Analysis of Data Remaining on Second Hand ADSL Routers

Patryk Szewczyk
secau – Security Research Centre
Edith Cowan University
Perth, Western Australia

Abstract

In theory, an ADSL router can provide an additional layer of security to a wired and wireless network through; access control, wireless encryption, firewall rule sets, and network event logging. An ADSL router may also contain the users' usage habits and broadband account credentials. However, end-users may be unaware of the intricacies of the security measures available and the potentially confidential information stored on their device. As a result a second hand ADSL router may contain a wealth of user-specific information if not wiped and disposed of in a secure manner.

This paper shows the data that was acquired from a selection of second hand ADSL routers purchased during the first quarter of 2011. From the data acquired and analysed, individuals are not removing their personally identifiable information and are leaving confidential data which may lead to detrimental outcomes if misused. The paper also shows that end-user applied security on these devices was alarmingly low. Thus many consumers may fall victim to new and emergent Internet based crimes if the full security capabilities of their ADSL router are not applied.

Keywords: ADSL router forensics, broadband router, data recovery, remnant data

1. INTRODUCTION

As of December, 2010 the Australian Bureau of Statistics (ABS, 2010) reported that there are over ten million active Internet connections in Australia. The ABS figures state that over nine million of these connections are non-dialup (ABS, 2010). The number of active broadband connections will gradually increase with the implementation of an Australian Government initiative the National Broadband Network – replacing existing copper communication lines with fibre optics. This is set to provide consumers and businesses with high-speed broadband access to ninety-three percent of Australia's population (Australian Government, 2011).

ADSL router manufactures and Internet Service Providers (ISPs) sell the ADSL routers preconfigured thus eliminating the tedious and confusing configuration process faced by novice users. This allows consumers to connect to the Internet in

a streamlined ("hassle-free setup") manner (Westnet, 2011). ADSL routers have two sets of authentication credentials. The first set of credentials includes the username and password used to access the broadband service provided by the ISP. The second set of credentials is utilized to access and configure the ADSL router. Australian ISPs may dispatch or professionally install ADSL routers and configure the ADSL router on behalf of the customer (Bigpond, 2011). Vendors on the other hand populate network or modulation settings in a manner which allows the device to be used directly out of the box. For instance, this may include enabling the wireless access point without any security such as Wired Equivalent Privacy (WEP) or Wi-Fi Protected Access (WPA), or setting the most common modulation settings for the region of use. Collectively this is eliminating the difficulties faced by novice computer users to access their network and the Internet. Consequently, if end-users are not exposed to the product literature or never configure the ADSL router themselves, then they may be unaware of its functionality and the specific personal and confidential data stored persistently on the device. This assumption is reinforced through a 2009 survey (Szewczyk & Furnell, 2009), whereby a respondent purchased a non-wireless based ADSL router as they were unaware that the wireless feature could be switched off.

A large focus of current research is centred around remanent data on hard disks, USB drives and gaming consoles sold through second hand auction websites (Jones, Valli, & Dabibi, 2009; Valli & Woodward, 2008; Xynos, Harries, Sutherland, Davies, & Blyth, 2010). This previous research has identified a continuous trend in sellers leaving confidential data on the devices intact. In a few rare occurrences sellers format the storage media, but do not use an appropriate method by which to wipe or destroy the data permanently (Jones, et al., 2009).

An ADSL router when compared to a modern computer system contains limited volatile and non-volatile storage. Any specific user activities such as browsing habits are stored in the volatile Random Access Memory (RAM). The device is disconnected from the wall power outlet during the sale process and as a result volatile data is lost and cannot be retrieved at a later date. However, the ADSL router's non-volatile storage contains account authentication credentials, pre-configured data for accessing remote network services and security settings. In addition had the device been compromised through malware specimens inclusive of psyb0t or the Chuck Norris Botnet (Bridges, 2008; Symantec, 2009) this would result in static changes to the configuration data which will remain present in non-volatile storage when the device is powered down (Čeleda, Krejčí, Vykopal, & Drašar, 2010).

The discipline of ADSL router forensics and data acquisition from these devices still remains in its infancy. Unlike a hard disk or a USB storage device, there is limited storage space available to store confidential information. In most instances the persistent storage capacity of an ADSL router will range from 1-8MiB. However, this is not to say that interest in the area is not growing. Recently the

United States National Institute of Justice developed the first commercial ADSL router forensics software namely Router Marshal (ATC-NY, 2010). Router Marshal whilst mimicking the author's procedures and methods used in this paper, is only available to a subset of law enforcement agencies in the United States of America upon a special request.

2. ADSL ROUTER INVESTIGATION

To gain a perspective of the level of sensitive information, and the security state of the second hand devices, a series of questions were formulated. The first question "*Do second hand ADSL routers contain user specific information?*" was centred on discovering whether or not an end-user would sell a device with user-specific information intact. No incentives or explanations detailing how or why to remove personal information currently exist. As a result it is expected that the devices will contain confidential data overlooked by the seller prior to shipping.

The second question "*Are second hand ADSL routers utilizing a recent firmware image?*" is based on the prevalent threat of end-users not updating their firmware. This may result in the device being susceptible to emergent malware specimens which exploit the vulnerabilities of the operating system (Baume, 2009; Čeleda, et al., 2010). End-users may continue utilizing the default firmware on the ADSL router that was present when the device was purchased. Alternatively, an end-user who is aware of the reason for updating the firmware and understands the procedure may then update the firmware.

Implementing effective security controls and safeguards onto a workstation is a complicated task for many individuals due to the usability constraints of security software (Ibrahim, Furnell, Papadaki, & Clarke, 2010). An ADSL router has the capability of providing various layers of defence. Specifically, the device can incorporate numerous wireless encryption protocols, denial of service prevention through firewall rule sets, and network logging for review or analysis of network events. In addition, the device can be configured to filter traffic according to internal or external IP addresses and ports, or specific Uniform Resource Locators (URLs). As a result the third question "*To what extent is the ADSL router secured?*" is aimed at identifying what security approaches end-users utilize on their device.

The author's research to date, has predominantly focused on the development of a sound approach into acquiring data of interest from Australian based ADSL routers (Szewczyk, 2009a, 2009b). Subsequently, this same approach and specifically the SSH and Serial Console methods were utilized in this experiment. As each device was purchased and received, it was then disassembled to view and determine which connection point would be utilized to acquire data. The connection point deemed appropriate was chosen based upon accessibility and the feasibility of soldering on a pin header without unnecessarily damaging the device. The appropriate cable (Szewczyk, 2009b) was subsequently attached to each ADSL router and a series of command line arguments and software were

initiated to begin the transfer of data to a host workstation. The subsequent images which were extracted from each device were carved using a hexadecimal editor as per the method demonstrated by Szewczyk (2009a). The resultant ADSL router image is viewed via an XML style sheet for simple data interpretation.

Each device was purchased from the second hand auction site - eBay Australia. For the purpose of this research a second hand ADSL router constitutes a device in which the seller on eBay claims that it has been used previously. This was undertaken by narrowing down eBay results according to the *condition* category of either *used* or *refurbished*. The selection of ADSL routers was biased in that purchases were made over a thirty day period (January through to February, 2011) and limited to the home or small business array of devices. This approach was selected in that a subsequent study would be undertaken on the high-end range of ADSL routers which contained server and multimedia capabilities at a later date.

An initial outcome of the study was the lack of ADSL routers available on the second hand auction site eBay. The price of many ADSL routers has decreased over the years and consumers are now able to purchase devices with newer and advanced features such as the inclusion of 802.11n Wi-Fi or an inbuilt media server (D-Link, 2011). As a result there appears to be little incentive for an individual to purchase a second hand device which could be deterring sellers from auctioning their used device on eBay. Over the thirty day period it was evident that D-Link and Netgear were the predominant ADSL routers available. This could be influenced by many Australian retail outlets predominantly selling these brands. At the conclusion of the purchasing period, a total of twenty-three devices were obtained from the manufactures; D-Link, Netgear, and 2Wire (which is sold by Australia's ISP – Bigpond. Table 1 in the discussion section lists the make and model of the devices purchased.

3. RESEARCH RESULTS

The following data presents the findings for the study of twenty-three ADSL routers obtained from second hand auction site. Data could be successfully acquired from twenty-two devices corresponding to a ninety-six percent success rate. One ADSL router was damaged. This was known to the researcher upon the time of sale. However, an attempt to recover data was still made although unsuccessful. After a careful examination it appeared that the device had suffered an electrical shock resulting in various capacitors and memory chips being damaged.

Two of the twenty-three devices had been reset to their factory default state (presumably by the seller) resulting in no individual data being available to extract and analyse. Factory resetting the device can be achieved by loading the default vendor configuration values via a script obtainable through the vendor website. Alternatively, the user may physically reset the device by the switch located at the back of the device. This results in the configuration partition of non-volatile flash memory being overwritten with the vendor default values – located

in a separate flash partition (OpenWRT, 2010).

Three of the ADSL routers had partial data removed. In this instance the broadband authentication credentials consisting of the username and password could not be located. Upon investigation it appeared that the seller or previous owner may have manually deleted the data, and permanently committed the changes to non-volatile storage.

Fifteen of the ADSL routers had all their data intact. In these specific instances broadband authentication credentials and resultant passwords were still present. In addition, nine of these fifteen devices (sixty percent) incorporated a wireless access point, in which all wireless related information was present.

Two of the ADSL routers were non acquirable due to access point constraints. In this instance the D-Link DSL-200 device does not encompass on chip access points to acquire data from the device. An invasive HTTP approach was utilized, although the devices had been password protected. The process of factory resetting the device was used which permitted the default username and password to be used, granting access to the device. Figure 1 presents an overview of the devices which were acquirable and had recoverable data pertinent to this study.

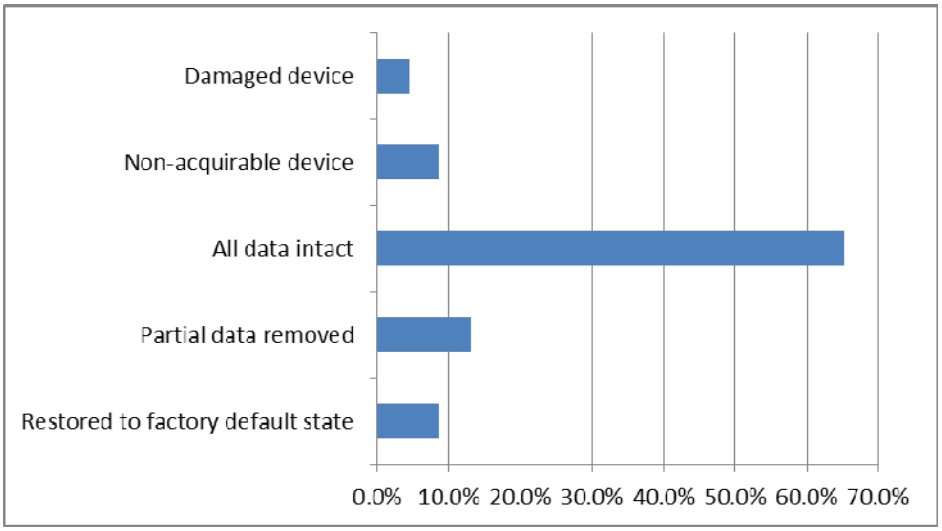

Figure 1 Percentage comparison of obtainable information

There is insufficient data to develop definitive trends and draw conclusions. However, from the sample examined it does appear that individuals and commercial entities are selling ADSL routers with information that would be misused if made available to the wrong parties. In three instances it was identified that the owner had logged into the device and manually removed broadband authentication credentials.

A depiction of data which appeared more prominent from a security perspective

has been presented below:

- Two devices, specifically the D-Link DSL-2730 had its firmware updated to the latest July, 2010 version. In the worst instance, one device (Netgear DG834g) was using firmware from 2006 even though significant updates had been made available from the manufacturer's website. The remaining nineteen devices were utilizing firmware from either 2007 or 2008.
- Fifteen devices had their broadband service credentials present. It could be possible that the seller altered or used fictitious data prior to selling the device. However, in each instance the username was in the format of *username@isp.com.au* or *username@isp.net.au* and clearly reflected an Australian based ISP. This was further coupled with the password associated with the broadband service which was available in clear text.
- One device had its device access authentication credentials strengthened. In this instance the password selected was eleven characters long and made up of alphanumeric characters. The remaining devices were using the default usernames and passwords implemented by the manufacturer.
- One device had its firewall disabled with specific rule sets de-selected. Two of the devices namely the D-Link DSL-200 do not encompass any firewall blocking feature.
- Four ADSL routers had the name of a business used as the SSID which was further validated as a business via the World Wide Web (WWW). The SSID had a similar name to the username used as part of the credentials required to access the broadband service. In addition the business premises clearly resided in the Australian state the product was sold from.
- Nine devices had a wireless access point which was enabled. One device was utilizing WPA security and Media Access Control (MAC) filtering. Two devices were using WEP. The remaining six devices had an open connection.
- The peer-to-peer file sharing protocol BitTorrent was a common trait amongst eleven devices. This was evident through the rule sets and ports mimicking torrent clients. Two devices had Remote Management enabled to a predefined Internet Protocol (IP) address. Specifically Web and Telnet were selected.

- Two of the business based devices were utilizing Dynamic Domain Name System (DynDNS). In each instance the user configuration data consisting of account username and password were clearly intact and acquirable from the device.
- Twenty ADSL routers encompassed the network logging and notification feature. However, none of these devices had any of these features enabled.

Table 1 depicts an overall summary of the devices utilized in the study, and the corresponding points of interest that were notable amongst the data that was analysed. The areas shaded represents devices which did not encompass a wireless access point and resultantly do not apply to the categories used.

Table 1 ADSL Router Information of Interest

Make Model	Broadband Credentials	Default Device Credentials	Most Recent Firmware	Firewall Enabled	Allow Remote Management	Wireless Access Point Enabled	Wireless Keys 1-WEP 2-WPA	Network Logging
D-Link DSL-2730B	✔		✔	✔		✔		
D-Link DSL-2730B		✔	✔	✔		✔	1	
D-Link DSL-G604T	✔	✔		✔	✔	✔	2	
D-Link DSL-G604T	✔	✔		✔		✔		
D-Link DSL-G604T	✔	✔				✔		
D-Link DSL-G604T	✔	✔		✔		✔		
Netgear DG834g	✔	✔		✔		✔	2	
Netgear DG834g	✔	✔		✔		✔		
Netgear DG834g	✔	✔		✔		✔		
D-Link DSL-504T	✔	✔		✔	✔			
D-Link DSL-504T	✔	✔		✔				
D-Link DSL-504T	✔	✔		✔				
D-Link DSL-502	✔	✔		✔				
D-Link DSL-502		✔		✔				
D-Link DSL-302	✔	✔		✔				
Netgear DG834	✔	✔		✔	✔			
Netgear DG834	✔	✔		✔				
Netgear DG834		✔		✔				
Netgear DG834		✔		✔				
2Wire 2071-A		✔		✔				
2Wire 2071-A		✔		✔				
D-Link DSL-200								
D-Link DSL-200								

4. DISCUSSION

In 2008, it was identified that the number of second hand disks being securely wiped was marginally increasing compared to previous years (Valli & Woodward, 2008). This could be due to the publicity and media coverage (Moscaritolo, 2010) given to individuals who dispose of magnetic media in an insecure manner. Furthermore, there is a significant array of commercial and freely available tools to securely wipe hard disks (Caloyannides, 2009). As a result, an end-user does have means by which to eliminate confidential data should they wish to do so.

From a mobile phone perspective, second hand auction sites continue emphasising to sellers that personal data should be removed from their electronic device prior to shipping the item (eBay, 2011). This process works as an education and awareness approach, and in-turn, individuals are at the very least informed of the possibility of someone obtaining their confidential information. Similar information and tutorials can be obtained by end-users who search the Internet as to how to prepare a mobile phone or similar electronic devices prior to sale and in-turn can follow step-by-step procedures. Tools which can erase data from hard disks are not compatible with ADSL routers. Subsequently, there are currently no specifically made tools by which to quickly and easily erase data securely from ADSL routers. Furthermore, search engines do not currently yield any supportive information or instruction on the topic.

4.1 User Specific Information

In answering the first question in this study, ADSL routers do contain user specific information. One of the main results from this investigation is associated with broadband authentication credentials remaining on the device after a sale. The value of a password is high in that end-users often recycle passwords for numerous accounts (Notoatmodjo & Thomborson, 2009) and rarely change their online passwords (Hart, 2008). This creates two significant issues. Firstly, having acquired this data, an individual with malicious intent could misuse the broadband account and its associated features. More importantly, this data can be utilized to access the broadband account through the respective online portal. Broadband accounts are usually populated with a wealth of user related information. This may include the owner's name, an address, but more crucially direct debit and credit card information.

In two of the devices obtained, the data shows that the entity previously utilizing the device was in fact an organisation. This was evident through the SSID which clearly contained the name of the company. Furthermore, the broadband authentication credentials (username and password) coincided with SSID.

4.2 Firmware Currency

The second research question dealt with the currency of the firmware on the ADSL router. The outdated firmware on many of the devices can be problematic for end-users. Many ADSL routers can be exploited as a result of vulnerabilities in the operating system. For instance the first generation Netcomm routers encompassed an operating system flaw by which an individual who had administrator privileges could remotely access the device (Baume, 2009; Bridges, 2008). The firmware was severely outdated on all but two of the devices used in this study.

A potential reason for the lack of firmware updates could be a result of no actual enforcement to the end-user. On a Microsoft Windows workstation the end-user may configure how updates are downloaded and installed for the operating system. The default option being for any available updates to be automatically downloaded and installed, although the end-user may also disable this entirely (Gerace & Cavusoglu, 2009). Such a feature is not available on current ADSL routers. In addition, manufacturers have not implemented a means by which to inform users that a critical firmware update has been made available.

The issue of ensuring end-users update their firmware can be rectified in a simple manner. The manufacturer Quality Network Appliance Provider (QNAP) incorporates a feature within its devices which notifies the end-user when a firmware update is available. This is achieved via a notification window when the end-user logs in to configure the device. However, many end-users may follow a "setup-and-forget" approach meaning there is no reason to access the configuration options on a regular basis. However, QNAP also developed a solution for this issue via the QNAP Finder (QNAP, 2011). The QNAP Finder is a Windows application that allows an end-user to quickly check and apply any firmware update that becomes available. Similar processes can be applied to ADSL routers which in-turn would safeguard end-users confidential information, and prevent the device from being compromised due to existing vulnerabilities.

4.3 ADSL Router Security

Changing the default username and password utilized to access the ADSL router would seem obvious and a simple security solution. However, an end-user would need to be informed of the process and aware of the reason of doing so. Malware such as psyb0t is specifically exploiting devices which utilize default vendor based usernames and passwords (Baume, 2009; Symantec, 2009).

Based on the results from this study, end-users are failing to make their devices secure. This may be associated with product literature supplied with ADSL routers that does not adequately encourage or provide information on how end-users should change the default settings (Szewczyk & Valli, 2009). Based on the results of this study alone it would appear that vendors must take greater initiative

to promote and encourage end-users to secure their devices. In-turn consumers must also be responsible for proactively identifying the available security methods for their device and applying these when and where appropriate.

Of all security settings present on the devices, it was expected that wireless networking would at the very minimum incorporate secure protocols. Television and print media have continued to report on wireless threats and promoted good wireless security practices (Seymour, 2010; Sinclair, 2010). As a result, it was anticipated the devices sold would be at the very least use some form of wireless security with a larger emphasis on WPA which is more secure than WEP (Lashkari, Mansoor, & Danesh, 2009). This was not the case. Most wireless access points were utilizing an unprotected *open* based connection which is usually the default settings on many ADSL routers.

4.4 Secure Disposal Strategies

Education and awareness of remanent data of electronic media must be addressed. Deciding who specifically is responsible for informing end-users about security and proper disposal of data is a separate and debatable issue beyond the scope of this paper. However, as newer networking devices incorporate a much more sophisticated array of features then similar issues may arise as are common with the disposal of hard drives. The D-Link DIR-685 for instance incorporates; a four port switch, a wireless access point, network attached storage, multimedia sharing capabilities, printer and media server (D-Link, 2011). In-turn such advanced functionality will permit different forms of data of interest to be acquired and subsequently used in a court of law.

A solution to mitigate the issue of end-users disposing of their ADSL router with confidential data intact would be for the news and media to continually highlight the security risks of selling of alternative electronic products. The same ongoing approaches (Moscaritolo, 2010) used to show what is being thrown out on hard disks and USB drives, could also be applied to ADSL routers thus raising awareness amongst ignorant end-users.

The second hand auction site eBay could take greater initiative to educate and make end-users aware of the privacy risks associated with selling electronic products. Currently eBay provides warnings to end-users whom sell devices such as mobile phones or computers (eBay, 2011). In these warnings end-users are instructed to remove personal and confidential information before shipping the item. However, in 2011, eBay Australia does not provide any warning or notification about removing private data when listing an ADSL router for sale. Incorporating clear notifications could prove highly successful. End-users could be deterred from selling their second hand ADSL router knowing that there is a possibility that personal data could be extracted.

To date each vendor releases a configuration quick start guide and a detailed manual. Although neither meets any specific standard (Szewczyk & Valli, 2009)

it does seem that vendors should be encouraged to release security guides. Briefly detailing potential attacks and simple solutions may not only make consumers aware, but could also be utilized to showcase the security features of the device itself. Further education should be provided to end-users. In the manuals supplied with the ADSL routers, there is no evidence of the vendors providing details regarding how to dispose of the device in a secure manner.

Restoring factory default settings is a feature hidden away in configuration or settings component of ADSL routers. End-users should be further made aware of the reason and necessity of utilizing this function. Alternatively, end-users may also undertake a *hard restore* via the reset/restore switch located on the device. Unfortunately, this switch is not always accessible with some instances showing the switch being located within the actual device post disassembly.

5. CONCLUSION

ADSL routers have not yet grown to their full maturity. As consumers continue to adopt broadband, the demand for greater functionality shall also increase. As shown in this study, it is evident that end-user do sell their ADSL router, with plenty of useful information in-tact. As these devices become network media centres, the interest in the remanent data may also increase. Education and awareness must be provided and emphasised immediately, to prevent these simple devices from leaking confidential data into the public realm.

Future studies will specifically analyse a larger sample size over a twelve month period, incorporating both home and small business based ADSL routers, and the more high-end multimedia capable devices. This initial study has also identified potential projects into exploring approaches that could be utilized to educate end-users, install firmware updates autonomously, and applying security which meets current best practices.

REFERENCES

ABS. (2010). Internet Activity, Australia, Dec 2010. Retrieved July 8, 2011, from http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/

ATC-NY. (2010). Router Marshal. Retrieved December 29, 2010, from http://routermarshal.atc-nycorp.com/index.php/about

Australian Government. (2011). What is the National Broadband Network. Retrieved April 22, 2011, from http://www.nbn.gov.au/content/what-national-broadband-network

Baume, T. (2009). Netcomm NB5 Botnet – PSYB0T 2.5L. Retrieved September 10, 2009, from http://users.adam.com.au/bogaurd/PSYB0T.pdf

Bigpond. (2011). Home Broadband. Retrieved July 8, 2011, from http://go.bigpond.com/broadband/setup/

Bridges, L. (2008). The changing face of malware. *Network Security, 2008*(1), 17-20.

Caloyannides, M. A. (2009). Forensics Is So "Yesterday". *Security & Privacy, 7*(2), 18-25.

Čeleda, P., Krejčí, R., Vykopal, J., & Drašar, M. (2010). *Embedded Malware - An Analysis of the Chuck Norris Botnet* Paper presented at the 2010 European Conference on Computer Network Defense (EC2ND), Technische Universität Berlin, Germany.

D-Link. (2011). D-Link Xtreme N Storage Router. Retrieved December 6, 2010, from http://files.dlink.com.au/products/DIR-685/Datasheet/DIR-685_A1_datasheet_02.pdf

eBay. (2011). Advice for selling mobiles phones sasfely on eBay. Retrieved January 20, 2011, from http://pages.ebay.co.uk/buy/guides/mobile-phone-advice/#1

Gerace, T., & Cavusoglu, H. (2009). The critical elements of the patch management process. *Communications of the ACM, 52*(8), 117-121.

Hart, D. (2008). Attitudes and Practices of Students Towards Password Security. *Journal of Computer Sciences in Colleges, 23*(5), 169-174.

Ibrahim, T., Furnell, S., Papadaki, M., & Clarke, N. (2010). *Assessing the Usability of End-User Security Software.* Paper presented at the 7th International Conference on Trust, Privacy & Security in Digital Business, University of Deusto, Bilbao, Spain.

Jones, A., Valli, C., & Dabibi, G. (2009). *The 2009 Analysis of Information Remaining on USB Storage Devices Offered for Sale on the Second Hand Market.* Paper presented at the 7th Australian Digital Forensics Conference, Edith Cowan University, Perth, Western Australia.

Lashkari, A. H., Mansoor, M., & Danesh, A. S. (2009). *Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA).* Paper presented at the 2009 International Conference on Signal Processing Systems, Singapore.

Moscaritolo, M. (2010). Security risk to office equipment disposal. Retrieved April 22, 2011, from http://www.adelaidenow.com.au/business/security-risk-to-office-equipment-disposal/story-e6fredj3-1225877502647

Notoatmodjo, G., & Thomborson, C. (2009). *Passwords and Perceptions.* Paper presented at the 7th Australasian Information Security Conference, Wellington, New Zealand.

OpenWRT. (2010). D-Link DSL G604t ADSL 2/2+ Wireless Router. Retrieved July 9, 2011, from http://wiki.openwrt.org/inbox/dsl-g604t

QNAP. (2011). QNAP Finder for Windows. Retrieved April 10, 2011, from http://www.qnap.com/download_description.asp?pl=1&p_mn=135&d_id=76263

Seymour, B. (2010). Drive-by-hackers. Retrieved May 10, 2011, from http://au.todaytonight.yahoo.com/article/7907101/consumer/drive-hackers

Sinclair, L. (2010). Half of home wi-fi 'can be hacked in under five seconds'. Retrieved March 21, 2011, from http://www.theaustralian.com.au/news/world/half-of-home-wi-fi-can-be-hacked-in-under-five-seconds/story-fn3dxix6-1225938812124

Symantec. (2009). Linux.Psybot—Is Your Router Secure? Retrieved March 2, 2010, from http://www.symantec.com/connect/blogs/linuxpsybot-your-router-secure

Szewczyk, P. (2009a). *ADSL Router Forensics Part 2: Acquiring Evidence.* Paper presented at the 7th Australian Digital Forensics Conference, Kings Hotel, Perth, Western Australia.

Szewczyk, P. (2009b). ADSL Router Forensics: Methods of Acquisition. *Journal of Network Forensics, 1*(1), 16-29.

Szewczyk, P., & Furnell, S. (2009). *Assessing the online security awareness of Australian Internet users.* Paper presented at the 8th Annual Security Conference, Las Vegas, NV.

Szewczyk, P., & Valli, C. (2009). Insecurity by Obscurity: A Review of SoHo Router Literature from a Network Security Perspective. *Journal of Digital Forensics, Security and Law, 4*(3), 5-16.

Valli, C., & Woodward, A. (2008). *The 2008 Australian study of remnant data contained on 2nd hand hard disk: the saga continues.* Paper presented at the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth, Western Australia.

Westnet. (2011). Westnet Broadband Hardware. Retrieved July 8, 2011, from http://www.westnet.com.au/hardware-and-software/broadband-hardware.html

Xynos, K., Harries, S., Sutherland, I., Davies, G., & Blyth, A. (2010). Xbox 360: A digital forensic investigation of the hard disk drive. *Digital Investigation, 6*(2010), 104-111.