An exploration of the security weaknesses of the Wired Equivalent Privacy (WEP)

http://www.openxtra.co.uk/articles/wep-weaknesses

What is WEP?

WEP stands for Wired Equivalent Privacy. The 802.11 designers intention was to provide wireless users with a level of security equivalent to that achievable on a wired network. Unfortunately WEP has turned out to be much less secure than intended.

How does WEP work?

WEP uses secret keys to encrypt data. Both AP and the receiving stations must know the secret keys.

There are two kinds of WEP with keys of either 64bits or 128bits. The longer key gives a slightly higher level of security (but not as much as the larger number would imply). In fact the user keys are 40bits and 104bits long, the other 24bits in each case being taken up by a variable called the Initialization Vector (IV).

When a packet is to be sent it is encrypted using a combination of the IV and the secret key. The IV is different (in theory) for each packet, while the secret key is fixed. The resulting packet data looks like random data and therefore makes the original message unreadable to an outsider not knowing the key. The receiving station reverses the encryption process to retrieve the message in clear text.

What's wrong with WEP?

IV values can be reused

In fact the standard does not specify that the value needs to change at all. Reusing keys is a major cryptographic weakness in any security system.

IV length is too short

24 bit keys allow for around 16.7 million possibilities. Sounds a lot, but on a busy network this number can be achieved in a few hours. Reuse is then unavoidable.

Some manufacturers use 'random' keys. This is not the best way to ensure against reuse. A better solution is to start with a key and increment by one for each subsequent key. Unfortunately many devices revert to the same value at start up and then follow the same sequence providing lots of duplicate values for hackers to work on.

Weak keys are susceptible to attack

Certain keys value combinations, 'Weak IVs', do not produce sufficiently random data for the first few bytes. This is the basis of the highly publicized attacks on WEP and the reason that keys can be discovered.

Manufacturers often deliberately disallow Weak IV values. This is good in that it reduces the chances of a hacker capturing weak keys, but also has the effect of reducing the already limited key possibilities further, increasing the chance of reuse of keys.

Master keys are used directly

From a cryptographic point of view using master keys directly is not at all recommended. Master keys should only be used to generate other temporary keys. WEP is seriously flawed in this respect.

Key Management and updating is poorly provided for

Administration of WEP keys is not well designed and difficult to do on large networks. Users tend to change keys very infrequently which gives a potential hacker lots of time to collect enough packets to launch an attack.

Message integrity checking is ineffective

WEP does have a message integrity check but hackers can change messages and recompute a new value to match. This makes the checking ineffective against tampering.

Conclusion

Although WEP is far from an ideal security solution you should still use it. Some security is better than none. A determined attacker may be able to discover your keys given time and enough weak IVs, but that's no reason to leave all of your doors open.

Check if your equipment manufacturer has an updated driver that avoids sending weak IVs. Use 128 bit encryption if your equipment supports it. Change the key if there is any suspicion of an attack. Ideally install an Intruder Detection System (IDS) to monitor attacks.

Take these precautions and your wireless network will be reasonably secure. For stronger security consider using WiFi Protected Access (WPA).