



Chameleon RF™ Teaming up with Agere to Secure your WLAN:

One of the most talked about subjects relating to wireless LAN's and 802.11b in particular is security.

The 802.11b standard as it now exists, addresses security through several mechanisms. The most important being Wired Equivalent Privacy (WEP). WEP was intended to provide the equivalent to a non-encrypted wired network. WEP supports two sizes of encryption keys, 64bit and 128bit RC4.

The keys are generated by combining two components. The Secret Key entered by the user and an Initialization Vector supplied by the Wireless Adapter. The Secret Key is either 40 bits (for 64bit WEP) or 104bits (for 128bit WEP). The Secret key is entered either in hex or in ASCII. This is why the keys are 5 ASCII or 10 Hex characters for 64bit WEP and 10 ASCII or 26 Hex characters for 128bit WEP.

The Initialization Vector is the other component. It's always 24bits and is determined by the firmware in the wireless adapter. This IV is added to the Secret Key to get the 64 or 128bit encryption key. This 24bit IV is the source of the weaknesses discovered in the WEP system.

Several papers published by researchers at Berkeley University and others have pointed out the weaknesses of WEP. The IV should vary with each transmitted frame. But the problem with the IV as currently implemented is the IV starts at the same value each time the wireless card is initialized. This creates IV's that are considered "weak". Programs such as AirSnort and WEPCrack were designed to take advantage of these weak keys. By obtaining enough sample data from a wireless network, AirSnort can scan the encryption keys in each frame looking for the "weak" ones.

When enough of the keys are found, the program can then break the key and decrypt the data.

Although the 802.11 committee has been working on a new encryption mechanism (802.11i), this new mechanism will not be ratified for a while. Until then, how does one secure an existing network from intruders?

Several companies have come out with solutions for security. These include VPN support, KERBEROS, and IPSec. These solutions while valid, do not address the needs of existing DOS based data collection systems. They also require special client side software and external authentication systems like RADIUS. DOS based data-collection terminals due to their proprietary implementations of DOS, older IP Stack software and low powered processors; make it difficult to implement VPN clients.

Although VPN clients are in the works for these terminals, there is another way to provide better protection until then.

Agere is soon to implement an extension to the WEP mechanism called WEPPlus. WEPPlus changes the way the Initialization Vector is determined. This avoids what they call the "Weak Key" syndrome. This mechanism is implemented in the card firmware and Access Point firmware thus avoiding any special drivers or client side software. A simple firmware update made available in the Agere Winter 2002 release provides WEPPlus support. The upgrade however, does not affect the 802.11 WiFi compatibility of the agere-based hardware. Access Points with WEPPlus weak key avoidance will interoperate with stations that do not have the update, but the frames for these stations won't be protected from programs like AirSnort.

At least one end user has implemented WEPPlus and has used AirSnort to attempt to break the keys. The user captured over 1 week's worth of data and AirSnort was not able to crack the key. Using WEPPlus and changing the keys on a regular basis can protect a network from most attacks.

Since the radios in Chameleon RF™ products are Agere, they can take advantage of WEPPlus. All Chameleon RF™ products such as the TR1200, WT2200, VT2400, PB2100 and FL3500 will be shipped with the WEPPlus firmware installed. Any existing ChameleonRF terminals can be upgraded to support WEPPlus. Contact Chameleon RF™ for information on how to schedule terminals for upgrade.

For more information, or to upgrade your current Chameleon RF™ terminals to WEP Plus, contact us today at 866.CHAMRF2, or visit us at www.chameleonrf.com

Authored by Mr. Chuck Bolvin, V.P. of Technology-WAV™, Inc