Wide open wireless?

Wireless networking may offer attractive benefits to organisations – but it also offers attractive opportunities to hackers.

Drive-by hacking, or 'war-driving', is a relatively new variation on an old theme: hackers randomly searching for networks to break into. The difference is that instead of dialling random phone numbers or scanning random Internet addresses, the mobile hacker drives around, armed with a wireless-equipped laptop, trying to detect an unsecured network.

Some analyst groups, such as Gartner, have dismissed the threat of war-driving as scaremongering. But Jocelyn Honeybunn, business development director at professional services firm FailSafe, counters that by saying they are just sticking their heads in the sand. "[Some analysts have] dismissed the threat on the grounds that it has been exaggerated and that no significant cases have been reported. This is a bit like claiming that it's okay to leave your door unlocked if you've never been burgled," she argues. She also notes that, "In the same week Gartner announced its views, press reports stated that a Pringles crisps tube could make an effective aerial for intercepting data travelling on wireless networks."

"There is a major implication of WLANs [wireless local area networks] – they are simply not secure," agrees Scalable Networks' UK managing director Alan McGibbon. "It's frighteningly easy for a hacker to stand outside a building with a scanner and hack into a company's wireless network within minutes."

Wireless networking has many things going for it: simplicity of set-up, lack of cabling, mobility of users. But unlike the wired world, it is relatively easy for someone from outside an organisation to access its infrastructure since there is no need for a physical connection to the local area network (LAN). So how can CIOs prevent unauthorised access to their networks?

IMPEDING ADOPTION

Not all organisations are complacent when it comes to the risks of wireless technologies – in fact, it is a major impediment to adoption at many companies. A recent Gartner survey, for example, shows that 76% of European IT managers are worried about investing in mobile communications solutions. Another by the Opus Group lists security as the most important barrier to wireless LAN implementation, with 28% of the IT and network management professionals naming it the chief obstacle. Sara Gemmell, UK business development manager at flexible working specialist Nextra, says that in the company's yearly survey of CIOs in Europe, concern over security was the main reason cited by respondents for not adopting wireless technology.

The main wireless technologies they are cautious about are Bluetooth and Wi-Fi (otherwise known as 802.11b). Bluetooth is short-range connectivity technology, predominantly used to connect peripherals and handheld devices to each other. Wi-Fi, by contrast, is a longer range technology, and is Ethernet-like so computers can join corporate networks via Wi-Fi bridges. Each has its own security mechanisms: Bluetooth has two secure modes that involve keys for encrypting traffic for each connection, while Wi-Fi has the Wired Equivalent Privacy (WEP) protocol, which uses similar key-based mechanisms.

But each is vulnerable to attacks. Bluetooth's most secure system requires a PIN number for every connection, and since that is only four digits long, it is relatively easy to crack. Dick Clark, senior consultant at systems integrator Consult Hyperion, says that Bluetooth security is lacking. "Security is far from organised in the Bluetooth world. Wireless companies are keen to present the frequency-hopping that is built into Bluetooth to prevent interference as performing a security function as well, but it just doesn't. End-to-end security is some way off, most of the building blocks are there, but it's complicated and inconvenient to configure. But what may happen is that the convenience Bluetooth offers will make security a back-burner issue – at least until someone gets burnt."

WEP, in contrast, is vulnerable to statistical analysis of traffic – along with various other attacks (see box, *Wi-Fi Security: Vulnerability timeline*). "Standard WEP provides 128-bit encryption of data between the wireless access point and the end user," says Chris McNab, technical director of information risk management firm Matta Security. "The same WEP key is used by each and every end user and can be compromised by an attacker with freely available tools within a couple of hours." Although an improvement to the WEP standard is available that

WRITTEN BY ROB BUCKLEY

WI-FI SECURITY: VULNERABILITY TIMELINE

Researchers have identified a number of vulnerabilities in the Wired Equivalent Privacy (WEP) protocol used to encrypt Wi-Fi (802.11) traffic.

October 2000: WEP encapsulation is shown to be breakable no matter what the key size.

March 2001: Problems are found with the access control and authentication mechanisms used.

May 2001: Researchers discover a cryptographic attack that can be launched against both WEP and WEP2 (a proposed enhancement to WEP) that works regardless of key size.

June 2001: Tim Newsham of security company @Stake finds a problem in the algorithm that some vendors use to automatically generate WEP keys. He also builds code to perform 'dictionary attacks' against intercepted WEP traffic.

August 2001: A flaw in the RC4 key set-up algorithm can result in a total recovery of the secret key by hackers. Implementing the attack requires hackers to collect and analyse wireless traffic.

February 2002: Design flaws in the combination of the 802.1X and 802.11 protocols are shown to permit man-in-the-middle and session hijacking attacks.

"Organisations planning wireless networks should look at what services are required and use a 'layered' approach to security."

involves dynamic key generation, it can take several minutes for the authentication process to complete – a problem for users roaming from access point to access point – and researchers have found flaws in this system too.

McNab's advice to WLAN owners is clear: "If you are looking for a scalable model, it is currently a good idea to use standard WEP and then openly admit that WEP can be compromised by a determined attacker. So use virtual private network (VPN) tunnels that support the IPsec (Internet Protocol security) standard, and network intruder detection systems to improve security and manage risks and threats in the future." Nextra's Gemmell says that she does not foresee security being an issue for too long, because of technologies such as IPsec and VPN. "Vendors are working on the problem right now," she says.

Ollie Whitehouse, managing security architect at security company @Stake (which discovered a flaw in WEP in June 2001), says the problem with wireless networks is that CIOs have less control over the range of transmission of data. "The first rule is only to unstring [provide wirelessly] services where there is a real business benefit to be gained from wireless connectivity: not all internal network services need to be made available to wireless users. Organisations planning to deploy wireless networks should look at what services are required, and use an appropriate 'layered' approach to security. It's not sufficient, for example, to omit the finance department from the wireless network without making sure that all the systems accessed by finance department employees can not be accessed through the wireless gateway."

Further good security measures, adds Whitehouse, include good network filtering, systems and network monitoring, log retention, multi-factor authentication and encryption, and a set of business-driven security policies and procedures identifying potential security threats.

Whitehouse also recommends using a VPN over the wireless network to add a second layer of encryption and authentication, something with which Daniel Fuller-Smith of Toshiba's server business agrees. "Security is constantly being posted as a show-stopper by the cynics, but there is so much development going on in this area that there are few situations where wireless communications present any more security risk than a hard-wired network. Innovations like dynamic encryption, firewall equipped hardware, watertight authentication and VPNs mean peace of mind coupled with vastly increased productivity," he claims.

McNab agrees that it is possible to have good control over a wireless network by dedicating as much attention to it as to a wired network that is open to the outside world. "By deploying firewalls and VPN gateways on the wireless segment that authenticate users, good control over the network can be realised. Authentication can be improved by using 'two-factor' products such as RSA SecurID or Secure Computing's Safeword. Even single sign-on can be realised by using x.509 digital certificates across the wireless infrastructure and accessible servers that are protected by VPN gateways and firewalls," he says. While Bluetooth is relatively insecure, its bigger brother Wi-Fi is capable of utilising almost the full range of security tools from the wired world.

Still, until organisations educate themselves about the security options available to them, and fight to counteract complacency within IT departments, Chris Potter, information security partner at consultancy PricewaterhouseCoopers, says he will remain uneasy about wireless technologies. "Roughly 8% of large UK businesses are currently using wireless networks, but less than half are encrypting their wireless network traffic. This is a potential security time bomb," he says.

CONTACT:

Article by Rob Buckley
Email: rbuckley@infoconomy.com