1-1-2011

Insecurity by obscurity continues: are ADSL router manuals putting end-users at risk

Kim Andersson
Edith Cowan University

Patryk Szewczyk
Edith Cowan University

DOI: 10.4225/75/57b52975cd8b4
9th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

INSECURITY BY OBSCURITY CONTINUES: ARE ADSL ROUTER MANUALS PUTTING END-USERS AT RISK

Kim Andersson, Patryk Szewczyk
secau Security Research Centre, School of Computer and Security Science,
Edith Cowan University, Perth, Western Australia
p.szewczyk@ecu.edu.au

Abstract

The quantity and sophistication of threats targeting ADSL routers is on a steady increase. There is a reliance on end-users to ensure that their ADSL router is secure by continually updating the firmware, using strong authentication credentials, and enabling the in-built firewall. However, to do this, the end-user must be presented with well written procedural instructions, and an explanation of why this is important. This paper examines the design quality and security content provided by vendors in ADSL router manuals. This paper reveals that the lack of security related content and poor overall design could impact on end-users' interpretation and willingness to implement security controls on their ADSL router.

Keywords
ADSL router; manuals; quick start guide; network security; wireless

INTRODUCTION

The Australian Bureau of Statistics (ABS, 2010) reported that there are over ten million active Internet connections in Australia as of December, 2010. The ABS figures state that over nine million of these connections are non-dialup (ABS, 2010). The number of active broadband connections may gradually increase with the implementation of the Australian Government initiative, the National Broadband Network (NBN). The NBN will allow all Australian premises to access a high-speed Internet connection, either through fibre optic cabling, or fixed wireless technologies (DBCDE, 2011). Unfortunately, with the growing number of broadband services being created, there is a greater incentive for individuals to purposefully compromise Asymmetric Digital Subscriber Line (ADSL) routers. An ADSL router in the context of this paper is an embedded system, used by computer networks within Small office Home office (SoHo) environments, and may encompass an Ethernet switch, a wireless access point and an in-built modem. With the appropriate configuration an ADSL router may provide security to its local clients through an in-built firewall, wireless encryption, access control, content filtering and network address translation (NAT).

The default firmware of many first generation Netcomm ADSL routers encompassed a web server flaw which permitted the device to be accessed, compromised and controlled remotely (Sajdak, 2009). In the first quarter of 2009, Psyb0t a new form of malware had been detected worldwide which was specifically targeting MIPS architecture - Linux based, ADSL routers (Baume, 2009). Psyb0t hijacked consumer grade ADSL routers for the purposes of creating a botnet (Hunt, 2009). Psyb0t was capable of infecting approximately fifty-five types of ADSL routers and was pre-populated with approximately six-thousand usernames, and thirteen-thousand passwords (Magnus & Gassmann, 2009; Sajdak, 2009). This threat may have been mitigated through a firmware update and by changing the default authentication credentials.

The Chuck Norris Botnet exploited vulnerable ADSL routers which encompassed outdated firmware, coupled with default and/or weak, username and password combinations (Celeda, Krejci, Vykopal, & Drasar, 2010). In 2011, Trend Micro reported on an ELF_TSUNAMI malware specimen targeting D-Link devices that not only attempted to control an ADSL router, but also had the capabilities to reset the router's configuration, allowing anyone to access and control the device (Mendoza, 2011). The attacks on ADSL routers do not cease to exist with malware. Television media continues to portray the dangers of using unsecured wireless networks (Seymour, 2010). The issue of vulnerable wireless networks has been an ongoing issue with many end-users unaware of the technical aspects of their ADSL router or the need for security (Reznik et al., 2011). In a recent war-driving study (Mousionis, Vakaloudis, & Hilas, 2011) many wireless networks were found to be open or using weak, Wired Equivalent Privacy (WEP) as their main form of security (Mousionis et al., 2011). Attackers

may need little skill in breaking into wireless networks with authentication credentials and wireless keys easy to locate throughout the Internet.

Two factors may influence end-users willingness to apply appropriate security to their ADSL router. Firstly, the end-user must be aware of the risks and the potential outcomes if sufficient security is not applied. Secondly, end-users must have the appropriate supporting step-by-step literature to guide them through the process. Television, print and online media continue to promote the ease by which an individual could break into a wireless network and access or steal data (Seymour, 2010) thus making end-users aware of the risks. To compliment the awareness of risks, ADSL router manuals should actively promote good security practices to ensure that such crimes are mitigated. End-users believe that once an ADSL router is functioning properly that it no longer needs to be reconfigured or modified in the future (Szewczyk, 2006). Hence, there is significant value in vendors encouraging end-users to securely configure the ADSL router upon its initial setup. There is the option of venturing on to the vendors website, or accessing security information through media sources such as YouTube. However, end-users will rarely revisit the configuration options of their ADSL router once the device is functioning appropriately (Szewczyk, 2006).

Johnson (1995, p.409) explains how computer manuals are generally not written to be understood by novice end-users. The end-user is often faced with the problem of finding information which is scattered throughout a complex document. A longitudinal study between 2005 and 2009 discovered that many ADSL router manuals were of very low quality and did not prioritise or enforce security to the end-user (Szewczyk & Valli, 2009). This paper evaluates the ADSL router literature supplied by vendors in 2011. This study aims to determine if improvements have been made, in terms of the design quality of the manual and the enforcement or recommendations towards security.

METHOD

Manuals should conform to a standard that allows end-users with varying technical competencies to use and understand the set of procedures. Wieringa, Moore and Barnes (1993, p.3) suggest that a well designed manual will include; a well written set of procedures, information on the most effective way of completing a task, and be suitable for both a skilled and novice user. Perelman, Paradis and Barret (1998, p.148) assert that five criteria should be embedded in all high quality procedural literature. A technical manual should;

1. Incorporate descriptive page headers, an index page and a table of contents.
2. Outline the reasons for its creation, the intended audience, and required level of expertise.
3. Include a detailed glossary to elaborate on uncommon terminology.
4. Make use of white space to enhance presentation quality.
5. Use numerous large labelled graphics, clearly depicting each step in the procedure.

The way in which procedures are written by vendors in manuals may also have significant impact on its interpretation. Studies have shown that in many instances professional documents written by governments and commercial entities often exceed the literacy levels of the target audience (Mueller, Reid, & Mueller, 2010; Paz, Liu, Fongwa, Morales, & Hays, 2009). A common method to evaluate the readability of literature is through the Gunning Fog Index – which measures the required literacy level based on, sentence length and occurrence of multi-syllable words (Williams-Jones & MacDonald, 2008). The Gunning Fog index is commonly targeted at health publications however, the Linsear Write readability formula can address such issues as the algorithm has been specifically designed to calculate the readability of technical manuals (Christensen, 2007). The Linsear Write formula may be used to assess and alter a text prior to its public release, ensuring that the target audience may understand the literature.

From an ADSL router perspective the security features that a novice end-user could utilise effectively are quite limited. However, there are still sufficient mechanisms available to reduce the risk of the device being compromised. As a result, an ADSL router manual should recommend that the default password (and username if possible) be changed, whilst making suggestions for good password creation. The manual should in-turn detail the security benefits of checking and updating the firmware on a regular basis as this would mitigate many firmware specific issues that current malware is exploiting. The in-built firewall if turned on may reduce many network threats. The manual should recommend that Wi-Fi Protected Access (WPA) is used rather than Wired

Equivalent Privacy (WEP) or an open network to prevent unauthorised access. Media Access Control addresses filtering and disabling of SSID broadcasting can limit the exposure and vulnerability of the wireless network to outside intruders. Additional devices such as a wireless printer are beyond the scope of this paper and are not considered in the overall security state of the ADSL router.

Each manual was evaluated according to three separate criterions. Firstly, an analysis was made to determine how closely it follows or conforms to the five guiding criteria for procedural technical manuals. Secondly, the Linsear Write formula was applied to the Introduction of each manual to determine the literacy level required to understand the opening comments by the vendor using the free online Readability Formula (Byline Media, 2011). Lastly, the manual was evaluated according to the quality of the security recommendations made by the vendor.

A simple survey approach was utilised to identify which devices the large and small retail outlets in Western Australia were currently selling. The devices selected were those offered by retail outlets across Western Australia, and provided by Internet Service Providers' when a consumer adopts a new broadband service. The ADSL routers selected and the subsequent manuals included;

6. Billion 7800N (Billion, 2010)
7. Netgear DGN 1000 (Netgear, 2011)
8. D-Link DSL-2740B (D-Link, 2011)
9. Netcomm NB6 (Netcomm, 2010)
10. TP-Link TD-W8151N (TP-Link, 2011)
11. Belkin F7D1401 (Belkin, 2011)

EVALUATION OF MANUALS

A notable characteristic amongst the manuals was the required literacy skills. Using the introductory or overview page as a basis the content was analysed with the results shown in Table 1. The Linsear Write scores, with the exception of two manuals sit within the value of fourteen. This signifies a score which requires a level of literacy far beyond that of a high school education, generally targeting those with a tertiary education. Belkin wrote its information in a very basic format, allowing end-users to be presented with the relevant information without needing to read paragraphs of complicated text.

Table 1 Linsear Write Manual Readability Scores

Vendor Manual	Linsear Write Readability Score
Billion 7800N	14.2
Netgear DGN 1000	15.3
D-Link DSL-2740B	13.5
Netcomm NB6	14.6
TP-Link TD-W8151N	9.4
Belkin F7D1401	4.7

Overall the quality of the product manuals examined was far from impressive as demonstrated in Table 2. In the previous study, (Szewczyk & Valli, 2009) Netgear presented a manual of much higher quality compared to its competitors. This trend continued amongst the manuals examined in this study. Netgear still continued to include vital elements to make the procedural manual simple and effective to use by novice end-users.

All of the product manuals included a contents page which clearly reflected the content of the entire document. However, for a novice user, the clarity could have been improved by using less technical (computer jargon) words. A glossary of terms could be considered essential in computing due to the high number of technical words and acronyms. However, many of the manuals did not include any glossary. Specifically, many of the manuals discuss and use complicated words with the presumptions that the end-user would already be familiar with the concepts. Netcomm provided an online means by which an end-user could locate the meaning of

computer based terminology. However, this provides little help for an individual who cannot access the Internet as a result of not understanding complicated technical words.

An index page was only provided by Netgear and Netcomm. This is unfortunate seeing as an index page is as an easy and time efficient approach to finding relevant information on a given topic. The lack of an index page coupled with a confusing table of contents may result in an end-user needing to read the entire manual in order to locate a desirable topic. This unfortunately contradicts rationale human behaviour. Schriver (1997) identified that very few individuals would ever read a procedural product manual from beginning to end. As a result, end-users could reasonably be expected to overlook critical security elements for use with the ADSL router.

Table 2 Comparison and Contrast of Product Literature Design

	Billion	Netgear	D-Link	Netcomm	TP-Link	Belkin
Descriptive Page Headers		✔	✔			✔
Contents Page	✔	✔	✔	✔	✔	✔
Index Page		✔		✔		
Detailed Glossary				✔		
Professional Layout	✔	✔	✔		✔	✔
Large and Clear Graphics	✔		✔		✔	✔
Description of Graphics		✔				
Explanation of Intended Audience				✔		

In the previous study, there was a small improvement by vendors in encouraging end-users to implement good security practices as the years progressed (Szewczyk & Valli, 2009). Unfortunately, it appears that vendors have gone backwards in encouraging the use of security as shown in Table 2. Belkin in particular did not encourage end-users to implement any specific security and appeared to present it as a deterrent. This may have been due to the very small manual size of thirty pages. Billion and TP-Link had manual sizes near one-hundred pages yet still failed to encourage end-users to implement sufficient security. Unfortunately some of the vendors further discouraged end-users from securing their product. As demonstrated through the quote below, TP-Link only recommended that the firmware be updated if the end-user is experiencing difficulties. It could be difficult to determine if an ADSL router is misbehaving due to the sophistication of current malware.

"If the router is not experiencing difficulties, there is no need to download a more recent firmware version, unless the version has a new feature that you want to use."

D-Link does make an attempt to encourage that end-users implement security, especially from a wireless perspective. Unfortunately, nowhere in the product manual does it explicitly give recommendations or advice in terms of what would be most beneficial. Billion did provide a detailed outline of every possible security control that an end-user could implement.

Overall Netgear, was most influential in providing security recommendations. For instance, when choosing a password, Netgear clearly states that dictionary words from any language should be omitted, and that numbers, symbols, uppercase, and lowercase characters should be used. Netgear further depicted the dangers with end-users utilising wireless networks and provided a clear contrast of the merits and disadvantages of using a wireless network. To further mitigate the issue of end-users failing to update their firmware, Netgear has incorporated and explained the automatic update checker on the device. In this instance, a clear explanation has been provided detailing the security risks of not updating the firmware coupled with encouraging messages stating that the latest firmware should always be applied when it becomes available.

Table 3 Comparison of Security Recommendations in ADSL Router Manuals

	Billion	Netgear	D-Link	Netcomm	TP-Link	Belkin
Changing default password		✔	✔			
Password choice		✔				
Checking/updating firmware		✔				
Outlines risks of wireless		✔		✔		
WPA or WPA2		✔	✔			
Use of in-built firewall				✔		
MAC address filtering		✔				
Disable SSID broadcasting		✔		✔	✔	

A study of 312 participants (Herath & Rao, 2009) showed that end-users must be appropriately encouraged or forced to use a high level information security measures. One of the prevalent outcomes of this study was the choice of words used to encourage the use of security on the vendors' product. There is a distinct difference between a vendor stating that a security setting exists and recommending or encouraging that it be used. Unfortunately, many of the vendor manuals analysed in this study, only state that a particular setting or feature is available on the ADSL router. Netcomm outlined the potential issues which could emerge if the firmware on the product is updated, such as the product may no longer function correctly. This may significantly deter end-users from applying any update. However, at no point did the Netcomm manual outline the advantages such as enhanced stability or security. From the end-users perspective it would appear that the disadvantages significantly outweigh the advantages of updating the firmware.

CONCLUSION

The ongoing releases of ADSL router literature may create many problems for the end-user. From a psychological perspective the end-user could be driven away from the information in the product manuals particularly where it is difficult to interpret what the vendor is articulating. As ADSL routers tend to encompass little or no security by default, vendors should make product literature useable and attractive to ensure that security is implemented. The design quality and content presented in many of the manuals is far from adequate. In the first instance when this study was undertaken the manuals were poorly delimitated but the issue of insecure ADSL routers was not a significant issue. The number of attacks specifically targeting ADSL routers is on a significant increase. There are simple measures that end-user can take to alleviate themselves from the dangers. Future research will continue to examine ADSL router manuals in the effort to determine if vendors eventually improve their product literature. There is also an avenue of research in examining what end-users learn or take away from using the product literature to setup and secure a networking device.

There are simple solutions to mitigate many of the issues that are present in the manuals. The essential introduction of a glossary and index page in every manual will reduce the burden of end-users locating desirable information. Vendors must also stop assuming prior knowledge. Vendors have the luxury in that they can easily educate end-users of the dangers and risk of using the Internet, whilst at the same time providing detailed solutions for mitigating many threats through the product manuals. Lastly, vendors must make significant recommendations as to which security feature should be enabled on the device. With countless security features available, end-users may often choose the weaker or obsolete measure. Vendors should recommend a superior countermeasure through the manual to alleviate many of the pressures already faced by novice computer users.

REFERENCES

ABS. (2010). Internet Activity, Australia, Dec 2010. Retrieved May 9, 2010, from http://www.abs.gov.au/ausstats/abs@.nsf/mf/8153.0/

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

Belkin. (2011). Retrieved June 25, 2011, from http://www.belkin.com/PDF/F7D1401au_Basic_Modem_Router_2.pdf

Billion. (2010). BiPAC Billion 7800NL 802.11n ADSL2+ Firewall Router User Manual. Retrieved June 25, 2011, from http://au.billion.com/product/usermanuals/BiPAC_7800NL_FM%202.02a.dc1_UM_1.11.pdf

Byline Media. (2011). Readability Formulas. Retrieved November 4, 2011, from http://www.readabilityformulas.com/free-readability-formula-tests.php

Celeda, P., Krejci, R., Vykopal, J., & Drasar, M. (2010). *Embedded Malware – An Analysis of the Chuck Norris Botnet.* Paper presented at the 2nd European Conference on Computer Network Defense, Berlin, Germany.

Christensen, J. (2007). Linsear Checks Easy and Hard Words. Retrieved November 3, 2011, from http://www.csun.edu/~vcecn006/read1.html

D-Link. (2011). User Manual DSL-2740B Version 1.0. Retrieved June 25, 2011, from ftp://files.dlink.com.au/products/DSL-2740B/REV_C3/Manuals/DSL-2740B_C3_Manual_1.00.pdf

DBCDE. (2011). What is the NBN? Retrieved October 20, 2011, from http://www.nbn.gov.au/about-the-nbn/what-is-the-nbn/

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Hunt, S. R. (2009). New worm can infect home modem/routers. Retrieved October 11, 2009, from http://apcmag.com/new-worm-can-infect-home-modemrouters.htm

Johnson, E. (1995). Computer Documentation: Writing about technology. *Computers and the Humanities, 29*, 409-411.

Magnus, N., & Gassmann, B. (2009). Psyb0t Attacks Linux Routers. Retrieved October 10, 2009, from http://www.linux-magazine.com/Online/News/Psyb0t-Attacks-Linux-Routers-Update

Mendoza, E. (2011). Router-Compromising Malware in Latin America. Retrieved August 11, 2011, from http://blog.trendmicro.com/latin-america-router-compromising-malware-found/

Mousionis, S., Vakaloudis, A., & Hilas, C. (2011). *A Study on the Security, the Performance and the Penetration of Wi-Fi Networks in a Greek Urban Area* Paper presented at the 5th International Conference on Information Security Theory and Practice, Heraklion, Greece.

Mueller, L. A., Reid, K. I., & Mueller, P. S. (2010). Readability of state-sponsored advance directive forms in the United States: a cross sectional study. *BMC Medical Ethics 2010, 11*(6), 1-6.

Netcomm. (2010). Netcomm Gateway Series ADSL2+ Modem Routers. Retrieved June 25, 2011, from http://media.netcomm.com.au/public/assets/pdf_file/0015/40218/NB6Plus4W_REV2_UG.pdf

Netgear. (2011). Wireless-N 150 ADSL2+ Modem Router DGN1000 User Manual. Retrieved June 25, 2011, from http://support.netgear.com/app/products/model/a_id/12208

Paz, S. H., Liu, H., Fongwa, M. N., Morales, L. S., & Hays, R. D. (2009). Readability estimates for commonly used health-related quality of life surveys. *Quality of Life Research, 18*(7), 889-900.

Perelman, L. C., Paradis, J., & Barret, E. (1998). *The Mayfield Handbook of Technical & Scientific Writing*. Mountain View, CA: Mayfield Publishing Company.

Reznik, L., III, V. J. B., Lewis, J., Dipon, A., Milstead, S., LaFontaine, N., et al. (2011). *Security of Computer Use Practice: The Case of Ordinary Users Survey.* Paper presented at the 14th Annual 2011 NYS Cyber Security Conference, New York, USA.

Sajdak, M. (2009). *Remoterootshellon a SOHO classrouter.* Paper presented at the Confidence 2009, Krakow, Poland.

Schriver, K. A. (1997). *Dynamics in Document Design*. New York, USA: John Wiley & Sons.

Seymour, B. (2010). Drive-by-hackers. Retrieved September 13, 2011, from http://au.news.yahoo.com/today-tonight/consumer/article/-/7907101/drive-hackers/

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

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.

TP-Link. (2011). TP-Link TD-W815N User Guide. Retrieved June 25, 2011, from http://www.tp-link.com/resources/software/TD-W8151N%20User%20Guide.pdf

Wieringa, D., Moore, C., & Barnes, V. (1993). *Procedure Writing*. Piscataway, NJ: IEEE Press.

Williams-Jones, B., & MacDonald, C. (2008). Conflict of Internet Policies at Canadian Universities: Clarity and Content. *Journal of Academic Ethics, 6*(1), 79-90.