WEP cracking

Bartosz Chodorowski

<chomzee@ethernet.pl>

Selected choice from computer science
October 26, 2009

WEP

- WEP (Wired Equivalent Privacy) – algorithm to secure IEEE 802.11 networks

WEP

- WEP (Wired Equivalent Privacy) – algorithm to secure IEEE 802.11 networks
- Introduced in 1997

WEP

- WEP (Wired Equivalent Privacy) – algorithm to secure IEEE 802.11 networks
- Introduced in 1997
- Was intended to provide security comparable to that of a traditional Ethernet

WEP

- WEP (Wired Equivalent Privacy) – algorithm to secure IEEE 802.11 networks
- Introduced in 1997
- Was intended to provide security comparable to that of a traditional Ethernet
- Vulnerable to crypto analytic attacks

Encryption details

- Stream cipher RC4 for confidentiality

Encryption details

- Stream cipher RC4 for confidentiality
- CRC-32 checksum for integrity

Encryption details

- Stream cipher RC4 for confidentiality
- CRC-32 checksum for integrity
- 64-bit and 128-bit variants

64-bit WEP

- Also known as WEP-40

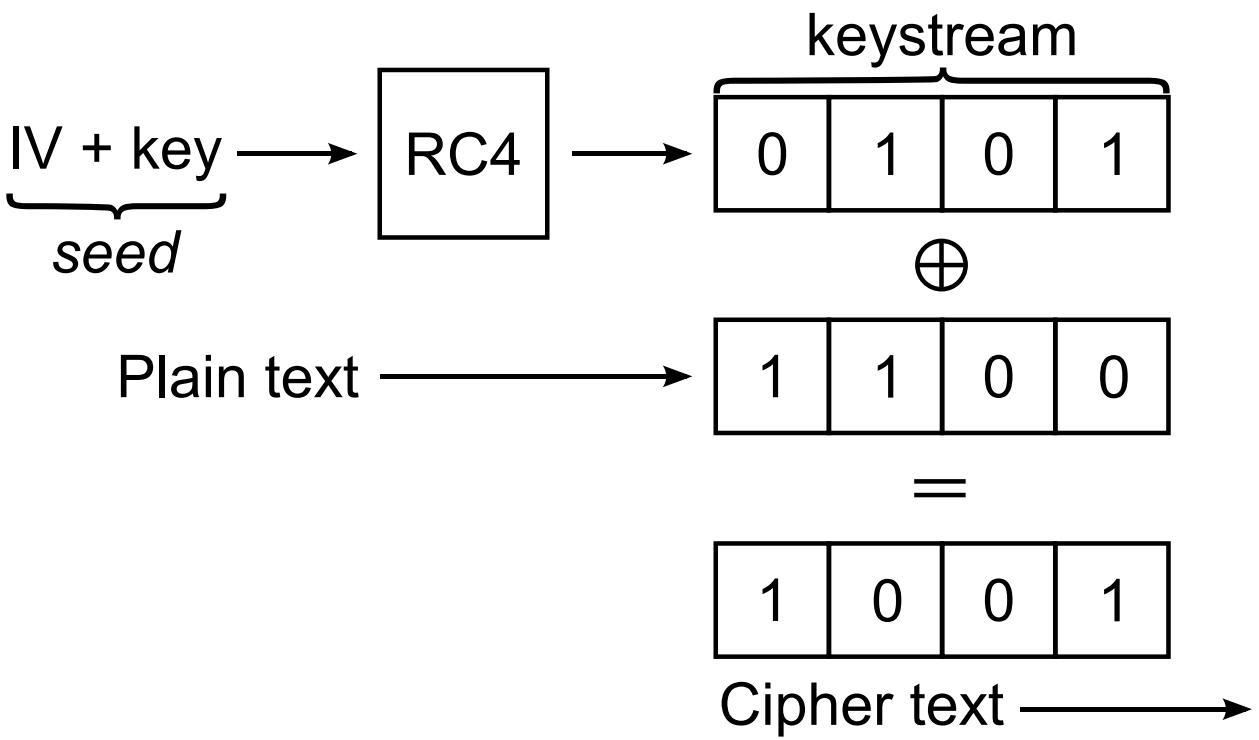
64-bit WEP

- Also known as WEP-40
- 10 hexadecimal digits as a key, e.g. `AB:CD:E1:23:45`

64-bit WEP

- Also known as WEP-40
- 10 hexadecimal digits as a key, e.g. `AB:CD:E1:23:45`
- Concatenated with a 24-bit initialization vector (IV) to form RC4 key.

64-bit WEP


keystream
IV + key
seed
RC4
0 1 0 1
⊕
Plain text
1 1 0 0
=
1 0 0 1
Cipher text

128-bit WEP

- Also known as WEP-104

128-bit WEP

- Also known as WEP-104
- 26 hexadecimal digits as a key, e.g.
  `AB:CD:E1:23:45:1F:12:34:AB:30:6C:36:55`

128-bit WEP

- Also known as WEP-104
- 26 hexadecimal digits as a key, e.g.
  `AB:CD:E1:23:45:1F:12:34:AB:30:6C:36:55`
- Concatenated with a 24-bit IV

WEP weakness

- August 2001 – Scott Fluhrer, Itsik Mantin, Adi Shamir published crypto analysis of WEP. Attack based on this method is known as FMS

WEP weakness

- August 2001 – Scott Fluhrer, Itsik Mantin, Adi Shamir published crypto analysis of WEP. Attack based on this method is known as FMS
  - at least 200 000 IVs – 64-bit key
  - at least 500 000 IVs – 128-bit key

WEP weakness

- August 2001 – Scott Fluhrer, Itsik Mantin, Adi Shamir published crypto analysis of WEP. Attack based on this method is known as FMS
  - at least 200 000 IVs – 64-bit key
  - at least 500 000 IVs – 128-bit key
- 17 KoreK's attacks

WEP weakness

- August 2001 – Scott Fluhrer, Itsik Mantin, Adi Shamir published crypto analysis of WEP. Attack based on this method is known as FMS
  - at least 200 000 IVs – 64-bit key
  - at least 500 000 IVs – 128-bit key
- 17 KoreK's attacks
- 2007 – Erik Tews, Andrei Pychkine and Ralf-Philipp Weinmann (PTW attack)

WEP weakness

- August 2001 – Scott Fluhrer, Itsik Mantin, Adi Shamir published crypto analysis of WEP. Attack based on this method is known as FMS
  - at least 200 000 IVs – 64-bit key
  - at least 500 000 IVs – 128-bit key
- 17 KoreK's attacks
- 2007 – Erik Tews, Andrei Pychkine and Ralf-Philipp Weinmann (PTW attack)
  - 40 000 IVs – 128-bit key – 50%
  - 85 000 IVs – 128-bit key – 95%

ARP replay

- Way to generate extra flow in encrypted wireless network

ARP replay

- Way to generate extra flow in encrypted wireless network
- Capture encrypted ARP request and replay it rapidly

ARP replay

- Way to generate extra flow in encrypted wireless network
- Capture encrypted ARP request and replay it rapidly
- Remote machine should respond with ARP reply

ARP replay

- Way to generate extra flow in encrypted wireless network
- Capture encrypted ARP request and replay it rapidly
- Remote machine should respond with ARP reply
- Effect – **20 000 IVs per minute**, which is enough to crack 128-bit key in 5 minutes

Essential hardware

- PC

Essential hardware

- PC
- Wireless Network Interface Card

Essential hardware

- PC
- Wireless Network Interface Card **based on a good chipset!**

Essential hardware

- PC
- Wireless Network Interface Card **based on a good chipset!**

  `http://www.aircrack-ng.org/doku.php?id=compatibility_drivers`

Essential hardware

- PC
- Wireless Network Interface Card **based on a good chipset!**

  `http://www.aircrack-ng.org/doku.php?id=compatibility_drivers`

  Atheros is highly recommended

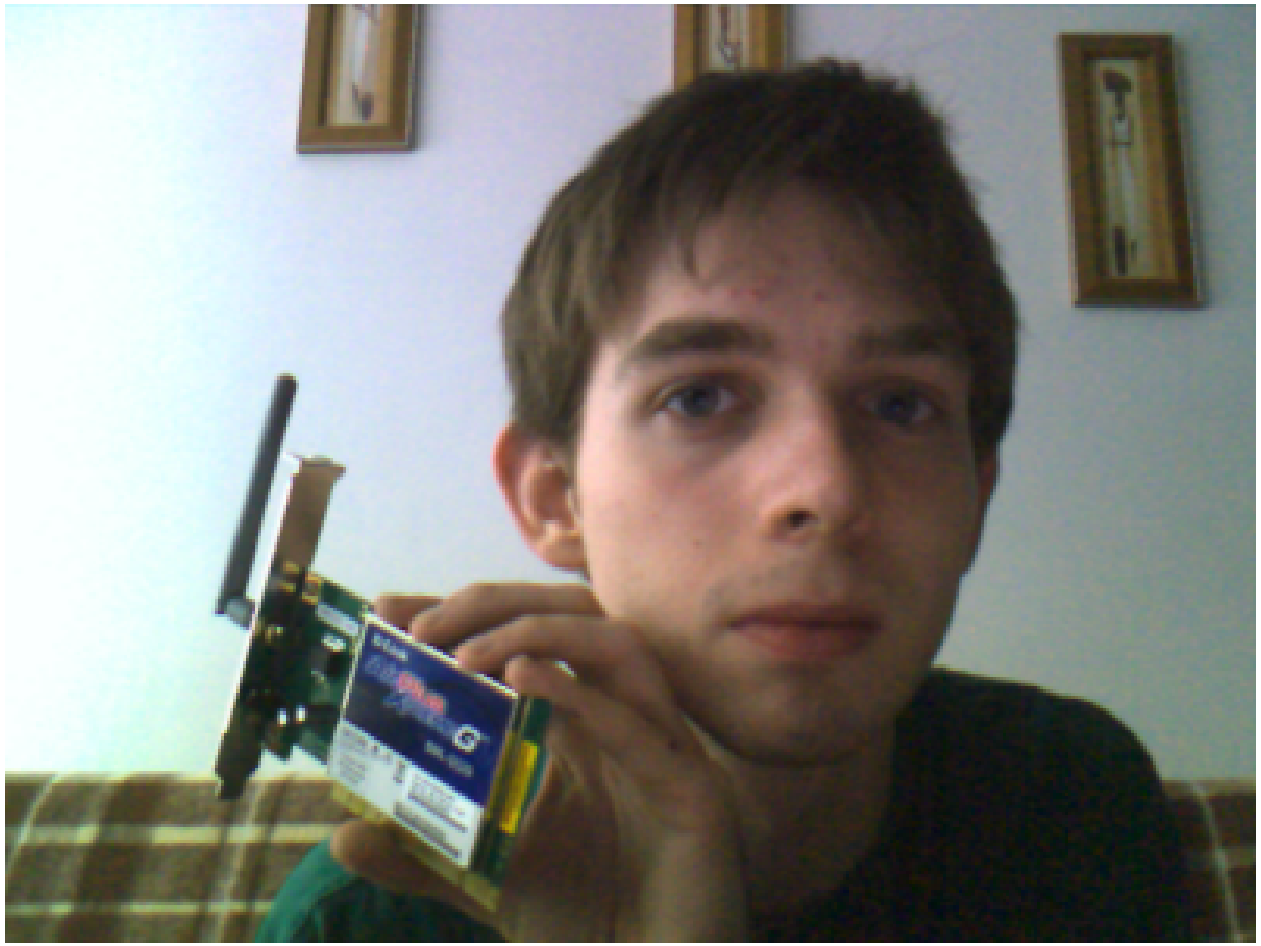
Essential hardware

- PC
- Wireless Network Interface Card **based on a good chipset!**

  `http://www.aircrack-ng.org/doku.php?id=compatibility_drivers`

  Atheros is highly recommended
- External antenna to enhance the range

NIC – D-LINK DWL-G520



NIC – PCMCIA NIC

Pringles antenna

Needed software

- GNU/Linux

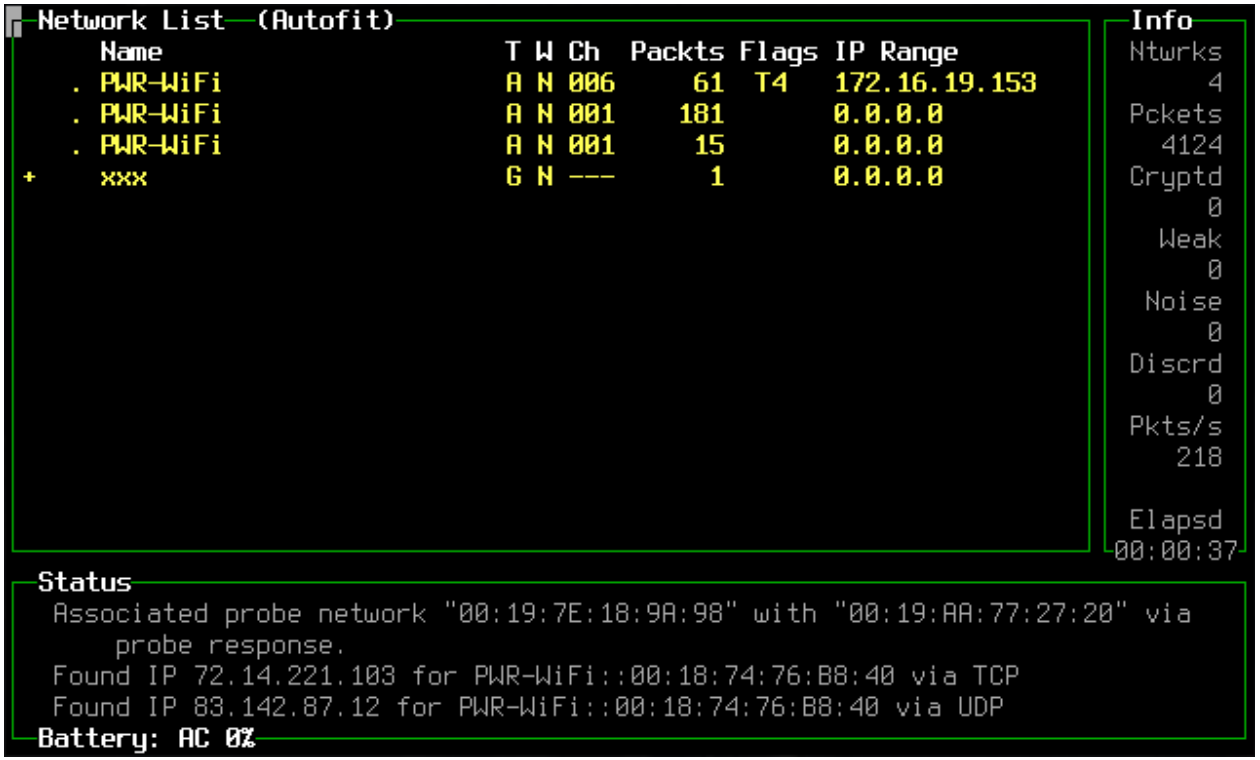
Needed software

- GNU/Linux
- `aircrack-ng`

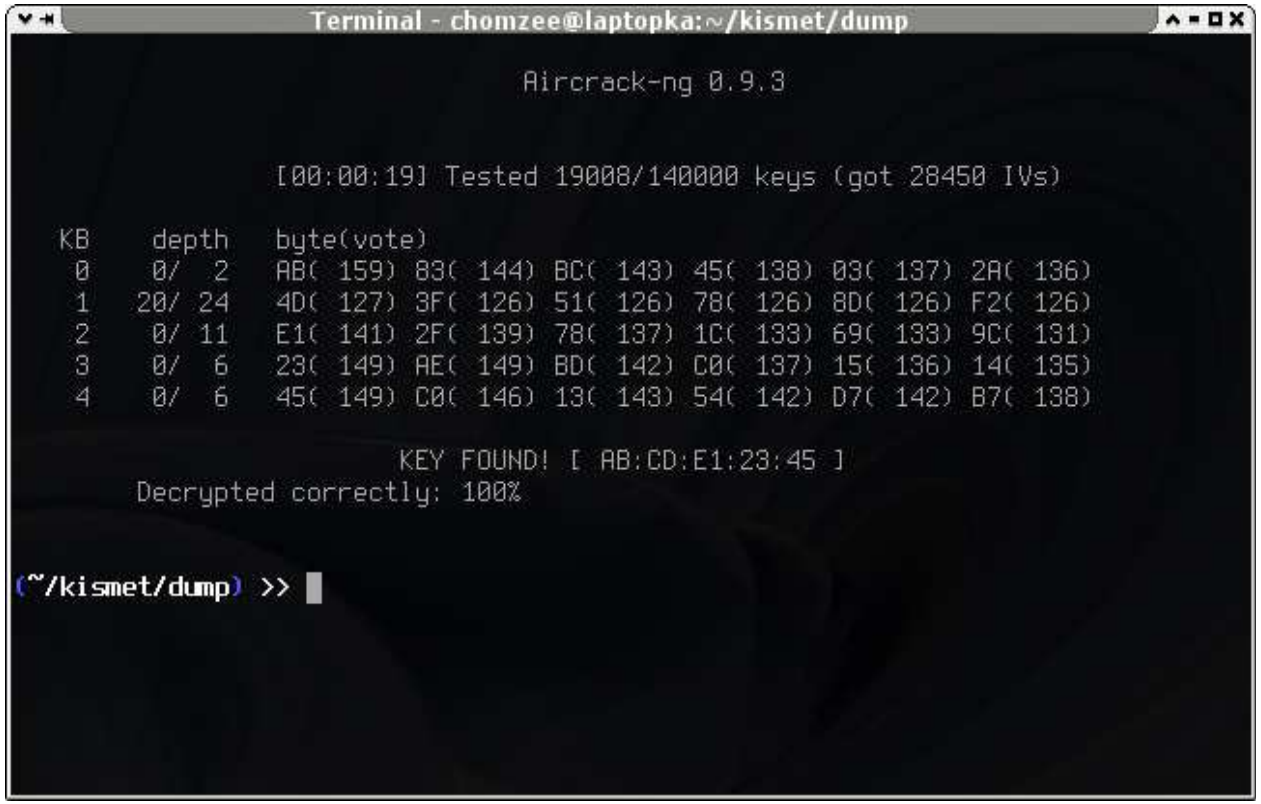
Needed software

- GNU/Linux
- `aircrack-ng`
- Kismet

Kismet


Network List (Autofit)
Name T W Ch Packts Flags IP Range
. PWR-WiFi A N 006 61 T4 172.16.19.153
. PWR-WiFi A N 001 181 0.0.0.0
. PWR-WiFi A N 001 15 0.0.0.0
+ xxx G N --- 1 0.0.0.0
Info
Ntwrks 4
Pckets 4124
Cryptd 0
Weak 0
Noise 0
Discrd 0
Pkts/s 218
Elapsd 00:00:37
Status
Associated probe network "00:19:7E:18:9A:98" with "00:19:AA:77:27:20" via probe response.
Found IP 72.14.221.103 for PWR-WiFi::00:18:74:76:B8:40 via TCP
Found IP 83.142.87.12 for PWR-WiFi::00:18:74:76:B8:40 via UDP
Battery: AC 0%

aircrack-ng


Terminal - chomzee@laptopka:~/kismet/dump
Aircrack-ng 0.9.3
[00:00:19] Tested 19008/140000 keys (got 28450 IVs)
KB depth byte(vote)
0 0/ 2 AB(159) 83(144) BC(143) 45(138) 03(137) 2A(136)
1 20/ 24 4D(127) 3F(126) 51(126) 78(126) 8D(126) F2(126)
2 0/ 11 E1(141) 2F(139) 78(137) 1C(133) 69(133) 9C(131)
3 0/ 6 23(149) AE(149) BD(142) C0(137) 15(136) 14(135)
4 0/ 6 45(149) C0(146) 13(143) 54(142) D7(142) B7(138)
KEY FOUND! [AB:CD:E1:23:45]
Decrypted correctly: 100%
(~/kismet/dump) >>

Summary

Summary

- Do not use WEP to protect your Wi-Fi network

Summary

- **Do not use WEP to protect your Wi-Fi network**
- Use WPA2 instead

Summary

- **Do not use WEP to protect your Wi-Fi network**
- Use WPA2 instead
- ... or more sophisticated remedies like OpenVPN

Questions?

Bibliography

- „Weaknesses in the Key Scheduling Algorithm of RC4" – Scott Fluhrer, Itsik Mantin, Adi Shamir

  http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf
- http://www.aircrack-ng.org/
- http://en.wikipedia.org/
- http://images.google.com/

Thank you for your attention.