Common Wi-Fi Hacking software

NetStumbler
A Windows-based tool used to locate open wireless networks

Kismet
Displays SSIDs that are not broadcasted

Airsnort
Cracks WEP encryption keys

Cowpatty
Cracks WPA- pre-shared key

Wireshark
Sniffs data transferred over a wireless network

protected and never re used. WPA2 is the advanced version of WPA. Since WPA is a newer technology it is possible that many routers may not support it, so the user needs to do a firmware update.

WPA Key can be enabled by going in the Wireless Setup tab and selecting WPA Security option. Using a Passphrase which is an alphanumeric keyword, we can generate one or more WPA keys. The passphrase should be greater than 16 alphanumeric characters and should only be known to the administrator.

Wi-Fi Jargon

Encryption
Its the process of scrambling legitimate information using algorithms called ciphers, such that the information can be decrypted only by someone or something that has the encryption key.

Service Set Identifier (SSID)
It is a name that identifies a particular 802.11 wireless LAN network. For the client machine to connect to the network its SSID should match with that of the router.

WarDriving
Its the act of locating and logging onto wireless access points from a moving vehicle using a laptop or a PDA or a cell phone.

Plugging the loopholes

The hackers take advantage of the many loopholes that users tend to overlook while securing their Wi-Fi networks. Configuring the security settings on your Wi-Fi router is time consuming.

Administrator password

All the routers are shipped with default factory settings which many users do not change, while connecting to the internet. These default settings are commonly known, as they are specific to manufacturers. The first thing you should do while setting the router is change the default username and administrator password, so that it is only known to you.

Enabling WEP or WPA Encryption

As discussed above, the need to scramble data while using a wireless network is paramount. You should activate the necessary encryption key. It is advisable to choose WPA or WPA2 encryption rather than WEP if your router supports it. To configure the WPA encryption you have to enter a unique passphrase.

Broadcasting SSID

SSIDs are public names of wireless networks. All the client machines communicate within a network using similiar SSIDs. Router manufacturers generally give default SSIDs eg. Linksys router will have a default SSID 'Linksys'. A user should change this default SSID. Broadcasting SSID is a feature that is ideal for businesses and mobile hotspots where users move in and out of networks. For home broadcasting SSID may make the system vulnerable to attack if the router is not protected by a username and password.

MAC address filtering

Media Access Control (MAC) address is an identification for all the hardware connected to your network. In a home network where there are limited number of users it is better to find out the MAC addresses of all the machines connecting to the network (enter ipconfig/all in the command prompt to get the whole list) The administrator should then feed these numbers under the "permit only" tab in the Wireless Network Access tab. This will ensure that any system whose MAC address does not pass the filter, will not be able to access the network.

What the law says?

We spoke to Karnika Seth, Attorney at Law and Chairperson - Cyber Laws Consulting Center on the subject. Here's what she had to say: "Under the IT Act 2000 there is no provision as such, to fine individuals who leave their Wi-Fi connections unsecure. But if a terrorist uses the open network to conduct his nefarious activities, then the owner may be called in for questioning. The user has to ensure that his connection is secure and should invest some time in securing the network. Leaving your Wi-Fi network open is analogous to leaving a signed chequebook unattended. Its vulnerable to misuse."

Positioning the router

The range of wireless routers may exceed the boundaries of your house, but its stength reduces with distance. It is deemed best to have the wireless router inside the house rather than on the window so that there is very little leakage.

Switching off the router

This may seem a very trivial thing to be included in this section. But many users just do not bother to switch off the router when its not being used for a long period of time.