TRENDS & ISSUES
in crime and criminal justice

Australian Government
Australian Institute of Criminology

No. 329 November 2006

Mobile and wireless technologies: security and risk factors

Gregor Urbas and Tony Krone

Mobile and wireless technologies have evolved beyond recognition since the first radio signals were transmitted by pioneers including Nikola Tesla and Guglielmo Marconi in the late nineteenth century. Radio waves have been used since then as a basis for telephony, audio and video broadcast, and navigation and radar systems. More recently, the advent of mobile phones and similar devices has transformed business and social interactions. Today, many of us use mobile access to the internet to communicate in real time across the globe, to access business and government services online, to shop, view, read, search, explore and even simulate physical activities. Internet access no longer depends on a wired system such as a modem connected to a telephone landline – rather, it can be achieved using a mobile enabled device whenever and wherever a mobile access point is available. Such access points or hot spots are now widely available in airports, hotels, educational institutions and other public buildings. Increasing numbers of wireless networks are being installed in commercial buildings and private homes. With increasing mobile access to wireless networks, the demarcation between public and private space is being redefined. This has important implications in terms of security for those who make a mobile access point available and for those who use it. The security and risk factors associated with mobile and wireless technologies need to be understood and addressed to ensure safe and secure business and personal use of mobile technologies.

Toni Makkai
Director

Mobile and wireless technologies

Wireless technologies have advanced with great speed in the past few years. Not only have the capacity and performance of wireless communications systems improved exponentially, but so has the range of information and services that can now be accessed using mobile devices. Mobile phones and other handheld devices such as palm pilots allow greatly increasing amounts of information to be retrieved, stored and transmitted in real time. This includes text as well as audio and video data, as illustrated by the ease with which mobile phone users are today able to converse by voice, email or SMS, take and transmit digital photographs, stream audio and/or video files, and upload/download a range of material directly via the internet.

The information and communications technology (ICT) revolution continues as more users adopt wireless systems, both for personal uses and in business dealings. Today, up to half of all broadband connected households in some countries have wireless access. Major cities are increasingly being serviced by multiple wireless providers and access points, so that wireless devices can be used from almost any urban location. In Australia, the number of internet subscribers reached

ISSN 0817-8542

ISBN 1 921185 25 2

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9272
Fax: 02 6260 9293

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: http://www.aic.gov.au

Project no. 0074a

approximately 6 million in mid-2005, with strong growth in the proportion of non dialup subscribers, such as integrated service digital network (ISDN) and digital subscriber line (DSL) broadband connections (ABS 2005). Many households and businesses have introduced some elements of wireless connectivity into their networks either through fixed wireless or mobile wireless (hotspots) internet access, though direct wireless access to internet service providers (ISPs) remains less common. Other applications of wireless connectivity include automated transmitting technologies such as radio frequency identification (RFID) and other identification and access devices used in transport and building security.

Table 1 shows the four main types of wireless connectivity, based on the distances over which they operate.

The range of some of these technologies means that networks can now be accessed from previously unconnected locations. For example, travellers using wireless enabled laptops and mobile devices can now connect to their offices and exchange data from the comfort of an airliner flying 10,000 metres above land (TISN 2006a). Technological changes such as these can have significant effects on behaviour.

Behavioural changes

As more people become connected online through mobile technologies, there is a shift in their behavioural patterns including social interaction. This is particularly evident in the ways in which the demarcation between public and private space is understood. Davis and Pease (2000) have observed:

> There are increasing opportunities for people to be isolated in public space. Business, inter-personal and entertainment activities have moved from the social and static to the personal and mobile. People have greater choice as to who they 'meet' and how. Physical society may, therefore, become a more hostile place, through which people travel rather than in which they expect to interact. In a dehumanised environment, people may become less 'real' to one another, leading to more extreme reactions and interactions.

Part of this social change is illustrated by behaviour patterns associated with mobile phone usage, whereby many people conduct private conversations in public places with little regard for their own privacy or security (or the sensitivities of those around them). To an increasing extent, mobile access to the internet is also shaping behaviour in public (Isobar & Yahoo 2006):

> As the Internet becomes more pervasive, a blurring will occur between online and the 'real world'. It will become commonplace for people to store many personal items online. It will also affect socialising, in terms of the places where people congregate and the people with whom they interact.

These behavioural aspects of new technologies are not only interesting from sociological perspectives. They also have consequences in terms of criminal opportunities to exploit the security vulnerabilities that mobile and wireless networks entail. These opportunities can be understood in terms of the benefits and risks associated with the technologies.

Benefits and risks

As with previous advances in communications systems, there are many advantages to wireless and mobile technologies (Krone 2006):

- *flexibility* – systems can be installed and reconfigured at minimal cost and with minimal disruption, which is particularly important in heritage buildings, or where a business needs to be flexibly configured
- *mobility* – people can connect to the internet from many more places, freeing them from the necessity of being physically located in an office and large amounts of data can now be downloaded onto small devices (such as data sticks, also known as USB keys).

However, there is a trade off between convenience and security. Just as with cyberspace, wireless technology blurs the distinction between the real and virtual, between physical and ICT security. Without the boundaries of a hard wired network, users are vulnerable to both intrusion and exploitation by other technology

Table 1: Types of wireless connectivity

Abbreviation	Name	Example	Distance
WWAN	Wireless wide area network	GSM mobile phones, 3G mobile phones	10 km
WMAN	Wireless metropolitan area network (IEEE 802.16)	Suburb of city connected to the internet at broadband speeds	1 km
WLAN	Wireless local area network (IEEE 802.11)	Local area network on the floor of a building connecting all workstations and servers	100 m
WPAN	Wireless personal area network (Bluetooth, Infrared)	Connecting and controlling various products and devices	1 m

Source: Trusted Information Sharing Network (2006a)

Note that terminology varies and further technical variations exist within each of these categories. For example, WMAN is also known as WiMAX (worldwide interoperability for microwave access). WPAN uses IEEE 802.15 standard (which includes Bluetooth from June 2002) and IEEE 802.15.3a (known as Ultrawideband). WWAN includes wide coverage area technologies such as 2G cellular, cellular digital packet data (CDPD), global system for mobile communications (GSM), general packet radio service (GPRS) and Mobitex. WMAN along with mobile broadband wireless access (MBWA) includes 802.16 and emerging standards such as 802.20 (NIST 2006; TISN 2006b).

users, without necessarily being aware that this is happening. Particular security risks associated with mobile and wireless systems include:

- *intrusion* – networks are more open to intruder access unless protective measures (such as passwords, encryption and identifier disabling) are adopted and this may result in a greater susceptibility to theft or misuse of information contained on networks, unauthorised destruction or modification of data, and abuse of network capacity
- *leeching* – bandwidth can be used by intruders at the expense of legitimate businesses and users
- *exploitation* – network access can be misused to launch denial of service (DoS) attacks against third parties, transmit illicit material such as child pornography, or engage in other criminal activities.

The increased use of mobile devices to store large amounts of data also carries a risk of loss or theft, which can compromise the security of information. In order to minimise the risks of such abuses, mobile and wireless users need to be aware of security issues relating to the technology.

Mobile and wireless security

The key difference between wired and wireless networks from a security perspective is access to the system. With a wired system, there must be a physical connection in order to access data on the network. With wireless networks however, this is not the case – any person who is within the effective distance covered by a wireless access point (hotspot) has the potential to access the network by tuning in to the appropriate frequency (Kang 2005: 6). This means that an unsecured or poorly secured wireless network is highly vulnerable to accidental or deliberate intrusion. Accidental intrusion is a relatively common occurrence and is not itself normally regarded as harmful, unless the access is then exploited for further illicit purposes.

Security threats to computer networks include both physical and virtual aspects. A lack of adequate security in wireless networks can lead to criminal attacks such as theft of data, corruption of system integrity, hacking, sabotage, espionage, theft of capacity, and loss or theft of mobile and portable devices (Krone 2006). These can be broadly divided into active and passive attacks (NIST 2006; Rahman & Imai 2002; TISN 2006b).

Active attacks include:

- ID spoofing or masquerading in order to impersonate an authorised user of an access point or to obtain unauthorised privileges (including de-authenticating a legitimate user)
- message modification by deleting, adding to, or altering content
- DoS attacks whereby communications facilities are impaired by incoming messages
- 'replay attacks' to cause a DoS, or accelerate data flow to aid in the cracking of wired equivalent privacy (WEP) encryption
- dictionary attacks to guess the base station service set identifiers (SSID).

Passive attacks rely on the collection of data in transit without interrupting the communication between authorised devices. These can take the form of:

- eavesdropping – monitoring transmissions for message content
- traffic analysis – monitoring transmissions for patterns of communication.

Any of these techniques can be used in the commission of criminal acts exploiting mobile and wireless systems. There are several steps in deliberate exploitation.

Step 1: Discovery

The process of intentionally probing wireless networks to reveal whether they are accessible is known as sniffing or, where a laptop computer is used from a vehicle, war driving (Kang 2005). The latter term derives from the 1983 movie *WarGames*, in which a teenage hacker is depicted searching for modem lines by means of a computer program that dials a series of listed phone directory numbers until a successful connection is made – sometimes referred to as war dialling (Ryan 2004). Similarly, war drivers are able to drive around detecting the SSIDs and security settings of wireless networks in a given area such as an urban centre and physically map these onto a geographic map, either for later use or to share the information obtained with others. Variants of war driving are war chalking, whereby individuals walk around an urban centre with wireless detection devices and mark network hotspots using chalked symbols intended to be read by other participants in the activity (Ryan 2004; Freeman 2006), and war flying, which has reportedly been successful in picking up numerous wireless networks from a plane flying over an Australian city (Dreyfus 2002).

Step 2: Connecting

The next step in wireless intrusion is to obtain access, typically from outside the premises in which the network operates. Such unauthorised access is commonly referred to as LAN-jacking. This is done by simply connecting to the wireless network. Where necessary to overcome security settings, further tools can be used to crack passwords and/or discover any encryption keys used by the wireless system, tools which can all be obtained with a minimum of effort from internet sites (Kang 2005).

An exercise conducted by KPMG using honeypot sites (created to test vulnerabilities by providing a measurable target for illicit activity) found that most probes to detect wireless connections in the London central business district were attempted during early and late workday hours – suggesting that the source was war driving commuters – but that only 16 percent of these probes went on

to obtain network access, with three-quarters of these engaging in further acts that could be described as hostile, such as tampering with settings and commands (Judge 2002; OutLaw.com 2003). A recent South Australian study using three honeypot sites in Adelaide, found that these probes were more likely when the honeypot was surrounded by other wireless networks. The majority of unauthorised connections made were seeking access to the internet submitting DNS queries for popular websites or instant messaging. Two of the honeypots experienced malicious connections involving port scans or attempts to penetrate the honeypot's virtual host (Pudney & Slay 2005).

Step 3: Exploiting access

One consequence of unauthorised access to a wireless network is that the intruder obtains free use of the network and its capabilities, including connection to the internet, at the expense of the legitimate owner (leeching). Such open ended availability and access can result in problems for both the intruders and the networks they join. For example, leeching may constitute a further offence, particularly if accompanied by dishonest intent. In some cases, stolen bandwidth can amount to a significant cost, analogous to the illegal abstraction of electricity from a building. Beyond this, however, unauthorised access allows for a number of further forms of exploitation:

- unauthorised access to information held on the network
- unauthorised creation/modification of data on the network
- DoS attacks on the network or other networks.

Unauthorised access to a network can be exploited to send spam or other messages, download or distribute illegal content such as child pornography, launch further attacks or engage in other online criminal acts. The costs to affected owners extend beyond mere unauthorised use of computing resources, and directly affect the security and privacy of information held on the system. In some cases, the major security problem is that the wireless intruder is able to assume the identity of the legitimate business concerned and conduct fraudulent or illegal transactions using that identity until discovered. This may also mean that the business owner is wrongly accused or suspected of responsibility for the acts, which apart from the risk of prosecution, may also entail significant damage to commercial reputation.

National information infrastructure

The national information infrastructure (NII) includes telecommunications, transport, distribution, energy, utilities, banking and finance industries as well as critical government services including defence and emergency services (TISN 2004). Because the electronic systems supporting the NII rely to a large extent on wireless connections (for example, communication between control towers and aircraft), it is imperative that these systems be protected by effective security measures. Although Australia has to date not suffered any major attacks against its NII through wireless networks, the risks are illustrated by the Boden case (discussed below) in which a water and sewerage system in Queensland was subject to attack (Krone 2006).

Law enforcement responses

Neither the community of technology users nor law enforcement is in a position to deal alone with all threats to communications systems, nor is it reasonable to expect the costs to be borne by only one sector. A cooperative approach is necessary to keep cyberspace as safe as possible. The Australian High Tech Crime Centre exemplifies this approach to policing technology-enabled crime by working closely with private sector personnel such as bank security experts as part of its investigation operations (AHTCC 2006).

Law enforcement responses can be divided into three key areas: prevention; detection and investigation; and prosecution.

Prevention

As ICT has largely been developed without building in security mechanisms from the beginning, ICT platforms are readily misused and once a criminal application has been developed it can persist in ways that cannot easily be stopped. As a result, there is often an iterative cycle of vulnerability–exploit–patch for each new vulnerability. Public authorities have limited influence over the architecture of the wireless environment. Prevention is therefore largely in the hands of users, and the police interest is in ensuring that users take into consideration the full impact of their decisions when committing to wireless technology (Krone 2006). There is a wide range of commercially available products and services designed to enhance security of mobile and wireless networks, including encryption tools, access controls and intrusion detectors (Lopez 2004).

Wireless risks occur at several levels – including users, mobile devices, wireless networks, wireless applications and the internet (Bahli & Benslimane 2004) – so there is no single prevention strategy that will remove all risks. Recommendations made by the Advanced Computing Research Centre, based on a survey of industry experts, include strengthening of physical barriers to access points, use of authentication requirements, firewalls and intrusion detection systems, encryption and password protection, disabling of SSID broadcasting facilities and employee eduction (Krone 2006).

Detection and investigation

Law enforcement agencies have limited powers and capacity to monitor electronic signals for signs of illegal activity. There is therefore not a major role for police in the detection of illegal mobile

and wireless usage. Law enforcement depends to a large extent on complaints from the public, and computer users are often unaware of intrusions on their wireless networks or unwilling to report them (Krone 2006). The annual AusCERT computer crime and security survey indicates that there is generally a low rate of reporting attacks on computers to the police. In the most recent survey, 69 percent of organisations that experienced electronic attacks or other forms of computer crime within the previous 12 months chose not to report the attack to law enforcement (AusCERT 2006). Only seven percent reported one or more incidents to the Australian High Tech Crime Centre, 22 percent to another Australian law enforcement agency, 15 percent to an external computer security incident response team (such as AusCERT) and 10 percent to legal counsel for civil remedy.

Where enforcement authorities do try to trace wireless intrusions, the investigative trail may lead only to a numeric internet protocol address in the case of a public network or the innocent owner of a wireless home network (Schiesel 2005).

Prosecution

Prosecutions for wireless network intrusion remain rare in Australia. The Boden case (see box) illustrates how wireless intrusion can affect components of critical infrastructure such as public utilities.

Overseas, the emerging picture reveals prosecutions for a range of computer offences committed against or using wireless networks. Reported cases include that of a Toronto man who allegedly used his neighbour's internet connection to download child pornography (Schiesel 2005), while in the United Kingdom a man was reportedly fined £500 for obtaining unauthorised access to a wireless network in a residential building after being caught standing outside it with his laptop (Reade 2005). In the United

WIRELESS HACKING CASE (AUSTRALIA)

During March and April 2000, Vitek Boden made 46 attempts using wireless connections to hack into Maroochy Shire Council's computerised waste management system. He had lost his job in developing the wireless network that controlled the sewage and drinking water system. During the attack his laptop identified itself as Pumping Station 4 and sent commands leading to the release of millions of litres of raw sewage into rivers and parks, with considerable environmental costs. In October 2001, Boden was found guilty on various charges involving computer hacking, theft and causing environmental damage, and sentenced to two years imprisonment. On appeal, convictions on two of the charges were set aside but the sentence was left unchanged: *R v Boden* [2002] QCA 164 (10 May 2002). A subsequent special leave application to the High Court of Australia was dismissed on 25 June 2003.

Sources: Krone 2006: 34; Smith, Grabosky & Urbas 2004: 205

WIRELESS HACKING CASE (USA)

Three suspects in Michigan were indicted in November 2003 over a scheme to steal credit card records by hacking into a wireless connection for the Lowes home improvement chain. Using a laptop, they allegedly hacked into the Michigan store's wireless network late at night from a car parked outside, thereby gaining access to the company's central data centre in North Carolina and seven other Lowes stores around the country, at one point crashing the point of sale terminals at a California store. Their purpose was to install a data capturing program used to process credit card transactions, thus enabling theft of credit card details. In December 2004, one of the three, Brian Salcedo, was sentenced to nine years in prison while an accomplice received 26 months plus two years court supervised release.

Sources: Poulsen 2003, 2004; United States Department of Justice 2003, 2004a

WIRELESS WAR SPAMMING CASE (USA)

In September 2004, Nicholas Tombros pleaded guilty in a California court to obtaining unauthorised access to wireless computer networks in order to send spam emails advertising pornographic websites. According to the United States Department of Justice, Tombros admitted that he went war driving around the Venice Beach community in California, and sent the spam messages each time his laptop connected to unprotected wireless access points. This war spamming case was the first ever prosecuted under the US CAN-SPAM Act, the United States' anti-spamming legislation introduced in 2003.

Source: United States Department of Justice 2004b

States, several prosecutions have been brought against suspects accused of wireless intrusion, including a widely reported case in Michigan involving a home improvement retailer (see box).

Those who disseminate viruses or other malware, send massive amounts of unsolicited messages (spam) or distribute pornography and other potentially offensive content are finding new ways to shift their activities to mobile phones and other handheld devices, exploiting the rapidly growing popularity of instant messaging services such as SMS. Because of the widespread use of these modes of communication by children, there is a danger that they will be targeted by predators or exposed to illicit content (Read 2005). The use of war driving to exploit wireless networks for pornography spamming is illustrated by the United States case of Tombros (see box).

Conclusion

Mobile and wireless security need to be addressed by both the users of technology and law enforcement agencies in order to minimise the risks of criminal misuse. Wireless systems installed by home users, businesses and other institutions have obvious advantages in terms of convenience and access, but this feature also increases the risks of outside intrusion and misuse. Some types of misuse can constitute criminal offences, and law enforcement agencies need to be aware of the ways in which criminals have begun to exploit the vulnerabilities of these new forms of information and communications technologies.

Dr Gregor Urbas and Dr Tony Krone are former high tech crime analysts at the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series: Dr Toni Makkai, Director, Australian Institute of Criminology, GPO Box 2944 Canberra ACT 2601
Note: *Trends & issues in crime and criminal justice* papers are peer reviewed.

The AIC is a statutory body with a Board of Management comprising Australian, state and territory government representatives, administered under the *Criminology Research Act 1971*.

Acknowledgment

The Australian High Tech Crime Centre funded this research.

References

All URLs were correct at October 2006

AusCERT 2006. *Australian computer crime and security survey*. http://www.auscert.org.au/

Australian Bureau of Statistics (ABS) 2005. *Internet activity*. ABS cat. no. 8153.0. http://www.ausstats.abs.gov.au/ausstats/subscriber.nsf/0/E85DB7DE828A7B64CA25705A00762081/$File/81530_mar%202005.pdf

Australian High Tech Crime Centre (AHTCC) 2006. *Joint Banking and Finance Sector Investigation Team (JBFSIT)*. http://www.ahtcc.gov.au/about_us/jbfsit

Bahli B & Benslimane Y 2004. An exploration of wireless computing risks: development of a risk taxonomy. *Information management & computer security* 12(2/3): 245

Davis R & Pease K 2000. Crime, technology and the future. *Security journal* 13(2): 59

Dreyfus S 2002. War driving takes to the air over Perth. *The Age* 27 Aug 2002. http://www.theage.com.au/articles/2002/08/24/1030052995854.html

Freeman EH 2006. Wardriving: unauthorized access to Wi-Fi networks. *Information systems security* Mar–Apr: 11–15

Isobar & Yahoo 2006. *Fluid-lives.com 2006*. http://www.fluid-lives.com/docs/fluid_lives_highlights.pdf

Judge P 2002. Wi-Fi 'wartrappers' snare the drive-by hackers. *ZDNet* 9 Oct. http://news.zdnet.co.uk/internet/0,1000000097,2123600,00.htm

Kang M-C 2005. Wireless network security: yet another hurdle in fighting cybercrime. In Reich P (ed), *Cybercrime & security* vol.1 part IIA-2

Krone T 2006. Gaps in cyberspace can leave us vulnerable. *Platypus* 90 Mar: 31–37

Lopez J 2004. WLANs vulnerable to hacking. *NewsFactor magazine online* 14 Jun. http://www.newsfactor.com/perl/story/25380.html

National Institute of Standards and Technology (NIST) 2006. *Guide to IEEE 802.11i: Robust Security Networks*. Draft special publication 800-97. 5 Jun. http://csrc.nist.gov/publications/drafts.html

OutLaw.com 2003. KPMG honeypot lures London's wardriving commuters. *Out-Law.com news*. http://www.out-law.com/page-3443

Poulsen K 2003. Wireless hacking bust in Michigan. *Security focus* 12 November. http://www.securityfocus.com/news/7438

Poulsen K 2004. Long prison term for Lowe's wi-fi hacker. *Security focus* 16 Dec. http://www.securityfocus.com/news/10138

Pudney P & Slay J 2005. An investigation of unauthorised use of wireless networks in Adelaide, South Australia. Proceedings of Information Security and Privacy: 10th Australasian Conference, Brisbane, 4–6 July 2005. *Lecture notes in computer science* vol. 3574/2005: 29–39

Rahman MG & Imai H 2002. Security in wireless communication. Wireless personal communications 22(2): 213–228

Reade Q 2005. Man fined for hacking into wireless connection. *Webuser magazine* 25 Jul. http://www.webuser.co.uk/news/news.php?id=66432

Ryan PS 2004. War, peace or stalemate: wargames, wardialling, wardriving, and the emerging market for hacker ethics. *Virginia journal of law & technology* 9(7): 1–57

Schiesel S 2005. Growth of wireless Internet opens new path for thieves. *New York times* 19 Mar. http://www.nytimes.com/2005/03/19/technology/19wifi.html

Smith R, Grabosky P & Urbas G 2004. *Cyber criminals on trial*. Port Melbourne: Cambridge University Press

Trusted Information Sharing Network (TISN) 2004. *Critical infrastructure protection national strategy*. http://www.tisn.gov.au/

Trusted Information Sharing Network (TISN) 2006a. *Wireless security: overview for CEOs*. http://www.tisn.gov.au/

Trusted Information Sharing Network (TISN) 2006b. *Wireless security: overview for CIOs*. http://www.tisn.gov.au/

United States Department of Justice 2003. Three men indicted for hacking into Lowe's companies' computers with intent to steal credit card information. *Press release* 9 Dec. http://www.usdoj.gov/criminal/cybercrime/salcedoIndict.htm

United States Department of Justice 2004a. Three plead guilty to computer hacking. *Press release* 4 Aug. http://charlotte.fbi.gov/dojpressrel/2004/lowescomputerhack.htm

United States Department of Justice 2004b. Guilty plea by local 'war-spammer' is first-ever conviction under Can-Spam Act. *Press release* 28 Sep. http://www.usdoj.gov/usao/cac/pr2004/131.html