2006

Does your wireless LAN have criminal intent?

Michael Crowley
Edith Cowan University

Andrew Woodward
Edith Cowan University

DOI: 10.4225/75/57b659e43476a
Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006

Does your wireless LAN have criminal intent?

Michael Crowley
School of Justice and Law
m.crowley@ecu.edu.au

Andrew Woodward
School of Computer and Information Science
a.woodward@ecu.edu.au

Edith Cowan University
Perth, Western Australia

Abstract

All of the literature relating to wireless network security has focused on the flaws, newer alternatives and suggestions for securing the network. There is much speculation and anecdotal statements in relation to what can happen if a breach occurs, but this is mostly from a computer security perspective, and mostly expressed in terms of potential for financial loss. This paper examines the potential legal ramifications of failing to properly secure a wireless network. Several scenarios are examined within based on usage of wireless on the various category of attack. Legal opinion, backed up with case law, is provided for each scenario. Several examples are given for unauthorised use, with other aspects having potential for prosecution. The conclusion is that no matter whether you are a home user of wireless, a small to medium business or a large enterprise, there a legal as well as financial reasons to properly secure your wireless network.

Keywords

Wireless networks, security, legal liability, unauthorised use, health and safety, data integrity, data confidentiality

INTRODUCTION

There have been many articles published in relation to the problems and flaws in wireless security (Fluhrer *et al*, 2001; Bellardo & Savage, 2003; Woodward 2004). There have also been other works suggesting solutions for various types of application and business type (Woodward 2005a). Current data indicates that the message is not getting through, with many people failing or lacking the knowledge to adequately secure their wireless networks (Szewczyk 2006). Many of these documents discuss the lack of security, and provide some means of how to better secure a wireless LAN. However, in relation to the law, there is much speculation and anecdotal statements made in relation to what can happen if a breach occurs, but rarely are actual examples provided (Miller 2005; Posey 2005). Whilst some authors have indicated that there may be legal ramifications for failing to secure a wireless LAN (McLaughlin 2006), none have explored this in terms of actual civil and criminal implications of using an insecure wireless network.

This paper examines the potential legal ramifications of failing to properly secure a wireless network. Several scenarios are examined within based on usage of wireless in various applications: home, small office, medical practice. Legal opinion, backed up with case law, is provided for each scenario. Implications for failing to secure wireless networks from a financial loss point of view do not seem to have made a significant impact: perhaps a legal prosecution might? A good analogy as to why computer security is important can be found in the alleged comment by Willie Sutton, a notorious American bank robber who once said that the reason he kept robbing banks was “because that’s where the money is” (Grabosky & Smith 1998).

WIRELESS NETWORKS, THE LAW AND YOU

There is little value to be gained from restating in detail the vulnerabilities that are present with wireless networks, as this has been covered abundantly by previous papers (Woodward 2004; Woodward 2005). However, the vulnerabilities can be summarised in terms of their potential for problems from a legal perspective. The major issues confronting wireless LAN users can be summarised as health and safety, denial of service, unauthorised use, data confidentiality, and data integrity. Except for health and safety these represent the present challenges confronting computer users and computer network installers. Essentially, the inventiveness of those with criminal intent continues to take account of and adapt to take advantage of technological change.

What could once only be achieved by sitting at a computer keyboard linked to a cable or telephone line can now be take place behind the relative anonymity of a wireless LAN.

Health and Safety

Wireless LAN is no more than an extension of wireless communications introduced by Marconi at the end of the 19th century. For a long time the only health and safety issue was 'telegraphist's cramp' which lead to successful claims for damages (Murphy v Amalgamated Wireless Association Ltd, 1991).

Technology has moved on and recently Australia has agreed to be bound, subject to one declaration (No. 91) in regard to sovereignty over segments of geosatellite orbit, by the Partial Revision of the Radio Regulations and Final Protocol as incorporated in the Final Acts of the World Radiocommunication Conference of the International Telecommunication Union (ITU), in Istanbul on 2 June 2000 (WRC-2000). The WRC-2000 provides for the release of additional electromagnetic spectrum for third generation international mobile telecommunications including wireless internet access (Radio Regulations, 1998). Australia had, and still has, an existing obligation to ensure 'the radio spectrum…is used in a manner that will prevent harmful interference to services, and which will allow distress calls and messages to be freely conveyed (Articles 45 and 46, ITU Constitution) (at paragraph 19).

There is a community concern that facilities that emit electromagnetic energy will harm health and safety of persons. This concern has resulted in challenges to facilities/antennas that emit radio waves. Courts have been careful to examine these health concerns over radio emissions. In Cable Wireless Optus Ltd v Knox CC (2000) VCAT 901 (30 April 2000) the Court made it clear that all radio frequency emissions from antennas shall comply with Australian standards (at paragraph 8). There is also the Australian Communications Authority who set up clear rules as to what power outputs can be used and at what frequencies.

Health concerns was one of the key issues in a recent Land and Environment Court decision in Sydney, Australia; *Telstra Corporation Limited v Hornsby Shire Council* [2006] NSWLEC 133 (24March 2006) wherein some local residents challenged the erection of a mobile telephone base station. Preston CJ found, after hearing and considering expert evidence, that in the present case in regard to electromagnetic energy, 'there is no probative evidence upon which the Court could make findings of adverse effects on the amenity of the locality or on the health and safety of persons in the locality or on the environment' (at paragraph 204, p.39). In this case Dr Black explained how mobile phone technology uses the higher end of current Australian Radiation Protection Standard "Maximum Exposure Levels to Radiofrequency Fields 3kHz to 300GHz: Radiation Protection Series No. 3" ("Australian Standard RPS3") (at 54, pp. 11 – 15). He went on to explain that amongst other things RPS3 sets "limiting values to deal with both thermal and athermal effects of radiofrequency electromagnetic energy (RFEME)" (at 89, p.20). Dr Black's evidence that RF EME which would radiate from the proposed base station could not cause any adverse biological or health risk if the proposed tower was built to specifications (89 at p.20).

The implication is that wireless technology, which uses part of the radiofrequency spectrum, does not at this stage pose any identifiable health risk so long as equipment, both transmitting stations and computer hardware, are built to comply with Australian specifications. Manufactures of wireless hardware, including towers have little to fear from any health and safety litigation so long as their equipment complies with recognized Australian standards and they have no knowledge of research that contradicts these standards. There is however, much paranoia surrounding the use of EMF emitting devices (Bale 2006), despite over 30 years of research failing to show any causal link between power lines and negative health effects. A summary of available research studies and data examining the effects of radio and microwave EMF radiation on humans conducted by the European Commission for Health and Consumer Protection concluded that there is no conclusive or significant risk (CSTEE 2001). A good analogy is to be found with the tobacco industry. The tobacco industry promoted cigarette smoking notwithstanding evidence they possessed, and suppressed, that indicated smoking was injurious to health. Litigation against tobacco companies has been fierce and judgements have been significant.

Intellectual Property

Wireless LAN technology is a developing area and competition for 'ideas' and 'advances' can lead to interesting court cases. As IP theft is being reported by organisations (AUSCERT, 20006), it seems likely that wireless networks may have been the conduit that was used to steal the information. However, there do not appear to be any specific examples in the literature or the media in relation to theft via wireless LAN. Interestingly, there has been a case in relation to the technology itself. In Delegarde Legal Services Pty Ltd v Commonwealth Scientific and Industrial Research Organisation [2006] AATA 722 (21 August 2006), the applicant, Delegarde sought access to documents under freedom of information legislation. These documents related to the Commonwealth Scientific and Industrial Research Organisations (CSIRO) work on wireless LAN technologies, specifically the orthogonal frequency division multiplexing used to achieve high data rates on 802.11 a and g. The Court denied access on the grounds that the documents sought were brought into existence by CSIRO for commercial purposes and were thus exempt from the disclosure pursuant to s.24(5) Freedom of Information Act 1982 (Cwealth).

Denial of Service

This category of attack refers to preventing access to, or use of the wireless network. This may be either intentional or unintentional, but either way, then end result is still the same. It may be carried out with malicious intent by targeting the access point (AP) with a high power RF signal at the same frequency. It may occur through the use of a device which operates at the same frequency such as a microwave oven or Bluetooth device (Geier, 2002). The latter is more likely, but either method is fairly easy to perpetrate, and difficult to prevent.

There are two areas in which computer attacks can have significant impacts upon unsuspecting populations. The first is hospitals and the second is computers that support/maintain key infra-structure. For the former a potential scenario is a hospital using wireless to access drug information about a patient. The WLAN becomes unavailable due to a DoS attack, and in an emergency and a patient is given the wrong dose of a drug, or the wrong drug. This is no so far-fetched. Recently, in January 2005 a Californian man was sentenced to 3 years in goal and fined a quarter of a million dollars after his malware attack caused damage to Defence computers, hospital and school district computers (infoZine 2006a). The hospital attack shut down computers in intensive care and disrupted doctors pagers. While such an attack can be carried out by cable/telephone line and/or wireless LAN the latter increases the chances of the attacker escaping because of the nature of wireless LAN technology.

Australia has experienced infra-structure attack via wireless LAN. In March and April 2000 Maroochy Shire Council on Queensland's Sunshine Coast found its sewage treatment works under attack. Raw sewage was pumped into the local water supply. The water provider used the SCADA system to control its sewage management system. Vitek Boden used a stolen laptop, control management software, commercial radio equipment and knowledge of water management systems gained from prior employment to access the system some 46 times gaining control of the sewage system operations. Millions of litres of raw sewage was spilled into local parks, rivers and a 5 star resort. Boden was fined and sentenced to two years in goal. The exercise cost the Council A$13,000 in clean up costs, A$176,000 in extra monitoring and security plus undisclosed in-house costs and loss of reputation (ITSEAG 2006). In this instance, it was the ability to alter telemetry data which caused the problem, and not a denial of service, however, a DoS attack against such a target using SCADA would be trivial, and almost impossible to prevent. SCADA systems are particularly vulnerable as they are often used in remote locations, making detection, let alone prevention, of attack a difficult task. ITSEAG also noted the damage the SQL Slammer Worm did to the Davis-Besse nuclear power plant in Ohio USA. Worm activity blocked SCADA traffic, causing, amongst other things, a shutdown of the plants safety display system for almost five hours (ITSEAG 2006, p7).

Unauthorised use

This area relates to restricting access to the wireless LAN only to those who are authorised to do so. If the WLAN is not set up correctly, and with an appropriate authentication mechanism, then anyone can connect to, and use the network. This has many implications, which will be examined in detail later. Initial authentication

methods were limited and flawed, such as WEP shared key authentication (Fluhrer *et al*, 2001), but newer methods such as WPA are more secure (Woodward 2005b). The problem is that they can be quite difficult to configure, or require more IT knowledge than many WLAN users would have (Szewczyk 2006).

While the above examples raised criminal consequences of improper use of computer technology there can also be civil consequences for using someone else's wireless LAN without permission. Some civil consequences include criminal consequences. Kueser (2006) argues that wireless computer networks should be treated as private property. This follows on from developed property interests in radio and cellular communications. However, wireless computer networks are create more complicated property rights issues because they operate on unlicensed spectrum (Kueser (at 2). However, this unlicensed spectrum is controlled by governments who issue licenses. Holding a license is the vehicle to property rights. This is because the owner of the license owns, operates and can sell this license (Kueser at 3). Property rights can exist in emission rights, admission rights, use rights and transferability rights (Kueser at 5). Courts have accepted some of these rights. In eBay, Inc v Bidder's Edge, Inc 100 F.Supp.2d 238 (N.D.Cal 2000), the court recognized that signals can trespass approving Thrifty-Tel v Beznik, 46 Cal. App. 4th 1559, 1556 (1996) "the electronic signals generated by the [defendants'] activities were sufficiently tangible to support a trespass cause of action" (e-Bay at 16.18). Assigning property rights to electromagnetic spectrum/wireless LAN implies owners exercise responsibility meaning being proactive to minimize interference (Kueser at 6).

Legislation is also changing. In the United Kingdom the outdated Computer Misuse Act (1990) that predated the world wide web has had a few loopholes filled via changes to the Police and Justice Act 2006. David Lennon had been charged with sending five million emails to his former employer, but no offence had been committed because of the wording of the old legislation. The new legislation criminalizes anybody who does an unauthorized act in relation to a computer with the requisite knowledge and intent. Penalties include up to 10 years for paying someone to launch an attack or more relevant to wireless LAN, supplying software tools to launch an attack (Out-Law.com, 2006a). This opens up the potential for persons who supply software tools knowing that those tools were going to be used to illegally access wireless LAN networks to be charged as an accessory (Bainbridge [1959] 3 All ER 200). Likewise, persons who associate with individuals who illegally access wireless LAN networks (DPP for Northern Ireland v Maxwell [1978] 3 All ER). In both cases it was sufficient that the accused knew or contemplated the general type of offences proposed to be committed. Bainbridge has wider application as it theoretically applies to all offences committed by persons using the 'equipment' notwithstanding duration of time after the sale. There is no evidence this has happened (Bronnitt and McSherry 2005).

While these authorities are considered good law in Australia, Bainbridge has not had the same wide application as in the United Kingdom. In Giorgianni v The Queen (1985) 156 CLR 473 the High Court interpreted accessorial liability as an intention related to the actual offence committed by the principal offender (at 505). In essence this means that an accessory who sells software or hardware must sell with the intention that the software and/or hardware will be used for illegal purposes. Put another way, 'an accessory need intend only to assist or encourage an offence of the type committed in due course by the principal offender' (Bronitt et al op cit at p.363). Section 11.2(3)(a) Criminal Code (Cwealth) states that a person is guilty if "his or her conduct would aid, abet, counsel or procure the commission of the offence (including its fault elements) of the type the other person committed". The relevance to wireless LAN extends beyond the supply of hardware and software to wireless LAN routers. Should the wireless LAN router owner know that their equipment is being used for illegal purposes there is the potential for criminal prosecution. This is unlikely at first instance but a scenario could develop whereby the wireless LAN router owner is on notice that his/her equipment is being used illegally. In such a situation common sense requires that owner install appropriate security restricting access to verifiable and legal users, not someone parked in a car or unit across the road.

Interestingly, there haven't yet been cases of homeowners in the United States being prosecuted for the activities of other users who access their WLANs to conduct criminal activity (McLaughlin 2006). This is mostly due to identification problems. For example, in the United States of America (USA) the music industry launched a civil

suit against Tammie Marson of Palm Deset, California USA because it was alleged she had downloaded music files via her wireless LAN. She was lucky, and hence we now have the 'cheerleader defence' because Tammie had no network security, was a cheerleader teacher and had hundreds of girls going through her house, any of whom could have used her computer. The law suit also failed because her wireless LAN was open for anybody with wireless LAN technology. In addition, there was the reasonable possibility that one of her many visitors may have downloaded the music files whilst visiting (Out-law.com 2006b). The same article advised against 'opening your network' and 'relying upon the cheerleader defence' because of the potential aggravation from authorities who may well seize your computer and charge you requiring you to give evidence that you did not download pornography or files without paying (Out-law.com 2006b). Out-law news reports that a quarter of business networks are unsecured and in London 22% of access points have default settings that put networks at risk (Out-law.com 2006b). Out-law goes on to raise the not unsurprising result of anonymity defences being a push to make unsecured networks illegal. In the United Kingdom the Data Protection Act (1998) requires certain protections be in place to protect data bases holding personal data (Out-law.com 2006b).

Garyl Luo, aged 17, of Singapore has not been so lucky. The Singapore authorities have charged Luo with 'having gained unauthorized access' under their Computer Misuse Act. If convicted he faces up to 3 years in goal and S$10,000 in fines. Luo is alleged to have tapped into someone else's wireless internet connection (International Herald Tribune, 2006). Nor was the dating hacker in the United Kingdom. He received a suspended sentence for gaining unauthorized access to databases and demanding money in return for not deleting the contents of these databases (Out-law.com, 2006c). Another example is that of an Illinois man in the United States who was fined $250US for illegally accessing a non-profit organisations wireless network (Bangeman 2006a). A similar case in the US highlights the difference in laws between states. A 20 year old man was arrested in Washington after accessing the wireless network of a coffee shop (Bangeman 2006b). He was arrested and charged with "theft of services", whereas the first offender was simply fined.

There can also be a loss of reputation (Snow, 2006). This is because an unsecured wireless LAN connection is open for use by anybody with the right equipment the equipment owner/holder might find their IP address is linked to child pornography sites and uploads/downloads. Investigating authorities who may and do monitor such sites may well visit the owner/holder seizing all computer equipment with a view to prosecution (Haglund, 2005). The presence of police vehicles and boys and girls in blue taking computer equipment away may be explainable, but the news that this was because of a reasonable suspicion that the owner/holder was engaged in child pornography may not be as easy to explain. A whiff of suspicion will always remain in the minds of some especially when politicians and shock jocks attack first for political/ratings gain before authorities and courts can adjudicate.

Snow (2006) finds no actionable trespass in capturing wireless transmissions/radio signals because the nature of these signals make them incapable of exclusive control and possession. This is not the case with the router which is a chattel. In CompuServe, Inc v Cyber Promotions 962 F.Supp. 1015 (S.D. Ohio 1997) sending unsolicited mass e-mails was found to be trespass to chattel because these e-mails "intermeddled" with the equipment. Following this decision trespass to chattel quickly became the legal weapon of choice in the United States of America (Snow 2006).

Electronic signals have been found sufficient to support civil actions alleging trespass. For example, in AOL v LCGM, In. et al 46 F.Supp.2d 444 (E.D. Va 1998) the court ruled that the defendants by transmission of thousands of unsolicited messages to AOL members advertisings the companies pornographic websites on the World Wide Web committed fraud because of the methods used to defeat AOL's spam filtering techniques. The court also found the defendants had violated AOL's trademark and ordered damages. Of interest to wireless LAN is the courts finding of fraud. The court found the defendants had violated the Virginia Computer Crimes Act, Va. Code §18.2-152.3(3), which provides that "any person who uses a computer or computer network without authority and with intent to convert the property of another shall be guilty of the crime of computer fraud" (at Count V p.6). The facts of fraud included unauthorised use of "aol.com", blocking filters without approval and obtaining free advertising at cost to AOL (at Count V p.6). This decision does not distinguish between

cable/telephone line access and wireless LAN. It focuses on the effect of the improper access upon the legitimate user.

More recently, in eBay, Inc v Bidder's Edge, Inc 100 F.Supp.2d 238(N.D.Cal 2000) the court ruled that spidering deprived eBay of the use of its personal property and granted injunctive relief. Bidders Edge used automated agents to access eBay. eBay argued two types of harm, system harm and reputational harm. While eBay did not pursue the latter it was successful with the former because eBay successfully argued that the use of 'robot' had the potential, if used by others searching eBay, to reduce performance, make eBay systems unavailable and lead to data loss. Again the relevance to wireless LAN is the potential to access and hide behind legitimate sites for illegal or improper purposes. Authorities have problems tracking hackers who illegally access wireless LAN because the MAC address of a wireless LAN card can very easily be changed. There is not other static or traceable part of a WLAN system, so unless the attacked didn't change the MAC, then prosecution may prove difficult. Also, the fact that the MAC can be changed may be enough doubt to lodge a sufficient defence against a prosecution.

Data Confidentiality

This could also be called eavesdropping, and relates to whether the data being transmitted on the wireless network is secure. The problem is that if weak, or no, encryption is used, the potential is there for a third party to intercept the transmission and be able to reconstruct emails, internet traffic (bank details, customer or patient data), or anything that travels over the wireless link. Various encryption methods are available to protect data travelling over the wireless segment of a network. As with authentication, earlier mechanisms like WEP were flawed, and provided a low level of data confidentiality. However, the newer WPA security measures, as well as the use of VPNs, have increased data confidentiality.

The increasing use of computers in legal and medical professions poses special problems because of confidentiality requirements. When litigation support services are employed because of the magnitude of the litigation special care needs to be taken if significant sums of money are involved. In courts in which wireless technology is used to facilitate proceedings including document handling care needs to be taken if and when the Court hears evidence that is classified under security legislation or ruled confidential.

However, the biggest risk lies in protecting privileged information. Lawyer-client privilege is an essential pillar of legal service. Widespread use of wireless LAN raises special problems in protecting matter subject to lawyer-client privilege. The presence of other parties can destroy the veil of protection offered by lawyer-client privilege. The use of wireless LAN to communicate and transmit data opens the door for a third party to have access to material covered by lawyer-client privilege. The same can be said for confidential legal documents/transmissions using wireless LAN.

A lawyer who uses wireless LAN and does not look to appropriate security to protect client information may not only be negligent but could also be liable in an action for damages.

The third person, the eavesdropper may also be liable. The issue is the status of the wireless LAN transmission. If it is property or a chattel then the eavesdropper is trespassing and legally liable. However, because the radio message goes everywhere there are fundamental difficulties with holding the radio waves as property. This is not so with the router. The router is a physical object that remains in the possession of the owner and

Data Integrity

This relates to being able to change or alter data after it has been sent, but before it reaches its destination. The specifics of how this is done are not important to this discussion, but the implications are. Other than maybe a home user, there is not one other level of WLAN use where the alteration of data can have significant ramifications, both legal and financial. Fortunately, newer authentication and encryption methods make this category of attack difficult

A good analogy on the need to protect wireless LAN and your personal and business data can be found in two recent examples where the significance of data integrity was highlighted. The first example is that of the standard Nigerian letter, although this one is from Ghana:

Dear Michael,

I am Mr. Abii Debe, staff of Citco Trust & Finance House Accra Ghana, I am the Credit management and recovery manager with the Company office in Ghana before I was transferred to our head office here in Lagos Nigeria, Late Engineer Wilson Michael was my personal Client before he died in an accident, he was a contractor with Shell Development Company and he is from your Country.

On the 21st of April 2002, Engr. Wilson, his wife and their two children were involved in a car accident along Platue express road and all occupants of the vehicle unfortunately lost their lives. Before the time of his death, he had a deposit of $14.5Million which he declared as family treasure in the Finance House Accra office where I was working then, which is only I and his lawyer knows the true content, Unfortunately, till this moment no person has come as his relation for his chattels with us. I humbly request your attention to this matter so that I can present you as his next of kin and beneficiary to his chattels. It is not a very difficult thing to do and it will not take time.

All I will need is to put your name and particulars as his next of kin to in our computer database and we file in an application for the release of the fund. It does not necessarily mean that you must be in Ghana to conclude the deal; we may request that the money be sent to Europe for your collection. Please contact me as quickly as possible through this email address (adebe30@yahoo.dk) treat this matter as very important and confidential. When I hear from you, we shall discuss the terms of sharing of the money after the claim. Contact me now so that I can delegate the Attorney who is also going to be part of the deal.

I await your urgent response.

Best regards,

Mr Abii Debe

The letter asks for personal details so you can receive lots of money after you provide the details.

In an age of technology and internet banking access to personal banking data gives ‘criminals’ and ‘conmen/conwomen’ an advantage. Rather than turn up with a gun and get-away-car, they use the internet. Wireless LAN makes it easier if individuals do not use appropriate authentication and encryption. Financial institutions that do not ensure their customers use appropriate authentication and encryption are negligent. It is not much good having the bank say, ‘We have advanced authentication and encryption technology” if the customer is using a wireless LAN with a static WEP key for encryption and no authentication. Or even worse, the user has no authentication or encryption of any sort. A tool such as Hotspotter could then be used in order to set up a rogue AP running a copy of the bank web site, so that when the user logs on, they are diverted to the fake site, and give up their authentication details.

On a more personal level hackers with criminal intent can use computers in varied and interesting ways. This second example comes from a United Kingdom malware case where a pervert posed as a teenager to plant malware onto girls computers allowing him to take over their computers, steal personal information which he then used as blackmail for explicit pictures. A British court sentenced Adrian Ringland to ten years gaol (infoZine 2006b). Using someone else’s wireless LAN to achieve the above outcomes enhances the hacker’s prospects of escape due to the MAC address being so easily changeable, which introduces reasonable doubt. It also highlights the need to make sure that at a minimum, WPA shared key authentication is used, reducing the likelihood that someone can connect to the computers on your home network and plant information.

CONCLUSION

This paper has given examples of where wireless LANs have been cause for prosecution, and others where there is the potential for it. Strong evidence has been presented that unauthorised use of wireless networks seems to be the biggest issue, and the most likely avenue for abuse. Denial of service has great potential for abuse, and thus prosecution, but there does not appear evidence of it. The conclusion is that not only are there strong financial reasons for securing your wireless network, there is also a strong legal argument, which can in turn have financial consequences.

The United States Court of Appeals for the Fourth Circuit has indicated that computer users who communicate their IP address to third parties can no longer have a reasonable expectation of privacy (Haglund 2005). If this was applied to wireless LAN users who do not secure their wireless LAN claims against hackers and others who use and abuse their system causing damage may prove difficult.

Many jurisdictions now have what are termed long-arm legislation. This is legislation that provides a means whereby a hacker can be bought into a local jurisdiction regardless of the hacker's place of residence. The implication for wireless LAN is that should a hacker in Australia use wireless LAN to cause damage to a company in the USA and by chance the hacker is traced and identified, long-arm legislation can be utilised to bring civil proceedings in the USA. The same hacker could also find extradition treaties result in the hacker facing criminal sanctions in the USA.

It is hoped that this paper has provided sufficient reason for all users of wireless networks, both SOHO and corporate, to make sure that they use appropriate and effective security measures to protect their wireless LAN. Your wireless network may not have criminal intent, but there are plenty of wireless users who do.

REFERENCES

AOL v LCGM, In. et al 46 F.Supp.2d 444 (E.D. Va 1998), URL http://www.legal.web.aol.com/decisions/dljunk/lcgm.html, accessed 21st November 2006

AUSCERT (2006). 2006 Australian computer crime and Security survey, URL http://www.auscert.org.au/images/ACCSS2006.pdf accessed 20th October 2006

Bale, J. (2006). Health fears lead schools to dismantle wireless networks, URL http://www.timesonline.co.uk/article/0,,591-2461748,00.html Accessed 20th November 2006

Bangeman, E. (2006a). Illinois WiFi freeloader fined US$250, URL http://arstechnica.com/news.ars/post/20060323-6447.html accessed 20th November 2006

Bangeman, E. (2006b). WiFi freeloader arrested in Washington, URL http://arstechnica.com/news.ars/post/20060622-7111.html accessed 20th November 2006

Bellardo, J. and S. Savage (2003). *Disassociation and De-auth attack*. 2003 USENIX Security Symposium, USENIX.

Bronitt, S and McSherry, B. (2005). *Principles of Criminal Law*, Thomson/Lawbook, Pyrmont NSW, p.363

Cable Wireless Optus Ltd v Knox CC (2000) VCAT 901 (30 April 2000). URL **http://www.austlii.edu.au//cgi-bin/disp.pl/au/cases/vic/VCAT/2000/901.html?query** , accessed 25th October 2006

CSTEE (2001). Opinion on Possible effects of Electromagnetic Fields (EMF), Radio Frequency Fields (RF) and Microwave Radiation on human health, 27th CSTEE plenary meeting Brussels, 30 October 2001, URL http://www.mityc.es/NR/rdonlyres/FDCD3C06-363B-46CE-96EE-403451120852/0/ccue_oct.pdf accessed 8th November 2006

Delegarde Legal Services Pty Ltd v Commonwealth Scientific and Industrial Research Organisation [2006] AATA 722 (21 August 2006) URL http://www.edu.au//cgi-bin/disp.pl/au/casecth/aat/2006/722.html?query=wireless , accessed 25th October 2006

eBay, Inc v Bidder's Edge, Inc 100 F.Supp.2d 238(N.D.Cal 2000), URL http://www.legal.web.aol.com/decisions/dldecen/ebay.html, accessed 20th November 2006

Fluhrer, S., Mantin, I. & Shamir, A. (2001) *Weaknesses in the key scheduling algorithm of RC4*. URL: http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf Retreived 27/10/06

Geier, J. (2002). *Wireless LANs. Implementing high performance IEEE 802.11 networks*. 2nd Edition. USA: SAMS Publishing

Grabosky P N and Smith R G (1998) *Crime in the digital age*, Federation Press, Leichhardt NSW p.1 citing Keyes, R, 1993*, Nice Guys Finish Seventh: False Phrases, Spurious Sayings and Familiar Misquotations*, Harper Collins

Haglund R.(2005). What happens to the fourth amendment when the USA Patriot Act enters wireless hot spots, *Journal of Internet Law* Jul 2005;9, 1 at 16

infoZine (2006a). Three Year Jail Sentence for Zombie King Who Infected US Military Computers , URL http://www.infozine.com/news/stories/op/storiesView/sid/17433, accessed 20th November 2006

infoZine (2006b). Trojan Pervert Jailed; Wake Up to Online Threats or This Will Happen Again, warns Sophos, URL, http://www.infozine.com/news/stories/op/storiesView/sid/18943/ accessed 20th November 2006

International Herald Tribune (2006). Report: Singapore teen faces 3 years' jail for tapping into another's wireless Internet, URL http://www.iht.com/bin/print.php?id=3493124 , accessed 13th October 2006

ITSEAG (2006) *SCADA Security – advice for CEOs*, IT Security Expert Advisory Group (ITSEAG), Trusted Information Sharing Network for critical infrastructure protection at p.7, URL http://www.tisn.gov.au/agd/WWW/rwpattach.nsf/VAP/(930C12A9101F61D43493D44C70E84EAA)~SCADA+Security.pdf/$file/SCADA+Security.pdf accessed 25th November 2006

Kueser, J,M. (2006). This is my LAN, this LAN is your LAN: the case for extending private property rights to wireless local area networks, 72 UMKC L. Rev. 787 URL http://www.westlaw.com accessed 8th November 2006

McLaughlin (2006). Locking the wireless network, URL http://www.crn.com/showArticle.jhtml?articleId=189600264, accessed 20th November 2006

Millaer, D.W. (2005). Road warrior at risk: The dangers of ad-hoc wireless networking, URL http://www.circleid.com/posts/road_warrior_at_risk_the_dangers_of_ad_hoc_wireless_networking/, accessed 20th November 2006

Murphy v Amalgamated Wireless Association Ltd (1991) SASC 2881 (31 May 1991) at http://www.austlii.edu.au//cgi-bin/disp.pl/au/cases/sa/SASC/1991/2881.HTML?query.

Out-Law.com (2006a). UK bans denial of service attacks, URL http://out-law.com/page-7462, accessed 10th November 2006

Out-Law.com (2006b). Do not try the cheerleader defence, URL http://out-law.com/page-7448, accessed 10th November 2006

Out-Law.com (2006c). Dating site hacker avoids jail, URL http://out-law.com/page-7459, accessed 10th November 2006

Posey, B. (2005). Wireless network security for the home, URL http://www.windowsecurity.com/articles/Wireless-Network-Security-Home.html, accessed 20th November 2006

Radio Regulations (1998) Final Protocol and Partial Revision of the 1998 Radio Regulations URL, **http://www/austlii.edu.au//cgi-bin/disp.pl/au/other/dfat/nia/2001/32.html?query=wireless** accessed 25th October 2006

Snow, N. (2006). Accessing the internet through the neighbour's wireless internet connection: physical trespass in virtual reality, 84 Nebraska Law Review 1226 URL, http://westlaw.com, accessed 8th November 2006

Szewczyk, P. (2006). Individuals' Perceptions of Wireless Security in the Home Environment. In Proceedings of the 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia

Telstra Corporation Limited v Hornsby Shire Council [2006] NSWLEC 133 (24March 2006), URL http://www.edu.au//cgi-bin/disp.pl/au/cases/nsw/NSWLEC/2006/133.HTML?query , accessed 25th October 2006

Woodward, A. (2004) An analysis of current 802.11 wireless network layer one and two attacks and possible preventative measures. *Journal of Information Warfare*. **3(3):** pp37-47

Woodward, A. (2005a). Recommendations for wireless network security policy: an analysis and classification of current and emerging threats and solutions for different organisations, In Proceedings of the 3rd Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, pp.133-140.

Woodward, A. (2005b). WPA/WPA2 – Panacea or Placebo? In Proceedings of the 6th Australian Information Warfare Conference, Deakin University, Geelong, Victoria, 24-25 November, 2005

COPYRIGHT