Reliability, Availability and Security of Wireless Networks in the Community

Carsten Maple, Geraint Williams and Yong Yue
Institute for Research in Applicable Computing
University of Bedfordshire
Luton Campus, Park Square, Luton, Beds, LU1 3JU, UK
E-mail: carsten maple@beds.ac.uk, geraint williams@beds.ac.uk, yong.yue@beds.ac.uk

Keywords: security, WEP, WLAN, WPA, risk assessment, risk management, threat analysis.

Received: March 12, 2007

Wireless networking increases the flexibility in the home, work place and community to connect to the Internet without being tied to a single location. Wireless networking has rapidly increased in popularity over recent years. There has also been a change in the use of the internet by users. Home users have embraced wireless technology and businesses see it as having a great impact on their operational efficiency. Both home users and industry are sending increasingly sensitive information through these wireless networks as online delivery of banking, commercial and governmental services becomes more widespread. However undeniable the benefits of wireless networking are, there are additional risks that do not exist in wired networks. It is imperative that adequate assessment and management of risk is undertaken by businesses and home users. This paper reviews wireless network protocols, investigates issues of reliability, availability and security when using wireless networks. The paper, by use of a case study, illustrates the issues and importance of implementing secured wireless networks, and shows the significance of the issue. The paper presents a discussion of the case study and a set of recommendations to mitigate the threat.

Povzetek: Zanesljivost, varnost in dosegljivost brezžičnih omrežij.

1 Introduction

The use of the Internet is increasing by home users has been continually increasing for some time, and this increase can also be seen in the context of businesses, banking and governmental services. According to the Office for National Statistics, more that half of the households in the UK had some form of Internet connection in 2005. The number of households that have an Internet connection is a statistic that has steadily risen from just over 30% of households in 2000, to 54% of households in 2005 [Office for National Statistics 2007]. In an article in New Scientist in 2005, Graham-Rowe predicted the growth of broadband Internet connection and wireless networks in the home up until the year 2009. It was predicted that in 2006 the percentage of households in Western Europe with both a broadband connection and wireless network would be approximately 12% [Graham-Rowe 2005]. As the number of households that utilise an Internet connection, so too does the range of services that are accessed.

In recent years, industry has recognised the benefits in teleworking. Companies are no longer concerned that those working away from the office are simply not working. Indeed, if anything, those working away from the office now tend to work too much. In 2004 in all US government departments, there 751, 844 employees deemed to be eligible for teleworking out of 1, 749, 998, a total of 43% of the workforce. Of those eligible for teleworking, 102, 291 undertook the activity at least some of the time, 14% of those eligible or 6% of the total workforce.. In the UK similar statistics were witnessed in 2001. In the spring of 2001, 2.2 million people in the UK, representing 7.4 per cent of the total labour force, worked from home at least one day a week using both a telephone and a computer to undertake their duties. This had represented a dramatic growth over previous years. The total number of teleworkers in the UK in 2001 had increased by nearly 70 per cent over the period 1997 to 2001 [Office for National Statistics 2002]. According to the Sunday Times the percentage of staff working one morning or afternoon a week at home has more than doubled in the past two years. The newspaper reports that according to research for The Sunday Times 100 Best Companies to Work For 2007 List, the figure has risen from 14.1% to 31.7% [Thomas 2007].

The nature of how teleworkers operate has also changed. In 2001, 71% of teleworkers operated in different places using home as a base. This percentage had increased to 75% of all teleworkers operating in different places using home as a base. The increase in the number of teleworkers operating in a different place using home as a base had increased from 1.05 million in 2001 to 1.77 million in 2005, an increase of 60% [Office

for National Statistics 2005]. This increase in the mobility of teleworkers presents a significant increase in risk of security compromises.

Year	Homeworkers			Teleworkers		
	Works mainly at home	Work in different places	Total	Works mainly at home	Work in different places	Total
2001	673	1, 916	2, 590	433	1, 051	1, 484
2002	698	2, 062	2, 760	484	1, 381	1, 185
2003	707	2, 207	2, 915	516	1, 553	2, 069
2004	761	2, 243	3, 004	562	1, 599	2, 161
2005	768	2, 324	3, 092	603	1, 774	2, 377

An increase in the number of employees' teleworking represents a risk that can undermine security in business. However, there are other trends that point to an increase in risk to the public in general as well as businesses. In the UK a high percentage of adult users use e-government services to retrieve information; however, the actual level of interaction with the service is low, especially compared to Europe [Eurostat Online European Statistics 2006]. With traditional governmental services, a citizen usually visits a government office and is authenticated by presenting papers. Identification to an official is replaced with a digital service where credentials are electronic and identity theft can become an increasing problem. Security of the citizen's connection is an important part of ensuring a secure e-government service. Where the services are provided to the citizens of a country the term c2g (Citizen to Government) is used in much the same way as b2c and b2b are used for business to consumer and business to business, respectively. The UK government has defined c2g as the online relationship between its citizens and various government departments they communicate with.

In Europe the eEurope 2005 Action Plan sets 7 targets for e-services. These are:

- Interactive public services: Member States should have ensured that basic public services are interactive, where relevant, and accessible for all. The Commission and Member States must agree on a list of public services for which interactivity and interoperability are desirable. Relevant issues include exploiting the potential of broadband networks and multi-platform access, and addressing access for people with special needs;
- Public procurement: Member States should carry out a significant part of public procurement electronically, cutting costs and raising efficiency in government procurement. The European Parliament and Council should adopt as quickly as possible the legislative package on procurement;
- Public Internet Access Points (PIAP's): All citizens should have easy access to PIAP's, preferably with broadband connections, in their communes or municipalities, In establishing PIAP's, Member States should use structural funds and work in collaboration with the private and/or voluntary sector, where necessary;
- Broadband connections: Member States should aim to have had broadband connections for all public administrations by 2005. Authorities should not discriminate between technologies when purchasing connections;
- Interoperability: The Commission presented a staff working paper on the importance of interoperability for e-Government services at the 2003 e-Government Ministerial Conference and intends to proposed a European interoperability framework for pan-European e-Government services that provides a series of recommendations and defines generic standards with regard to organizational, semantic and technical aspects of interoperability, offering a comprehensive set of principles for European co-operation in e-government;
- Culture and Tourism: The Commission, in co-operation with Member States, the private sector and regional authorities, will defined and launch e-services to promote Europe and to offer user-friendly public information. Building on the Communication "Working together for the future of European tourism", the Commission is now developing a European Tourism Portal. This work is being undertaken through an ETD project that involves a collaboration between EC3, LiXto, ITC-irst, Siemens Austria and Tiscover and is currently in the second stage of development;
- Secure communications between public services: The Commission and Member States have proposed to examine the possibilities to establish a secure communications environment for the exchange of classified government information.

The EU has agreed a list of 20 basic services that should be available as part of e-government. These consist of 12 relating to citizens and a further 8 services are aimed at businesses:

Citizen services	Business Services
Job search	Social contribution for employees
Income taxes	Corporate tax
Social security benefits	VAT
Personal documents	Registration of a new company
Car registration	Submission of data to the statistical office
Application for building permission	Custom declaration
Declaration to the police	Environment-related permits
Public libraries	Public procurement
Birth and marriage certificates	
Enrolment in higher education	
Announcement of moving	
Health-related services	

It is also these 20 services that have been used by the EU and researchers for benchmarking the performance of e-government accessibility.

For e-government to be a success with the citizens, they must be able to connect to the government infrastructure in a dependable manner where there is

reliability, availability and security of connection. A government has great control of the infrastructure connecting its offices and departments together but not the connection to business and in particular its citizens rely on external third parties. Additionally, some of the responsibility for the dependability will rely on the citizen's ability to set-up a connection which implies a level of knowledge that is likely that the citizen does not have [Furnell 2005].

An important aspect of the e-government is how its citizens access the systems and the infrastructure extends beyond the government offices and officials to wherever the citizens access the services within the community.

In a household where the Internet connection is either direct to the PC or a wired network, anybody trying to access the network will have to come through the modem/termination unit and if it has been configured correctly there should be a firewall and/or NAT set-up. In a wireless networked environment, the security of the network is not as controlled.

2 WLAN security

Wireless networking has experienced a huge increase in popularity over the last couple of years. The necessary hardware is widely available to consumers, it is affordable, and relatively easy to install and configure. Gateway devices, such as "routers" or "firewalls", that allow users to share a broadband connection with and protect multiple computers on a home network have been utilised for some time and have increased in popularity as more users in the home see the need for the use of an Internet connection and access to the same peripherals, such as printers. The addition of wireless capabilities to these gateway devices gives the user the convenience of taking a computer anywhere in the house without running wires through floors and attics.

2.1 Operation of 802.11 networks

Wireless communication under 802.11 [802.11 Working Group 2006] comes in two flavours: the Independent Basic Service Set (IBSS) or ad-hoc mode, and the Basic Service Set (BSS) Infrastructure mode. The IBSS mode allows wireless clients to talk directly to each other without a central controlling mechanism. To join such a network all that is needed is the Service Set Identifier (SSID) and the channel it operates on. This mode is generally considered to be insecure. Although it supports Wired Equivalent Privacy (WEP), it is not supported by WiFi Protected Access (WPA); however under 802.11i and the introduction of WPA2 ad-hoc networks will support better encryption. It is these ad-hoc wireless networks form the basis of mesh wireless networks being implemented by cities across the world. The Cloud, a wireless broadband service provider, has announced the creation of meshes in 9 cites across the UK. The BSS mode uses a controlling mechanism, normally by an access point to control the communication. The BSS functions in a manner similar to a switched wired network while the IBSS operates in a manner comparable to a hub based wired network. In BSS mode all traffic is routed through the access points (AP) even between peer wireless devices. There is an extension to the BSS where multiple BSS can be connected via a wired network connecting the access points known as the Extended Service Set (ESS).

An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. The SSID on wireless clients can be set either manually, by entering the SSID into the client network settings, or automatically, by leaving the SSID unspecified or blank. SSIDs are case sensitive text strings containing a sequence of alphanumeric characters with a maximum length of 32 characters. All access points come with a default SSID set, some of the more common ones are:

Manufacturer	Default SSID
Cisco	tsunami
3Com	101
Lucent/Cabletron	RoamAbout Default Network Name
Various	Default SSID
Compaq	Compaq
Addtron,	WLAN
Intel	intel
Linksys	linksys
Various	Wireless

Wireless networks work in two modes: the standard default 802.11 mode of broadcasting their SSID and a mode in which the SSID is not broadcast. The former is known as an open system and the latter is a modified closed system which is a propriety addition to the standard.

An open system will broadcast management beacon frames at a fixed interval that contain capability information of the access point. This is intended to enable wireless clients to detect the closest access point and if there is a stronger signal with the same SSID, it re-associates with the signal allowing roaming between access points.

A closed system does not broadcast the SSID as part of the beacon management frame and a client must have prior knowledge of the SSID to enable it to join a closed system using a probe request. However, some access points will respond to probe requests that contain a blank SSID or contain an SSID set to "any". This behaviour is modifiable on some access points, typically enterprise class equipment.

The Microsoft Windows XP SP 1-based Wireless Zero Configuration service suffers from what Microsoft calls "behaviour by design." If the wireless network is set to so that it does not broadcast its SSID, Microsoft's wireless manager periodically drops its non-broadcasting WiFi connection in response to the presence of a broadcasting SSID-based network.

2.2 Detecting wireless networks

There are two basic techniques for locating wireless access points: passive or active searching based on 802.11. Both approaches are easy to implement and only

need the most basic equipment and set-up. Each if these techniques employs a process known as "sniffing", where the wireless card listens for management packets. There is a great deal of commercial and open source software that can do this and will also record the details of the packets; the wireless client on a device does this as part of its normal function. Sniffing software takes this functionality and applies additional techniques to allow listening to take place on all possible channels; by switching the channel the card is working on at a regular interval.

Additionally, certain wireless card chipsets are more flexible and are more suitable for use with sniffing software. The best cards are ones that can be placed into what is called the Monitor mode, also known as RFMON mode, which is similar to promiscuous mode on wired network interface cards. It allows the wireless card to sniff all the traffic that the card receives instead of sniffing all the traffic from the associated network. Usually, the card is unable to transmit or otherwise be used when in this mode. It is also used for passive stumbling, a technique used in wardriving where the wireless card listens for base stations instead of actively probing them to determine their presence.

Passive searching is to purely listen for the transmitted management beacon frames. It only needs to be within receiver range to detect a network; no traffic is generated by passive sniffing. Passive sniffers are also capable of recording data packets for additional dissection. However, they require a card and driver capable of radio frequency (RF) Monitor support, which enables raw packet detection. They cannot detect a non-beaconing network with no data traffic, though it is possible to record packets for analysis for encryption breaking and MAC address searching.

Active searching uses the probe response/request feature where a probe request sent from the client to the access point for information results in the probe response frame if the access point is so configured. Inexpensive wireless access points intended for home use do not normally allow the user to disable the beaconing mechanism; this level of configuration is normally found on enterprise class equipment. This method does not need traffic to be transmitted across the network for a network to be found; however, it does generate packet traffic that can be detected by intrusion detection systems. This form of active scanning using probe requests is not completely effective at finding all wireless access points.

An alternative active method of scanning to detect networks, where both SSID broadcast and probe response are only actuated by a probe request with a valid SSID, is to passively listen for a communication session between the access point and client and then issue a disassociation request. This causes the client to break the communication link and after a short period of time, it issues a probe request and re-associates with the access point allowing the management frames to be captured and the SSID to be identified.

Typically, the minimum wardriving kit consists of a laptop, wireless network card and sniffing software though many use a Global Positioning System (GPS) unit to provide geographical location information. Additional mapping utilities are needed to generate maps of locations of detected wireless networks if the positional data is recorded. GPS is an American system of 24 orbiting satellites that can provide a positional fix to a resolution of a metre though most commercial equipment is less accurate than this.

2.3 Wireless security measures

The main insecurity with wireless networks compared to wired networks is the easy of accessing the transmission medium used, i.e. with a wired network to sniff packets, there has to be a physical access to the network whilst with wireless networks, the transmission is easily available outside the physical building. Insecurities on wireless networks other than those caused by the ease of accessing the transmission media are the same as for a wired network, i.e. packets can be sniffed if sent in clear text across wires if someone has packet sniffing software on the same segment of the network as the packet is being transmitted across.

In order to establish some form of protection for wireless networks, the WEP algorithm, has been developed as part of the 802.11 standard. It restricts access to the network to those who has the same key and is supposed to give the equivalent privacy as those on a wired network. However, a number of flaws have been discovered in the WEP algorithm [Fluhrer, et al 2001, Mead and McGraw 2003], which seriously undermine the security of the system and leaves the system open to a number of attacks:

- Passive attacks to decrypt traffic based on statistical analysis.
- Active attack to inject new traffic from unauthorised mobile stations, based on known plaintext.
- Active attacks to decrypt traffic, based on tricking the access point.
- Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.

It is practical to mount these attacks using only inexpensive off-the-shelf equipment. It is recommend that anyone using an 802.11 wireless network does not rely on WEP for security, but rather employ other security measures to protect the wireless network. The effectiveness of the attacks applies to both the 40-bit and the so-called 128-bit versions of WEP equally well.

The 802.11 standard uses Ethernet packets across wireless networks, Ethernet use a Media Access Control (MAC) address which is a hardware address that uniquely identifies each node of a network and is configured as part of network interface card (NIC) and regulated by the IEEE. This allows a further method of securing a network by the use of MAC filters, which restricts access to an AP to authorised MAC addresses only. Most APs provide this capability for checking the MAC address of the station before allowing it to connect to the network, thus providing an additional control

layer. However this approach requires that the list of MAC addresses be configured and maintained. This can be circumvented since MAC addresses are transmitted as part of the Ethernet frames and can be read from captured packets. It is , however, possible to spoof the MAC address of node using various software such as SMAC, a MAC address modifying utility for Windows operating systems, regardless of whether the manufactures allow this option or not. This allows an intruder to alter the MAC address of the node to match a known node on the network.

Further security is available using WiFi Protected Access (WPA and WPA2) which was created in response to the serious weaknesses in WEP. WPA implements the majority of the IEEE 802.11i standard, and is intended as an intermediate measure to take the place of WEP while 802.11i is prepared. It is designed to work with all wireless network interface cards, but not necessarily with first generation wireless access points. WPA2 implements the full standard, but does not work with some older network cards. There are two modes of operation for WPA:

- Personal mode or Pre-Shared Key (PSK) mode is designed for home and small office networks that cannot afford the cost and complexity of an 802.1X authentication server. Each user must enter a passphrase to access the network. The passphrase may be from eight to 63 ASCII characters or 64 hexadecimal digits (256 bits). The passphrase may be stored on the user's computer at their discretion under most operating systems to avoid re-entry. The passphrase must remain stored in the WiFi access point.
- Enterprise mode is designed for larger offices and enterprises various Extensible Authentication Protocol (EAP) types are now supported in enhanced WPA/WPA2 compared to just the Temporal Key Integrity Protocol (TKIP) in the original WPA and EAP-TLS in WPA2

Additional security can be obtained by deploying standard TCP/IP security protocols over the connections, such as IPSec and the use of Virtual Private Network (VPN).

2.4 Legal issues

The legality or rather the illegality of accessing a wireless networks is not in question; under most legal systems accessing a computer system without permission is illegal. However, the activity of wardriving is more of a grey area as often the legality is dependent on local laws.Law enforcement officials, increasingly concerned about wireless networks, say the possibilities for mischief run the gamut. A wireless hacker's intentions could be as malevolent as identity theft or as benign as using a neighbour’s Internet connection to check e-mail or scan the newspaper online. Sometimes they drain other people's bandwidth to illegally download movies and other copyrighted material or access pornography. Others are pranksters, who maliciously lock people out of their wireless networks just for fun, others still are those that are spammers, using unauthorised Internet access to send masses of unsolicited e-mail.

In the UK, it should be said that listening to broadcasts in the Industrial, Science and Medical (ISM) band is not illegal as this is a license exempt band, indeed the 802.11 standard is written so that wireless networks broadcast their presence and hence only the built-in mechanism of the transport system is used. This effectively allows passive scanning to take place, and since active scanning uses the mechanisms built into the standard to identify a network. Though a slight increase in electrical power usage may be witnessed or a very slight delay in a transmission of a packet may be caused, this is not considered to be illegal as it is part of the client functionality to identify and attach to a network with a hidden SSID. Whilst this is the case, there may be moral and ethical considerations of what is done with the information gathered from active scanning. Any activity resulting in an association with an access point, even accidentally, could be considered illegal - accessing information or sending data across the network without the permission of the network administrators would be consider illegal in many places around the world.

If a disassociation packet is issued, causing a client to lose contact with the network and reconnect to the network to generate extra traffic this would result in a degradation in performance of the network and this may be deemed illegal in some countries.

An interesting consideration is whether it should be illegal if, by using passive means, enough information is collected to decode the WEP key and no further use of the key made. No connection is made to the network, its performance is unaffected and the information is transmitted publicly and any information broadcast on the ISM can be listened to. However, information vital for the security of the network has been gained leading to a potential compromise.

2.5 Availability and reliability

Interference to wireless networks can come from a number of sources, the 802.11 standard uses the 2.4GHz and the 5GHz bands which are generally unlicensed or license exempt around the world. The 2.4GHz band which is part of the ISM band is crowded with a large number of devices ranging from wireless baby monitors, microwave ovens to cordless phones. Wireless networks working in this band have to contend with all these devices, plus other wireless access points in the same area.

Although the 2.4GHz band is divided into 14 channels (not all are available around the world), the bandwidth of each channel is sufficient that adjacent or near adjacent channels interfere with each other. Of the 11 channels commonly used in the USA or the 13 channels used in the majority of Europe, a maximum of three channels are spread enough apart to avoid interference problems.

One of the problems in hiding or disabling the SSID is that it becomes harder for those configuring wireless networks to identify nearby networks operating on the same or adjacent channels.

Additionally most emerging radio technologies for Wireless Personal Area Networks, such as the Bluetooth protocol, are designed also to operate in the 2.4GHz ISM band. Since both Bluetooth and IEEE 802.11 devices use the same frequency band and are likely to come together in a laptop or may be close together at a desktop, interferences may lead to significant performance degradation.

802.11 is a Collision Sense Multiple Access Protocol where each wireless point checks for another wireless point transmitting: if it detects a transmission it will wait for a random length time delay and try again; if two transmit at the same time, both detect a collision and wait for a random time delay and try again. The more points on the same channel within the range, the more likelihood of a collision exists and increased collision results in reduced data transmission rates. However, the 14 usable channels allocated worldwide allow wireless networks in close proximity to each other to use different channels. The drawback is that the channels are separated by 5MHz; each channel has a bandwidth of 22MHz causing it to interfere with adjacent channels which actually means that in the 11 or 13 channel implementation, it is only possible to utilise three channels concurrently without any overlap in frequency, typically taken as channels 1, 6 and 11.

2.6 Security risks

With a wired network, the only possible access for an intruder would be through the broadband connection and normally through a firewall in the case of a broadband modem. With Network Address Translation (NAT) and security software on the individual computers, there is a fairly comprehensive layered defence system whose effectiveness would depend on the ability of the installer or the default settings.

A wireless network allows access from outside the property onto the network behind the broadband modem with its firewall and NAT. This means instead of intruders needing to get through the broadband connection, the network has to deal with intruders connected directly to the network. Since the wireless router is designed to provide a wireless Internet connection and its range can reach as far as 150 feet it can often reach many public roads and nearby homes. An attacker could be outside a home or business with a laptop with a WiFi card and the right software, gain access to private information on the network.

Instead of gaining access the public side of the gateway device, the intruder connects directly to the network on the private side of the gateway device, completely bypassing any hardware firewall between the private network and the broadband modem. Many people assume that since they are behind a firewall their private network is safe, letting down their guard, sharing drives, and generally being less careful about security. The intruder can take advantage of this by perusing devices and gaining access to confidential data such as personal information (financial data, tax records and wills) and work-related information such as confidential specifications and trade secrets that the victim brings home from the office. By employing a sniffer an intruder can also sniff email or FTP user names and passwords since they are usually transmitted in clear text. This allows unauthorised access to email accounts or web servers without the victim's knowledge.

Another risk posed by lack of security is identity theft. Whilst there has been no direct conviction for this there is certainly a great deal evidence that it occurs. By using information such as tax returns and resumes obtained by compromising a home network, it is possible to use the name, address, date of birth and National Insurance number to create a bogus identity. The increasing use of on-line services for banking and government makes it more tempting to use alternative identities or to gather information on an individual to impersonate them. A poll by Winmark Research, on behalf of RSA Security, found that two-thirds of consumers used the same password to access different types of websites - from email to bank accounts [Leyden 2004]. One third even admitted to sharing passwords with friends and family, massively increasing the risk of fraud. In the survey, the most common password categories were family names such as partners or children (15%), followed by football teams (11%) and pets (8%), the most common password being "admin". Many workers who regularly had to change their passwords kept them on a piece of paper in their desk drawers, or stored them with a Word document. With the ability to search people’s computers via a wireless attack, it makes it easier for identity theft to occur. Secured networks could be jeopardised as a result of human vulnerabilities such as lack of awareness and adherence to usage policies [Bhagyavati, et al 2004].

3 Case study of luton

During Dec 2005 and Jan 2006, an extensive wardrive around Luton was undertaken as part of a research project into the extent of security in wireless networks in the community. The wardrive was conducted by one of the authors using equipment only capable of detecting 802.11b and g networks and works only in the 2.4GHz band range. It uses active scanning and only detects networks that respond to a general probe request. The analysis looked at number of secure and unsecured networks, distribution of channels and percentage of the population of Luton and combined it with data from the last national census conducted in 2001 and statistics from the National Statistics Office on number of households with Internet and Broadband access. The wardriving survey of Luton shows similarities with those conducted in London and Bristol in the UK and in Frankfurt and Paris in Europe [Jaques 2005].

Luton is a typical town in the UK within the southeast of the country about 30 miles north of London on the M1 with good communication links. It has a population of

187000 living in 70775 households (Data obtained from the 2001 Census results), covering an area of 436 hectares and used to be a major automotive manufacturing town in the 60's and 70's. Looking at the national average of 55% households having Internet access, about 38900 households in the town would have Internet access; however in the southeast, the percentage of households with Internet access raises to 64% and if Luton was typical of towns in this region, the estimate would be 45300 households.

Tentative results from the wardriving survey shows that for the whole of Luton, it is expected that there are around 4000 wireless networks with 50% of these being unsecured. These results are only for the 2.4Ghz band and 802.11b and g wireless networks. This means that there may be networks that have not been detected and the number of networks would then be higher.

There are 24,479,439 households in the UK, of which it is estimated that around 13,463,700 have Internet access. It is also thought that 10% of these have a wireless network, meaning an estimated 1,346,370 wireless networks. If the figure of 50% of all wireless networks being insecure holds throughout the country, it would mean that there were approximately 673,185 unsecured wireless networks in the UK. Confirmation of the order of magnitude of wireless networks can be seen in a report by Contractor UK [Contractor UK 2005] quoting research by IDC who estimated there were 958,000 wireless networks in the UK, with this figure expected to double to almost two million by the end of the year.

A further characteristics examined in the case study was the channel usage of the detected networks. As expected, channels 1, 6 and 11 were the most commonly used channels with channel 11 being used by 52% of the detected networks. The actual distribution of the channels has not been fully analysed but it can be expected that in some areas the wireless networks are not running at the best possible bandwidth expected from ideal conditions due to the devices suffering from collisions generated by nearby networks. The average user, however, will be unaware that such collisions may be taking place and may well apportion blame elsewhere

A further characteristics examined in the case study was the ratio of ad-hoc to infrastructure and the usage of SSID's. In the survey, 2% of the detected networks were in IBSS or ad-hoc mode, and the majority detected were infrastructure mode. In a sample of 2363 networks, there were 1077 distinct SSID's; however, the majority of the SSID's found were the original default settings of the equipment.

4 Recommendations

There are a great deal of sources available that provide information regarding the construction of secure wireless networks. These sources can be found easily and can be implemented with tittle difficulty for those with some technical knowledge and confidence. However, most of those installing a wireless network do not have technical knowledge nor confidence and may fail to understand the problems associated with wireless networks.

We recommend that to improve the availability and reliability of a wireless network, a person configuring the network should conduct a small site survey using widely available free of charge software. The results of this survey can then inform the choice of location and channel. Due to the large increase in use of wireless networks, one should also check regularly to examine if the conditions around the location have changed and adjust settings accordingly. This may well be beyond the ability of most of the general public and additionally they may not have the tools to conduct the survey. In such cases this could be a service that is sourced and should be of low cost. It is also possible using most wireless client software, to display a list of available networks but this will not normally show those with hidden SSIDs. However, as a minimum it is possible to use the client software to detect wireless networks and the channel they are working over and then setting the channel of the access point to one that will have the least interference.

There are a great deal of information sources that recommend users stop or to disable the SSID broadcast; we strongly recommend against this action. The disabling of an SSID broadcast offers very little increase in security to anyone attempting to access a network, it only stops beacon broadcast on the access point. Essentially, disabling SSID broadcast just stops the inclusion of SSID's in the broadcast beacon frame which is the one of the five SSID broadcast mechanisms. Using Microsoft Windows XP SP 1-based Wireless Zero Configuration service to manage the wireless network card suffers from what Microsoft calls "behaviour by design." If the wireless network is not set to broadcast the SSID, Microsoft's wireless manager periodically drops the non-broadcasting WiFi connection in response to the presence of a broadcasting SSID-based network. Thus, in practice, it does not improve security to stop the SSID broadcast and doing so can cause problems with wireless networks. The inclusion of the SSID in the standard was to aid management of wireless networks and it really should be used for doing this. Allowing users of wireless networks to identify channels being used and select other channels can reduce interference. Whilst those with advanced knowledge can examine networks in the vicinity, the average user will not be able to examine those that withhold the SSID and so collisions may be rife. This can be seen in the case study in which 52% of networks were operating on the same channel.

A recommended approach to wireless security would be to use a layered approach with MAC filtering and WPA or WPA2 at the access point. The use of IPSec and VPNs on the network and ensuring the machines on the network are protected. Ultimately, it may be the best to follow the practice to put publicly accessible servers into a Demilitarised Zone (DMZ) and put the wireless access point into a firewalled section of the network with rules governing communications to the rest of the network; however until equipment for the home can support this, it will remain a security weakness.

In general it is recommended to apply extra caution to wireless connections in a public area as they may not provide as much security as wired Internet connections. In fact, many "hotspots" - wireless networks in public areas like airports, hotels and restaurants - reduce their security. Unless a security token is used, it may be decided that accessing an online bank account through a wireless connection is not worth the security risk of a snooper capturing your packets and decoding them.

One of the most important recommendations would be to the manufacturers of wireless networking equipment to provide information in an easy to understand format on setting up wireless network and possible for governments to put pressure on the manufactures to do so. A better informed public will result in better set-up wireless networks and hence better availability, reliability and security of them.

5 Conclusions

In this paper we have discussed some of the key concerns surrounding the security of wireless networks. We have highlighted a number of weaknesses in existing protocols and configurations of wireless networks including how these weaknesses can be exploited. The paper has also considered some of the legality aspects of accessing information regarding the configuration of a wireless network as well as the accessing of transmitted or stored information on the network.

A case study has been presented that demonstrates the extent of the problem and this study is to be used as a basis for further work. Additional equipment will be used later in the study to detect 802.11,b and g across both the 2.4GHz and 5GHz bands The research investigates wireless networks within the community and looks at aspects of reliability, security and whether education or training would help reduce potentially insecure networks and improve the reliability and availability of them. The wardrive identifies the number of wireless networks and their distribution around the town.

We have presented a number of recommendations that can ensure the greater security of wireless networks. These recommendations require action from both manufacturers and those configuring a wireless network, most often the end user of the equipment.

References

[1] 802.11 Working Group, 2006. http://grouper.ieee.org/groups/802/11/

[2] Bhagyavati, Summers, W.C. and DeJoie, A. 2004. Wireless security techniques: an overview, *Proceedings of 2004 Conference for Information Security Curriculum Development*, Kennesaw, Georgia,.

[3] Contractor UK, 19 January 2005. Wireless hackers creep nearer to UK homes. http://www.contractoruk.com/news/001908.html

[4] Eurostat Online European Statistics, http://epp.eurostat.cec.eu.int/portal/page?_pageid=1073,46870091&_dad=portal&_schema=PORTAL&p_product_code=IR111

[5] Fluhrer, S., Mantin, I. and Shamir, A. 2001. Weaknesses in the Key Scheduling Algorithm of RC4, *Selected Areas in Cryptography 2001, Lecture Notes in Computer Science*, Vol. 2259, pp. 1-24. Springer.

[6] Furnell, S. 2005. Why users cannot use security, *Computers & Security*. Vol. 24, pp. 274-279.

[7] Graham-Rowe, D., 22 January 2005. Wireless boom is hackers' heaven, New Scientist, http://www.newscientist.com/article.ns?id=dn6894

[8] Jaques, R. 10 Mar 2005. UK firms haemorrhaging data to drive-by hackers: Unsecured Wi-Fi in one third of all wireless networks. http://www.vnunet.com/vnunet/news/2126948/uk-firms-haemorrhaging-drive-hackers

[9] Leyden, J. 20 April 2004. Brits are crap at password security. http://www.theregister.co.uk/2004/04/20/password_surveys/

[10] Mead, N.R. and McGraw, G. 2003. Wireless Security's Future, *IEEE Security and Privacy*, 1 (4), pp. 68-72.

[11] Office for National Statistics (ONS), 2002. Teleworking in the UK http://www.statistics.gov.uk/articles/labour_market_trends/Teleworking_jun2002.pdf

[12] Office for National Statistics (ONS), 2006. Home-based working using communication technologies http://www.statistics.gov.uk/articles/labour_market_trends/teleworking_Oct05.pdf

[13] Office for National Statistics (ONS), 2007. Monthly, On-line edition http://www.statistics.gov.uk/statbase/Product.asp?vlnk=8251

[14] Thomas, Z. 11Feb 2007. Best companies see surge in working from home http://www.timesonline.co.uk/tol/news/uk/article1496840.ece