

# [TOOL] Aircrack-ptw – WEP Cracking Tool (ARP)

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2007-04/msg00042.html>

---

- *From:* SecuriTeam <[support@xxxxxxxxxxxxxx](mailto:support@xxxxxxxxxxxxxx)>
  - *Date:* 26 Apr 2007 14:21:50 +0200
- 

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

Aircrack-ptw – WEP Cracking Tool (ARP)

---

## SUMMARY

## DETAILS

WEP is a protocol for securing wireless LANs. WEP stands for "Wired Equivalent Privacy" which means it should provide the level of protection a wired LAN has. WEP therefore uses the RC4 stream to encrypt data which is transmitted over the air, using usually a single secret key (called the root key or WEP key) of a length of 40 or 104 bit.

### A history of WEP and RC4

WEP was previously known to be insecure. In 2001 Scott Fluhrer, Itsik Mantin, and Adi Shamir published an analysis of the RC4 stream cipher. Some time later, it was shown that this attack can be applied to WEP and the secret key can be recovered from about 4,000,000 to 6,000,000 captured data packets. In 2004 a hacker named KoReK improved the attack: the complexity of recovering a 104 bit secret key was reduced to 500,000 to 2,000,000 captured packets.

In 2005, Andreas Klein presented another analysis of the RC4 stream

## [TOOL] Aircrack-ptw – WEP Cracking Tool (ARP)

cipher. Klein showed that there are more correlations between the RC4 keystream and the key than the ones found by Fluhrer, Mantin, and Shamir which can additionally be used to break WEP in WEP like usage modes.

### Aircrack-ptw attack

Aircrack-ptw is able to extend Klein's attack and optimize it for usage against WEP. Using aircrack-ptw's version, it is possible to recover a 104 bit WEP key with probability 50% using just 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 deauth and ARP re-injection, 40,000 packets can be captured in less than one minute under good condition. The actual computation takes about 3 seconds and 3 MB 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 too with an even higher success probability.

### Countermeasures

We believe that WEP should not be used anymore in sensitive environments. Most wireless equipment vendors provide support for TKIP (as known as WPA1) and CCMP (also known as WPA2) which provides a much higher security level. All users should switch to WPA1 or even better WPA2.

### How the attack works

A <http://eprint.iacr.org/2007/120> paper describing the details and methods we used in our attack is available on the <http://eprint.iacr.org/> IACR ePrint server.

### Implementation

We implemented a proof-of-concept of our attack in a tool called aircrack-ptw. It should be used together with the aircrack-ng toolsuite.

### Reproduction of our results

The tool is quite similar to aircrack-ng. You can find a very good tutorial on the [http://www.aircrack-ng.org/doku.php?id=simple\\_wep\\_crack](http://www.aircrack-ng.org/doku.php?id=simple_wep_crack) aircrack-ng homepage. For usage with our tool, you need to make some little changes.

\* In Step 3, you MUST NOT use the parameter -ivs. Just skip this parameter, the other command line arguments still apply.

\* In Step 5, you should use aircrack-ptw instead of aircrack-ng. `ls -la output*.cap` will give you a list of capture files airodump-ng has created. Usually, if you did not interrupt airodump-ng, there should be only one file named `output-01.cap`. Just start `aircrack-ptw output-01.cap` to get the key. If aircrack-ptw was not successful, wait a few seconds and start it again.

### Questions and answers

Does aircrack-ptw work with arbitrary packets?

No, aircrack-ptw currently only works with ARP requests and ARP responses. Using methods like ARP re-injection, it is usually not a problem to generate a sufficient amount of ARP traffic.

[TOOL] Aircrack-ptw – WEP Cracking Tool (ARP)

In a future version, aircrack-ptw could be extended to work with other packets too.

Does aircrack-ptw work with 256 bit keys?  
Currently, aircrack-ptw does not support 256 bit WEP.

Does aircrack-ptw work on WPA1 or WPA2 too?  
No. WPA is a complete redesign. Although the TKIP specified for WPA still uses RC4 as encryption algorithm, related-key attacks are not possible in this case since the per-packet keys do not share a common suffix. Furthermore, re-injection attacks on WPA protected networks will not work: WPA requires multiple packets with the same IV to be discarded. Although no cryptographic attacks against WPA1 are known, we recommend WPA2 over WPA1 if you have the choice.

Does aircrack-ptw work against WEPplus?  
This has not been tested due to lack of equipment supporting WEPplus. Since WEPplus only avoids the weak IVs of the original FMS attack, we foresee no problems in applying the attack against WEPplus.

Does aircrack-ptw work against Dynamic WEP?  
This has not been tested as well. In principle we expect our attack to work on networks protected by Dynamic WEP. Since Dynamic WEP allows for re-keying, the attack will provide a key that may only be valid for a certain time frame. After the key has expired, the attack needs to be performed again.

ADDITIONAL INFORMATION

The information has been provided by <<mailto:snorky@xxxxxxxx>> Sn0rkY.  
To keep updated with the tool visit the project's homepage at:  
<<http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>>  
<http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/>

=====

This bulletin is sent to members of the SecuriTeam mailing list.  
To unsubscribe from the list, send mail with an empty subject line and body to:  
list-unsubscribe@xxxxxxxxxxxxxxxxx  
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxxxxxx

=====  
=====

DISCLAIMER:

[TOOL] Aircrack-ptw – WEP Cracking Tool (ARP)

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.