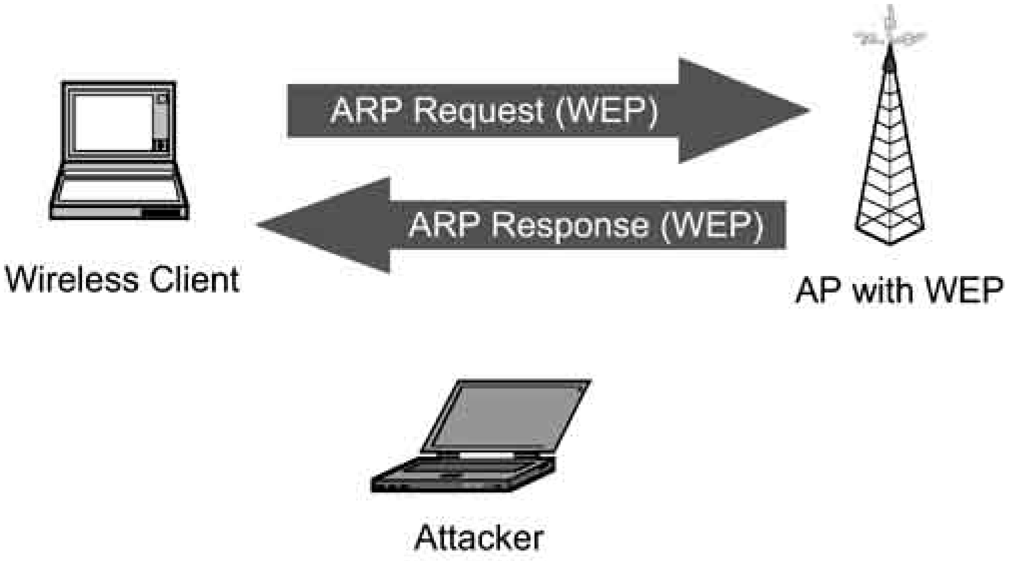
Packet Injection - Breaking WEP Faster

Before I explain what packet injection is or how it works, one needs a basic understanding of the available attacks against WEP. There are two main types... the dictionary attack and the FMS attack. A dictionary attack runs through a wordlist checking if the secret key is a normal dictionary word. Only one encrypted packet is required to run this attack (which is good!) and it usually takes under 30 minutes to go through a 30Mb wordlist. If you are interested in using a dictionary attack, check out **wepattack**.

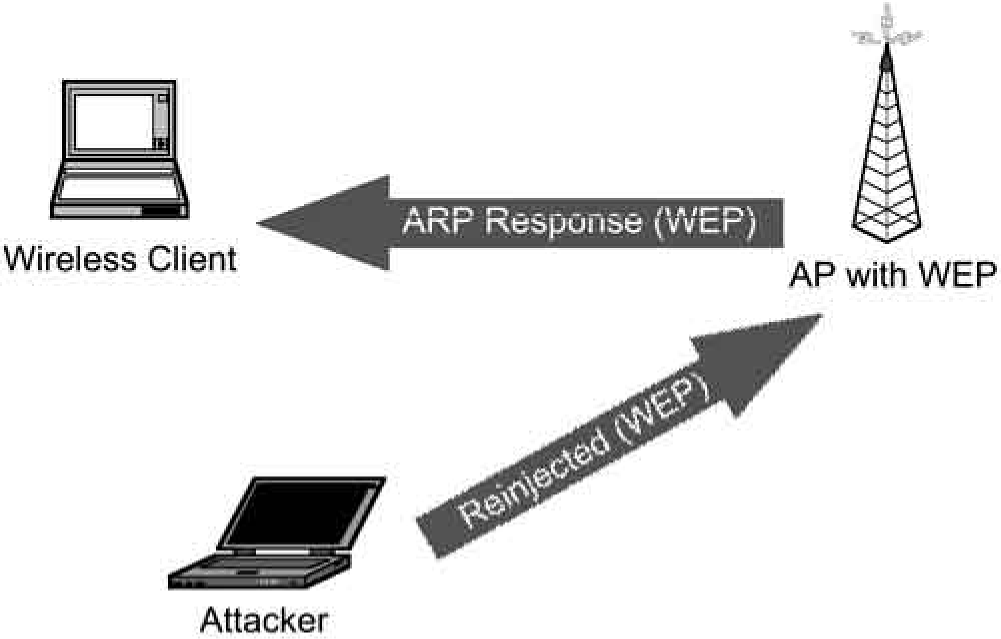
The FMS attack (named after Fluhrer, Mantin, Shamir, the guys who **discovered it**) is a statistical approach and requires tons of packets to expose the password. Why tons of packets? Well, when WEP encrypts a packet, it concatenates a random string, called the initialization vector (IV) with the password you chose. So take the [IV] + [secret key] --> [RC4] shove it into an RC4 cipher... and RC4 generates the keystream. A new IV is generated for every packet. The problem is that the IV is only 24-bit, and with heavy network traffic the same IVs will be re-used many times. FMS uses this weakness to determine the secret key.

Up until this point, only businesses with massive amounts of wireless traffic were at risk for an FMS attack. Under normal circumstances, Joe Linksys would never create this much traffic in 666 years. Of course on your home network, you can **ping flood** the access point or transfer data to another computer to generate a lot of wireless traffic in a short time. Then you'll probably brag to your friends that you broke WEP in a half an hour and WEP sucks! etc. Well, WEP does suck. However, generating traffic in this manner does not prove that an attacker can get to your network from the outside. This is exactly where packet injection comes in.

Packet injection allows an outsider to generate a large amount of traffic on a network without being associated in any way. First, an attacker must look for a specific packet type being sent across the network and capture it. The type of packet, although hidden behind encryption, can be easily guessed based on packet size. For example, an ARP request packet is always 28 bytes. The first picture shows an attacker monitoring ARP traffic between a legitimate client and an access point.



After an attacker captures a packet, they can re-inject it into the network. (See second picture) The access point will respond to this forged request and send out packets to the legitimate client. This additional traffic is used to gather encrypted packets faster and ultimately allows the attacker to find the secret WEP key in much less time.



There's no script kiddie way of doing this (yet), but it is possible to pull off with the right know how. To break WEP on your own network, check out **aircrack**, which performs an optimized FMS attack (optimized == less packets required == less time). And to learn more about "cutting edge" packet inject techniques, check out the **Netstumbler Forums** - Unix/Linux Section. Pictures above taken from **phptr.com**, without permission ;)