Not All ISPs Equally Secure Home Users
An Empirical Study Comparing Wi-Fi Security Provided by UK ISPs

Z. Cliffe Schreuders, and Adil M. Bhat
School of Computing, Creative Technologies and Engineering, Leeds Metropolitan University, Caedmon Hall, Headingley Campus, Leeds, UK
c.schreuders@leedsmet.ac.uk, a.bhat3968@student.leedsmet.ac.uk

Keywords: *Wardriving, Wi-Fi Security, ISPs*.

Abstract: A majority of home users rely on their Internet service providers (ISPs) to provide them with wireless equipment that is secure, and assume that they are appropriately protected from threats such as piggybacking and eavesdropping. In this paper we present the results of an empirical study comparing the security provided to home users by their ISPs. Passive wireless data collection was used to gather information on 7,847 unique wireless access points within Leeds, UK. Non-parametric inferential statistical analysis was used to compare the security provided by the corresponding ISPs, as identified via the SSID naming used by ISPs in the UK. The ISPs identified included BT, O2, Orange, Plus Net, Sky, TalkTalk, and Virgin Media. Statistically significant differences in the security of the networks were found between ISPs, which we contend can in part be explained by their upgrade policies. These results are contrasted with the security configuration provided by three of the largest ISPs to new customers. For example, BT (the largest ISP in the UK) was found to have a greater number of access points configured with the cryptographically broken Wireless Equivalent Privacy (WEP) encryption method in use, compared to most of the other large ISPs, and this is in contrast to the favourable security configuration of the routers that are provided to new customers. The paper concludes with recommendations for when ISPs provide Wi-Fi enabled routers to home users.

1. INTRODUCTION

Many ISPs make a point of advertising that the Wi-Fi networks of the routers that they provide to home users are secure. Furthermore, many home users lack the expertise to configure their own access points, and assume that the router provided by their ISP is adequately secure. While many routers provide relatively secure configurations at the time of purchase, over time weaknesses are discovered in protocols that were previously considered secure.

Encryption methods such as Wireless Equivalent Privacy (WEP) have long been considered cryptographically broken (Borisov et al., 2001; Fluhrer et al., 2001). WEP was introduced by IEEE in 1999 to provide data confidentiality and integrity for 802.11 wireless networks, with the intent that the security was "equivalent" to wired networks. However, design flaws were quickly discovered – such as the small initialisation vector (IV) value, which results in susceptibility to a Fluhrer, Mantin and Shamir attack (Fluhrer et al., 2001). Other flaws in the WEP algorithm make the attacks more efficient, and even enable real-time decryption (Bittau et al., 2006; Stubblefield et al., 2004; Tews et al., 2007). These flaws effectively render WEP networks unsuitable for most security purposes.

Wi-Fi Protected Access (WPA) provides a more secure alternative for protecting Wi-Fi networks. However, weaknesses have been found, such as weaknesses in the pre-shared key mode with TKIP, which can result in decryption and injection of packets (Tews and Beck, 2009). As a consequence WPA has been deprecated in favour of WPA2. WPA2 is currently considered the most secure of the common encryption options for securing 802.11 networks.

Wi-Fi Protected Setup (WPS) is a key distribution method built into many modern network devices, which reveals the network key (regardless of encryption method used) when a client specifies

the correct 8 digit PIN. On some devices, this request can be made wirelessly. It has recently been reported that in many cases this technology is enabled by default and is vulnerable to (reduced search space) online brute-force attacks (Stefan Viehböck, 2011). This is an example of an attack that many current routers are vulnerable to and, as subsequently discussed, the problem is analogous to the upgrade to more secure encryption methods.

It is common practice in the UK for ISPs to provide "free" routers with wireless access points (APs) to customers, included with their subscription. BT is currently the largest broadband provider in the UK, with reportedly over 6 million subscribers. Virgin Media, TalkTalk, and Sky are the next largest, with approximately 4 million broadband customers each. Other ISPs that provide Wi-Fi APs include O2, Orange, and Plusnet. The security of the home routers provided by these ISPs are explored throughout this paper.

2. AIMS

This study aimed to identify whether various ISPs provide different levels of Wi-Fi security to their home customers, and aimed to identify any discrepancies between the protection provided. This research question was evaluated for a relatively large population of wireless home networks, and in order to explore the change over time, the default configuration of routers recently provided by three of the largest ISPs were also compared in terms of the level of security provided to home users.

3. METHODS

Data collection was conducted in two stages:

1. Wardriving to collect information on wireless networks in Leeds, UK as it pertains to the security provided by ISPs
2. Manual investigation of routers recently provided by BT, Virgin Media, and Sky

3.1 Wireless Data Collection

Wardriving was conducted using the following equipment:

- 9dBi omnidirectional antenna
- 802.11b/g/n USB adaptor
- GPS USB dongle
- Laptop running Backtrack 5 R2 with Kismet

Wireless data collection was performed towards the end of 2012. The antenna was mounted to the roof of a car, which was driven around high-density residential areas of Leeds, UK. Specifically wardriving (wireless data collection from a motor vehicle) was conducted in select streets in these areas: Hyde Park, Woodhouse, Headingely, Armley, Bramley, Beeston, Roundhay, Harehills, Chapeltown, Hunslet, Kirkstall, and Horsforth. These areas were chosen as they were expected to have a high density of home Wi-Fi networks.

Kismet was the software used to log details of wireless networks. Kismet is a passive network detection tool. It cycles through Wi-Fi channels listening to information that is publicly broadcast by networks, and records information from packets indicating the presence of access points. Kismet was configured not to log traffic content (which arguably would have further ethical ramifications), but to record high-level details of existing networks, such as the SSID and security protocol in use.

Ethics approval was granted by the governing university. Legal precedent seems to suggest that piggybacking (that is, actually using someone else's network) without permission is illegal in the UK. However, the information collected for this study is broadcast publicly (so no unauthorised access occurs) and is also routinely collected and stored by many consumers and businesses; for example, for location-based services.

After data collection was complete, the data was exported from Kismet for analysis.

For each network, as determined by the security flags recorded, a simple security rating score was assigned, as illustrated in Table 1. This enables a mean score to be calculated to give an approximate view of differences, and defines an ordinal scale for non-parametric data analysis.

Table 1. Security score calculation

Encryption method	Security rating
None	0
WEP	1
WPA	2
WPA2	3

As a passive tool, Kismet records the properties of each network corresponding to a MAC address. It is possible for an SSID to appear multiple times due to multiple devices connecting to the same network. When this occurred, multiple records where reduced to one unique record for the network by keeping the record with the highest level of security: for the case

where a WPA and WPA2 connection were both found on the same access point. This approach was taken in order to ensure that each access point was depicted once and security levels were not under reported.

The ISP of each connection was established based on the SSID in use. In the UK, ISPs consistently name the access points provided to their customers: for example, an SSID of "SKY84946" indicates the router was provided to a Sky home user, while an SSID of "virginmedia8395730" was provided by Virgin Media. Using this technique, the ISPs associated with networks were identified.

Open hotspots were pre-filtered out of the data set based on SSID. Other networks included manually configured routers, and hidden SSIDs. These networks were categorised as "other", and were excluded from inferential analysis; however, descriptive statistics were produced.

Finally, inferential statistics were applied to investigate correlations between ISP and security.

3.2 Manual Router Investigation

Although wardriving provides information about an extensive number of networks, manually investigating routers can provide more depth into details such as the strength of network keys and default settings. For this reason, routers from three of the largest ISPs, which had been provided to home users within the last year, were analysed in terms of their security properties. Analysis was based on a convenience sample of routers from BT, Virgin Media, and Sky. This information illustrated notable differences in the approach of the various ISPs and, as discussed herein, was in contrast with the results based on wireless data collection.

4. RESULTS

4.1 Analysis of Wireless Data

Just over 10,000 networks were recorded during wardriving. After filtering of hotspots and removal of duplicate SSIDs 7,847 networks remained. Of these, 5,158 were identified as being associated with a specific ISP. The ISPs identified were: BT, O2, Orange, Plus Net, Sky, TalkTalk, and Virgin Media.

Initial descriptive analysis is presented in Table 2. The table shows the number of wireless networks of each ISP, and the number and proportion of each encryption method found in use on access points provided by the ISP.

Table 2. ISPs and use of encryption methods

	None	WEP	WPA	WPA2	Total
BT	8 (1%)	116 (13.8%)	12 (1.4%)	706 (83.8%)	842
O2	0 (0%)	112 (38.6%)	0 (0%)	178 (61.4%)	290
Orange	0 (0%)	4 (9.1%)	0 (0%)	40 (90.9%)	44
Other	120 (4.5%)	277 (10.3%)	719 (26.7%)	1573 (58.5%)	2689
Plusnet	1 (0.8%)	1 (0.8%)	0 (0%)	116 (98.3%)	118
Sky	1 (0.1%)	23 (1.7%)	398 (29.3%)	936 (68.9%)	1358
Talk-Talk	0 (0%)	6 (1.2%)	4 (0.8%)	510 (98.1%)	520
Virgin Media	2 (0.1%)	9 (0.4%)	11 (0.5%)	1964 (98.9%)	1986

The mean of the scores for each ISP is illustrated in Figure 1, and are as follows: BT=2.68, O2=2.23, Orange=2.82, Other=2.39, Plusnet=2.96, Sky=2.67, TalkTalk=2.97, and Virgin Media=2.98. Although this view of the data is an approximation (being means of ordinal data), it illustrates that differences appear to exist between ISPs.

Non-parametric statistical tests were applied to investigate whether the ISP has a significant effect of the level of security of home users.

A Kruskal-Wallis H test was conducted to compare the effect of ISP on Wi-Fi security rating. There was a statistically significant effect of the ISP ($H(6)=827.211$, $p < 0.001$). It can be concluded that there is a difference in wireless security correlated with the ISPs.

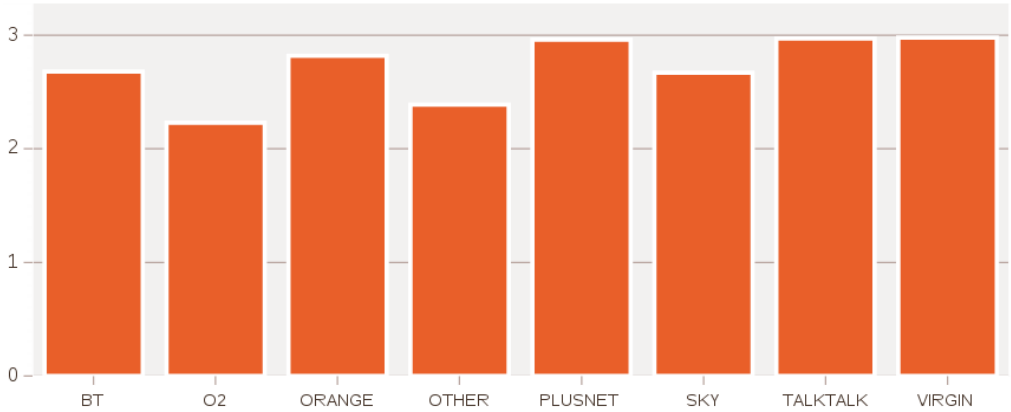

Figure 1: Mean security rating scores by ISP

Post-hoc analysis was conducted using the Mann-Whitney U test with Bonferonni adjustment applied. In each pairwise comparison between three of the largest ISPs (BT, Virgin Media, and Sky) the differences were found to be statistically significant ($p < 0.001$). That is, all the three ISPs were significantly different from each other in terms of wireless security. Pairwise comparison was performed between each ISP, and the other significant results include:

- O2 was found to provide statistically significant lower levels of security when compared with all the other ISPs. WEP usage was of the highest proportion, compared to other ISPs.
- BT was found to provide significantly different levels of security when compared to all the ISPs, except Orange (likely due to the small sample of Orange networks). BT had notably higher proportions of WEP networks compared to others, except in comparison to O2. Means and proportions are previously reported.
- Sky was also found to provide statistically different security in comparison with all the other ISPs, except Orange. Although Sky had a lower WEP proportion than some others, WPA (rather than WPA2) usage was higher than the other ISPs.
- Virgin Media, TalkTalk, and Plusnet were statistically different to O2, BT, and Sky, as mentioned above. Comparison with other ISPs did not indicate significant difference of the security.
- Orange (with a small sample size) was significantly different only to O2.

4.2 Analysis of Routers

Recent routers provided to UK customers of BT, Virgin Media, and Sky were investigated. A summary of the findings is presented in Table 3.

	BT	**Virgin Media**	**SKY**
Encryption options	WEP, WPA, WPA2, WPA/WPA2 (mixed mode)	WEP, WPA, WPA2, WPA/WPA2 (mixed mode), WPA/WPA2 -Enterprise (802.1X)	WEP, WPA, WPA2, WPA/WPA2 (mixed mode), WPA Enterprise (802.1X)
Default encryption	WPA/ WPA2 Mixed mode	WPA/WPA2 Mixed mode	WPA/WPA2 Mixed mode
Authentication option available	PSK	PSK	PSK
WPS-PIN	Yes	Yes	Yes
Default network key	Alphanu-meric	Alphabetical (Lower case only)	Alphabetical (Uppercase only)
Default network key length	10-digit	8-digit	8-digit
Key size	62^{10}	26^{8}	26^{8}
Default router administration password	Alphanu-meric	“changeme”	“sky”

Table 3: Standard router configurations for BT, Virgin Media, and Sky

5. DISCUSSION

It is commendable that, across all the ISP provided routers that were identified, WPA2 adoption was quite high. Also, amongst the ISPs studied in greater detail, new customers were typically provided with access points which by default are configured for a WPA/WPA2 mixed mode, which is generally considered to provide security adequate for home use.

However, in the population studied, there was still a disturbing number of WEP networks in use on routers provided by ISPs, and even a number of networks with no encryption in use. Many of the three largest ISPs' (BT, Virgin Media, and Sky) routers included home networks with no encryption. These networks are very few in number and represent less than 1% of the total analysed networks. However, if this is representative of the millions of home Wi-Fi networks, this could be considered to represent a large total number of users. One explanation for home routers configured this way is deliberate configuration by end users to open their networks to others.

Of the routers provided by ISPs, over 5% (271) were configured to use WEP. The distribution clearly varies between ISPs, with some ISPs with substantially higher proportions of WEP networks than others.

Data analysis showed that the ISP has a significant effect on the level of security on their

users' home networks. Which raises the question: should ISPs be considered responsible for the Wi-Fi security of their customers? It could be argued that ISPs have a "duty of care" when they provide routers with wireless access points, given that ISPs often advertise that they provide secure networks, and the fact that many home users are unlikely to reconfigure the routers provided to them.

In many cases ISPs were found to have significantly different distributions of encryption employed by their routers. Some ISPs appear to have kept their users' security more up-to-date than others. This may be of interest to consumers who could be determining their own future security status when choosing an ISP.

Of the largest ISPs (BT, Virgin Media, TalkTalk, and Sky), BT was found to have the highest proportion of routers configured to use WEP encryption, at 13.8%. If the sample in this study was representative of the population at large, BT's customer base could have upwards of 800,000 home users using WEP in the UK. This could be considered cause for concern, as these networks would be vulnerable to easy attack, and could be targeted for eavesdropping, piggybacking, and various other threats.

This is in contrast to the findings from the analysis of recently provided routers, which illustrates that BT does seem to provide comparatively well configured routers to new users.

BT home networks using the "BT Home Hub" 1.0 and 1.5 were all using WEP encryption. These networks were identifiable based on their SSID, starting with "BTHomeHub-" followed by an alphanumeric pseudo-random string: for example, "BTHomeHub-7AFC". Other BT networks, using newer routers (SSID names starting with "BTHomeHub2-", "BTHomeHub3-" and "BTHub3-") were found to be using WPA2.

This suggests that many of the insecurely configured routers were installed some time ago, and have yet to be updated with more modern encryption methods. We contend that this is likely due to the upgrade policies of the ISPs.

The recent vulnerabilities discovered in WPS authentication, as described in the introduction, illustrates the ongoing importance of ISP response time to Wi-Fi security threats, and applies to many of the routers provided by ISPs. The way that ISPs react to these issues is expected to have a significant effect on the ongoing security posture of their customers.

6. RECOMMENDATIONS

Based on these findings, when ISPs provide routers to their customers, the following recommendations are offered:

- ISPs should make an effort to track which model of router and the version of firmware their customers are using, and automatically push updates and upgrades to users
- ISPs should proactively upgrade their users' routers (software and/or hardware) as soon as possible after critical security vulnerabilities are discovered and fixes are available – or *at least* contact customers and educate them on risks and provide update options
- When fixes are not yet available (as may currently be the case with some WPS configurations), ISPs should inform customers of the threats they face and estimate time until solutions will be available
- WEP should be removed as an option from new routers, or at least trigger obvious and informative alerts to users if they choose to switch to this *non-default* configuration
- Routers should come securely pre-configured, including adequately pseudo-random network keys and web administration passwords (rather than default passwords such as Sky's "sky" or Virgin Media's "changeme")
- Unless it has been demonstrated to be significantly less usable, as far as is practical, larger key spaces should be employed for pre-configured passwords: for example, by using alphanumeric rather than alphabetical passwords
- Other ISP specific recommendations:
    - BT should consider ways to improve the security posture of customers currently using BT Home Hub version 1 or 1.5
    - O2 should investigate and act upon their customers' routers employing WEP
- Users should be educated regarding maintaining the security of their networks

7. RELATED RESEARCH

Various small scale wardriving efforts have been conducted in Leeds, UK: such as a report from 2004 of 66 networks, all reported to be using either WEP or no encryption (Dlaverty, 2004).

Some other independent work has also analysed and critiqued the security of the routers provided by UK ISPs to their customers. For example, the security of the BT Home Hub router has received extensive criticism, not only for the choice of

encryption and key length (as discussed herein), but also for insufficient entropy of pseudo-random passwords, vulnerabilities in the web interface, and open ports for management services (Adrian Pastor, 2007). Problems have also been discovered with Sky's pseudo-random passwords (in this case with their older Netgear v2 DG934g routers), passwords can be deduced based on the (public) MAC address (John Leyden, 2008). These routers are also vulnerable to an attack that can determine the ADSL password, when the username is known (NewsreadeR, 2008).

As far as we are aware, this is the first empirical study to investigate correlations between security and ISPs, and how ISPs differ from each other in terms of the types of security provided to their users.

8. CONCLUSIONS

Analysis of data collected via wardriving in Leeds, UK, has shown a statistically significant effect on Wi-Fi security by ISPs, and significant differences between many individual ISPs. A number of networks were found to be using WEP, despite this being known to be a cryptographically broken encryption method, and these routers were provided by identifiable ISPs, who are in a position to be able to keep track of out-of-date routers. We contend that this highlights the importance of router upgrades, and have provided a number of recommendations for ISPs, router manufacturers, and home users that apply when ISPs provide routers with wireless access points to customers.

The question of duty of care was raised: should ISPs be considered responsible for the Wi-Fi security of their customers when they provide routers with wireless access points, given that ISPs often advertise that they provide secure networks, and many home users are unlikely to reconfigure the routers provided to them?

9. REFERENCES

Adrian Pastor, 2007. BT home flub: pwnin the BT Home Hub [WWW Document]. GNUCITIZEN. URL http://www.gnucitizen.org/blog/bt-home-flub-pwnin-the-bt-home-hub/ (accessed 10.28.12).

Bittau, A., Handley, M., Lackey, J., 2006. The final nail in WEP's coffin, in: Proceedings of the 2006 IEEE Symposium on Security and Privacy, SP '06. IEEE Computer Society, Washington, DC, USA, pp. 386–400.

Borisov, N., Goldberg, I., Wagner, D., 2001. Intercepting mobile communications: the insecurity of 802.11, in: Proceedings of the 7th Annual International Conference on Mobile Computing and Networking, MobiCom '01. ACM, New York, NY, USA, pp. 180–189.

Dlaverty, 2004. Open all hours - Wardriving in Leeds, West Yorkshire, England [WWW Document]. Openxtra. URL http://www.openxtra.co.uk/articles/wardriving-leeds (accessed 10.28.12).

Fluhrer, S., Mantin, I., Shamir, A., 2001. Weaknesses in the key scheduling algorithm of RC4, in: Vaudenay, S., Youssef, A. (Eds.), Selected Areas in Cryptography, Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 1–24.

John Leyden, 2008. Sky Broadband puts the fault into default Wi-Fi security: Users in guess-able random keys quandary [WWW Document]. The Register. URL http://www.theregister.co.uk/2008/02/21/sky_broadband_wi_fi_keys_unpicked/ (accessed 10.28.12).

NewsreadeR, 2008. Is your router secure? [WWW Document]. Sky User. URL http://www.skyuser.co.uk/skyinfo/783.html (accessed 10.28.12).

Stefan Viehböck, 2011. Brute forcing Wi-Fi Protected Setup: When poor design meets poor implementation [WWW Document]. URL http://packetstorm.foofus.com/papers/wireless/viehboeck_wps.pdf

Stubblefield, A., Ioannidis, J., Rubin, A.D., 2004. A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP). ACM Trans. Inf. Syst. Secur. 7, 319–332.

Tews, E., Beck, M., 2009. Practical attacks against WEP and WPA, in: Proceedings of the Second ACM Conference on Wireless Network Security, WiSec '09. ACM, New York, NY, USA, pp. 79–86.

Tews, E., Weinmann, R.-P., Pyshkin, A., 2007. Breaking 104 Bit WEP in less than 60 seconds, in: Proceedings of the 8th International Conference on Information Security Applications, WISA'07. Springer-Verlag, Berlin, Heidelberg, pp. 188–202.