Choosing the Right Wireless LAN Security Protocol for the Home and Business User

Carsten Maple¹ Helen Jacobs¹ ² Matthew Reeve²

¹ Institute for Research in Applicable Computing, University of Luton, Luton, Bedfordshire, LU1 3JU, United Kingdom.
² Modern Networks, Knowl Piece, Wilbury Way, Hitchin, Hertfordshire, SG4 0TY, United Kingdom.
carsten.maple@luton.ac.uk hjacobs@modern-networks.co.uk mreeve@modern-networks.co.uk

Abstract

The introduction and evolution of security standards for wireless networking has been a problematic process. Flaws in the initial security standard resulted in quick-fix solutions and interoperability issues. As wireless networks are not confined to a building, there is an added security risk that radio signals can be detected externally. Wireless networking has rapidly increased in popularity over the last few years due to the flexibility it provides. Given the simultaneous growth of e-government services there is particular risk to the citizen of identity theft. This article discusses the progression of wireless security protocols since their introduction and the effect this has had on home and business users. The risks of using wireless networks are outlined in the paper and recommendations for securing wireless networks are reviewed.

Keywords: WLANs, security, TKIP, WEP, WPA

1. Introduction

Wireless networking increases the flexibility in the home, work place and community to connect to the internet without being tied to a single location. At present Western Europe has 42% and North America has 26% of all global hotspots, and for the end of 2005 it was estimated that there would be 100,000 public Wi-Fi hotspots worldwide [1]. In 2002, the Department for Trade and Industry (DTI) estimated 2% of UK companies had wireless networks, this grew to 47% in 2004 [2].

With the benefits of Wi-Fi there are also some risks which users should be aware of. Without any security implemented, unauthorised users may steal data or load malicious code onto the network with the intention of creating havoc. Unlike wired networks, the radio signal produced by wireless networks can penetrate walls, ceilings, floors and are therefore not confined to a building. Hackers can effortlessly pick up these signals from the outside of the building using easily available wireless detection tools.

Whilst a typical user would normally not transmit sensitive data, the increasing growth of the use of e-government services has meant that more sensitive data is being transmitted by citizens to local and national government. The range of e-government services available electronically to citizens and businesses is shown in Table 1.

Table 1. E-Government Services for Home and Business Users.

<table>
<thead>
<tr>
<th>Service</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Income tax returns</td>
<td>Home</td>
</tr>
<tr>
<td>Voting</td>
<td>yes</td>
</tr>
<tr>
<td>Job search/offers</td>
<td>yes</td>
</tr>
<tr>
<td>Benefits: including social security; child tax credits</td>
<td>yes</td>
</tr>
<tr>
<td>Birth and marriage certificates</td>
<td>yes</td>
</tr>
<tr>
<td>Car registration</td>
<td>yes</td>
</tr>
<tr>
<td>Application for building permission</td>
<td>yes</td>
</tr>
<tr>
<td>Enrolment in higher education</td>
<td>yes</td>
</tr>
<tr>
<td>Announcement of moving</td>
<td>yes</td>
</tr>
<tr>
<td>Health-related services</td>
<td>yes</td>
</tr>
</tbody>
</table>

It can be obviously seen that the interception of such data may be of serious harm to citizens. Indeed, governments (in particular in the US) have used queries such as “What was the figure on your last tax return?” to authenticate a caller. The reason this was chosen as an authentication question was because it was felt that only the legitimate citizen would have
access to such knowledge. This method of authentication is seriously compromised if such data is transmitted over unsecured wireless networks.

Many WLANs used in the home still operate with no measure of encryption, and this is certainly inappropriate when using e-government services. However, there does arise something of a problem for the home user when establishing a WLAN, namely which encryption protocol to use. This paper considers the major encryption protocols, gives recommendations on their use and analyses their abuse.

The majority of wireless networks use the IEEE 802.11 standard for communication. Initially the IEEE 802.11b was the de-facto security standard for wireless networking technology for small businesses and home users, with all Wireless Access Points equipped with Wired Equivalency Protocol (WEP). Flaws in WEP were soon discovered and in response to this, the 802.11i task group were developed to address the major problems with security. They addressed three main security areas: authentication, key management and data transfer privacy. The Wi-Fi Alliance developed Wi-Fi Protected Access (WPA) as a Wi-Fi standard, which accelerated the introduction of stronger security. As the security standards have evolved other wireless security options have become available which are pre-installed on devices, these include WPA and Temporal Key Integrity Protocol (TKIP).

Initially, when Wi-Fi networking was in its infancy, war-walking, war-driving and war-chalking were well publicised phenomena. Developed by Peter Shipley in April 2001, these terms describe the process used by hackers walking or driving around areas looking for unsecured wireless networks. Symbols were left on the walls or pavements to indicate the security status of nearby Wi-Fi points. War-driving did highlight the worrying results that firstly a large proportion of Wi-Fi users do not enable any form of encryption and secondly that the standard wireless encryption protocol (Wired Equivalency Protocol – WEP) can easily be cracked. In 2003 it was estimated that around 60-70% of all wireless networks did not use any security [3], when users do deploy security they use the manufacturer’s default settings. Even after much publicity about wireless encryption and new improved protocols were made available, a survey conducted by WhiteHat in January 2005 [4] found 51% of businesses, within a one-mile radius of Bristol town centre, did not use any form of encryption. Of those who did use encryption, 25% used the default service set identifier (SSID) and therefore probably still had the factory passwords.

1.1.1. Possible Security Threats

Like wired networks, wireless networks are subject to malicious attacks. The radio signals do not remain within the confines of the building, and indoor routers have a range of approximately 20 – 150 metres, depending on the 802.11 standard and the data rate. Therefore, the radio signal can easily be detected externally or in a neighbouring building. This means the attacker does not need to infiltrate the building to hack the network. With the right equipment, it is possible for the radio signal to extend up to 125 miles [5]. However, such distances can only be reached in certain environments such as deserts, which lack structures such as buildings and trees. Obstacles such as walls and distance can cause the radio signal to attenuate and the threat of attack will decrease. Wireless detection devices work in two modes, passive and active. The passive mode listens for the access points’ broadcast, which may or may not contain the SSID. Whereas active mode uses the probe request and response to detect access points, which involves the access point responding to the probe request. Attacks on WLANs can be categorised as passive attacks which include War-Driving and Sniffing (via a promiscuous mode); and active attacks include Spoofing (impersonation), Denial-of-Service attacks (DoS) and Man-in-the-middle attacks. These threats are just as real for businesses as they are for citizens. Businesses too are now transmitting increasingly sensitive data to government. Services available to businesses include: Social contribution for employees; Corporate tax; VAT; Registration of a new company; Submission of data to the statistical office; Customs declaration; Environment-related permits; and Public procurement.

1.1.2. Passive Attacks - Accidental users

Occasionally when trying to connect to an Access Point the computer may automatically connect to a different network and the user may “accidentally” use that connection without realising it belongs to a third party. However, it is illegal in the UK to use bandwidth without the consent of the owner according to sections 125 and 126 of the Communications Act of 2003 [6]. This may occur in the work place when users are unfamiliar with the company’s SSID and pick up a neighbouring company’s unsecured network.

1.1.3. Active Attacks - Brute force attack

A brute force attack is the systematic testing of different letters, numbers and symbols until the correct password or key is guessed. There are a number of software programmes available on the Internet that can be used to recover encryption keys on wireless LANs, these include AirSnort and WEPCrack. AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been collected, AirSnort can guess the encryption password in under a second.

WEP can easily be cracked because the Initialisation Vector is sent as plaintext within the encrypted packet. This means that if anyone intercepts the data...
1.1.4. Denial-of-Service attacks

A Denial-of-Service attack (DoS) can cause a network to slow down or become unusable. A DoS attack may occur if the attacker for hours or by attacking the resource itself. Another form of DoS attack is the use of a strong radio signal. This denies legitimate users from accessing a resource. Distributed Denial-of-Service attacks (DDoS) occurs when many computers are used against the target. A single master program can be loaded onto a commandeered computer via an insecure wireless network; the master program can communicate to “agent” computers anywhere on the Internet infected with the agent program and initiate an attack. DoS attacks can also inadvertently affect businesses by causing the share prices to drop by 1-4% on the day of the attack [8].

1.1.5. Man-in-the-middle attack - Evil Twin

A Man-in-the-middle attack occurs when an attacker is able to read and modify communications between two parties without them being aware of the attacker’s presence. An Evil Twin attack (also known as base-station cloning/access point cloning) is similar to a Man-in-the-middle attack. The term is used for fake hotspots/access points, which pretend to be a legitimate hotspot. The Evil Twin is a malicious server, which may be used to extract sensitive information such as bank details. The hacker sets up the SSID to be the same as the local hotspot or corporate wireless network. The hacker may disrupt or disconnect the access point by directing a Denial-of-Service attack against it, or by creating radio signal interception around it. The hacker may then intercept the traffic. The user is unaware that they are not using a legitimate hotspot and may unknowingly provide their user name and password as they log on to the fake hotspot. Evil Twin networks may be avoided by enabling the WEP or WPA security, so the user is unable to join the “evil network” as the key will not match. The practise of Skimming ATMs has similarities to Evil Twin attacks. In both cases, a false façade is placed over the genuine access point or ATM. With Evil Twin attacks, it is a virtual interface, however with ATMs it is a physical skimming device which will record users’ bank details.

1.1.6. Stealing data

Attacks from within the company are likely to come from disgruntled employees rather than intruders. A Department of Trade and Industry survey in 2004 found one in five of the UK companies questioned were victims of staff abuse on the Internet. The abuse ranged from web browsing, unauthorised access to systems and legal infringements [2]. Apart from having restricted access to certain files, it is difficult to prevent staff with access to customers’ personal information from misusing it. Personal information of the customers may be stolen and used for identify fraud or other illegal activities. For example, in 2004 an American was charged with stealing email addresses from the customers of a credit card aggregation company he previously worked at. He drove around looking for unsecured wireless networks, from which he sent untraceable spam messages advertising pornography sites to the email addresses he had collected [9].

1.2. Internet threats to businesses or organisations

Within a business or organisation, there are a number of security risks that may occur when computers are connected to the Internet. These risks include the unauthorised viewing of sensitive information by intruders or legitimate users. The deletion, modification or disclosure of information by internal or external users may occur on an unsecured network. The use of software programs such as NetStumbler can identify networks vulnerable to attack, which may lead to a penetration attack by an unauthorised person. The unauthorised connection of a personal Wi-Fi access point to a company’s network could put the whole network at risk if the security options are not properly set up. Security breaches may be caused by either internal or external events. It has been estimated that 53% of the worst security incidents to occur in small UK companies (1-49 people) was caused by external events and 32% of incidents were due to internal events. In larger UK companies (250+ people), 38% of incidents were caused by external events and 44% by internal events [2].

2. Wireless devices and built in security options

To prevent attacks on wireless networks, access point devices such as routers have built-in security settings. Over time, the level of security has increased with the realisation that the original security settings were flawed.

2.1. Wireless Equivalent Privacy (WEP)

In 1997, WEP was developed by the 802.11b task force with the introduction of wireless technology,
2.1. WEP weaknesses

It was soon discovered that the WEP security protocol was flawed and in 2001, Fluhrer et al. [11] published a cryptanalysis of WEP that exploited the way the RC4 algorithm and IV was used in WEP. It was discovered that a passive attack could recover the RC4 key after eavesdropping on the network for a few hours and collecting 100,000-1,000,000 packets. A hacker could use an XOR function to mathematically link two packets of a session that have been processed with the same IVs, i.e. identical RC4 keys, which can be used to recover the key.

Another fault with the WEP protocol was that the authentication only verifies the client machine, not the actual user accessing the machine [12]. This occurs as the only key condition is that the WLAN card and the access point use the same algorithm. Therefore, everyone on the local network uses the same secret key, which the RC4 algorithm uses to generate an infinite, pseudorandom keystream.

Both the 40-bit and the 104-bit keys are vulnerable to attacks, due to various weaknesses internal and external to the protocol supporting WEP. These vulnerabilities include the heavy reuse of keys, the ease of data access in a wireless network, and the lack of any key management within the protocol [13]. For example, the IV will be duplicated within 5 hours at a busy access point when 1500-byte packets (the standard Maximum Transition Unit for an Ethernet network) are transmitted at a rate of 11 Mbps. It is therefore possible to determine the RC4 keystream over several hours after the IV has been repeated.

Originally, it was thought that increasing the key size from 40-bits to 104-bits would overcome some of the security problems [14], however the implication of 128-bit WEP has caused problems for heterogeneous environments in which interoperability was an issue. In 2005, using a combination of statistical techniques focusing on unique IVs captured and brute-force dictionary attacks to break 128-bit WEP keys, the U.S. Federal Bureau of Investigation cracked WEP in 3 minutes [15]. With the proper equipment, it is possible to eavesdrop on a WEP-protected network from distances of a mile or more away from the target [16]. With the tools and information available on the Internet, an inexperienced hacker could crack WEP encoded data in a matter of days.

A report conducted in 2005 by Webtorials found 40% of the users surveyed still used WEP for securing their wireless network and only 22% deployed WPA2/802.11i security [17].

2.2. Temporal Key Integrity Protocol (TKIP)

Temporal Key Integrity Protocol (TKIP) was the immediate replacement for WEP, which aimed to fix the problems associated with WEP including small initialisation vectors (IV) and short encryption keys (Mead & McGraw, 2003). TKIP is a suite of algorithms that wrap around the WEP protocol to make it more secure. The reason why TKIP is an improvement on WEP is that it rotates the temporal keys; therefore, a different key is used for each packet. Each packet transmitted using TKIP has a unique 48-bit serial number that is incremented every time a new packet is transmitted.

Each time a wireless station associates with an access point, a new base key is created. The base key is built by hashing together a special session secret with some random numbers generated by the access point and the station as well as the MAC address of the access point and the station. This mixing operation is designed to put a minimum demand on the stations and access points, yet have enough cryptographic strength so that it cannot easily be broken. Putting a sequence number into the key ensures that the key is different for every packet. This resolves another problem of WEP, called "collision attacks," which can occur when two messages have the same key. This could potentially be a problem if one message says “I agree to pay X £500.00 on 01/01/2007” and the second message says “I agree to pay X £1,000,000.00 on 30/12/2010”. The attacker could get the victim to
digital sign the first message, but claim the signature was for the second message of a greater value and use the key as proof of authentication [18]. With different keys, collisions are prevented.

TKIP also utilises an integrity-checking feature called Message Integrity Check (MIC or Michael). This part of TKIP closes a hole that would allow a hacker to inject data into a packet, which allows the hacker to deduce the streaming key used to encrypt the data. MIC uses a cryptographically protected one-way hash in the payload, which ensures packet-tampering detection occurs immediately upon decryption. Compared to WEP, TKIP is a costly process and may degrade performance at many access points, where it can consume every spare CPU cycle.

TKIP also uses RC4 as the encryption algorithm, but it removes the weak key problem and forces a new key to be generated every 10,000 packets. In addition, it hashes the initialisation vector (IV) values that were sent as plaintext in WEP. TKIP is useful as it can be used on old hardware, which supports WEP but not WPA, and new hardware that only supports WPA.

2.3. Wi-Fi Protected Access (WPA)

WPA was created by the Wi-Fi Alliance once the flaws associated with WEP were discovered, and used as an intermediate standard until the IEEE 802.11i working group developed a more secure protocol. WPA was based on the WEP protocol, but utilises the stronger encryption technology used in TKIP, which offers pre-packet key mixing and a message integrity check.

Although WPA is stronger then WEP, it is, however, vulnerable to Denial-of-Service attacks. Initially designed as a safety feature, WPA shuts down the network if at least two packets using the wrong key are sent every second. A hacker could use this security feature to their advantage and potentially bring down a WPA protected LAN. If this happens the access point assumes the hacker is trying to gain access to the network. The access point shuts off all connections for 1 minute to avoid the possible compromise of resources on the network. Thus, a continuous string of unauthorised data could keep the network from operating indefinitely. While this feature was designed to safeguard against breaches of security, it presents a prime opportunity for a hacker.

WPA comes in two modes, enterprise mode and consumer mode. Enterprise mode uses Remote Authentication Dial In User Service (RADIUS) for authentication. The RADIUS server checks that the information is correct using the authentication scheme Extensible Authentication Protocol (EAP) to process the information. If accepted, the server will then authorise access to the ISP system, select an IP address and Layer 2 Tunneling Protocol parameters. Although the 802.1X standard uses RADIUS for authentication, it does not specify that it must be RADIUS, other authentication protocols could be used such as TACACS+ (Terminal Access Controller Access Control System). RADIUS is the de facto standard for authentication and other protocols are rarely used. A RADIUS server can be used for different internet connections other than dial-up. The authentication server is a certificate authenticator that only allows client stations to connect with the access point if it sees a valid certificate on the client, which the server provided earlier. Many access points now come with integrated Authentication Servers (AS), which act as RADIUS servers, giving Small Office and Home Office (SOHO) users the ability to use WPA-802.1X authentication schemes if they want, even for small groups. The Enterprise mode is more complex and expensive to install because it requires the use of a RADIUS server to manage keys and is therefore not suitable for home users.

The consumer mode (or personal mode) of WPA uses a combination of pre-shared keys (PSK), TKIP and MIC. The consumer version is typically used in homes or small offices, which require each user to enter a common password. If consumer mode users select the typical 6-8 character passwords that corporate networks require for login purposes, the resulting system will still be insecure. WPA-PSK (Wi-Fi Protected Access with Pre-Shared Key) is the better choice for SOHO users, because of its simple setup and deployment across a multi-vendor environment. Although WPA-PSK was originally intended for home users, it has been adopted by small offices due to the cost and difficulty in setting up a RADIUS server.

2.3.1. Cracking WPA-PSK

Brute-force cracking tools such as coWPAtty are capable of cracking WPA-PSK by systematically testing numerous passwords and combinations of characters. It is estimated that on a Pentium 4 3.8 GHz system, coWPAtty can try 70 words per second, however it would take over 3452 days to test all the possible eight letter passwords (over 208,000,000,000 combinations) [19]. Therefore, it is unrealistic to use such a tool to crack a key and the information still to be relevant [20].

2.4. Wi-Fi Protected Access 2 (WPA2)

The current standard for wireless security, Wi-Fi Protected Access 2 (WPA2), was introduced in September 2004. The IEEE 802.11i standard WPA2, addresses three main security areas: authentication, key management, and data transfer privacy. WPA2 uses the Advanced Encryption Standard (AES) for data encryption and is backward compatible with WPA. Like WPA, WPA2 is also available in Personal and Enterprise modes (Table 3). WPA2 allows an easy transition from WPA mode by using WPA/WPA2 mixed mode, so networked computers can use either WPA or WPA2. However, although WPA2 implements the full standard, it will not work with some older network cards.
The encryption algorithm used in the 802.11i security protocol is AES-Counter Mode CBC-MAC Protocol (AES-CCMP). It uses the AES block cipher (see below), but restricts the key length to 128 bits. AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBC-MAC). The counter mode uses an arbitrary number that changes with each block of text, making it difficult for an eavesdropper to spot a pattern. The CBC-MAC protocol (Cipher Block Chaining-Message Authentication Code) is a message integrity method, which ensures that none of the plaintext bits that were used in the encryption were changed.

2.5. Extensible Authentication Protocol

WPA and WPA2 enterprise modes both utilise the Extensible Authentication Protocol (EAP) as an authentication framework. EAP is an 802.1X standard that allows developers to pass security authentication data between the RADIUS server, the access point and wireless client. EAP has a number of variants, including EAP-MD5, EAP-Tunnelled TLS (EAP-TTLS), Lightweight EAP (LEAP), and Protected EAP (PEAP). EAP resides in the access point and keeps the network port disconnected until authentication is completed. Depending on the results, either the port is made available to the user, or the user is denied access to the network.

2.6. Robust Secure Network (RSN)

Robust Secure Network (RSN) is a protocol used for establishing secure communications over an 802.11 wireless network, and is an element of the 802.11i standard. RSN dynamically negotiates the authentication and encryption algorithms to be used for communications between wireless access point and wireless clients. This means that as new threats are discovered, new algorithms can be added. Transitional Security Network (TSN) is a specification that is designed to allow RSN and WEP to coexist on the same wireless LAN.

2.7. Future developments - Protected Management Frames

Protected Management Frames (PMF) otherwise known as 802.11w, is a new standard that is due to be deployed in 2008. PMF improves the Medium Access Control layer to increase the security of management frames and data frames. As Wireless LANs send system management information in unprotected frames, they are vulnerable to interception. PMF protects against network disruption caused by malicious systems that create disassociation requests that appear to be sent by valid equipment.

3. Recommendations for securing a wireless network

In order to secure a wireless network users should follow a number of procedures to prevent the network from being penetrated.

From the outset, some devices have the security settings disabled as the default option, therefore it is important to switch on the security settings when setting up the device. Wireless detection tools can determine the level of security and an unsecured network is an easy target even for novice hackers. Although WPA and WPA2 are securer encryption protocols then WEP, and WEP is well renowned for its weaknesses, if the access point only supports WEP it is worthwhile enabling it. This will prevent neighbouring Wi-Fi users without the knowledge or intention to hack from sharing bandwidth.

If someone has the ability and intention to hack then WEP is not very protective. However, to make it more secure the user should make the password difficult to guess. Using a selection of random letters and numbers that are not in the dictionary could prevent attacks by programs that carry out dictionary attacks. It is also important to change the password regularly, as an attack may occur over a long period of time if the intruder is determined to gain the information. When using WPA or WPA2 encryption in consumer mode, the password should contain a minimum of 20 randomly selected letters.

The manufacturers default SSID, usernames and passwords are well known to hackers. Therefore, it is likely that if the user has not changed the SSID, then the username and password has also not been changed. This would enable the hacker to change the configuration of the access point to allow easy access. When changing the SSID it is important not to use personal details that could identify the owner. For example, the house number and street name, or business name. This would inform the hacker with the exact location of the network. Using a complicated SSID like X6£g#3Tk$PQ will avoid identifying the access point but may raise suspicion from hackers who may think the user has something to hide.

The SSID is automatically broadcast by the access point to allow wireless clients to identify the signal. By blocking the SSID broadcast, the SSID will not be picked up by clients that are unaware of its existence. This will not prevent wireless detection devices from determining the presence of a wireless network or the SSID, as the probe response packet contains different information to that of a broadcast frame. However, it will prevent casual users from seeing which access points are broadcasting in the local vicinity.

In smaller networks, it may be possible to filter the MAC addresses the access point can broadcast to. This means only selected devices will be allowed to connect to the network. In larger networks, it may be difficult to administer this level of security, however
the risk may out weigh the cost. Only allowing certain clients onto the network can prevent unauthorised devices being used on the network, which will also tighten security. It is possible for a wireless client to have its MAC addressed "spoofed" or impersonated. Therefore, if a hacker is determined enough, it is possible to overcome MAC address filtering.

The software supplied with access points can be too complicated for the average user and the security options are often difficult to find within the software or located under the heading “Advanced Settings” which may prevent some users from utilising it [21]. This leads us to recommend that software designers should ensure that security settings are readily accessible to users and that help information should be made intelligible for both technical and non-technical users.

In addition to offering specific guidelines for what to do and improving the user’s access to how to do it at the machine, there are other ways of encouraging improvements in wireless security through awareness raising and direct assistance.

In the context of e-government, any central or local government agencies rolling out services must consider whether they should assist users to make appropriate security decisions. In February 2005 the UK Government launched a new service, ITsafe,

“to provide both home users and small businesses with advice in plain English advice on protecting computers, mobile phones and other devices from malicious attack.” [22]

Yet, even a year later and despite the best of explicit intentions, information on this site is rudimentary, not well-maintained and does not cover Wi-Fi at all except for a cursory mention in the Glossary [23]. Beyond providing information, there is also the issue of publicising it to reach the intended audience. In the case of ITsafe, the SANS Institute reported in October 2005 that,

“Despite some early publicity, it is now rarely mentioned in press reports or other places where the target audience might see it.” [24]

However abortive that attempt may have been, the UK’s National Hi-Tech Crime Unit launched a new site on 27th October 2005, Get Safe Online [25]. This has support from the Government, some significant international telecommunications and Internet companies and media, and organised a series of roadshows to publicise the launch. This site makes a significant effort to supply easy-to-understand information, with a section dedicated to Wi-Fi [26], although it is perhaps too early to discern the impact it has or will have.

4. Conclusion

Most casual surfers will not attack a WEP encrypted network and are more likely to target a wireless network with no security setting. While most attackers attack just to gain internet access, although this is misuse, the loss is low, and spending hours searching for one credit card number is not worth the attacker’s time. To ensure the data is completely safe, WPA2 encryption should be deployed if the access point allows it. Using a RADIUS server for authentication, will also increase protection, however this may not be an option for a home or small office user.

Non-technical and technical users alike, whether home or business, are in danger of being left in the dark, or even abandoned, over key security features of their systems due to unintelligible design of security-specific software and hidden or unknown security benefits of application software [21]. Secured networks could be jeopardised as a result of human vulnerabilities such as lack of awareness and lack of adherence to usage policies [27]. Using default or easy-to-guess passwords is a common mistake, but may seem safer to the user than picking a difficult-to-remember password.

Although WEP encrypted data can be cracked, it is important to weigh up the costs of how sensitive the data is before deciding whether to use it or not. For the home or small office, the payoff for breaking into a wireless network is considered by some simply too small for an attacker to expend the effort required [12].

As the provision of e-government services to both home and business users gathers momentum, the risk to these users of suffering loss of control of information – interception, insertion, deletion, corruption and related physical assets will become of increasing concern both to individuals and to society in general. Many of these home and small business users may be considered naïve with regard to computer security and Wi-Fi security in particular. Thus, the onus is on software designers (in conjunction with hardware designers) and e-government service providers to ensure that users are able to make appropriate choices in the technical and demanding domain of security, otherwise we will all feel the effects of insecure systems, ranging from invasion of privacy, breach of confidentiality, transactional losses and personal and corporate identity theft.

Acknowledgement

The authors would like to acknowledge financial support from the East of England Development Agency in collaboration with Modern Networks Ltd. The authors would also like to thank Peter Norrington for his useful comments and recommendations that have improved the paper.
References


