Bell: be on guard against links

"Naturally bots have their antivirus and firewall protection turned off. Some bots hide from the user using rootkit techniques that make them invisible to the operating system and from antivirus software."

Perhaps the most significant recent trend noticed by industry observers is the increasing focus of viruses on mobile and wireless-enabled devices.

Mr Chue said Symantec had been seeing more attempts to probe and connect with wireless entry points to gain access to sensitive information on nominally private networks, or to use these networks as platforms for further illicit activity.

Smartphones with the ability to read e-mail or browse the internet are also an appealing target for hackers.

However, Goh Chee Hoh, managing director for Asia South at antivirus vendor Trend Micro, said most "malware" developers had so far mainly contented themselves with creating code simply to prove that vulnerabilities existed and could be exploited.

When viruses designed for phones grow more sophisticated, Mr Goh believes, their goal will be the same as many of those aimed at PCs: financial fraud.

"Hackers and bad guys are not so much interested in incapacitating devices as making illicit money," he said.

Mr Bell said a big virus outbreak had yet to occur, but as the number of phones increased they became a more attractive target for online criminals.

Even specialist devices such as the BlackBerry have been shown to be vulnerable.

It is a frightening picture, but experts believe administrators and users are well equipped to deal with it if they exercise caution and take a few key steps.

Mr Chue said IT managers needed to plan their anti-virus strategies carefully, taking pains to install well-rounded security solutions and to ensure any new best practices or patches were deployed quickly.

Mr Bell said in addition to scanning incoming e-mails for viruses or spam, larger organisations should consider central management tools to gain a "complete view" of their security situation that could flag out-of-date software or weak links in the computer chain. Avoiding viruses was also the responsibility of an employee.

"Exercise safe internet practices by avoiding opening e-mail attachments unless you know they're safe," Mr Bell said. "Many viruses spoof the e-mail address, so e-mail from friends is not a safety guarantee. With the number of phishing e-mails around, be careful about clicking on links."