

# Wireless Security Standards

Shay Ohayon - 28/09/2005



## **Table of contents:**

- Security Standards.
  - WEP (kinda obsolete)
  - WPA (WPA-PSK, WPA2)
  - VPN.
- Some applications.
- Auditing.
- Links.

## Security Standards

### WEP: Overview

- Not a standard anymore (too insecure – see <http://www.crimemachine.com/Tuts/Flash/wepcracking.swf> :-)
- It was intended to give wireless users security equivalent to being on a wired network.
- Uses the RC4 algorithm.
- The security flaws specifications (by Shamir, Fluhrer and Martin) can be found here:  
[http://online.securityfocus.com/data/library/rc4\\_ksaproc.pdf](http://online.securityfocus.com/data/library/rc4_ksaproc.pdf)
- Another problem: Key management.

## Security Standards

### WEP: The security flaw, ~~not so~~ simply explained...

The RC4 mechanism to encrypt the data:

1. data

2. data + RC4(40 WEP key + 24 random data)

3. sending packet: encrypted data + IV

4. encrypted data transmitted across the air waves

5. receiving data

1. plain-text data
2. the data is encrypted using 40 bits of the secret (WEP) key and random 24 bits.
3. the encrypted data is sent.
4. the data is transmitted across the air waves
5. the data is received and decrypted using the same key + weak IV

## Security Standards

### **WEP: The security flaw, ~~not so~~ simply explained...**

- The random 24 bit number (IV) is a number between 0 and 16,777,216.
- You can get 16,000 packages in 10 minutes.
- Some numbers in the range of 0 to 16777215 do not work well in the RC4 encryption mechanism.
- When the RC4 algorithm picks out these 'Weak IVs', the resulting encrypted packet can be run through mathematical functions to reveal part of the WEP key.

## Security Standards

### Wi-Fi Protected Access: Overview

- It was created in response to the several serious weaknesses encountered in WEP.
- Implements the majority of the IEEE 802.11i standard
- Designed for use with an 802.1X authentication sever - “WPA-Enterprise”
- Works with Pre-Shared Key (PSK) – the WiFi alliance calls this method “WPA-Personal”.
- Uses TKIP (Temporal Key Integrity Protocol)
- It works with the RC4 algorithm, using a 128 bit key and a 48 IV.
- It has the MIC (Message Integrity Check) CRC for integrity validation check.

## Security Standards

### Wi-Fi Protected Access: Security flaws

#### The MIC Denial of Service Attack:

- The MIC is created using Michael, which includes a built in protection mechanism to prevent brute force attacks. As a result, any attempted attack on a MIC value will result in a complete disconnect of all wireless devices for one minute, and a password change.
- The problem is that this 'attack' response only requires two invalid MIC values in one minute. While the attack is very difficult, it is possible for an attacker to essentially cause the wireless network to perform a Denial of Service attack on itself.

## Security Standards

### Wi-Fi Protected Access: Security flaws

The Pre-Shared Key (also known as WPA-Personal):

- Because not every home-user or small business can afford to have an authentication server, WPA uses a Primary Master Key, which is used by all the clients to connect to the access point.
- The MIC is created using the source and destination address, some random data and the PMK.
- All the data is passed as plain text for authentication.
- The password can be cracked using a dictionary-based password cracker.

## Security Standards

### WPA2: Overview.

- WPA2 implements the mandatory elements of 802.11i.
- The Michael algorithm is replaced by a message authentication code, CCMP, or the Counter-Mode/CBC-Mac Protocol, which is an IEEE 802.11i encryption algorithm. In the 802.11i standard, unlike WPA, key management and message integrity is handled by a single component CCMP built around AES.
- The RC4 Encryption algorithm is replaced by the AES algorithm.

## Security Standards

### Virtual Private Networking

- Most major corporations today use VPN to protect their remote-access workers and their connections. It works by creating a secure virtual "tunnel" from the end-user's computer through the end-user's access point or gateway, through the Internet, all the way to the corporation's servers and systems. It also works for wireless networks and can effectively protect transmissions from Wi-Fi equipped computers to corporate servers and systems.
- You can get the Linux's PPTP client and server (PoPTop) to work with Wireless Access.

## Applications

;-) The good ol' applications for wireless networks detection:  
(taken from the previous talk “Wireless and Linux”)

- Kismet (<http://www.kismetwireless.net/>)
- Aircnort (<http://aircnort.shmoo.com/>)
- Wavemon (<http://freshmeat.net/projects/wavemon/>)
- AirCrack (<http://www.cr0.net:8040/code/network/aircrack/>)

## Applications

### WPA clients

- wpa\_supplicant: ([http://hostap.epitest.fi/wpa\\_supplicant/](http://hostap.epitest.fi/wpa_supplicant/))
- xsupplicant: (<http://www.open1x.org/>)

## Applications

### WPA Auditing tools

- WPA Cracker

([http://www.tinypeap.com/html/wpa\\_cracker.html](http://www.tinypeap.com/html/wpa_cracker.html))

- coWPAtty

(<http://new.remote-exploit.org/images/5/5a/Cowpatty-2.0.tar.gz>)

## Applications

### VPN

- Linux's PPTP client.
- PoPToP: Linux's PPTP server.

(<http://poptop.lineo.com/>)

## Applications

Ways to use the EAP/TSL authentication methods on Linux

- Free RADIUS (<http://www.freeradius.org/>)
  - A good FAQ about implementing RADIUS can be found at:  
<http://www.missl.cs.umd.edu/wireless/eaptls/?tag=missl-802-1>

## Auditing.

- Tools and demonstrations on how to audit a WPA-PSK (WPA-Personal) based authentication method. -- see WPA.swf
- The demo can be downloaded from:  
<http://www.crimemachine.com/Tuts/Flash/WPA.swf>
- Tools used on the demo:
  - Kismet
  - airforge
  - aireplay
  - ethereal
  - coWPAtty(All this tools can be found in the “Auditor” LiveCD.)

## Links.

- <http://www.informit.com/guides/content.asp?g=security&seqNum=86&rl=1>
- <http://arstechnica.com/articles/paedia/security.ars/2>
- <http://new.remote-exploit.org/index.php/Tutorials>
- [http://www.hpl.hp.com/personal/Jean\\_Tourrilhes/Linux/](http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/)
- [www.wi-fi.org](http://www.wi-fi.org) The WiFi alliance.
- <http://en.wikipedia.org/> The Free Encyclopedia
- <http://www.iwhax.net>

**Thanks for your attention :-)**

**any comments, corrections,  
questions are welcome,  
[shay@shayohayon.net](mailto:shay@shayohayon.net)**

**(Signed and encrypted mail  
are welcome.)**