Assessing the usability of WLAN security for SOHO users

B.V.Ghita[1] and S.M.Furnell[1,2]

[1] Network Research Group, School of Computing, Communications & Electronics, University of Plymouth, Plymouth, United Kingdom
[2] School of Computer and Information Science, Edith Cowan University, Perth, Australia
info@network-research-group.org

Abstract: Wireless technologies provide the basis for a constantly increasing percentage of current Small Office/Home Office (SOHO) networks, particularly due to the connectivity and setup convenience that they can offer. Unfortunately, the security considerations counterbalance the connectivity advantages, as default settings for wireless access points often provide no encryption or network protection. This study assesses a number of wireless access points and highlights that although the devices may incorporate appropriate security functionality, users may face difficulties when attempting to understand and configure the related features. The causes here are often a lack of accompanying explanation and guidance, as well as confusing presentation of options at the user interface level. As such, it is concluded that usability factors may represent practical obstacles to the deployment of appropriately secured wireless networks.

1 Introduction

Wireless Local Area Network (WLAN) technologies have unquestionably risen to prominence in recent years, with significant adoption being witnessed in both business and domestic contexts. Major factors of this rapid proliferation have been the cost and convenience of the technology when compared to setting up traditional LANs, and the ease with which access can then be provided to wider networks such as the Internet. Unfortunately, however, the use of WLAN brings with it a number of notable risks (beyond those of traditional Internet access), and although these have been long-recognised by the security community, they are frequently unknown or unacknowledged by those deploying the networks. As a consequence, many WLANs are not secure.

A key realisation with WLAN technology is that everyone deploying one will effectively become a network administrator. This brings with it certain responsibilities. For example, in order to protect their wireless networks, administrators need to setup secure access through a secret key, used for encrypting all data carried between the clients and access point(s) in such a network. Although it may be reasonable to assume that larger organisations have dedicated IT staff who should be competent to deploy the technology appropriately (such that any deployment of unsecured wireless networks within large organisations could typically be blamed upon negligent administration), users within Small Office/Home Office (SOHO) environments may face legitimate difficulties that constrain their ability to do the right thing.

This paper evaluates the current support received by network administrators when configuring security features for their wireless environments. The study observes the level of information provided in user manuals to guide users through the setup security process, and considers whether this information may be perceived as too technical or insufficient by a non-technical user. The paper continues with an overview of current techniques employed to encrypt information for wireless environments, as well as the flaws (and associated exploits) identified for some of the discussed protocols. The scope of this paper is not to criticise these flaws; by presenting them, the study aims to underline the fact that a determined attacker may still be able to bypass a weaker security scheme. The discussion then includes a critical review of a number of access points, considered from the perspective of the user friendliness of the information presented (either as part of the manuals for each access point or the graphical user

interface used to configure each device). The review is then followed by a number of recommendations for improving the usability of the setup process while not reducing the user friendliness.

2 Basic WLAN security mechanisms

Before considering usability challenges, it is essential to establish the basics of the existing security options. As such, this section outlines the mechanisms that users need to be most aware of, in order to provide the context for later discussion.

2.1 Service Set Identifier

The first line of defence in securing wireless networks relates to mechanisms employed to reduce the possibility of an intruder being able to connect to the network. In order to make clients aware of its presence, a wireless access point periodically sends broadcast packets named beacons. After receiving beacons from one or more access points, a client sends a management frame that must include the Service Set Identifier (a string that defines an access point, which can be changed as part of the device settings) of the one it wants to use, in order for the two devices to communicate. By default, the beacons include the SSID string, in order to simplify the configuration process. This is beneficial for legitimate clients, who will require no prior knowledge of any parameters when connecting to the network, but it also allows non-legitimate clients to connect to the network by using the SSID from the beacons. In typical configurations, a network manager may choose to include in the SSID of his/her access points an indication of the company that owns the device.

Before resolving any of the flaws that this management dialogue introduces, consideration must be given to the name of the SSID. One option, but the poorest in terms of security, is to leave the SSID unchanged. This can prove damaging for two reasons. Firstly, if the credentials to access the device are also left unchanged, an attacker can control the entire network using information provided by the user manuals (which include the default credentials for each model). Secondly, even if the password required to access the device is changed, an intruder would still be able to illegitimately use the network. However, even the SSID is changed, the naming convention should be carefully considered. For example, changing from the default SSID to one that includes the name of the organization that owns it can actually assist attackers in locating and identifying a target network.

To eliminate these problems, two basic mechanisms were proposed. The first one consists of setting access points not to include the SSID in the broadcast beacons. However, such measure implies the use of another process to supply the SSID to legitimate clients so that they can connect the network. From a security perspective, this is very good practice, but from the usability perspective it may reduce the friendliness of the network for legitimate users. The second mechanism relies on a filter, based upon a list of Media Access Control (MAC) addresses of authorized devices. In this case, all MAC addresses would need to appear in an access control list on the wireless access point in order to be allowed to access the network. However, the level of security provided by this measure is weak as MAC addresses are transmitted in plaintext in each 802.11 frame (whether the connection is encrypted or not), and can then be “spoofed” by almost any wireless card, using appropriate software.

In spite of these weaknesses, the SSID does serve as a first-level barrier against intruders. While such mechanisms will not foil determined attackers, they may prevent opportunistic outsiders that seek to use a wireless Internet connection without the knowledge of the owner.

2.2 Encryption

Wired Equivalent Privacy (WEP) encryption is probably the most well-known, but also the most criticised, security standard for wireless networks. While it was the first wireless specific security method, its implementation suffers from a number of flaws, some of which have been used as the basis for WEP cracker software, now widely available on the Internet. Specifically, the flaws include: lack of authentication key limited lifetime, vulnerability to "disassociation requests" injections, low security MAC level authentication and identification, lack of central security management and weakness of the underlying cipher algorithm due to the Initialisation Vector (IV) generation method used. (Khan and Khwaja 2003)

With the breaches discovered in WEP-based wireless security, the IEEE 802.11i workgroup dedicated to security was created in order to publish a standard on Robust Security Network (RSN) (IEEE 2004). This method relies on Temporal Key Integrity Protocol (TKIP) and on the separation of user authentication and the message protection (preventing the possible decoding of data thanks to the observation of authentication processes). WiFi Protected Access (WPA) (WiFi Alliance, 2002) was implemented on the Wireless Fidelity (WiFi) manufacturers' initiative to release a secure replacement for WEP as fast as possible, without the need of major hardware changes. This method relies on TKIP and also includes mechanisms such as a Message Integrity Check (MIC) and extended Initialisation Vector (IV) with sequencing rules and re-keying mechanisms that address the previous breaches included in WEP implementation. However, WPA is based on a Pre-Shared Key (PSK), usually generated from a passphrase, and it has recently been proven to be prone to different kinds of attacks (Moskowitz, 2003). WPA2, an evolution of WPA based on the Advanced Encryption Standard (AES), and on a new MIC implementation, should replace the first version in the near future.

3 Deployment of WLAN security in practice

The previous section discussed the various mechanisms currently available to deploy encryption to a wireless network. As highlighted throughout the discussion, current authentication and encryption methods do include certain flaws which may eventually allow a persuasive attacker to penetrate the network, but it is clear that the level of protection provided by such methods is clearly superior to the case where no security is employed. In this context, it would be expected that current networks include at least one of the above methods to protect from intruders or/and attackers. Unfortunately, there is significant evidence to suggest that many WLANs are not deployed in a secure manner. As illustration of the problem we can consider the findings from the WorldWide WarDrive (WWWD) events, which ran a series of studies between 2002-2004 to evaluate the level of protection used in wireless networks across the United States of America (WWWD 2004). The investigation focused upon two issues: whether an access point still had the default SSID, and whether or not WEP had been enabled. The conclusions of the study were rather consistent over the three years, with variations of less than 10% for the statistics of the four resulting categories: WEP enabled, no WEP enabled, default SSID, default SSID and no WEP enabled. The results from the fourth (and final) WWWD event are presented in Table 1.

Category	Total	Percent	Percent change (from 2003)
Total AP Found	228537	100	+260
WEP Enabled	87647	38.30	+6.04
No WEP Enabled	140890	61.6	-6.04
Default SSID	71805	31.4	+3.57
Default SSID and no WEP	62859	27.5	+2.74

Table 1 - Results of WWWD4 study from 2004 (WWWD 2004)

The figures illustrate the current security environment for wireless networks: almost two thirds of the wireless access points identified did not have WEP enabled. Additionally, more than a quarter of the devices maintained the default SSID and did not have any encryption for the data exchanged. Although it may be argued that the figures are becoming dated, it is also unlikely that the situation today is substantially different.(the findings from the previous three WWWD events were not significantly different, and indeed changes compared to the 2003 results can be observed in the table). Furthermore, the results are not specific to the United States; for example, a similar study of access points in Plymouth, UK, reported comparable findings (Voisin *et al* 2005).

4 The usability of access point security

The WWWD study was only able to draw conclusions on the current level of security provided for wireless networks, without any observations regarding the reasons behind this apparent low deployment of security measures. Of course, two possible explanations are ignorance or disregard for security amongst the user base. While this is hard to evaluate without a more detailed study, it is fair to observe that recent years have witnessed a substantial increase in the media coverage of security-related incidents – a move that is likely to have raised administrators' awareness of the need to protect their networks. As such, while disregard could still be a significant factor, the proportion living in complete ignorance of the risks is likely to be reducing. However, a further issue that may present a challenge is the user friendliness of access points when attempting to configure the security settings, such that even if users are aware of security and interested in protecting themselves, they may still face obstacles. This is the focus of this section, which aims to objectively evaluate the difficulties that a less-experienced user may encounter when attempting to enable security protocols (encryption in particular) for the wireless network he/she administers.

This study focused on five wireless access points. The selection criteria did not consider the technical characteristics of the hardware, but rather their target market and availability. The two criteria were evaluated through a price comparison website (Pricerunner 2005), based on listing the wireless access points on the website by popularity; the availability was evaluated through the number of stores that sell that specific product – only products available on more than 10 Internet stores would qualify for this criterion. The resulting list included the following products: Belkin F5D7130UK, Netgear WG602, Linksys WAP54G-UK, 3Com 3CRWE454G72-UK, and D-Link DWL-2000AP+. The list was then completed with devices including ADSL router with wireless access point functionality: Netgear WGT614/624 and Belkin F5D7230UK4 + / F5D7633UK4A. The reason for adding such devices is due to the focus of the market for small networks. While larger networks may already have

an infrastructure in place, networks with 5-10 hosts may be constructed around the device that provides both intranet and Internet connectivity – a combined wireless access point and broadband router.

It is important to understand that, although the survey did not include any technical criteria, all the chosen products have encryption capabilities. Further, the ADSL routers also include firewall functionality, which is also relevant from the usability perspective. The survey aimed to determine whether novice users would be able to enable and use these facilities through the available user interface.

The survey used the user manuals for the shortlisted devices as a basis for the comparison. The rationale for this was that the manuals are the main (if not the only) source of support for a novice user aiming to configure their WLAN. The research at this stage is not based upon practical evaluation with end-users, and these initial conclusions are based upon the information presented to the users in the software and documentation.

4.1 Functionality

All of the surveyed access points shared connectivity and configuration characteristics. In order to configure any required settings, clients must to connect to web server running on the access point. This is clearly the simplest alternative, as it does not require any technical networking knowledge on behalf of the user to connect and configure the device. Another advantage was that once connected to the network, all devices provided wireless access out-of-the-box, without any need to modify settings. However, although advantageous in terms of setup, it can also be considered a problem in the sense that it effectively encourages the user not to need to look at the configuration settings; this issue will be discussed later, in section 4.3.

All manuals indicate the IP address of the access point, while some of the manuals go a step further and indicate the default credentials. This does have the advantage of simplifying the task faced by the user, but it also provides a potential attacker with information about the network. If (as in many cases) the defaults have not been changed, a typical line of attack would include observing the SSID, as broadcast by the wireless access point, followed by downloading the appropriate manual from the Internet. On an unencrypted network, this information would not only allow an attacker to get access to the network, but would also enable them to control it.

4.2 Interface and language

Although the design of the administrative interface differs considerably between the products, the settings to be altered are virtually the same, at least in the security part. However, in all cases the level of help provided for each setting is minimal. Instead of providing detailed information about the underlying technologies, as performed below in the manuals, the web interface provides minimal help, detailing only on the syntax and format. The availability of information on the web interface is understandable, as the hardware includes an embedded operating system (typically Linux) and any addition of information impacts on the size of the storage, and is not critical, as users may still find the required information in the manual. However, provision of information as part of the settings is likely to improve the chances for a user to make the right choice for each one.

4.3 Adequacy of supporting information for users

The specific information provided to support security configuration is now considered in relation to each of the vendors assessed in the study.

- **Netgear**
  The Netgear manual contains a substantial amount of technology background. One of the Appendices describes in detail the security-related concepts of wireless communication, from open system and shared key connectivity, to a comparison between WEP and WPA functionality. The text is clearly informative, but it fails to provide two important services. Firstly, this information does not link closely with the settings available on the product, such that the user may find it difficult to relate theory to practice (indeed, the manual provides only a brief overview of the settings themselves). Secondly, the information does not end with clear guidelines for the user in terms of choosing a particular technology or alternative. For example, the description of WEP settings indicates the availability of 64-bit and 128-bit encryption, but there is no further indication on how opting for one or the other will affect the level of security achieved. The manual includes only an example of a 64bit and a 128bit strings; the text does not explain the fact that any 64 bit or 128 bit combination can be used for the key, which could make a novice user believe that only specific strings may qualify and be used as a WEP key.

  It is worth noting that, under the 128-bit encryption heading, there is a note regarding the legal impact when using such encryption "128-bit encryption may not be available outside of the United States due to U.S. export regulations". This generates at least confusion for an end-user who wants to avoid any legal confrontation, and raises the question why a model sold on the UK market would include features that are illegal outside the United States.

- **Belkin**
  The Belkin F5D7230UK4 wireless access router is likely to be appreciated by the non-networking users, due to its user-friendliness. For the Belkin family of wireless devices, the standard information pack includes the user manual (Belkin 2005a), but in addition, a quick installation guide and a web-based wizard also support the installation process (Belkin 2005b). In this way, the users do not have to go through the configuration pages themselves; instead, they can follow the manual to understand which settings have to be enabled or modified, but all under the guidance of the wizard. The two additional features are not unique amongst the surveyed access points, but novice users are likely to prefer the 5-step quick installation guide, as it clearly describes all installation steps, from physical connectivity to running the wizard from the supplied CD. This is an advantage from the user-friendliness perspective, but, from the perspective of this study, the process has a significant flaw – the quick setup guide and wizard do not mention anything about security settings. As a result, inexperienced users who use the setup wizards are rather unlikely to implement any security measures for their network.

  In terms of additional web resources, the Belkin website provides a considerable amount of information on all aspects of setup. The product support page for the above router includes: a set of flash guides and a list of FAQs. However, it is interesting to note that none of these resources specifically mention security. Only one of the FAQ links ("Is Wi-Fi Protected Access an IEEE 802.11 standard?") refers to an encryption standard. In fact, by selecting the link, the reader can than follow links to more relevant questions, such as "What is Wi-Fi Protected Access?", although even the answer to this last question is rather technical (Belkin 2005c):

  > *Wi-Fi Protected Access (WPA) is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection*

(encryption) and access control (authentication) for existing and future wireless LAN systems. The technical components of WPA include Extensible Authentication Protocol (EAP), Temporal Key Integrity Protocol (TKIP) and 802.1X for authentication and dynamic key exchange.

This definition raises another problem for novice users when locating information for the wireless security standards. Although the information is perfectly correct, a non-technical user is unlikely to fully understand the WPA functionality and, more so, the WPA component protocols. The issue of correctness versus comprehensibility in the provided information will be raised again in the conclusions section.

- **DLink**

  In many ways the content of the manual for the Dlink DI-624 wireless router (DLink 2005a) resembles the information provided for the aforementioned Belkin product, and this device is again accompanied by a quick installation guide (DLink 2005b). In this case, however, the quick installation guide (and the associated web interface wizard) does include a security setup, as shown in Figure 1.

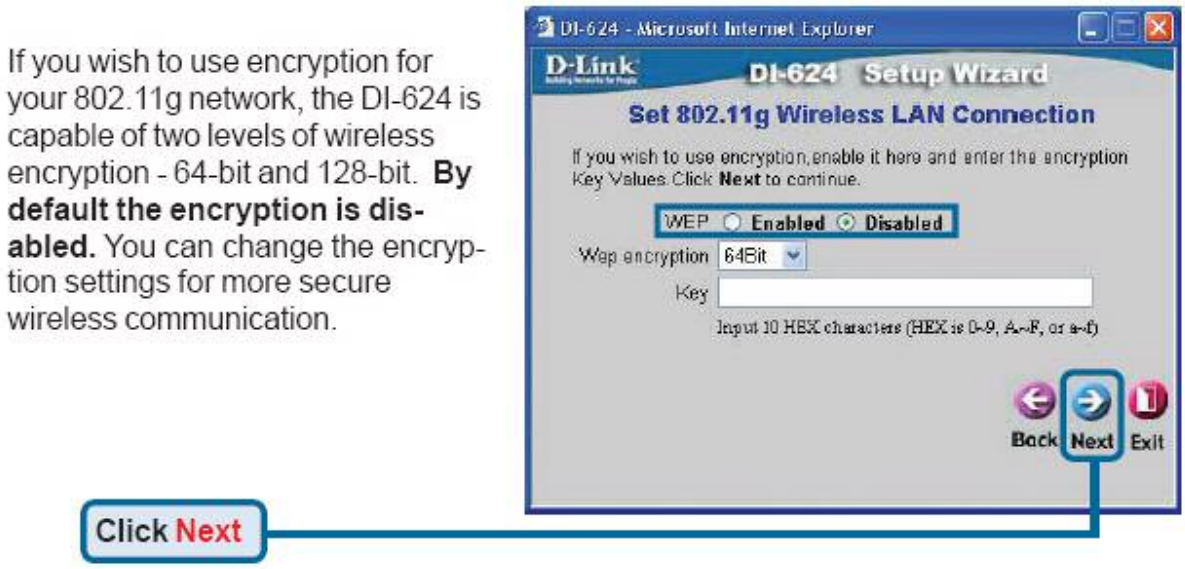

Figure 1 : Encryption setup for the DLink DI-624 broadband wireless router (from (DLink 2005b))

Having the security setup built into the quick installation is clearly a step forward, particularly in the context of the other models providing nothing on this issue. However, the material is not entirely consistent. In spite of the manual indicating on the Introduction page that the model supports WPA encryption, the only encryption alternative presented throughout the instructions available is WEP.

- **3Com**

  The user guide for 3Com's 3CRWE454G72 (3Com 2005) is a mixture of the previous cases. The guide does not detail any of the available encryption methods; there is minimal technical information about the WEP or WPA functionality. As with other products, the configuration wizard does not include any encryption settings, which reduces the chances for a novice user to implement any such network protection. The wizard does have a positive point – a step that gives the user the

opportunity to change the default password for the access point. The encryption section of the user guide is helpful for a non-technical user, as it does not focus upon technical matters but does highlight relevant practical issues, (such as the fact that a longer key would provide better security but may reduce the data transfer speed). Also, as shown below in Figure 2, the settings are part of the clearly marked *Encryption* tab, and the key may be introduced as either a passphrase or a raw hex value. This simplifies the configuration, particularly for users that do not understand the meaning of a hex value (some of the other products, such as Belkin, require strictly hex values, although the manual does not explain what a hex value is, apart from listing its possible values, 0-9, A-F).

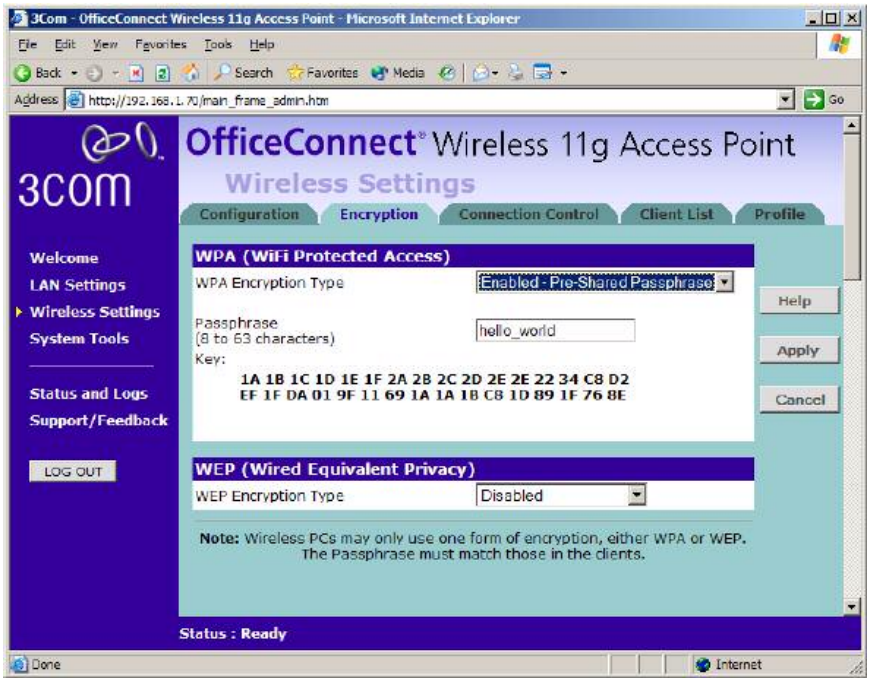

Figure 2 : Encryption settings page for 3Com wireless broadband router (from (3Com 2005))

A summary of the various findings is presented in Table 2, and it is easy to see that none of the manufacturers provides a complete set of the desirable elements to support the appropriate configuration and use of security by different user groups.

Features/Device	Netgear	Belkin	DLink	3Com
Manual details configuration of security features	✓	✓	✓	✓
Manual explains security concepts	✓	✓	×	×
Quick configuration guide covers security features	N/A	×	✓	×
Configuration Wizard covers security features	N/A	×	N/A	✓
WPA configuration support	✓	✓	×	✓

N/A = Not applicable (i.e. configuration guide and/or wizard is not provided with the device)

Table 2 - Support for configuring and using security in access point products

4.4 Updating the firmware

Wireless access points and/or broadband routers provide a robust solution in terms of maintenance and configuration. All devices include a reset button that will revert the device to the factory settings, which include predefined credentials, allowing the user to use the provided username and password from the manual, and remove any modifications, allowing reconfiguration from scratch. This convenience is due to the devices using stripped-down, embedded operating systems to provide the required functionality. However, this brings up another issue – newer versions of the operating system require a firmware update. Compared to a Windows update or other software patch, the operation presents two major problems for a non-technical user: the process itself and information about the updates. The firmware updating process is a simple operation but, as indicated on all firmware web resources, if the update fails the device is rendered unusable. As a result, it is very likely for novice users to avoid the operation unless they already have a problem with their network. The second problem is related to the availability of the update information. The Windows operating system has an update component that, if enabled, it periodically connects to the Microsoft servers to verify if new updates are available. In contrast, for a wireless access point, the user would need to specifically visit the vendor's support website to identify the firmware file, which will then need to be downloaded on a computer and then uploaded to the wireless access point. If the user selects the wrong device, the process will fail and, further, the device may be rendered unusable, as specified above.

Due to their compactness and limited functionality, embedded operating systems do not often require firmware updates. Typically, such an update would provide the user with extra functionality or improved performance/security. However, there are cases in which firmware upadates are issued to rectify vulnerabilities (DLink 2005c), (CoreLabs 2005), and without updating their device, the users remain exposed to any threat that may exploit them.

5 Recommendations

The analysis from the previous section raised a number of issues relating to the interface and the supporting information for setting up security on several current wireless access point devices. The surveyed access points appear to include all the encryption protocols currently available, ranging from WEP to WPA2 (although some of them may require a firmware update to support the latest available versions). While the support of various protocols is not questioned, the simplicity of the configuration interface and the friendliness of the supporting information can be clearly improved.

Rather than perceiving a choice of whether to provide or omit technical details, vendors ought to provide supporting information on two levels. The first should address users who do not need any technical details about the alternatives, but still require appreciable facts about their options. For example, WEP may be described as a backward-compatible protocol, but providing poor long-term security; in contrast, WPA2-PSK can be described as a better alternative, but with limited support. To some degree, such information is presented in the Netgear manual; unfortunately, it does not clearly indicate the possible choices (e.g. it only highlights the limitations of WEP and insists that WPA2 should be used instead of WPA, but only if the other wireless devices support it).

In terms of identifying their available security options, all the instructions rely on the user to determine any protocol incompatibility between the network devices. While this is not unacceptable, as each wireless access point manufacturer would not be required to run compatibility test all wireless interface cards, basic guidelines would considerably help a user when choosing a method or another. Such guidelines could include a minimum of generic information, such as how to determine the MAC address for a Microsoft Windows machine (i.e. using *ipconfig /all*). Further, the instructions could describe where to find the appropriate dialogues for enabling encryption on a wireless interface card.

Providing such information could clearly influence whether a user continues the process of setting up encryption for a wireless network he/she manages.

Finally, apart from the additional information that could be added to the user manuals to guide the user when configuring the device(s), the process can be improved via the help available as part of the configuration interface. It is worth noting that, unless experiencing malfunction or difficulties, a user might decide not to use the manual, and rely upon the GUI-level help when configuring the device. It became apparent for the majority of the surveyed devices that the level of information available through the web interface is minimal, providing details only on the available choices together with definition or/and syntax for each setting (e.g. without detailing to the user the impact that each choice may have onto the functionality of the device or the resulting architecture).

6 Conclusions

This paper presented a review of the information available to an end-user when configuring current wireless access points. The study identified that while the information provided is sufficient for a knowledgeable user to make an informed choice, it is likely to create confusion for a less experienced user.

WLAN access points are far from the only context in which problematic usability issues may be identified (Katsabas *et al* 2005). However, they are clearly an increasingly deployed technology, in which the presence or absence of protection can have significant implications. As such, poor usability represents an unwelcome additional barrier to ensuring that security is appropriately applied. Indeed, the usability problems observed in this paper are likely to account for at least a proportion of the insecure deployments that have been witnessed by wardrivers, and even though newer and more secure WLAN technologies are now available, the usability issues may still serve to undermine the protection.

References

3Com (2005), "3Com 3CRWE454G72 user guide", (online) http://support.3com.com/infodeli/tools/hubs/off-con/pdf/dua0045-4aaa01rev01.pdf

Belkin (2005a), "Belkin F5D7230-4 user manual", (online) http://web.belkin.com/support/download/downloaddetails.asp?file_id=2063

Belkin (2005b) – "Belkin F5D7230-4 quick installation guide", (online) http://web.belkin.com/support/download/downloaddetails.asp?file_id=1111

Belkin (2005c) – "Belkin F5D7230-4 support page", (online) http://www.belkin.com/support/download.asp?download=F5D7230-4&lang=1&mode=

CoreLabs (2005), "Vulnerability Report For Linksys Devices, CoreLabs advisory", (online) http://www1.corest.com/common/showdoc.php?idxseccion=10&idx=270, December 2002

DLink (2005a) "DLink DI-624 wireless broadband router user manual", (online) ftp://ftp.dlink.co.uk/di_broadband_gateways/DI-624_rev_cx/di-624_rev_cx_man_v104.pdf

DLink (2005b) “DLink DI-624 wireless broadband quick installation guide“, (online) ftp://ftp.dlink.co.uk/di_broadband_gateways/DI-624_rev_cx/di-624_rev_cx_qig_v102.pdf

DLink (2005c) “DLINK 624, script injection vulnerability“, (online) http://lists.nycwireless.net/pipermail/nycwireless/2004-July/008569.html , July 2004

IEEE (2004), “The 802.11 standard”, (online) http://grouper.ieee.org/groups/802/11/
Kershaw, M. (2004), “Kismet”, (online) http://www.kismetwireless.net

Katsabas, D., Furnell, S.M. and Dowland, P.S., (2005), Using Human Computer Interaction principles to promote usable security, Proceedings of Fifth International Network Conference (INC 2005), Samos, Greece, 5-7 July 2005, 235-242.

Khan, J. and Khwaja, A. (2003), “Building secure wireless networks with 802.11”, Wiley, Indianapolis.
Milner, M. (2003), “NetStumbler.com - The New World of WiFi”, (online) http://www.netstumbler.com

Mishra, A. and Arbaugh, W.A. (2002), “An Initial Security Analysis of the 802.1X Standard”, (online) http://www.cs.umd.edu/~waa/1x.pdf

Moskowitz, R. (2003), “Weakness in Passphrase Choice in WPA Interface”, Wi-Fi Networking News, (online) http://wifinetnews.com/archives/002452.html

Pricerunner (2005), “Pricerunner comparison website”, (online) www.pricerunner.co.uk

Voisin M, Ghita BV, Dowland PS (2005), “Survey of Wireless Access Point Security”, Proceedings of the Fourth Security Conference 2005, Las Vegas, USA, 30-31 March, 2005

WiFi Alliance (2002), Wi-Fi Alliance Announces Standards-Based Security Solution to Replace WEP, (online) http://www.wi-fi.org/OpenSection

WWWD (2004), “The WorldWide WarDrive website”, (online) http://www.worldwidewardrive.org/