Learning About The . Net
Home & Small Business Networking Vocabulary

Brute Force
The act of trying all possible letters, numbers, and/or symbols of a password or PIN in an attempt to guess the correct combination.

Encryption
The transformation of data into secret code so that only the intended recipient can read it. Encryption attempts to provide a secure means of communication.

Firmware
Firmware is specialized software that tells a device, namely a router, how to function. Firmware should be regularly checked for updates to help ensure the router is patched with the latest version of security fixes.

InSSIDer Application
InSSIDer is a free mobile application for PC, Mac or Android that allows a device to see information about surrounding wireless networks. This application will let a user know what type of wireless encryption or wireless mode a network is using (WEP, WPA, WPA2), SSID, channel, broadcast frequency, whether a network is vulnerable to the Reaver attack, and more. Available at: http://www.metageek.net/products/inssider/

IP Address
An IP address is a set of numbers which uniquely identify a device on the network (ex. Google's IP address is 173.194.77.147). An IP address is just like a postal address, it helps the router know where to send the information.

Packets
When information is requested from another computer or website, that information is split up into small chunks or packets of information. These packets are then sent via a wired or wireless connection to the router. The router checks the IP address and forwards it on to the appropriate device. The receiving device then reassembles all the small packets back into the original content.

Pre-shared Key
Used in encryption, the pre-shared key is a shared secret passcode or phrase that allows two devices to communicate in private, free from eavesdroppers. This pre-shared key acts as an invite to the network in order to negotiate encryption between two devices.

Reaver Attack
The Reaver attack works against routers that offer WPS service which allows users to connect their devices to the router using a pin or via a button push instead of a password. The Reaver attack can allow unauthorized users to gain access to your network, even those using WPA2, in as little as four hours. The attack is carried out by brute forcing the pin number similar to trying all combinations to a padlock. Until this vulnerability is fixed it is recommended the WPS feature be disabled (if possible).

Router
A router acts as a gateway between your local network and the rest of the internet. This device can also include a wireless component which allows the signal to be broadcast wirelessly.

SSID
The SSID is the name of the network. By default, this name is broadcast publicly to allow other devices to see the network and connect to it.

Traffic
Traffic refers to information that is being sent between two or more devices. Traffic between these devices is sent in packets. It travels between devices via their IP addresses.

War Driving
War driving is when someone drives (or walks) around with a GPS and a device that records publicly available information about wireless signals. Information collected might include GPS location, SSID, wireless encryption, and other network information.

WEP (Wired Equivalent Privacy)
WEP is a very outdated wireless mode. This encryption method has vulnerabilities that can easily be exploited to allow unwanted individual(s) access to a network in as little as six minutes. This encryption method is not recommended.

Wired Connection
Devices on a wired connection are joined together via an ethernet cable into a modem or router. Devices connected in this manner will see less interference and eliminate the risk of wireless eavesdropping.

Wireless Channels
In the United States there are 11 channels to broadcast a wireless signal on the 2.4 GHz range and at least 23 channels on the 5 GHz range. To improve signal quality and decrease interference of other devices, routers can be configured to broadcast on certain channels. Certain applications like inSSIDer can be used to view wireless networks nearby and see what channels they are broadcasting on to prevent overlap.

Wireless Connection
Devices are connected to a router via a wireless signal. This method offers great portability but is vulnerable to eavesdropping.

Wireless Frequencies
Wireless signals are broadcast on two frequencies – 2.4 GHz and 5 GHz. The 2.4 GHz frequency offers a greater distance but suffers from more interference from other devices such as cordless phones and microwaves. The 5 GHz frequency offers a shorter distance but is less prone to interference from other devices and appliances.

WPA (Wi-Fi Protected Access)
After WEP vulnerabilities were discovered, WPA was created in an attempt to address these known issues. While WPA improved upon the outdated WEP encryption, WPA has been replaced by a more secure wireless mode known as WPA2.

WPA2 (Wi-Fi Protected Access v2)
WPA2 is the current standard in wireless encryption. It offers a strong form of encryption to help protect wirelessly broadcast information.

WPS (Wi-Fi Protected Setup)
Designed to provide a one-push button to instantly set up a wireless home network, this option is available on most modern routers. However WPS has a known vulnerability which can be exploited by using the Reaver attack. This will allow unwanted users to gain access to a network in as little as four hours regardless of encryption method used. Therefore it is recommended that this feature is disabled.