2006

Individuals' Perceptions of Wireless Security in the Home Environment

Patryk Szewczyk
Edith Cowan University

DOI: 10.4225/75/57b6608534774
Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006

Individuals' Perceptions of Wireless Security in the Home Environment

Patryk Szewczyk
School of Computer and Information Science
Edith Cowan University
p.szewczyk@ecu.edu.au

Abstract

Research in 802.11 wireless networking has in the past focused predominantly on corporate wireless network use, or identifying the flaws in wireless security. This study was aimed to determine the individuals' perceptions of wireless security in the home environment. 163 volunteers completed a survey on their perceptions, knowledge, experiences and attitudes towards wireless networking. The results of the survey indicated that there is little difference in knowledge between those who had worked in the IT industry, and those who did not. The sources of information used to configure wireless networks are not improving the knowledge respondents had on wireless security. Respondents are aware of the various benefits of wireless networking. However, respondents do not appear to know the correct authentication and encryption methods which have been implemented on their wireless product.

Keywords

Wireless networking, wireless home user, wireless security perceptions

INTRODUCTION

Wireless Networking and Security

Australian 802.11 wireless networks operate in the 2.4 GHz frequency range (Golmie et al. 2003). The limiting property by which radio waves within this frequency naturally spread, limits feasible communication to a distance of 180 – 370 meters when using high gain antennas (Henderson 2005). Radio waves are beneficial in that they are not affected by sunlight in contrast to infrared rays. Hence wireless radio networks may operate both indoors and outdoors. Radio waves also have the potential to penetrate through objects such as buildings or trees. Radio waves may operate in various weather conditions, although signal strength may be reduced and/or cause transmission errors. All these seemingly beneficial properties of wireless networks permit consumers to use wireless network at home, through all weather conditions, in all rooms of their home

Wireless networks are increasing in popularity especially in the home environment with one reason being the simple and time efficient configuration process to enable the network (Peterson et al. 2004). Wireless networking products are combined with broadband modems. These modems are marketed as allowing the user to share files, printers and a single high speed Internet connection among a number of users (Burness et al. 2003). Consumers may also be persuaded into purchasing unnecessary wireless network products. Consumers may be persuaded by vendor marketing to purchase unnecessary wireless products. This may occur by being provided with the opportunity to upgrade their non-wireless broadband modem to a wireless network capable modem at a minimal expense. Wireless network modems are insecure when operated on the out-of-the-box installations generated by manufacturers. Hence, consumers may unknowingly be placing themselves at high risks by leaving their network vulnerable to wireless attacks. Wireless capable modems generally have wireless enabled by default, and utilise minimal or non-existent security settings. Alternatively consumers may not be persuaded by marketing, but rather forced to install a wireless network. This may occur when laying Ethernet cables, as this may prove difficult, time consuming, expensive or prohibited in heritage listed buildings.

Consumers are faced with a wide range of wireless security methods. However, the two predominant 802.11 wireless security schemes Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) have been publicised with numerous vulnerabilities that may be exploited. The main flaw in WEP is the small 24-bit initialisation vector (IV). This 24-bit IV creates a total of 16, 777, 216 unique values (Ciampa 2006). An access point in constant operation may transmit as many as 700 packets per second. Hence, when the wireless network is continuously operating the keys may begin repeating. Once enough keys are captured through packet capture software, the 'secret' pre-shared key may be recovered. This key can then be used to access and abuse the wireless network of an unsuspecting individual. Incorporating a stronger encryption algorithm, WPA may be cracked by utilising a pre-defined function (Woodward 2005). The master key may be recovered by appending the Service Set Identifier (SSID) and SSID length to the pass phrase which is then hashed 4096 times identifying the 256-bit master key. A stronger security method such as WPA Version 2 that utilises the Advanced Encryption Standard (AES) requires high processing requirements and hence may not operate on legacy computing equipment. These flaws demonstrate that home users are faced with either using weak encryption schemes which may easily be cracked or be forced into purchasing expensive equipment permitting WPA2 encryption to operate.

Previous research into wireless security has focused predominantly on large corporations and business that generally have devoted resources and/or expenditure towards IT security (Webb 2003; Shaw 2003). In 2003 a wireless wardriving experiment was conducted in the Perth Central Business District which reported that 63 percent of detectable businesses were using WEP encryption. Subsequently those 63 percent are vulnerable to highly publicised WEP attacks (Webb 2003). Home users may not have devoted expenditure to wireless security or the knowledge to implement appropriate methods. Hence, home users may be insecure and thus more vulnerable than their business counterpart.

Businesses and assumingly home users are operating insecure wireless networks. Thus home users may be disadvantaged by such policies that are being introduced throughout Europe. Several European countries have passed legislation authorising and demanding that ISP's collect and store the consumers Internet usage history (Swartz 2005). The consumer may have their Internet connection abused by an authorised individual. This intruder may access illegal or inappropriate material which may then lead to the consumer being falsely prosecuted. Alternatively the consumer may be charged with excessive Internet usage fees by their ISP. This creates an issue for a home user who may not necessarily have had implemented appropriate wireless security such as WPA2, or is using comparatively weak security such as WEP. Hence, a home user's wireless network accessing inappropriate material on the Internet could as per the legislation be falsely prosecuted.

If home users are provided with the option to upgrade their modem to a wireless capable modem for a minimal expense, this may seem as a windfall for the home user. This would also present itself as a benefit to keep in line with future technological advancements, and networking requirements. However, in Reykjavik, Iceland wireless network access is provided regardless of whether the consumer requires the technological advancement or not (Clyde 2003). The downfall of this seemingly beneficial arrangement between telecommunication companies and the home user is that there is no mention of who will educate or ensure that consumers are not left vulnerable to wireless attacks. Furthermore, there is also minimal documentation on the policies outlining how consumers will recuperate if a financial loss does occur through a wireless attack. The insecurities of wireless transmission coupled with a lack of knowledge and understanding of the wireless security requirements may only lead to major problems. Publications with a lack of credibility are presented to home users, as guidance advising of the minor issues surrounding the wireless technology along with recommendations. In May 2006 a particular media release recommended the use of WEP (Fenech 2006) as a security method for those running insecure wireless networks. A home user who reads and follows these instructions may be implementing almost no security on their wireless network.

Perceptions

Individuals may have their perceptions altered or misled by various marketing strategies about the security of home wireless networks. An individual's perception towards a given subject may be true or false due dependant on the level of understanding of a given subject (Swanson & Holton 1999). Hence, home users may believe WEP

is a secure encryption method due to publication lacking credibility, when in fact WEP has numerous flaws. In numerous instances consumers have had their perceptions altered to believe a product is advantageous over others by planned marketing. Television advertising for example shows vehicles dropping from the sky, not breaking on impact, showing endurance and robustness (Swanson & Holton, 1999). Wireless products have been promoted in a similar misleading and deceptive manner as fast, functional and highly secure. Wireless network products have various computing acronyms written on packaging such as stating that WEP and WPA encryption is supported. Therefore, individuals may falsely perceive these acronyms as secure and hence believe that their wireless product is secure by default and does not require the security features to be initialised or further configured.

Individuals may perceive a wireless networking product as secure and hence would not need to question the security functionality nor investigate methods to strengthen their security. Although WEP has been publicised in computing literature as insecure, one publication reported WEP as the recommended, easy to implement encryption scheme (Fenech 2006). The extensive use of computer terms such as WEP or WPA could possibly confuse the home user and they may perceive the product as secure. Investigations into the correlation between ones attitude and the associated behaviour were conducted during the 1960's, and found that a positive attitude towards an area showed a tendency to behave in an associated positive manner (Eagley & Chaiken 1993). Hence, an individual who has a positive experience configuring and utilising their wireless network should see them investigate further security methods in a proactive manner. However, as Westen (2002) states for an individual's attitude to impact their ongoing positive behaviour, they must have a clear understanding and awareness of that area also. Thus an individual must understand the need for security and why encryption schemes such as WEP are not feasible in home environments. Once the home user understands the fundamentals of wireless security they may then investigate better security scheme and enforce these measures.

RESEARCH METHODS

This study attempted to determine home users perceptions and attitudes on wireless networking and security and ascertain their understanding and knowledge of wireless security. By solely investigating perceptions and attitudes a foundation may be formed on the way individual's think and behave when it comes to security. The study did not aim to determine the individual's actual implemented security methods on their wireless product. It was not the intention to identify what percentages of respondents are operating insecure networks but rather how secure individuals perceive their wireless product to be.

An online survey was developed with 29 questions involving dichotomous response, Likert scale, filter and contingency and demographic questions relating to various aspects of wireless networking and security. The questions had a pre-defined set of responses from which the respondents could select the appropriate answer. Respondents voluntarily completed the survey via an invitation which was posted on various online bulletin boards, if they met the criteria of utilising a wireless network at home.

RESULTS

The online survey was accessible from 11 May 2006 to 2 June 2006, allowing a three week period for data collection. Over the twenty-one day period a total of 163 surveys were completed after the researcher removed incorrectly answered surveys.

In Table 1, the predominant type of Internet connection was Broadband which was utilised by 94.5 percent of respondents. This suggested that almost all respondents have at least 256 Kilobits of bandwidth available for exploitation by an unauthorised individual. The bandwidth provided by a broadband connection, could easily be exploited and used to download material from the Internet by an intruder. This high speed connection permits a greater bandwidth capacity than does a dialup connection. Hence, as more bandwidth is available for a bandwidth to abuse, this in turn can quickly diminish ones monthly download allowance which may incur excess use charges. Two respondents chose to not specify their gender, however the evidence suggests that there is no dominant connection type among either gender.

Table 1 Male and female respondents utilising either Broadband or Dialup

	Male	**Female**	**Unspecified**	**Total**
Broadband	119	33	2	*154*
Dialup	6	0	0	*6*
Other	2	1	0	*3*
Total	127	34	2	163

As demonstrated in Table 2 from 163 respondents who participated in the survey 52 percent have previously or are currently working within the IT industry. From the sample only 11.6 percent (19 respondents) had not successfully configured a computer network. A large majority of 88.3 percent (144 respondents) have configured a computer network successfully, and 52.1 percent (85 respondents) have worked in the IT industry. Given that 84 of respondents claimed to have worked in the IT industry and successfully configured a computer network, the expectation would be that they had a reasonably good understanding and awareness of wireless network security. However, the results indicated that this was not the case.

Table 2 Comparison of IT industry and networking experience

	Worked in IT	**Not worked in IT**
Configured network successfully	84	60
Not configured network successfully	1	18

The survey permitted the respondent to select a reason as to why they had chosen to utilise wireless networking at home. The survey provided a total of five selections for the respondents to choose from. Three reasons were given which are considered benefits of wireless network and two reasons which are not necessarily benefits in contrast to a wired Ethernet network. The majority of the sample had chosen the true benefits for choosing to use a wireless network at home as appose to Ethernet. As presented in Table 3 a minor percentage of respondents perceived speed and an easy setup process as genuine benefits of wireless networks.

Table 3 Reasons for choosing wireless amongst the sample

Reason	**Total number**	**Percentage**
Convenience	114	69.9%
No messy cables	98	60.1%
Mobility	131	80.4%
Speed	6	3.7%
Easy setup process	19	11.7%

The results in Table 3 suggest that the majority of respondents were choosing wireless networking for the true benefits of wireless networking. Individuals may choose wireless due to the benefits but may not be aware of the issues surrounding the wireless technology. When an individual endeavours to purchase wireless computing products, salespeople play a vital role in discussing the benefits and most critically the dilemmas associated with wireless networking. However, when respondents purchased their wireless computing product only 22 percent of respondents had experienced a salesperson initiate a discussion on the risks and/or countermeasures associated with wireless networking. In turn only 41 percent of respondents questioned the risks and security aspects of the wireless product they were purchasing as shown in Table 4.

Table 4 Experience when purchasing wireless networking products

Question	**Yes**	**No**
Salesperson discussed wireless security	36	127
Respondents questioned wireless security	67	96

The majority of respondents had stated that they configured their wireless network themselves. As shown in Table 5 only 6.2 percent relied upon a technician and a friend to setup the wireless network. The majority of respondents configured the wireless network themselves and hence are not leaking personal information such as keys to a third party. However, a respondent who configures the network themselves may not have the expertise or knowledge to implement quality wireless security as a skilled technician may have.

Table 5 Person who configured wireless product

Person who setup wireless product	**Number of respondents**	**Percentage**
Myself	140	86.4%
Household friend	12	7.4%
Outside friend	5	3.1%
Technician	5	3.1%

Respondents were asked what source or sources of information had been used to configure the wireless product. Prior knowledge and the vendor quick start guide were predominant selections among the sample as shown in Table 6. The ‘other’ selections were a combination of trial and error approaches, or completing a course or unit in wireless networking. Few respondents relied upon the vendor quick start guide which may have been due to difficulties in understanding the material, although this could not be determined from the answers provided by the respondent and could need to be further researched.

Table 6 Sources of information used amongst respondents

Source of information	**Number of respondents**	**Percentage**

Prior knowledge	110	67.5%
Vendor quick start guide	61	37.4%
Internet	18	11.0%
Support from friend	11	6.7%
Technician	2	1.2%
ISP Support	2	1.2%
Other	10	6.1%

As prior knowledge and the vendor provided quick start guide were the two predominant sources of information, it could imply that respondents perceived they had implemented good security methods. However, evidence from the survey indicated that this was not the case with individuals having very limited knowledge of their wireless security schemes in place. As shown by Table 6 respondents were asked to state which authentication method they were currently utilising on their wireless product. A total of 32 respondents had claimed to use either Open System or Shared Key authentication while the remainder either stated a false response (selecting both Open System and Shared Key) or stating that they do not know.

Table 7 Authentication methods used by sample

Authentication method	**Number of respondents**	**Percentage**
Open System	12	7.4%
Shared Key	20	12.2%
False Response	29	17.8%
Don’t Know	102	62.6%

Respondents did have a slightly better understanding of which encryption system they had implemented on their wireless product. Similar to the authentication method, respondents could select as little or as many responses as they deemed necessary as shown in Table 8. Over 50 percent of respondents did not know, or once again selected a false response (eg WEP and WPA/WPA-PSK simultaneously). The respondents seemed to have an unclear understanding of which encryption method was currently implemented on their wireless networking product. If respondents do not have an accurate understanding of their authentication and encryption techniques they cannot be proactive when the media discusses the flaws in various wireless security schemes.

Table 8 Encryption methods used by sample

Encryption method	**Number of respondents**	**Percentage**
WEP	36	22.1%
WPA/WPA-PSK	30	18.4%
False Response	63	38.0%

Don’t Know	34	21.5%

A home user of wireless networks who has worked in the IT industry could be expected to have an understanding and awareness of the insecurities surrounding the wireless technology. In light of this the 163 respondents were divided into two groups (referred to as A and B). Those respondents who are currently or have previously worked in the IT industry were placed in group A, while the remainder were placed in group B. Many respondents answered the authentication and encryption scheme questions by either false responses or answering that they did not know. Hence, separating respondents into two groups would determine if those working in an IT environment have a better awareness and perception of their wireless authentication and encryption methods. The two groups are outlined in Table 9 detailing the number of respondents in each:

- Group A of 84 respondents who currently or previously had worked in the IT industry.
- Group B of 79 respondents who had not worked in the IT industry at any point.

Table 9 Authentication method comparison among both groups

Authentication Method	**Group A: IT Industry**		**Group B: Non-IT Industry**	
	Number of Respondents	**Sample Percentage**	**Number of Respondents**	**Sample Percentage**
Open System	4	2.5%	8	4.9%
Shared Key	8	4.9%	12	7.4%
False Response	22	13.5%	7	4.3%
Don’t Know	50	30.7%	52	31.9%

Table 10 Encryption method comparison among both groups

Encryption Method	**Group A: IT Industry**		**Group B: Non-IT Industry**	
	Number of Respondents	**Sample Percentage**	**Number of Respondents**	**Sample Percentage**
WEP	20	12.3%	16	9.8%
WPA/WPA-PSK	21	12.9%	9	5.5%
False Response	36	22.1%	26	15.9%
Don’t Know	7	4.3%	28	17.2%

Although the evidence in Table 9 and 10 suggests that respondents are not aware of their implemented wireless security features, this does not necessarily make them susceptible to wireless networking attacks. The survey asked the respondent where they had positioned the wireless router within their home. Depending on the signal strength and antenna type, the wireless router if located at the front of the house may permit the radio waves to traverse beyond the house. As Table 11 presents the majority of respondents have situated the wireless router within the centre of the house. Hence, this could indicate that radio waves are limited in how far they may traverse beyond their property.

Table 11 Position of AP within respondents home

AP Position	**Number of respondents**	**Percentage**
Street front	22	13.6%
Side or rear of house	57	35.2%
Centre of house	83	51.2%

Respondents were presented with five 4-point Likert Scale questions to test their attitude concern towards five identified wireless security issues as discussed by Ciampa (2006). Of the 163 respondents, 158 completed all the questions. Table 12 shows that there is an almost equal low dispersion of concern among respondents towards money loss due to wireless fraud and theft of bandwidth. In contrast, respondents had higher concerns scores, towards other issues including ensuring personal data is not exposed, ensuring availability of their wireless network, and ensuring that their personal data is not exposed. The evidence suggests that respondents may believe that money loss, and bandwidth theft occur less frequently, and hence are concerned predominantly with threats which may impact them instantly. This may include their wireless access point not being available when they wish to utilise the wireless network.

Table 12 Attitude concern towards wireless security issues

Wireless Networking Issues	**Number of respondents**			
	Not concerned	Slightly	Moderately	Extremely
Money loss due to wireless fraud	48 (30%)	33 (21%)	30 (19%)	47 (30%)
Theft of bandwidth	35 (22%)	33 (21%)	47 (30%)	43 (27%)
Ensuring personal data is not exposed	23 (14%)	22 (14%)	39 (25%)	74 (47%)
Ensuring wireless is always available	7 (4%)	25 (16%)	56 (35%)	70 (45%)
Ensuring personal data is not altered	16 (10%)	22 (14%)	43 (27%)	77 (49%)

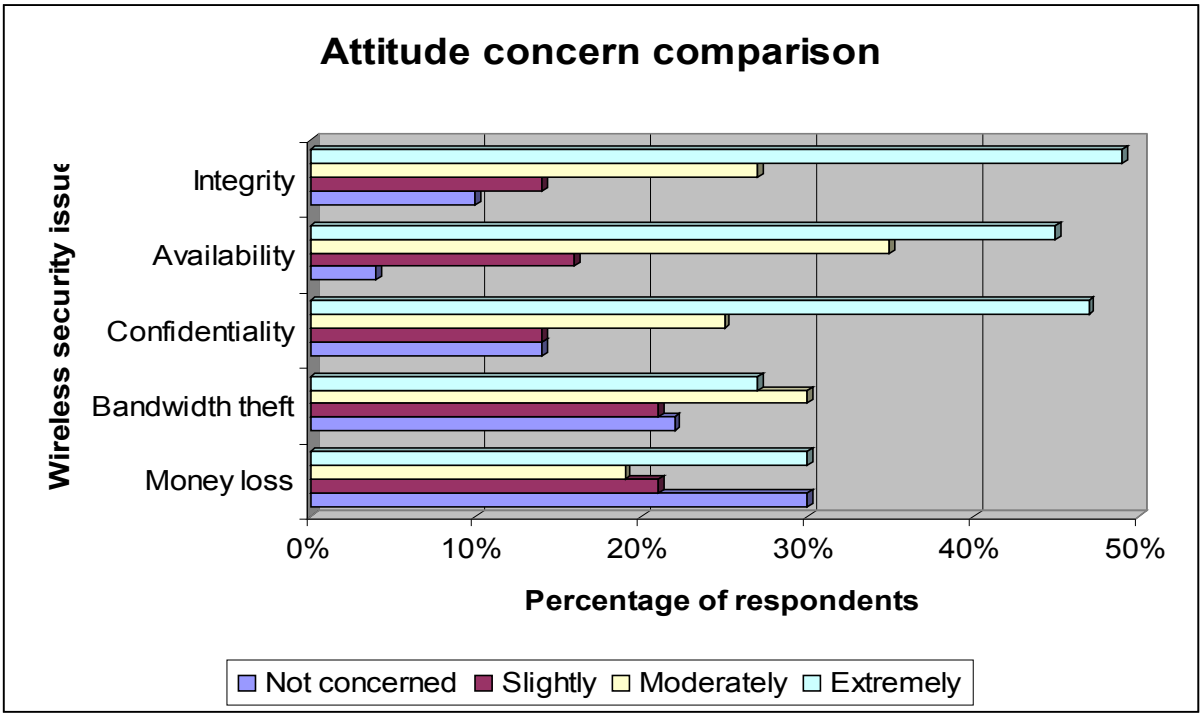

Figure 1 Attitude concern comparison

Respondents were questioned if they believed that they as a person were at risk when using wireless to access the Internet. Only 47 respondents believed they were at risk, and yet continued to utilise their wireless network. When asked how vulnerable they perceived their wireless product to be just under 50 percent thought that they were either 'extremely' or 'moderately' vulnerable. As Table 13 depicts 37 percent believed their wireless product was not at all vulnerable. If respondents do not believe their product is vulnerable then they may investigate and hence concern themselves with stronger security methods.

Table 13 Perceived vulnerability of wireless AP

Perceived vulnerability of AP	**Number of respondents**	**Percentage**
Extremely vulnerable	11	7%
Moderately vulnerable	68	42%
Not vulnerable	59	37%
Don't know	23	14%

Respondents were given the opportunity to state their experience (i.e. positive or negative) for configuring and utilising their wireless network. As Table 14 shows well over 85 percent felt that their experience was positive when using and configuring their network. Hence as the correlations between attitude and behaviour were discussed previously respondents should have had knowledge of the wireless security methods in place. However, this was not the case and may be a result of a lack of understanding due to the complexity and technicality wireless networking.

Table 14 Respondents experience configuring and using wireless networks

	Positive	Slightly Positive	Slightly Negative	Negative
Experience using	87 (54%)	60 (37%)	11 (7%)	3 (2%)
Experience configuring	83 (52%)	58 (35%)	17 (11%)	4 (2%)

CONCLUSION

The research determined the current state of wireless security within home environments through respondents' perceptions and knowledge of their wireless network. There is conflicting results where respondents do have a positive attitude however, do not have a good understanding of wireless security schemes. It appears that respondents are able to distinguish the benefits of wireless networking from the flaws. As Westen (2002, p. 594) suggested, respondents do need a good understanding of how wireless networks operating and the implications before they may proactively involve themselves in implementing quality wireless security. The research has identified that respondents do not have a good understanding of the security they have implemented which is disturbing due to the wide spread flaws of various encryption algorithms.

Further research would need to investigate the true security implemented on the wireless products by home users. If further tests do discover that in fact respondents are leaving themselves open and vulnerable to malicious attacks, appropriate actions would need to be taken to ensure individual's are not left victim to wireless crime with varying consequences. Following studies would again determine perceptions towards wireless security and compare this to the actual implemented security. This may help determine what is impacting the respondent to perceive in an incorrect manner.

REFERENCES

Burness, L., Higgins, D., Sago, A., & Thorpe, P. (2003) Wireless LANs - present and future. *BT Technology Journal, 21*(3), 32.

Ciampa, M. (2006) *CWNA guide to wireless LANs*. Boston, Mass: Thomson Course Technology.

Clyde, L. A. (2003) Wi-fi and warchalking. *Teacher Librarian, 31*(1), 44.

Eagly, A. H., & Chaiken, S. (1993) *The Psychology of Attitudes*. Orlando, FL: Harcourt Brace Jovanovich.

Fenech, S. (2006) Voila, opening the box of tricks. *The Sunday Times,* pp. 4-5.

Golmie, N., Dyck, R. E. V., Soltanian, A., Tonnerre, A., & Rebala, O. (2003) Interference Evaluation of Bluetooth and IEEE 802.11b Systems. *Wireless Networks, 9*(3), 201.

Henderson, T. (2005) Bountiful Router offers plentiful wireless range. *Network World, 22*(43), 50-52.

Peterson, B. H., Heninger, W. G., Lindstrom, C. J., & Romney, M. B. (2004) Install Your Own Wireless Network. *Journal of Accountancy, 198*(5), 51-57.

Shaw, T. (2003) Information Security Management and Small Business in Australia: Proceeding of the 1st Australian Information Security Management conference, Edith Cowan University, Perth.

Swanson, R. A., & Holton, E. F. (1999) *Results - How to Assess Performance, Learning, and Perceptions in Organisations*. San Francisco, CA: Berrett-Koehler Publishers.

Swartz, N. (2005) War on Terror Targets ISPs in Europe. *Information Management Journal, 39*(5), 10.

Webb, S. (2003) *Identifying Trends in the Deployment and Security of 802.11b Wireless Technology, in Perth, W.A.* Paper presented at the 1st Australian Computer, Information and Network Forensics Conference, Scarborough, Western Australia.

Westen, D. (2002) *Psychology - Brain, Behaviour, & Culture*. USA: John Wiley & Sons.

Woodward, A. (2005) *WPA / WPA2: Placebo or panacea?* Paper presented at the 6th Australian Information Warfare & Security conference, Deakin University, Geelong.

COPYRIGHT