An Investigation of Security Trends in Personal Wireless Networks

Lu Liu[1], Thomas Stimpson[1], Nick Antonopoulos[1], Zhijun Ding[2], Yongzhao Zhan[3]

[1]School of Computing and Mathematics, University of Derby, Derby, Derbyshire, DE22 1GB, United Kingdom
[2]Department of Computer Science and Technology, Tongji University, China
[3]School of Computer Science and Telecommunication Engineering, Jiangsu University, Jiangsu, China

Corresponding Author: Dr Lu Liu
School of Computing and Mathematics, University of Derby
Derby, Derbyshire, DE22 1GB
United Kingdom
Email: l.liu@derby.ac.uk
Tel: +44 (0) 332 59 1707
Fax: +44 (0) 332 59 7741

Abstract

Wireless networks are an integral part of day-to-day life for many people, with businesses and home users relying on them for connectivity and communication. This paper examines the problems relating to the topic of wireless security and the background literature. Following this, primary research has been undertaken that focuses on the current trend of wireless security. Previous work is used to create a timeline of encryption usage and helps to exhibit the differences between 2009 and 2012. Moreover, a novel 802.11 denial-of-service device has been created to demonstrate the way in which it is possible to design a new threat based on current technologies and equipment that is freely available. The findings are then used to produce recommendations that present the most appropriate countermeasures to the threats found.

Keywords

Personal Wireless Networks, Network Security, Wardriving

1. Introduction

Network security is a key issue in all the areas of computing. With the rise of smartphones, laptops, and tablets, which all utilise wireless networks for connectivity to the Internet, the effect of attacks on wireless security has become much larger and more significant. Vital and secretive information is broadcast through Wi-Fi daily, including E-Mail, instant messages and web browsing. Attackers can easily gain access to unsecure wireless access points and gather information needed to cause damage to users' computers or personal life.

Many end-users have little knowledge about computing; this has been reflected in their lack of home network security, with an absence of computer security, such as antivirus and firewalls. A new set of statistics about wireless security usage is created in this paper, with a comparison to previous research carried out in 2009, to demonstrate whether the development of security has occurred over a relatively short timeframe. By analysing this it is expected to exhibit the trends and evolution of consumer wireless security usage and whether or not home wireless networks are becoming more secure.

It has been over ten years since Fluhrer, Mantin and Shamir demonstrated the weakness of Wired Equivalent Privacy (WEP) [1]. Many home users are still not aware of the problems relating to this security standard. Overall, this paper will look at wireless security trends in the home user market, as well as creating novel wireless security attacks that aim to disrupt and deny wireless network usage together with theoretical design solutions. The idea behind this is to produce a set of statistics to display encryption utilisation and exhibit innovative threats or improvements on current attacks by furthering the damage potential. This research is to evaluate the functionality of freely available downloadable tools within a controlled environment and to use the process of Wardriving to create a set of statistics that present the trends of wireless local area networks in an easily read format. This research will be compared to previous studies done in December 2009 which will demonstrate the changes of security usage that have occurred within the past two years.

The rise of freely available downloadable tools threatens the security of all computer networks, whether wired or wireless. These tools, obtainable by anyone, compromise security on home and business networks, as well as throughout the Internet. This creates an environment that allows anyone with access to the Internet use of these tools to attack which may cause disruption to Internet services and computing resources. All the tools which have been analysed will have a walkthrough created to display how easily these tools can be used to cause the previously mentioned disruption or interception of communication within wireless networks. This should offer an excellent overall view of the most threatening freely available tools obtainable to anyone with Internet access. In addition, this paper will create a proof-of-concept device which integrate and advance the functionality offered by these tools.

The research outcome of this paper is not only useful for end users to improve the safety of their wireless networks and remove the network from some Wardriving attempts and useful for ISPs to work with consumers to ensure that customers are made aware of the important of wireless security, but also useful for government securities regulators to continue to innovate and change security standards to face the new security threats.

The rest of paper will be organized as follows: In Section 2, a literature review will be undertaken to display the past, present and possible future threats to wireless security, as well as network security as a whole. Following this, an in-depth analysis of threat from wireless security tools has been analysed in Section 3. The detailed design and implement is introduced in Section 4. In Section 5, the Wardriving research will be analysed and the statistics broken down into various types. Finally, Section 6 will provide the suggestions for improving any of the problems found during the research.

2. Related work

WEP has been cracked-or insecure-for some time now. This wireless security was initially thought to provide safety for everyone, including home users [2]. Today WEP can be cracked in as little as a few minutes [3]. With Internet Service Providers such as BT offering information on their websites stating, “WEP (Wired Equivalent Privacy) – Strong. Used by most computers and wireless routers.” [5], there is clearly a great problem in home user security, particularly when a large ISP such as BT is telling users that WEP is safe to use. Some authors comment that using WEP is preferable to no security and enabling it may make someone less of a target than the wireless access point of a neighbour [6].

With the situation of uninformed users utilising their home networks which may be running WEP unknowingly, there is a large percentage of unsecured home networks which could be compromised very easily [2], leading to a weakness which almost anyone with basic computer knowledge could exploit and gain entry to a network [2]. In a paper from 2008 mentioned that devices are regularly shipped with no security, or outdated technology such as WEP and that these access points can be cracked with common tools [7]. WEP is unsecure due to its basic foundation. WEP keys can either be 64bits or 128bits, 24bits of this being an initialisation vector. By utilising 128bits it gives the users a few more minutes of security. Cracking is done by sniffing traffic and discovering the needed packets and running such programs as Aircrack-ng [2].

WPA (Wi-Fi Protected Access) is the successor of WEP, created by Wi-Fi Alliance, significantly improves WEP’s encryption process by adding a concrete user authentication process. WPA introduces a new key security protocol, Temporal Key Integrity Protocol (TKIP) [19], which dynamically changes the keys during the session. WPA, although safer, is not fully secure. WPA has been noted as having a vulnerability to dictionary attacks, a process of using a list of words against a capture four-way handshake to find the pre-shared key [8]. This process is very slow and has a low probability, although it proves that it is possible to break WPA even though a more advanced standard has been used [8]. This creates a need for the passphrase to be in the dictionary file and a WPA four way handshake captured for the attack to be successful.

TKIP was believed to be secure, however, in late 2008 it was found to be vulnerable to attack. TKIP implements a ‘key mixing’ function that mixes the session key with an initialisation vector for each packet [10]. This is coupled with a 64bit Message Integrity Check (MIC) in every packet, which helps stop attacks on the fragile CRC32 integrity protection [10]. The attacks on TKIP rely on 802.11e QoS (Quality of Service) to be enabled; this allows an attacker to reuse previously transmitted initialisation vectors on 802.11e channels [8]. This dependency ensures the attack is limited, with few users utilising 802.11e [11].

WPA utilising TKIP has had two papers written about the vulnerabilities. The first by Beck and Tews proved the existence of insecurities but this attack is reasonably slow, around 12-15 minutes. The attack itself relies on 802.11e and an ARP packet being captured, then 7 custom packets re-injected to decrypt the ARP packet [9]. The second, by Ohigashi and Morii, proved that attacks on TKIP can take as little as 60 seconds. Neither of these attacks can, however, provide the encryption key/password of the wireless network [11]. This means that TKIP is generally safe for home usage until a greater threat is proposed, although due to these initial demonstrations it proves that AES should be used wherever possible.

Although WPA2 is still regarded as being extremely secure and should always be used on any device where it is possible. All new wireless devices will most likely be AES compatible. WPA2 is based on IEEE 802.11i [15] standard. WPA2 provides a new AES-based [8] algorithm CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) to replace the old RC4 stream cipher which has been used in WEP and WPA2. In WPA2, AES is defined in counter cipher-block chaining mode (CCM) and supports the Independent Basic Service Set (IBSS), which enables security between client workstations operating in ad hoc mode. A table is given in Table 1 to compare WEP, WPA and WPA2 [16].

Table 1. Comparison of WEP, WPA and WPA2

	WEP	**WPA**	**WPA2**
Encryption	RC4	RC4	AES
Key sizes	40/104 bit	128 bit	128 bit
IV size	24 bit	48 bit	48 bit
Per-packet key	Key + IV	TKIP	CCM
Data integrity	CRC-32	Michael	CCM
Data integrity	None	IV seq.	IV seq.
Key management	None	802.1X	802.1X

3. Threat Analysis

This section will outline a number of commonly found tools, analyse their threat against residential access points and then develop on them to create novel wireless security attacks within the results obtained section of this paper.

3.1 Aircrack

Aircrack-ng [3] is one of the most used and well-known wireless security tools, allowing even inexperienced users a way of breaking into wireless access points with ease. The command line based UI may be difficult for some to manage, although with many tutorials available, this is not likely to be a problem.

This tool is included within the Backtrack Linux suite of tools which has very few requirements - the main necessity being a wireless network card capable of capturing and injecting packets. Aircrack-ng includes many different wireless security tools, from the basic WEP and WPA cracking program, to a tool that sets a wireless network card into monitor mode to begin the most basic captures. This includes:

- Airbase-ng
- Aircrack-ng
- Airdecap-ng
- Airdecloak-ng
- Airdriver-ng
- Airdrop-ng
- Aireplay-ng
- Airgraph-ng
- Airmon-ng
- Airodump-ng
- Airolib-ng
- Airserv-ng
- Airtun-ng
- Easside-ng
- Packetforge-ng
- TKIPtun-ng
- Wesside-ng

These tools are all geared towards allowing attackers to gain unauthorised access to wireless access points. Many of which are easy for setting up the environment for an attack, such as Airmon and Airdriver.

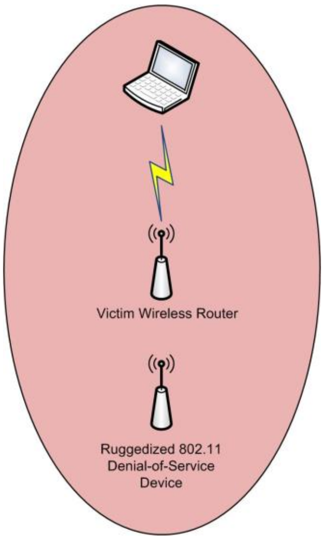

Figure 1: An Aircrack-NG attack topology

With the ease of use and ease of access, the Aircrack suite can be seen as one of the biggest threats to wireless security, although the equipment and wordlists necessary for a WPA attack may limit some attackers. As illustrated in Figure 1, to successfully attack a WPA based wireless access point, the four-way handshake should be captured. This is completed via the process of running Airodump-ng and utilising Aireplay-ng to deauthorise any connected users, thus forcing the four-way handshake produced during connection to occur once again. Once this is captured the handshake should then be decrypted using the process of bruteforce, or using Aircrack-ng to test a wordlist against the captured packet. This is a lengthy process with very little chance of succeeding and is dependent on the length and complexity of the password used.

A newer method for cracking WPA has recently been demonstrated [14]; this uses the process of hash tables to discover the password from the four-way handshake. Although much quicker, the procedure requires the pre-calculation of hash tables; as these tables should be pre-computed against the target SSID, which may take hours. However, there is a list of the top 100 SSIDs with pre-computed hash tables available. An attacker needs to decide whether or not it is worthwhile to pre-compute the needed hash table, or work with the slower wordlist. This method will be analysed within the results obtained section of this paper, with a possible theoretical design solution being demonstrated.

3.2 MDK3

MDK3[13] is the tool which will be used within the 802.11 ruggedized denial of service device that was created as a novel concept for this project. As illustrated in Figure 2, this tool can cause authentication, deauthentication and disassociation by flooding these packets to an access point, often causing a reboot or crash of wireless routers that are targeted. These attacks can either be widespread, targeting all nearby wireless routers, or by way of a black and whitelist. The usage of a blacklist within the parameters of the mdk3 command will only target the chosen access points, while a whitelist will cause the program to attack all access points in range apart from the selected MAC addresses.

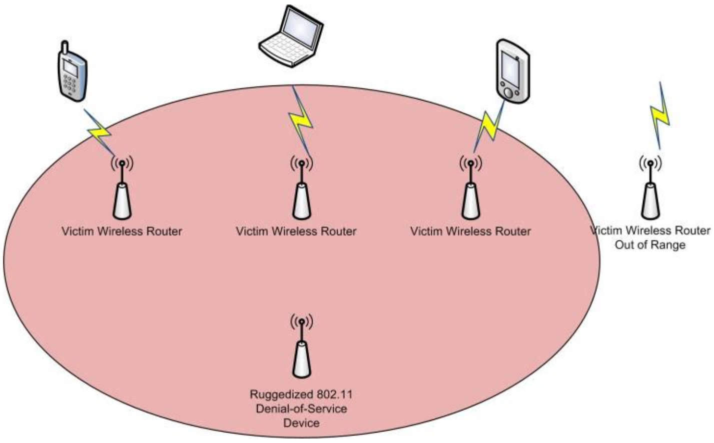
Victim Wireless Router
Victim Wireless Router
Victim Wireless Router
Victim Wireless Router Out of Range
Ruggedized 802.11 Denial-of-Service Device

Figure 2: An MDK3 attack topology, with an unaffected access point on the right

Overall this program is easily obtained and can be a threat to many wireless networks. The authentication mode DoS has been effective in tests along with the novel 802.11 DoS device that was created, although the other modes also have possibilities to cause damage. A demonstration of successful attacks will be provided in this paper.

3.3 Kismet

Kismet [12] is a passive wireless network detection tool used mainly for the process of Wardriving, although, it can also be used to audit wireless local area networks for any interference from neighbouring access points. Kismet excels at passively discovering wireless networks and logging their encryption type, network name, BSSID, location if there are any connected clients.

Kismet has been used as the core program for the research within this project which has led to the discovery of many unsecured access points, whether these are open or using WEP encryption. This detection, coupled with the location logging ability would allow attackers to complete a mass survey of access points and log the GPS coordinates of any access point that could be used in the future. Kismet may also be used in conjunction with Aircrack, with an Aircrack-PTW module capable of cracking WEP while a survey is taking place, although, this capability is restricted to passive cracking, meaning Kismet will not actively re-inject ARP packets or use an active attack such as fragmentation [12].

Whilst detection can be seen as an attack, it may also be used as an intrusion detection system, by showing the status of an access point and any connected clients. This makes Kismet a flexible tool with intrusion detection capability by alerting to a number of different vulnerabilities that can also be coupled with IDS such as Snort [12]. This exhibits the capacity for Kismet to be both an offensive and defensive application.

4. Development and Experiments

This section focuses on the methods of data collection and the proposed tools for analysis within the results obtained section of this paper. The Wardriving process is explained, along with the solution that will give the most accurate results in comparison to previous research. Past research from 2009 is briefly described and the reasons for updating and continuing the research for 2012 have been presented.

4.1 Wardriving Process

Wardriving will allow for an accurate primary data collection, coupled with an analysis of wireless security tools that will provide an insight into the current threats. Wardriving is the process of passively collecting the data sent out from wireless access points, such as, network name, encryption type, and BSSID. The data collection allows for a set of statistics to be created that display how wireless network encryption has evolved. This research will closely related an investigation completed two years previously to allow for an exact and detailed data collection process. By ensuring that the same restrictions and considerations relating to equipment are achieved, the research will be performed as scientifically as possible.

The most significant data for this project will be the encryption type, as this identifies the security used on an access point. Previous experience has shown that utilising GPS during this process ensures that results will be displayed in an easily read format as it permits the use of mapping software. This project will effectively mirror our previous research carried out in 2009.

There are many different programs that will passively collect the data needed for this research. However, one of the most popular and flexible is Kismet [12]. Privacy of the participants within the research is imperative and due to Kismet's passive data collection, this will not be an issue. While Kismet does have the capability to crack WEP encryption with an added Aircrack-PTW plugin, this will not be utilised within this project [12]. The Aircrack suite may be used later within this project to create a novel all-in-one ruggedized device capable of autonomously cracking wireless access point encryption, however the research into this capability should first be completed [3].

This project will use the Alfa AWUS036H Wi-Fi USB, along with a Globalsat BU-353 GPS USB and an EEEPC 900. This is due to the equipment being used previously and it is believed utilising this hardware again should provide the most accurate statistics possible. Furthermore, in order to ensure that a scientific approach is taken, the same route will be completed. However, it is likely that there will be more access points due to the growth of wireless networks and the Internet.

To further achieve a reliable result, the process of data collection will take place on two separate days. This will allow for a merging of results to ensure that as many access points are collected as possible. This approach was not taken in 2009; however, it will allow a comparison and analysis of results from 2012. The process will take place on a Saturday evening during peak hours from 6-7 pm and a Sunday morning from 8-9 pm, when it is presumed that many will be asleep. This should provide data as to whether users power down their Wi-Fi enabled routers overnight.

Overall, the planned route, dates, and times chosen, along with the equipment chosen, should provide excellent coverage with accurate data collection. All equipment chosen works effectively with the Backtrack Linux operation system chosen and Kismet output files will supply the format that can be exported into GISKismet.

Previous Wardriving research was a longer procedure due to the testing phase. During this, differing methods were examined, such as using a portable router as a Kismet drone. However, the equipment used, and that will be used again for this project, has given the best results in any of the tests and therefore, it will be used again. This will also allow the results to be scientific and fair.

Research highlighted that many users did not have suitable wireless security configured on their home wireless access points. In 2009, a total of 267 access points utilised WEP. Further analysis and comparison of these results will be given within the results obtained section of this paper, along with the comparison of 2012 results that differ due to the date and time of the data collection.

4.2 Ruggedized 802.11 Wireless Denial of Service Device

Mdk3[13] is a tool that creates the possibility for denial of service attacks in 802.11 environments. In this section, a novel use of this tool will be designed and developed to create a working ruggedized 802.11 denial of service device.

4.2.1 Design and Development

The architecture of the ruggedized wireless denial of service device is illustrated in Figure 3. The initial requirement for the design was a Fonera router custom firmware to create a wireless router that will accept the programs and libraries needed for a success attack platform. This was completed using a tftp server along with the firmware called Piranha and a custom serial cable made from a Nokia DKU-5 phone data cable in order to connect directly to the Fonera router.

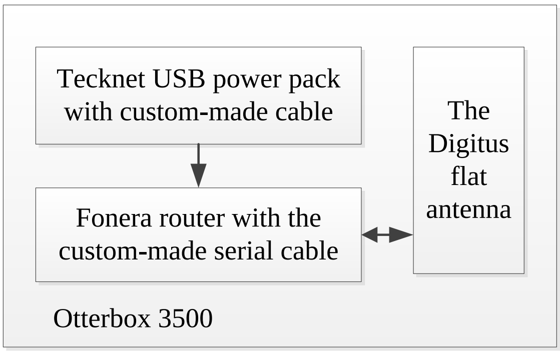
Tecknet USB power pack with custom-made cable
Fonera router with the custom-made serial cable
The Digitus flat antenna
Otterbox 3500

Figure 3: The architecture of the ruggedized wireless denial of service device

Following a successful flashing of the router with the custom firmware chosen, the next step was to ensure that the router could be powered while still being mobile. The approach taken was to purchase a Tecknet USB power pack that was aimed at mobile phone users. It was expected that this method would power the device for a long period of time. However, when the device arrived, none of the supplied power adapters would fit the Fonera router’s power socket, therefore a custom-made power cable had to be created. This was prepared by selecting a USB power cable and purchasing the correct size socket.

The rugged box chosen for this device was an Otterbox 3500 that was chosen due to its crushproof and waterproof design. The size of the box was also important as it had to be large enough to ensure that all the equipment was housed comfortably, while being small enough to be easily portable. This container featured modular foam, which the three components fit in securely. The Otterbox fit these requirements perfectly although there were problems with the antenna size as it was too large.

The antenna proved to be a problem with this design, as placement within the container was difficult. The solution was to source and purchase a flat, short wireless antenna; the Digitus Flat Antenna was the option for this. Due to the Otterbox featuring the aforementioned modular foam, the installation of this antenna was easily completed.

Once all the components were successfully placed within the Otterbox 3500, the device could then be tested for wireless connectivity. This was accomplished by enabling STA or station mode on the wireless router and testing the distance that the device was capable of. The container did not affect the overall connectivity or wireless signal and the range was that of a normal wireless device, around 10-20m. Cooling was guaranteed by ensuring that each device was kept separate, within enough room for a small amount of airflow. Overall the device was found to be compact with excellent connectivity; the next step was to configure Mdk3 to run at startup.

The process of using mdk3 at start-up is relatively easy. By using the created serial cable to access the router via SSH it is then possible to navigate to /etc/rc.common, which acts as the start-up script for the device. As an example, to use the device in beacon flood mode, the following is used:

```
--------------------------------------------------------------------------------
#!/bin/sh /etc/rc.common
Location of the file
START=90
wlanconfig ath0 destroy
ifconfig wifi0 down
Destroy and take down the wireless interface
macchanger --mac=22:22:33:33:44:44 wifi0
Change the wireless interface MAC address
ifconfig wifi0 up
Bring the wireless interface up
wlanconfig ath0 create wlandev wifi0 wlanmode monitor
Put the wireless interface into monitor mode
mdk3 ath0 b &
Start mdk3 in beacon flood mode
exit 0
--------------------------------------------------------------------------------
```

This is a demonstration of a novel threat that can be created using freely available firmware, equipment, and security tools from the Internet. This device is capable of authentication, deauthentication and disassociation attacks that can also be targeted using a black or whitelist. While built on pre-existing ideas, this novel threat creates a ruggedized device capable of withstanding outdoor conditions and furthering the scope for attacks.

5. Analysis of Obtained Results

The investigation has been conducted in Derby, UK; this involved the same route for our research completed in 2009 as well as the same equipment. Research results from 2009 displayed that 28% of users were using WEP. This section will compare these previous results with new findings, along with a comparison of two different times of day. This fair and scientific approach allows for data collection in a way that collects as many access points as possible, covering two days and two differing times. Wireless security is imperative to any network; by ensuring that a network is secure the users of the network can be confident that attackers cannot gain unauthorised access. This section will aim to compare and analyse the past and present statistics.

The method for data collection during the previous project was a lengthy process, involving various approaches to discover the best technique. This was initially done via a Kismet drone running on a Fonera 2210 router that was connected to an ASUS Eee PC 900 running a Kismet server. However, this did not allow for integration or signal strength that was optimal for data collection, therefore, the method was altered to utilise an Alfa AWUS036H Wi-Fi USB and Globalsat BU-353 GPS USB.

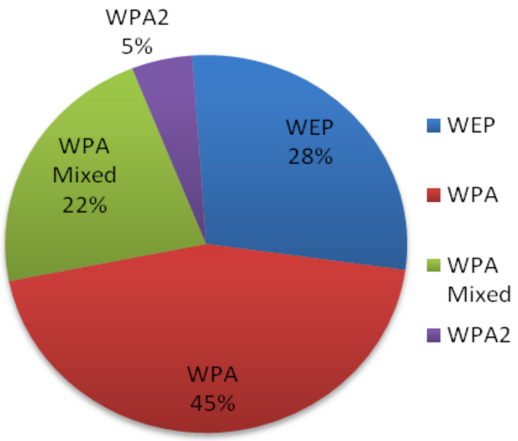

Figure 4: Derby wireless security usage in 2009

Clearly, the amount of users utilising WEP has dropped significantly since 2006, however, 28% of users were still using WEP as the only form of security on their access points in 2009. Lack of awareness relating to wireless security may be due to the inexperience of users, although ISPs and vendors should also share the blame. Poorly configured routers, including equipment shipped with default passwords allow any attacker to simply connect, or exploit weak security such as WEP. The solution for this was to utilise WPA on any newly installed equipment during the installation of Internet in residential and commercial properties.

Research from 2012 is promising, however, as is shows a very positive trend in wireless security usage. Figure 5 shows WEP usage has dropped significantly by around 15% to 13% in total, in comparison to Figure 4. This means that WEP usage has more than halved between 2009 and 2012. This is an encouraging trend that exhibits the changing face of wireless security, which change in security is most likely due to ISP installation practices changing, as with new home hubs are being installed with WPA, rather than WEP.

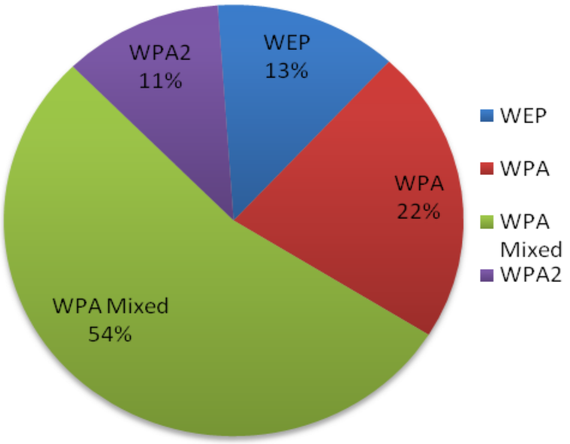

Figure 5: Derby wireless security usage in 2012

The research shows a large influx of BT OpenZone and BT FON access points as displayed in Figure 6. This shows that many people have either moved to, or now have Internet from, BT. These access points all utilise WPA as the standard encryption type; this, along with the usage of WPA-mixed used by Virgin wireless hubs, shows the sizeable move from WEP is clearly due to ISP default settings changing.

Figure 6 shows that ISPs have taken on their share of ensuring customer safety, as the majority of BT and Virgin Media access points now utilise WPA. However, despite this, the majority of WEP access points still display an SSID of either BT or Virgin Media. This illustrates the difficulties in changing user habits as well as the problems when dealing with computer illiterate users.

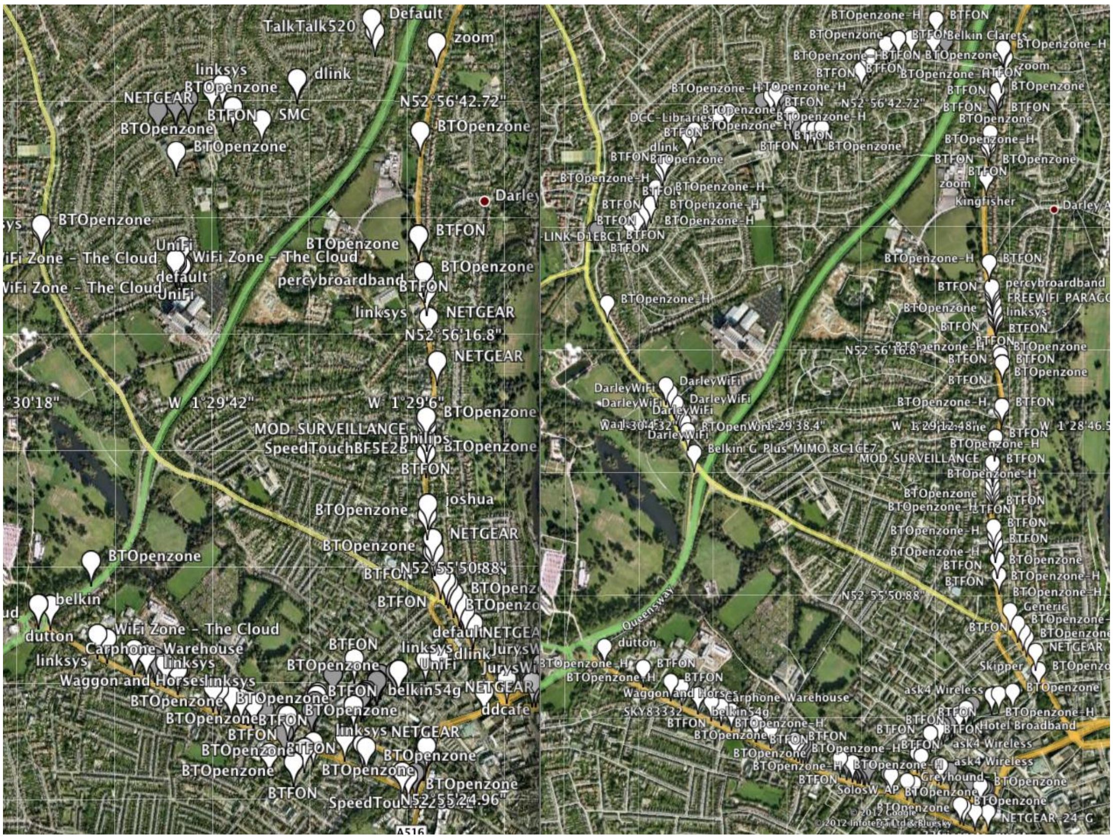

Figure 6: Open access points in Derby, 2009-2012

Research in 2012 was completed over a two-day period and then merged; this was also coupled with the same equipment used in prior research to ensure the most accurate data collection possible. Overall, both instances of data collection resulted in similar percentages of access points gathered. This was a positive outcome, as the data collection was confirmed to be precise and fair.

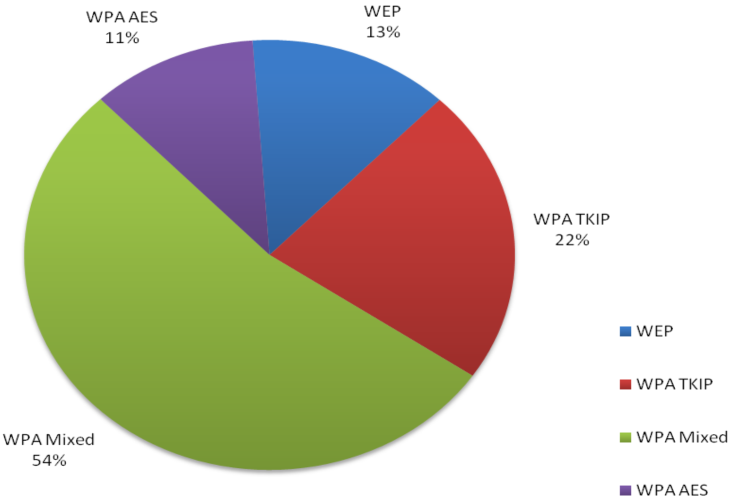

Figure 7: Derby wireless security usage collected on 03-03-2012

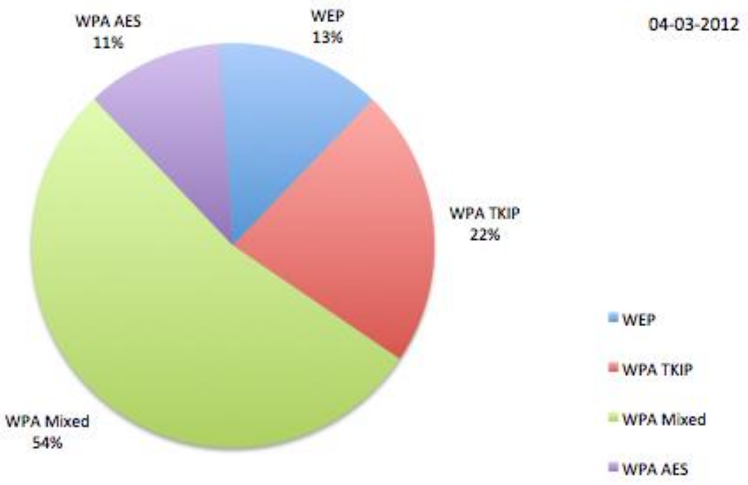

Figure 8: Derby wireless security usage collected on 04-03-2012

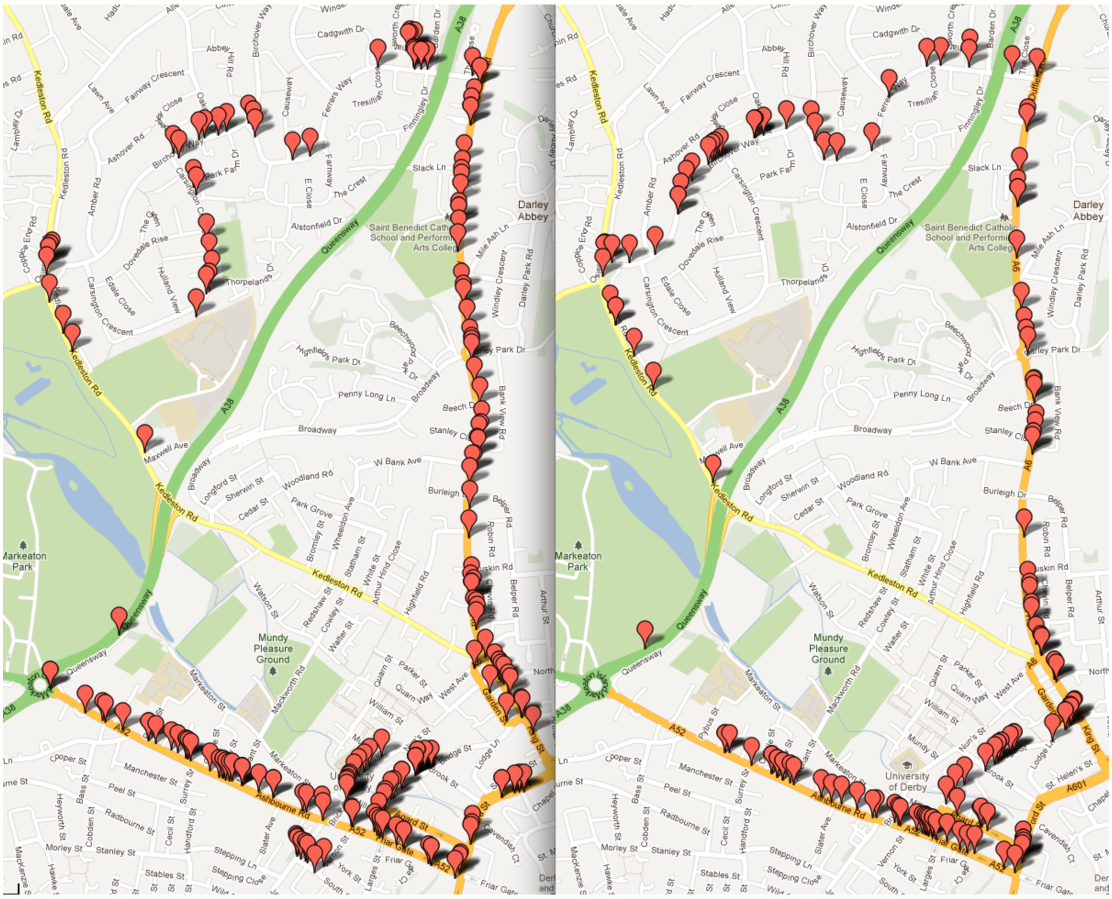

Figure 9: WEP usage in Derby 2009-2012

Wireless access points utilising no encryption whatsoever has dropped greatly. There were no residential open access points during the 2012 survey. This means that around 5% of previously unsecured wireless routers have now been protected. Figure 9 provides an insight into the usage of WEP, which shows only slightly more protection than open access points, from 28% down to 13% total, around 137 compared to 267 in 2009. This is a very encouraging trend as mentioned earlier.

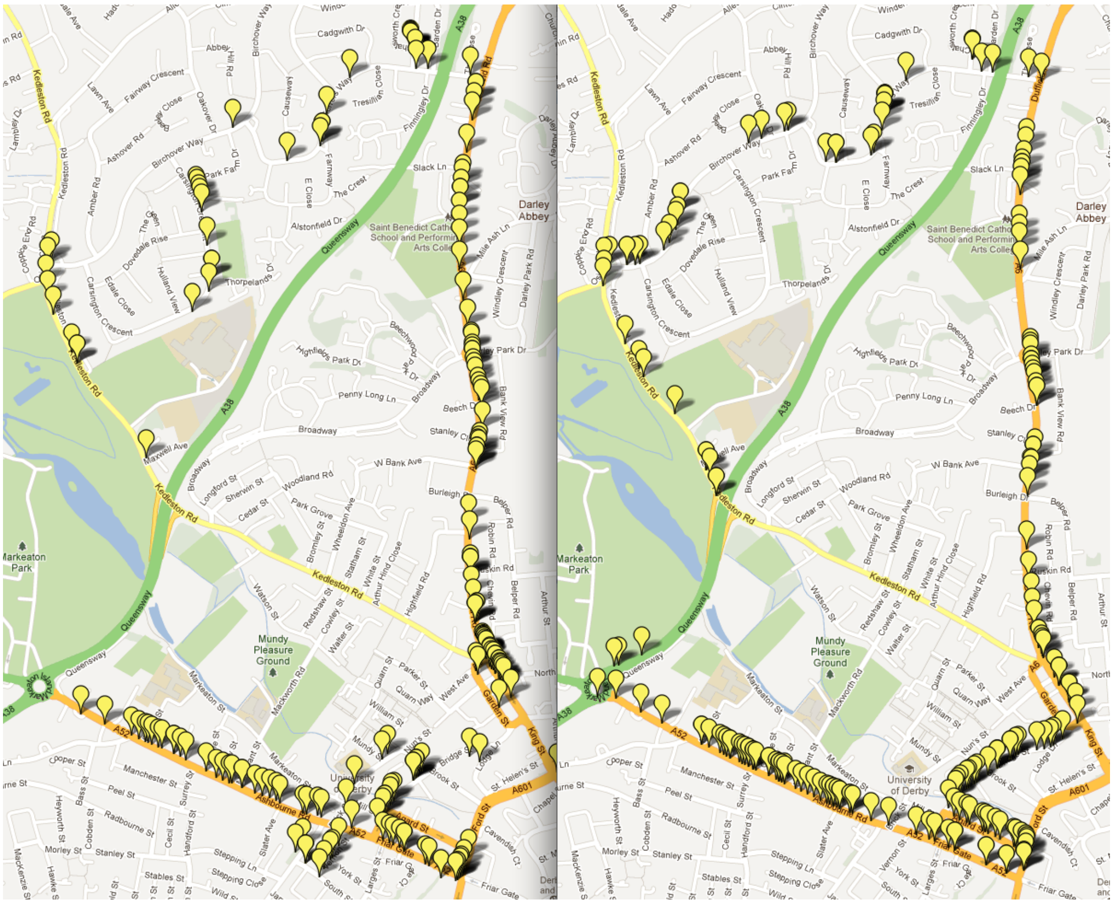

Figure 10: WPA usage in Derby 2009-2012

Figure 10 shows the access points using WPA in 2009 on the left, with 2012 on the right. In 2009 there were 421 WPA access points, in 2012 a total of 234 were collected. While at first this appears to be a negative trend, TKIP has been replaced in many instances with WPA Mixed. WPA is currently the most secure wireless security available for the average residential user, with WPA2 being the most secure version. 87% of users are utilising WPA currently, this is a very positive outlook in comparison to 2009. 22% of WPA access points employ WPA, this version has shown slight vulnerabilities and should be avoided where possible. However, a strong alphanumeric password ensures security in the majority of circumstances.

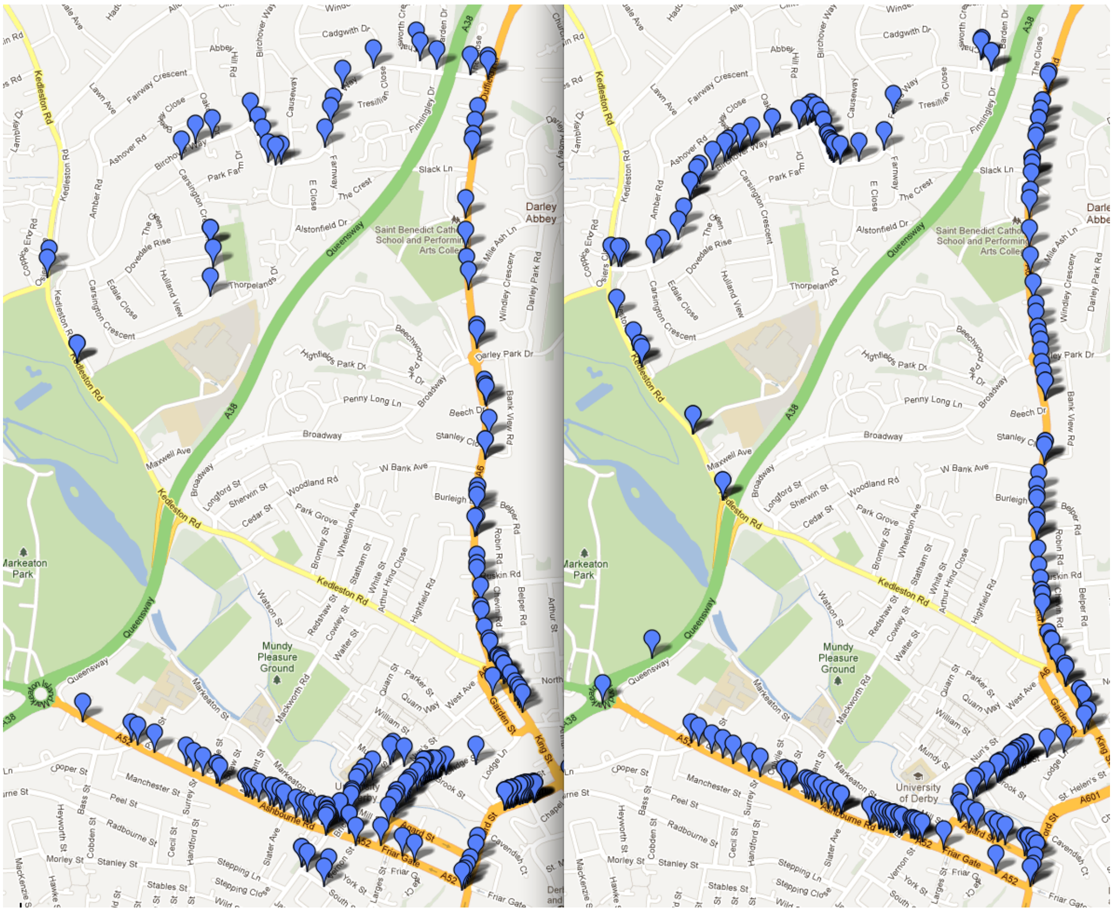

Figure 11: WPA Auto usage in Derby 2009-2012

WPA Mixed, or WPA Auto, allows the use of both WPA and WPA2. This mode is useful for any legacy hardware that does not support the higher speed link needed for AES encryption. A total of 209 access points utilised WPA Mixed in 2009, while in 2012 this number increased to 570, a 272% difference. This appears to be the foremost reason for the lower numbers in WPA usage and may be due to the way in which ISPs deal with default settings. This mode would be compatible with many users and still allow those with out-dated laptops to connect to new wireless routers. Figure 11 exhibits the sizeable difference clearly; with 2012 WPA Mixed access points far outnumbering those in 2009.

One of the most noticeable differences is the usage of WPA2, with a 258% rise. WPA2 is known as the most secure, as stated earlier within this project. A strong alphanumeric password coupled with WPA2 is the best form of security for the majority of residential users that can support the encryption type. This large rise is encouraging, as this shows that consumers are improving security not only by discontinuing their use of WEP but also utilising the most secure form of encryption. Figure 12 displays the difference between 2009 and 2012 and a stark contrast can be seen within three years.

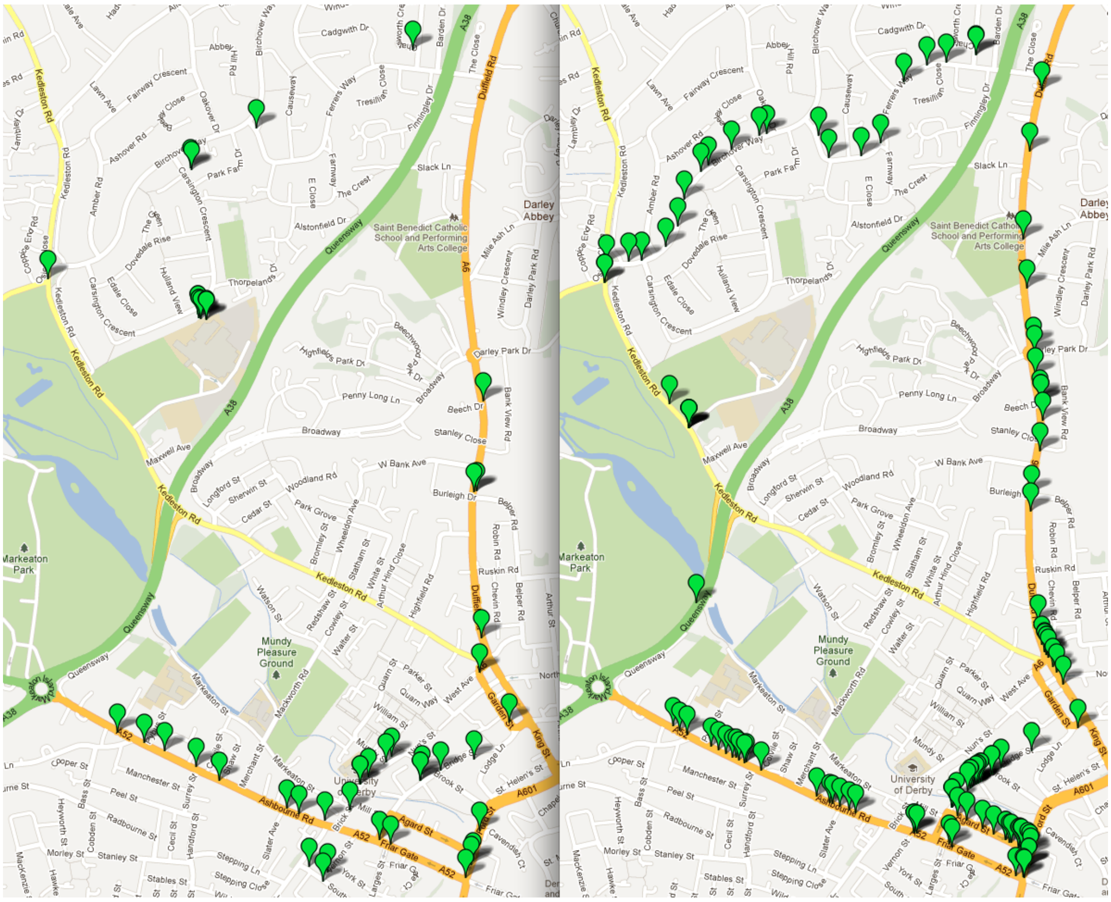

Figure 12: WPA2 usage in Derby 2009-2012

Tews et al. [15] also carried out research in both 2006 and 2007. This allows for a greater timeframe to be included and shows that a very positive trend has emerged. In 2006 and 2007, similar research was carried out in Germany that demonstrated the widespread usage of WEP. In 2006 a total of 59.4% of access points utilized WEP, while in 2007 this number reduced to 46.3%. This number continuously decreased to 24% and 10% in 2009 and 2012, respectively, according to our measurement. By creating a timeline of this wireless security usage by compiling all the data together, the rise of WPA1/2 and the fall of WEP, coupled with the increased number of residential access points with guest access can be demonstrated and is shown Figure 13, with the data from 2006, 2007, 2009 and 2012.

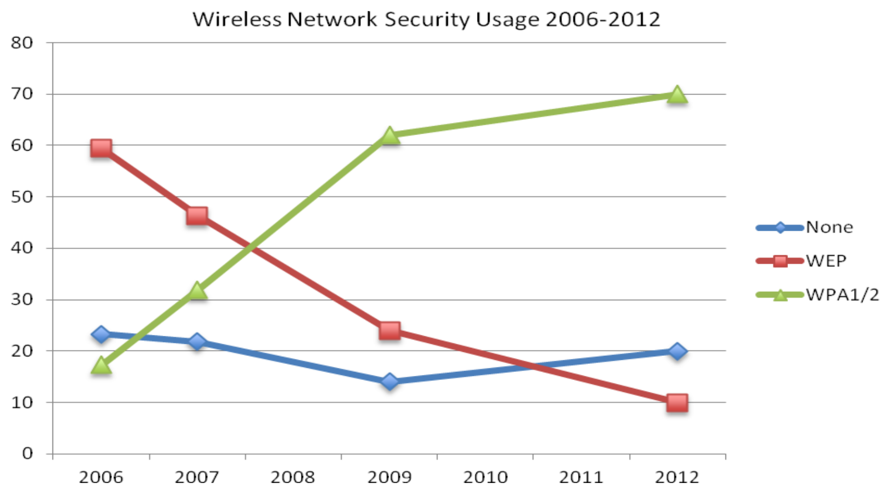

Figure 13: A timeline of wireless security usage 2006-2012

Overall, this research is very positive. WEP usage has reduced, while WPA1/2 has increased greatly, with WPA 2 usage increasing by 258%. As mentioned, this appears to be due to the new wireless router installations and upgrades to old and new customers, with BT and Virgin Media access points becoming far more secure than previous research has shown. This now means that only around 13% of users are utilising unsecured access points, leading to a decrease in the amount of targets for any attackers attempting to gain unauthorised access.

The trend throughout this research, including research from 2006 and 2009, has been the decreasing of the older security types which have long been known to be insecure, however, this change is taking a great deal of time. The ideal result for any future research would be a sample that only includes WPA2, although, due to legacy hardware and some incompatibility. The best that can be hoped for is for WEP to become unused entirely. This could be possible in future results, as the trend for WEP is an encouraging one, with a 63% fall within 6 years.

While the majority of wireless access points are secure, attackers can still target the ones that remain insecure and ISPs should focus on ensuring that these customers are helped. Further recommendations will be outlined within the final section of this paper; however, the results from this research show that the ISPs are very close to ensuring wireless security through the process of upgrading current and new customers to more secure wireless routers.

6. Conclusion and Recommendations

This paper investigates the trends within security usage in wireless networks and discovers wireless security threats that are freely available to download. This paper has demonstrated the evolution of wireless security. The overall findings display the fact that wireless security is improving in terms of encryption. This dramatic drop in WEP use is beneficial to the general view of computer security, as it indicates that ISPs are indeed upgrading users security when new installations of wireless routers are undertaken. In addition to this, the research appears to show that many of the access points in 2006 that used no encryption whatsoever have now been secured.

WPA2 usage is extremely important, with TKIP showing a sign of vulnerabilities [10], the need to utilise the security that provides the highest amount of protection is imperative for long-term safeguards. An increase of 258% demonstrates that not only has WEP use fallen by 50% within three years, but also the best form of encryption is on the rise. The research results demonstrate that from 2006-2009, the drop in WEP usage was sizeable and the slowing of this from 2009-2012 may be due to the difficulty in ensuring that computer illiterate users change their wireless security settings. Moreover, the novel threat created for this project displays the way in which pre-existing tools and equipment can be used to produce a device that furthers the scope of the original attack greatly. By creating a ruggedized 802.11 device from freely available tools and equipment purchased from the Internet, the demonstration has provided an insight into what is possible.

Research has shown a large increase in the number of BT and Virgin access points. The increase of new access points with guest access and WPA protection appear to be closely linked, showing that the ISPs clearly have the ability to improve wireless security as a whole during future upgrade plans. Along with this, new installation procedures, which have been introduced recently, include higher security during initial configuration and therefore, wireless security practices within residential properties have improved greatly. It is believed this practice should continue, and ISPs should ensure that customers are made aware of the important of wireless security, through emails or postal methods.

WPA2 is currently the only option available to the majority of consumers that has no known exploits or vulnerabilities other than brute force dictionary attacks. This means that this is clearly the only wireless security type that should be utilised on all wireless devices. However, due to the incompatibility with older wireless devices, this may mean that many devices should use WPA Mixed. Thus, WPA encryption type coupled with a lengthy password will generally protect almost all wireless access points.

In the future work, we will continuously monitor the security usage in personal wireless networks in the UK as well as other countries to identify the factors affecting the security usage in different countries. Moreover, detailed recommendations will be made to the ISPs and Internet users to improve their awareness of security threats and increase the usage of security mechanisms in home wireless networks.

Acknowledgment

The work reported in this paper has been supported by the Sino-UK Higher Education Research Partnership for PhD Studies, Natural Science Foundation of Jiangsu Province of China, RLTF e-learning Cloud Programme, National Natural Science Foundation of China Program (61272074), China 973 Fundamental R&D Program (2011CB302600) and Visiting Research Fellow Program of Tongji University.

References

[1] Fluhrer, S.R., Mantin, I., Shamir, A., (2001) Weaknesses in the Key Scheduling Algorithm RC4, Proceeding SAC '01 Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography, Springer-Verlag London, pp 1-24.

[2] Bradley, T., Carvey, H., 2007, Essential Computer Security: Everyone's Guide to Email, Internet, and Wireless Security, Rockland: Syngress

[3] Aircrack-ng, 2010. Aircrack-ng, Aircrack-ng Documentation, [Online], Available at: http://www.aircrack-ng.org/doku.php?id=aircrack-ng, [Accessed on: 20/10/12]

[4] Gast. M, 2002, 802.11 Wireless Networks, : The Definitive Guide Creating and Administering Wireless Networks, O'Reilly Media

[5] BT, 2010. Wireless Safety and Security, Wireless Safety and Security | Help | BT.com Help, [Online],Available at: http://bt.custhelp.com/app/answers/detail/a_id/13887/c/346, [Accessed on: 20/10/12]

[6] Hurley, C., Barker, B., Hiser, R., Barnes, C., Kanclirz, J., Bautts, T., McCullough, A., Bonawitz, D., Wheat, J.A., 2006, How to Cheat at Securing a Wireless Network, Rockland: Syngress

[7] Pescatore, J., Young G., Ant Allan, A., Gerard, J., Feiman, J.,MacDonald, N., 2008. Gartner 2008 IT Security Threat Projection Timeline, [Online], Available at: http://my.gartner.com/portal/server.pt?open=512&objID=260&mode=2&PageID=3460702&resId=747229&ref=QuickSearch&sthkw=WEP, [Accessed on: 20/10/12]

[8] Beck, M, 2010, Enhanced TKIP Michael Attacks, [Online], Available From: http://download.aircrack-ng.org/wiki-files/doc/enhanced_tkip_michael.pdf, [Accessed on: 20/10/12]

[9] Chandra, P., 2005. Security and Cryptography, Bulletproof Wireless Security, Oxford: Newnes

[10] Beck, M., Tews, E., 2008, Practical attacks against WEP and WPA, [Online], Available From: http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[11] Ohigashi, T., Morii, M., 2009, A Practical Message Falsification Attack on WPA, [Online], Available at: http://jwis2009.nsysu.edu.tw/location/paper/A%20Practical%20Message%20Falsification%20Attack%20on%20WPA.pdf

[12] Kismet, 2012, Kismet, [Online] Available From: http://www.kismetwireless.net/

[13] ASPj, 2009, ASPj's WiFi Page, [online] Available From: http://homepages.tu-darmstadt.de/~p_larbig/wlan/#mdk3

[14] Renderlab, 2012, The Renderlab: Church of Wifi WPA-PSK Rainbow Tables, [online] Available From: http://www.renderlab.net/projects/WPA-tables/

[15] Tews, E., Weinmann, R.P., Pyshkin, A., 2007, Breaking 104 bit WEP in less than 60 seconds, [Online] Available From: http://eprint.iacr.org/2007/120.pdf

[16] Hassinen T., 2006, Overview of WLAN security, Proceeding of Seminar on Network Security, TKK T-110.5290, 2006.