

# SECURITY OF WIRELESS NETWORKS

## AS SPECIFIED BY IEEE 802.11 STANDARDS

### 1 Wired Equivalent Privacy (WEP)

WEP was defined as a means of protecting the confidentiality of data exchanged among authorized users of a WLAN from casual eavesdropping. WEP is deprecated and its implementation for backwards compatibility is optional.

#### 1.1 Specification

WEP implementation uses the RC4 stream cipher as its encryption and decryption algorithm. RC4 uses a pseudorandom number generator (PRNG) to generate a key stream that is XORed with a plaintext data stream to produce cipher text or to recover plaintext from a cipher text.

Standard 64-bit WEP creates the RC4 key by concatenating 40-bit key with a 24-bit initialization vector (IV). However the encapsulation is unsafe at any key size.

#### 1.2 Attacks

Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets.

##### 1.2.1 Incorrect usage of RC4

Scott Fluhrer, Itsik Mantin, and Adi Shamir found a flaw in the RC4 key setup algorithm which results in a total recovery of the secret key. Implementing the attack requires the collection of traffic passively.

### **1.2.2 Flaws in the protocol**

In 2006, Bittau, Handley, and Lackey showed that the 802.11 protocol itself can be used against WEP to enable earlier attacks that were previously thought impractical. After eavesdropping a single packet, an attacker can rapidly bootstrap to be able to transmit arbitrary data. The eavesdropped packet can then be decrypted one byte at a time (by transmitting about 128 packets per byte to decrypt) to discover the local network IP addresses. Finally, if the 802.11 network is connected to the Internet, the attacker can use 802.11 fragmentation to replay eavesdropped packets while crafting a new IP header onto them. The access point can then be used to decrypt these packets and relay them on to a buddy on the Internet, allowing real-time decryption of WEP traffic within a minute of eavesdropping the first packet.

### **1.2.3 Correlations between the RC4 keystream and the key**

In 2007, Erik Tews, Andrei Pychkine, and Ralf-Philipp Weinmann invented a new attack, with which it is possible to recover a 104-bit WEP key with probability 50% using only 40,000 captured packets. For 60,000 available data packets, the success probability is about 80% and for 85,000 data packets about 95%. Using active techniques like re-injection, 40,000 packets can be captured in less than one minute under good conditions. The actual computation takes about 3 seconds and 3 MB of main memory on a Pentium-M 1.7 GHz and can additionally be optimized for devices with slower CPUs. The same attack can be used for 40-bit keys with an even higher success probability.

## **2 Wi-Fi Protected Access (WPA, WPA2)**

The recommended solution to WEP security problems is to switch to WPA2. WPA was an intermediate solution for hardware that could not support WPA2. WPA was introduced in an amendment 802.11i.

### **2.1 Specification**

WPA uses the Temporal Key Integrity Protocol (TKIP). The RC4 stream cipher is used with a 128-bit per-packet key, meaning that it dynamically generates a new key for each packet.

WPA2 uses an AES-based encryption mechanism Counter Cipher Mode with block chaining message authentication code Protocol (CCMP), that is stronger than TKIP.

### **2.2 Vulnerabilities**

#### **2.2.1 Weak password**

Shared-key WPA is vulnerable to dictionary attacks. It is important to choose a truly random password and to set an uncommon SSID, in order to protect the network against attacks using precomputed rainbow tables.

#### **2.2.2 MS-CHAPv2**

Several weaknesses have been found in Challenge-Handshake Authentication Protocol MS-CHAPv2, some of which severely reduce the complexity of brute-force attacks making them feasible with modern hardware. In 2012 the complexity of breaking MS-CHAPv2 was reduced to that of breaking a single DES key.

#### **2.2.3 Wi-Fi Protected Setup PIN recovery**

A serious security flaw was revealed in December 2011 by Stefan Viehböck that affects wireless routers with the Wi-Fi Protected Setup (WPS) feature, regardless of which encryption method they use. Many consumer Wi-Fi device manufacturers had taken steps to eliminate the potential of weak passphrase choices by promoting alternative methods of automatically generating and distributing strong keys when

users add a new wireless adapter or appliance to a network. These methods include pushing buttons on the devices or entering an 8-digit PIN. The Wi-Fi Alliance standardized these methods as Wi-Fi Protected Setup; however the PIN feature as widely implemented introduced a major new security flaw. The flaw allows a remote attacker to recover the WPS PIN and, with it, the router's WPA/WPA2 password in a few hours. Users have been urged to turn off the WPS feature, which is enabled by default in many cases. On some models it is not possible to disable the feature. The PIN is usually written on a label on most Wi-Fi routers with WPS, and cannot be changed if compromised.

### 3 Links

- IEEE 802.11 standards available for free download:

<http://standards.ieee.org/getieee802/download/802.11-2012.pdf>

<http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>

- Short list of some 802.11 Security Vulnerabilities:

<http://www.cs.umd.edu/~waa/wireless.html>

- Related wikipedia articles

[http://en.wikipedia.org/wiki/IEEE\\_802.11](http://en.wikipedia.org/wiki/IEEE_802.11)

[http://en.wikipedia.org/wiki/Wired\\_Equivalent\\_Privacy](http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy)

[http://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Access](http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)