Wired Equivalent Privacy

From MTU LUG wiki

WEP is short for Wired Equivalent Privacy. The purpose of WEP was to add a tiny level of security to make it difficult for the average person to listen in on traffic going on a WiFi network. WEP uses the RC4 algorithm. While it is no longer recommended for new systems, it is quite secure when implemented properly.

RC4 is a stream cipher. The algorithm is initialized with a specific seed value and then generates a pseudo-random stream of bits that is XORed with the data. WEP generates this seed using a 40-bit (later 104-bit) key and a 24-bit initialization vector. The key is shared across all devices, the initialization vector (IV) is regenerated for each packet sent across the network. The IV used to seed RC4 is sent in the clear as part of the transmission.

Original attacks against WEP relied on weak IVs that leaked information about the other parts of the key. An attack like this required approximately 1 million to 5 million packets to obtain the required number of weak IVs. Obviously, that is alot of traffic to capture and store. This attack was known as the FMS attack. Eventually vendors released updated drivers that simply didn't use weak IVs.

Luckily someone named KoreK came along with a new statistical attack against WEP that only relied on unique IVs. This attack requires about 250,000 unique IVs for a 40-bit WEP key. This still takes a long time to gather, but an order of magnitude fewer than the FMS attack. An attacker can use a tool like airodump to capture packets on a WiFi network. After gathering the required number of packets s/he then runs aircrack on the packet log and the key will be discovered.

Luckily WEP has another vulnerability we can exploit to generate encrypted traffic on the network. A replay attack is when you retransmit an encrypted message with the hopes that the destination will accept it. There is no check in WEP to ensure that it won't decode and pass on already decoded packets. The retransmitted packet will obviously use the same IV each time, but if a host on the network responds then it's response will use a new IV each time.

To usefully exploit this flaw you need a packet that a host will respond to. Most networks have lots of these; it's part of being an Ethernet network. ARP is used by hosts on an Ethernet network to discover what MAC address corresponds to an IP address. This is used to fill in the link-layer fields of the packet. This ARP packet is broadcast to all hosts on the network and a host will always respond to an ARP query that contains it's IP address. ARP packets are perfect for the replay attack because of this. Aireplay is a tool that is used to do exactly this.

The KoreK attack combined with the replay vulnerability can crack a 40-bit WEP key in under 30 minutes. 104-bit WEP in under an hour.

Wikipedia article on WEP

- This page was last modified on 15 April 2005, at 04:41.
- This page has been accessed 7,033 times.