WPA/WPA2

WPA was the first step to the 802.11i standard, and WPA2 is the next advancement to the ratification of 802.11i. WPA uses AES and TKIP. Now you may be wondering "Why do we have two forms of encryption??"

Well TKIP (Temporal Key Integrity Protocol) really isn't a form of encryption, but rather provides:

- Message Integrity
- Re-keying mechanism
- Per packet key mixing

You may be wondering what that means, so let's break it down.

Message Integrity is used to ensure that an error or third party isn't tampering with the data being transmitted. Using a Hashing algorithm, it is possible to create a unique hash of the data being transmitted. This is created by the sender, then the data is recalculated on the other side in order to ensure that the message integrity hasn't been compromised. Re-keying and per-packet key mixing, are means of changing the encryption key at a set interval. Rather than simply use one key to encrypt all messages, keys referred to as subkeys are generated from a master key. This ensures that the key used to encrypt the message is not vulnerable due to the fact that the key is constantly changing. Even if the hacker was able to gain access to the current key being used, he/she would have to obtain the master key in order to know the next key being used.

Advanced Encryption Standard (AES) is the actual encryption being used. If you're familiar with encryption algorithms, you should know that DES (Data Encryption Standard) was replaced by AES as the defacto standard.

Now the main difference between WPA and WPA2 is the change from TKIP to Counter Mode CBC MAC Protocol (or CCMP). CCMP is a more secure and scalable solution compared to the previous TKIP method. When 802.11i is ratified, CCMP will probably be part of it, rather than TKIP.

Of course this is a very basic overview of WPA vs WPA2. If you want more information about how the algorithms work, I would suggest the following links:

Cipher Blocks
Wikipedia CCMP
Wikipedia AES
Wikipedia TKIP
Wikipedia WPA
Wikipedia on WPA2

If you really want to learn more about wireless encryption, I would highly suggest you read *Real 802.11 Security: Wi-Fi Protected Access and 802.11i* by Jon Edney, William A. Arbaugh ISBN: 0321136209B06242003

This book covers, in detail, all methods of encryption and authentication used by 802.11. Be warned, it is very technical.

The question was asked: "WPA2 Pre-Shared Key Only" vs. "WPA2 Pre-Shared Key Mixed" What is the difference? Is "Mixed" WPA and WPA2???

BrainSlayer replied: 24 Dec 2005 23:16 In mixed mode, the unit tries wpa2 first and if its fails it uses wpa1