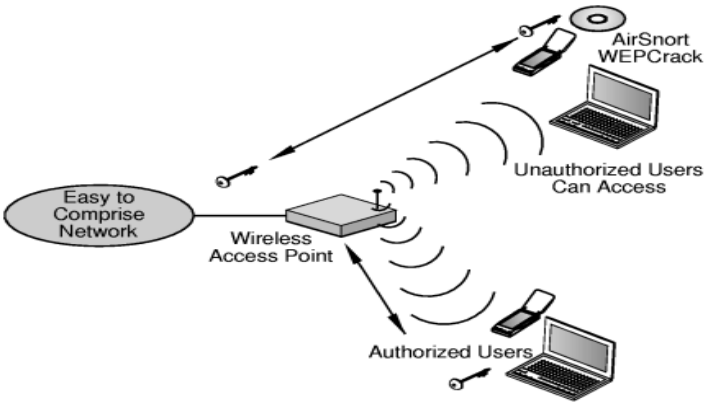
WEP (Wired Equivalent Privacy)

Wired Equivalent Privacy (WEP) is the encryption algorithm built into the 802.11 (Wi-Fi) standard.WEP encryption uses the RC4 stream cipher with 40 or 104 bit keys and a 24 bit initialization vector.

WEP Key Generation

Most 802.11 devices allow WEP keys to be entered using an ASCII passphrase or in hexidecimal format. The conversion between these two formats is an industry standard which is shared by*almost* all vendors of 802.11 equipment.
Some 802.11 devices have difficulty using ASCII passphrases or use a non-standard conversion algorithm. For those devices, you will need to use the hexadecimal version of your WEP key.
Powerdog Industries provides a WEP De Facto Key Generator on their web site. The key generator will convert a WEP passphrase to its 40-bit or 104-bit hexadecimal equivalent.

WEP Security Issues



WEP has led a troubled existence due to many security issues. The security issues with Wired Equivalent Privacy (WEP) include:

1. A high percentage of wireless networks have WEP disabled because of the administrative overhead of maintaining a shared WEP key.
2. WEP has the same problem as all systems based upon shared keys: any secret held by more than one person soon becomes public knowledge. Take for example an employee who leaves a company – they still know the shared WEP key. The ex-employee could sit outside the company with an 802.11 NIC and sniff network traffic or even attack the internal network.
3. The initialization vector that seeds the WEP algorithm is sent in the clear.
4. The WEP checksum is linear and predictable.

The number and scope of difficulties with WEP security have led to the creation of WPA (Wireless Protected Access).
For more information on security issues with Wired Equivalent Privacy (WEP), read Security of the WEP algorithm by Nikita Borisov, Ian Goldberg, and David Wagner.

WEP Security Tools

AirSnort

AirSnort is a wireless LAN (WLAN) tool which cracks encryption keys on 802.11 WEP networks. AirSnort operates by passively monitoring transmissions and computing the WEP encryption key when enough packets have been gathered.

BSD-Airtools

bsd-airtools is a package that provides a complete toolset for wireless 802.11 auditing. Namely, it currently contains a bsd-based Wired Equivalent Privacy (WEP) cracking application, called dweputils (as well as kernel patches for NetBSD, OpenBSD, and FreeBSD). It also contains a curses based ap detection application similar to netstumbler (dstumbler) that can be used to detect wireless access points and connected nodes, view signal to noise graphs, and interactively scroll through scanned ap's and view statistics for each. It also includes a couple other tools to provide a complete toolset for making use of all 14 of the prism2 debug modes as well as do basic analysis of the hardware-based link-layer protocols provided by prism2's monitor debug mode.

WEPCrack

WEPCrack is a tool that cracks 802.11 WEP encryption keys by exploiting the weaknesses of RC4 key scheduling.

WAP Attack

WepAttack is a WLAN open source Linux tool for breaking 802.11 Wired Equivalent Privacy (WEP) keys. This tool is based on an active dictionary attack that tests millions of words to find the right key. Only one packet is required to start an attack on WEP.

WEPWedgie

WEPWedgie is a toolkit for determining 802.11 WEP keystreams and injecting traffic with known keystreams. The toolkit also includes logic for firewall rule mapping, pingscanning, and portscanning via the injection channel and a cellular modem.

Source: http://www.tech-faq.com/wep-wired-equivalent-privacy.html