Wireless Networks: Basics & Security Issues

Burak Ekici
ekcburak@hotmail.com

Department of Computer Engineering,
Yaşar University,
Turkey.

April 22, 2012

Agenda

The Notion: A Wireless Network (WLAN)

Definition: Wireless Network (WLAN)

A **Wireless Network** *is a local area network (LAN) that enables two or more entities to communicate without network cabling, instead, by using radio signals and propagations of them within already defined frequency ranges.*

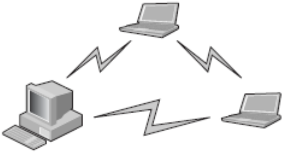


Figure: A Wireless Network with Three Devices

Image Source: Building a Simple Network (by Intel)

Wireless Networks in OSI Model

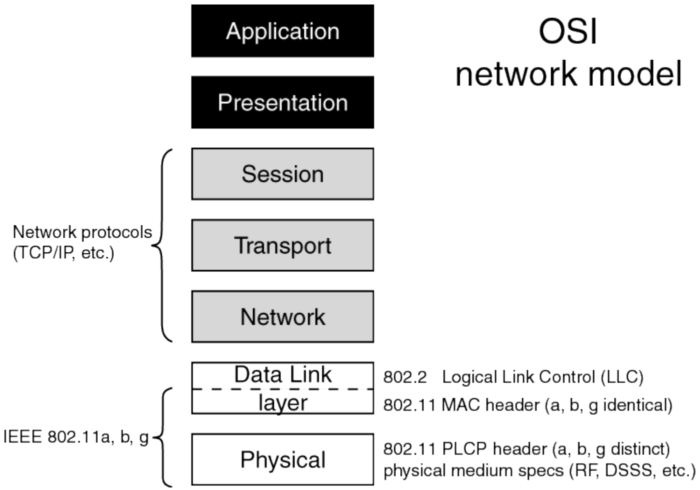


Figure: WLAN and OSI

Image Source: 802.11 WLAN Packets and Protocols, WildPackets

A Quick Reminder: Radio Signal Propagation

Definition: Radio Wave

A **Radio wave** *is a type of electromagnetic radiation with wavelengths in the electromagnetic spectrum longer than infrared which have frequencies ranging from 300 GHz to as low as 3 kHz, and corresponding wavelengths ranging from 1 millimeter to 100 kilometer.*

Definition: Radio Signal

A **radio signal** *is a radio wave that is used to transmit and receive information.*

A Quick Reminder: Radio Signal Propagation

Definition: Radio Wave

A **Radio wave** *is a type of electromagnetic radiation with wavelengths in the electromagnetic spectrum longer than infrared which have frequencies ranging from 300 GHz to as low as 3 kHz, and corresponding wavelengths ranging from 1 millimeter to 100 kilometer.*

Definition: Radio Signal

A **radio signal** *is a radio wave that is used to transmit and receive information.*

A Quick Reminder: Radio Signal Propagation

Definition: Modulation

Modulation *is the operation of adding information onto a radio signal.*

Modulation Types

There are two main modulation techniques:

1. **Analog Modulation**: *An analog carrier signal is modulated within the scope of the signal to be transmitted via either its amplitude or frequency or else no modulation is implemented at all.*
   - *Frequency Modulation (FM).*
   - *Amplitude Modulation (AM).*
2. **Digital Modulation**: *Discrete signals modulate a carrier analog signal by some shifting methodologies.*
   - *Frequency-shift keying (FSK).*
   - *Amplitude-shift keying (ASK).*

A Quick Reminder: Radio Signal Propagation

Definition: Modulation

Modulation *is the operation of adding information onto a radio signal.*

Modulation Types

There are two main modulation techniques:

1. **Analog Modulation**: *An analog carrier signal is modulated within the scope of the signal to be transmitted via either its amplitude or frequency or else no modulation is implemented at all.*
   - *Frequency Modulation (FM).*
   - *Amplitude Modulation (AM).*
2. **Digital Modulation**: *Discrete signals modulate a carrier analog signal by some shifting methodologies.*
   - *Frequency-shift keying (FSK).*
   - *Amplitude-shift keying (ASK).*

A Quick Reminder: Radio Signal Propagation

Definition: Modulation

Modulation *is the operation of adding information onto a radio signal.*

Modulation Types

There are two main modulation techniques:

1. **Analog Modulation**: *An analog carrier signal is modulated within the scope of the signal to be transmitted via either its amplitude or frequency or else no modulation is implemented at all.*
   - *Frequency Modulation (FM).*
   - *Amplitude Modulation (AM).*
2. **Digital Modulation**: *Discrete signals modulate a carrier analog signal by some shifting methodologies.*
   - *Frequency-shift keying (FSK).*
   - *Amplitude-shift keying (ASK).*

A Quick Reminder: Radio Signal Propagation

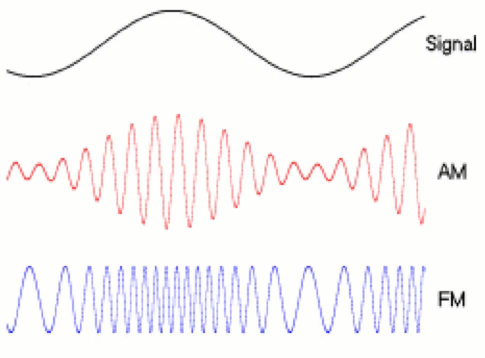


Figure: Analog Modulation

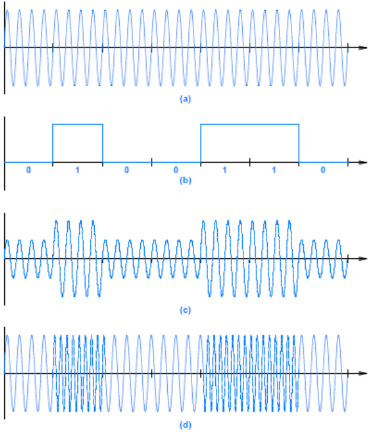


Figure: Digital Modulation

a: CAS; b: DS; c: ASK; d:FSK

A Quick Reminder: Radio Signal Propagation

Signal Propagation: Key Points

1. *The amount of information could be represented or transferred by an electromagnetic wave, is directly proportional to its frequency difference known as bandwidth.*
2. *The propagation characteristics of an electromagnetic wave is also determined by its frequency.*
3. *Therefore; there are three types of signal propagation techniques:*
   - *Propagation in Lowest Frequencies.*
   - *Propagation in Medium Frequencies.*
   - *Propagation in Highest Frequencies.*

A Quick Reminder: Radio Signal Propagation

Signal Propagation: Key Points

1. *The amount of information could be represented or transferred by an electromagnetic wave, is directly proportional to its frequency difference known as bandwidth.*
2. *The propagation characteristics of an electromagnetic wave is also determined by its frequency.*
3. *Therefore; there are three types of signal propagation techniques:*
   - *Propagation in Lowest Frequencies.*
   - *Propagation in Medium Frequencies.*
   - *Propagation in Highest Frequencies.*

A Quick Reminder: Radio Signal Propagation

Signal Propagation: Key Points

1. *The amount of information could be represented or transferred by an electromagnetic wave, is directly proportional to its frequency difference known as bandwidth.*
2. *The propagation characteristics of an electromagnetic wave is also determined by its frequency.*
3. *Therefore; there are three types of signal propagation techniques:*
    - *Propagation in Lowest Frequencies.*
    - *Propagation in Medium Frequencies.*
    - *Propagation in Highest Frequencies.*

Radio Signal Propagation: Typical Radio System

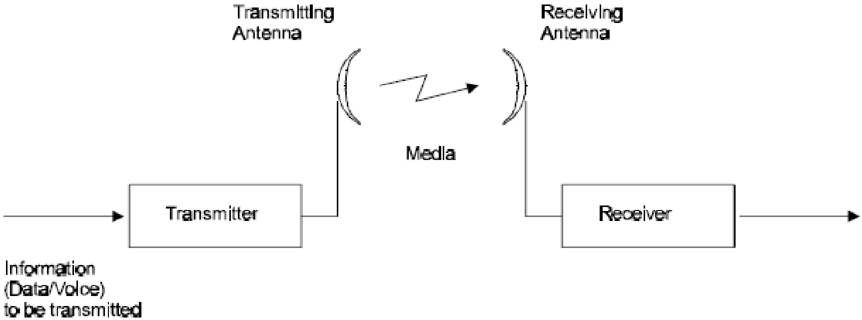


Figure: A Typical Radio System

Image Source: Radio Signal Propagation (by Breeze Wireless Communications Ltd.)

The Reason Why Wireless Networks are being Used?

Reasons for Wireless Network Usage

1. *Mobility*: *Information access beyond the desk.*
2. *Simplicity*: *Elimination of the needs for complex cabling and construction.*
3. *Flexibility*: *Being well suited for too many environments.*
4. *Accessibility*: *Being available at airports, hotels, coffee shops and convention centers are just a few places where hot-spot access.*

The Reason Why Wireless Networks are being Used?

Reasons for Wireless Network Usage

1. *Mobility: Information access beyond the desk.*
2. *Simplicity: Elimination of the needs for complex cabling and construction.*
3. *Flexibility: Being well suited for too many environments.*
4. *Accessibility: Being available at airports, hotels, coffee shops and convention centers are just a few places where hot-spot access.*

The Reason Why Wireless Networks are being Used?

Reasons for Wireless Network Usage

1. *Mobility: Information access beyond the desk.*
2. *Simplicity: Elimination of the needs for complex cabling and construction.*
3. *Flexibility: Being well suited for too many environments.*
4. *Accessibility: Being available at airports, hotels, coffee shops and convention centers are just a few places where hot-spot access.*

The Reason Why Wireless Networks are being Used?

Reasons for Wireless Network Usage

1. *Mobility: Information access beyond the desk.*
2. *Simplicity: Elimination of the needs for complex cabling and construction.*
3. *Flexibility: Being well suited for too many environments.*
4. *Accessibility: Being available at airports, hotels, coffee shops and convention centers are just a few places where hot-spot access.*

Components of Wireless Networks

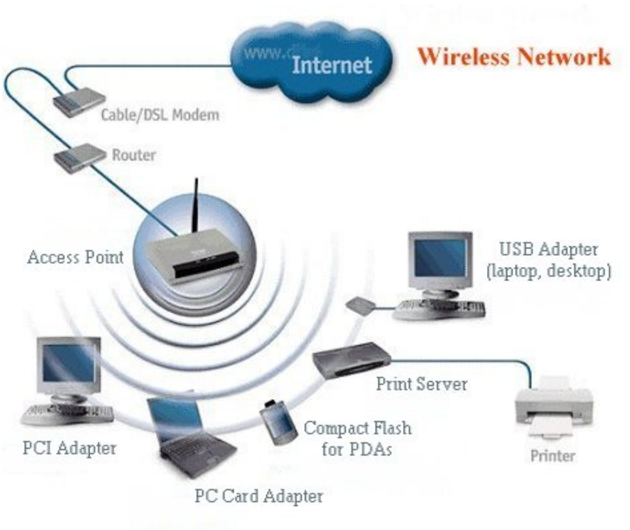


Figure: A Wireless Network

Modes of Wireless Networks Operations

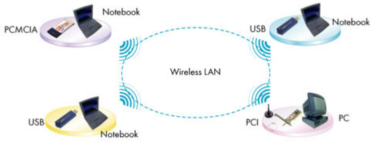


Figure: Ad-Hoc WLAN Mode

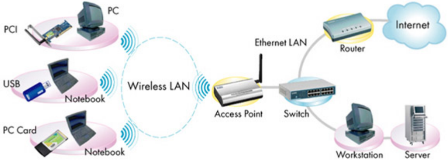


Figure: Infrastructure WLAN Mode

WLAN Modes

Ad-Hoc Mode:

- *No need for an access point.*
- *Communication in between the nodes is done directly.*
- *All nodes should have an SSID and a channel.*

Infrastructure Mode:

- *Access point is being used for local connections.*
- *All nodes should have an SSID and a channel.*
- *Authentication problem arises.*

Standards of Wireless Networks

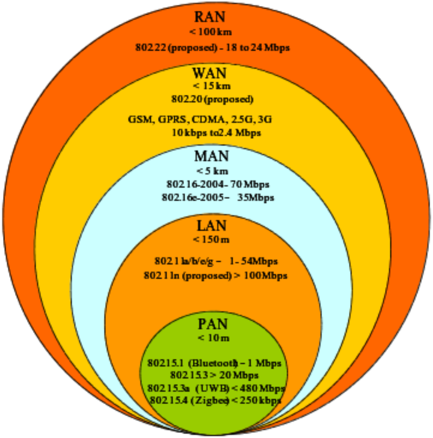


Figure: Wireless Standards

Image Source: Overview of IEEE Wireless Network Standards

Bluetooth: 802.15.1

Bluetooth

- *1994, Ericsson*
- *WPAN (wireless personal area network)*
- *Frequency: 2.4 GHz on ISM (International Scientific Medical) Band*
- *Data deployment speed: 24 Mbit/s*
- *Functionality Area: Inside the area of 10m dia. circle.*

WiFi (Wireless Fidelity): 802.11

802.11 Standards: WiFi Family

- *802.11a*
- *802.11b*
- *802.11g*
- *802.11n*

WiFi: 802.11a

Figure: WiFi (Wireless Fidelity) Logo

802.11a

- *1999*
- *WLAN (wireless local area network)*
- *Frequency: 5 GHz on ISM (International Scientific Medical) Band*
- *Data deployment speed: 23 - 54 Mbit/s*
- *Functionality Area: Inside the area of 13 - 100m dia. circle.*

WiFi: 802.11b

Figure: WiFi (Wireless Fidelity) Logo

802.11b

- *1999*
- *WLAN (wireless local area network)*
- *Frequency: 2.4 - 2.5 GHz on ISM (International Scientific Medical) Band*
- *Data deployment speed: 4 - 11 Mbit/s*
- *Functionality Area: Inside the area of 35 - 110m dia. circle.*

WiFi: 802.11g

Figure: WiFi (Wireless Fidelity) Logo

802.11g

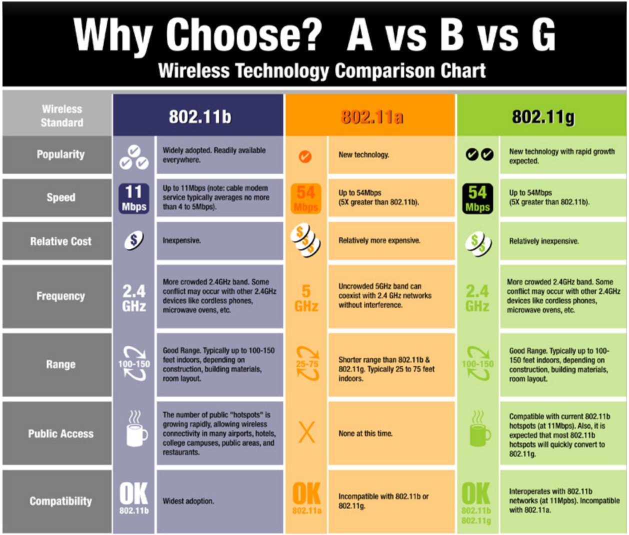
- *2003*
- *WLAN (wireless local area network)*
- *Frequency: 2.4 - 2.5 GHz on ISM (International Scientific Medical) Band*
- *Data deployment speed: 19 - 54 Mbit/s*
- *Functionality Area: Inside the area of 35 - 110m dia. circle.*

WiFi: 802.11n

Figure: WiFi (Wireless Fidelity) Logo

802.11n

- *2008*
- *WLAN (wireless local area network)*
- *Frequency: 2.4 or 5 GHz on ISM (International Scientific Medical) Band*
- *Data deployment speed: 74 - 248 Mbit/s*
- *Functionality Area: Inside the area of 70 - 200m dia. circle.*



Why Choose? A vs B vs G

Wireless Technology Comparison Chart

Wireless Standard	802.11b	802.11a	802.11g
Popularity	Widely adopted. Readily available everywhere.	New technology.	New technology with rapid growth expected.
Speed	11 Mbps — Up to 11Mbps (note: cable modem service typically averages no more than 4 to 5Mbps).	54 Mbps — Up to 54Mbps (5X greater than 802.11b).	54 Mbps — Up to 54Mbps (5X greater than 802.11b).
Relative Cost	Inexpensive.	Relatively more expensive.	Relatively inexpensive.
Frequency	2.4 GHz — More crowded 2.4GHz band. Some conflict may occur with other 2.4GHz devices like cordless phones, microwave ovens, etc.	5 GHz — Uncrowded 5GHz band can coexist with 2.4 GHz networks without interference.	2.4 GHz — More crowded 2.4GHz band. Some conflict may occur with other 2.4GHz devices like cordless phones, microwave ovens, etc.
Range	100-150 — Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.	25-75 — Shorter range than 802.11b & 802.11g. Typically 25 to 75 feet indoors.	100-150 — Good Range. Typically up to 100-150 feet indoors, depending on construction, building materials, room layout.
Public Access	The number of public "hotspots" is growing rapidly, allowing wireless connectivity in many airports, hotels, college campuses, public areas, and restaurants.	X — None at this time.	Compatible with current 802.11b hotspots (at 11Mbps). Also, it is expected that most 802.11b hotspots will quickly convert to 802.11g.
Compatibility	OK 802.11b — Widest adoption.	OK 802.11a — Incompatible with 802.11b or 802.11g.	OK 802.11b 802.11g — Interoperates with 802.11b networks (at 11Mpbs). Incompatible with 802.11a.

Figure: Comparison of Wireless Standards

Wireless Network Security Issues: Risks

WiFi Risks:

1. **Security issues**:
   - *ease of detection (War-driving and War-chalking)*
   - *ease of penetration into the network*
   - *ease of sniffing the network traffic*
2. **Physical issues**:
   - *noise in radio signals*
   - *physical obstacles in between AP and hosts*

Wireless Network Security Issues: Risks

WiFi Risks:

1. **Security issues**:
   - *ease of detection (War-driving and War-chalking)*
   - *ease of penetration into the network*
   - *ease of sniffing the network traffic*
2. **Physical issues**:
   - *noise in radio signals*
   - *physical obstacles in between AP and hosts*

Be Aware: War-driving

War Driving:

War driving *is the process of seeking wireless networks inside an area (city center) by driving around together with necessary equipments, such as:*

- *Laptop or a portable device with a wireless card*
- *Wireless network detection software (Kismet, Netstumbler)*
- *GPS receiver (optional)*
- *Mapping Software (optional)*

Be Aware: War-driving

War Driving:

War driving *is the process of seeking wireless networks inside an area (city center) by driving around together with necessary equipments, such as:*

- *Laptop or a portable device with a wireless card*
- *Wireless network detection software (Kismet, Netstumbler)*
- *GPS receiver (optional)*
- *Mapping Software (optional)*

Be Aware: War-driving

Figure: War-driving

Figure: War-driving in Milano

Be Aware: War-chalking

War Chalking:

War-chalking *is the process of drawing some specific symbols, on an already defined place, in order to demonstrate that a wireless LAN network is performing there; including:*

- *the SSID*
- *the encryption standard of the network (Open, WEP, WPA)*
- *contact information (connection password) and*
- *bandwidth*

Be Aware: War-chalking

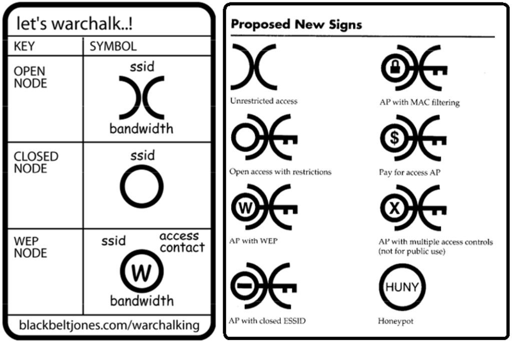


Figure: War-chalking Symbols

Figure: War-chalking Example: London

Wireless Network Security Issues: Main Problems

Problems:

1. **Physical security of the transferred data is not provided**. *Since the transmission environment is the air.*
2. *An obligation for using* **cryptographic protocols**.

Wireless Network Security Issues: Main Problems

Problems:

1. **Physical security of the transferred data is not provided**. *Since the transmission environment is the air.*
2. *An obligation for using* **cryptographic protocols**.

Wireless Network Security Issues: Cryptographic Approach

Security Protocols:

Due to being on-line working systems (wireless LAN communications) **stream ciphers** *are being used to encrypt and decrypt the data transferred (in between AP and hosts) and they are involved in some* **security protocols**, *such as:*

1. **WEP (Wired Equivalent Privacy)**
2. **WPA (Wi-Fi Protected Access)**

Wireless Network Security Issues: Cryptographic Approach

Security Protocols:

Due to being on-line working systems (wireless LAN communications) **stream ciphers** *are being used to encrypt and decrypt the data transferred (in between AP and hosts) and they are involved in some* **security protocols**, *such as:*

1. **WEP (Wired Equivalent Privacy)**
2. **WPA (Wi-Fi Protected Access)**

Wireless Network Security Issues: Cryptographic Approach

Security Protocols:

Due to being on-line working systems (wireless LAN communications) **stream ciphers** *are being used to encrypt and decrypt the data transferred (in between AP and hosts) and they are involved in some* **security protocols**, *such as:*

1. **WEP (Wired Equivalent Privacy)**
2. **WPA (Wi-Fi Protected Access)**

Cryptographic Approach: The WEP

Definition: What is WEP?

WEP *is a* **security protocol** *which is involved in* **wireless networks** *to:*

- *avoid unauthorized access and*
- *provide access control, data integrity and confidentiality against criminal minds in order to ensure that:*
  - *your access point is not used by unauthorized users.*
  - *your data is not modified.*
  - *contents of your traffic are kept secure.*

Versions of WEP

1. **Key Length**: **40 bits** *(weak key)*
2. **Key Length**: **128 bits** *(strong key)*
3. **Key Length**: **256 bits** *(strong key)*

Cryptographic Approach: The WEP

Definition: What is WEP?

WEP *is a* **security protocol** *which is involved in* **wireless networks** *to:*

- *avoid unauthorized access and*
- *provide access control, data integrity and confidentiality against criminal minds in order to ensure that:*
  - *your access point is not used by unauthorized users.*
  - *your data is not modified.*
  - *contents of your traffic are kept secure.*

Versions of WEP

1. **Key Length**: **40 bits** *(weak key)*
2. **Key Length**: **128 bits** *(strong key)*
3. **Key Length**: **256 bits** *(strong key)*

Cryptographic Approach: The WEP

Definition: What is WEP?

WEP *is a* **security protocol** *which is involved in* **wireless networks** *to:*

- *avoid unauthorized access and*
- *provide access control, data integrity and confidentiality against criminal minds in order to ensure that:*
  - *your access point is not used by unauthorized users.*
  - *your data is not modified.*
  - *contents of your traffic are kept secure.*

Versions of WEP

1. **Key Length**: **40 bits** *(weak key)*
2. **Key Length**: **128 bits** *(strong key)*
3. **Key Length**: **256 bits** *(strong key)*

Cryptographic Approach: The WEP

Definition: What is WEP?

WEP *is a* **security protocol** *which is involved in* **wireless networks** *to:*

- *avoid unauthorized access and*
- *provide access control, data integrity and confidentiality against criminal minds in order to ensure that:*
  - *your access point is not used by unauthorized users.*
  - *your data is not modified.*
  - *contents of your traffic are kept secure.*

Versions of WEP

1. **Key Length**: **40 bits** *(weak key)*
2. **Key Length**: **128 bits** *(strong key)*
3. **Key Length**: **256 bits** *(strong key)*

Cryptographic Approach: The WEP

Definition: What is WEP?

WEP *is a* **security protocol** *which is involved in* **wireless networks** *to:*

- *avoid unauthorized access* *and*
- *provide access control*, *data integrity* *and* *confidentiality* *against* *criminal minds* *in order to ensure that:*
  - *your access point is not used by unauthorized users.*
  - *your data is not modified.*
  - *contents of your traffic are kept secure.*

Versions of WEP

1. **Key Length**: **40 bits** *(weak key)*
2. **Key Length**: **128 bits** *(strong key)*
3. **Key Length**: **256 bits** *(strong key)*

The WEP Steps: Shared Key Authentication

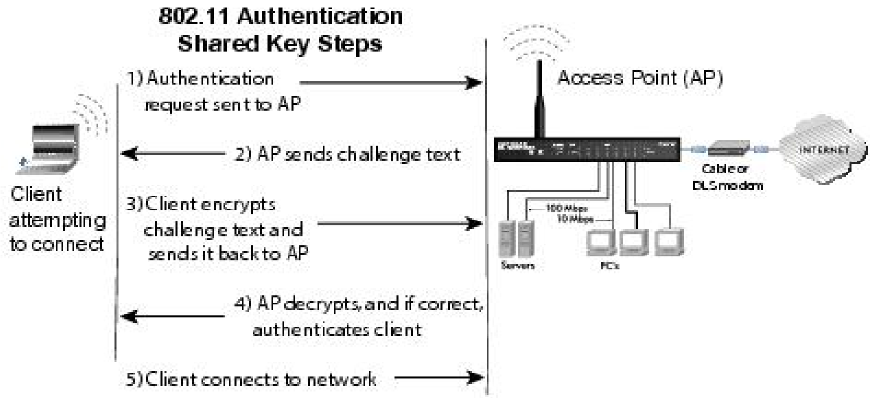


Figure: WEP Authentication Scheme

Image Source: Wireless Networking Basics by NETGEAR Inc.

The WEP Steps: Encryption

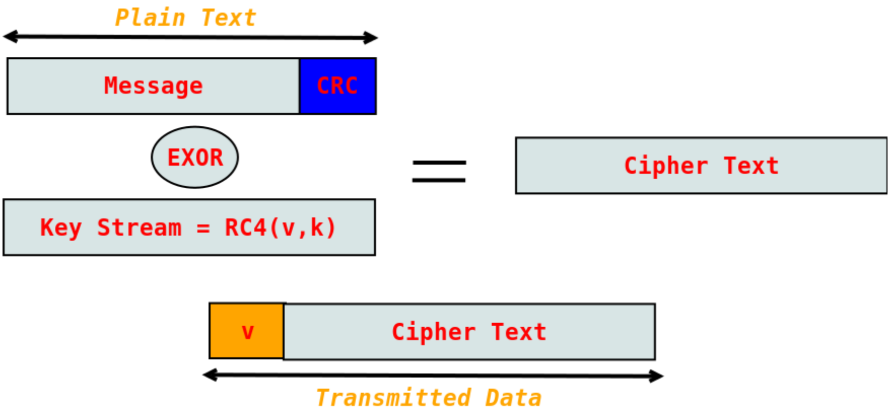


Figure: WEP Encryption Scheme

Image: FSU, Network Security PROTOCOLS Group by İlkay Çubukçu

The WEP Steps: Decryption

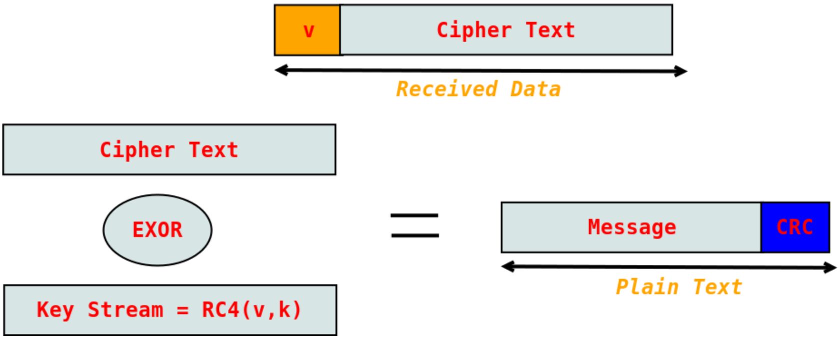


Figure: WEP Decryption Scheme

Image: FSU, Network Security PROTOCOLS Group by İlkay Çubukçu

The WEP: Vulnerabilities

Vulnerabilities: WEP

1. **Vulnerable Authentication Scheme**: *An attacker who is able to monitor the network traffic exactly during an arbitrary authentication to the WLAN, could easily calculate key stream used to encrypt the response and authenticate to the wireless network.*

Cipher Text $\oplus$ Plain Text $=$ Key Stream

2. **A Small Number of Initialization Vectors**:
   - *24 bit of IVs: 16,777,216 possible combination.*
   - *It is possible to capture a modest number of messages encrypted with the same key stream (IV reuse).*
     - $C_1 = P_1 \oplus RC4(k, IV_1)$ and $C_2 = P_2 \oplus RC4(k, IV_2)$ where $IV_1 = IV_2$
     - $C_1 \oplus C_2 = P_1 \oplus P_2$
   - *The more CTs captured with same IV; the less uncertainty of the key.*

Cipher Text $\oplus$ Cipher Text $=$ Plain Text $\oplus$ Plain Text

Passive Attacks via Network Sniffing!!!

The WEP: Vulnerabilities

Vulnerabilities: WEP

1. **Vulnerable Authentication Scheme**: *An attacker who is able to monitor the network traffic exactly during an arbitrary authentication to the WLAN, could easily calculate key stream used to encrypt the response and authenticate to the wireless network.*

Cipher Text ⊕ Plain Text = Key Stream

2. **A Small Number of Initialization Vectors**:
   - *24 bit of IVs: 16,777,216 possible combination.*
   - *It is possible to capture a modest number of messages encrypted with the same key stream (IV reuse).*
     - $C_1 = P_1 \oplus RC4(k, IV_1)$ and $C_2 = P_2 \oplus RC4(k, IV_2)$ where $IV_1 = IV_2$
     - $C_1 \oplus C_2 = P_1 \oplus P_2$
   - *The more CTs captured with same IV; the less uncertainty of the key.*

Cipher Text ⊕ Cipher Text = Plain Text ⊕ Plain Text

Passive Attacks via Network Sniffing!!!

Vulnerabilities: WEP

1. **Vulnerable Authentication Scheme**: *An attacker who is able to monitor the network traffic exactly during an arbitrary authentication to the WLAN, could easily calculate key stream used to encrypt the response and authenticate to the wireless network.*

Cipher Text $\oplus$ Plain Text = Key Stream

2. **A Small Number of Initialization Vectors**:
   - *24 bit of IVs: 16,777,216 possible combination.*
   - *It is possible to capture a modest number of messages encrypted with the same key stream (IV reuse).*
     - $C_1 = P_1 \oplus RC4(k, IV_1)$ *and* $C_2 = P_2 \oplus RC4(k, IV_2)$ *where* $IV_1 = IV_2$
     - $C_1 \oplus C_2 = P_1 \oplus P_2$
   - *The more CTs captured with same IV; the less uncertainty of the key.*

Cipher Text $\oplus$ Cipher Text = Plain Text $\oplus$ Plain Text

Passive Attacks via Network Sniffing!!!

The WEP: Vulnerabilities

Vulnerabilities: WEP

1. **Vulnerable Authentication Scheme**: *An attacker who is able to monitor the network traffic exactly during an arbitrary authentication to the WLAN, could easily calculate key stream used to encrypt the response and authenticate to the wireless network.*

Cipher Text ⊕ Plain Text = Key Stream

2. **A Small Number of Initialization Vectors**:
   - *24 bit of IVs: 16,777,216 possible combination.*
   - *It is possible to capture a modest number of messages encrypted with the same key stream (IV reuse).*
     - $C_1 = P_1 \oplus RC4(k, IV_1)$ and $C_2 = P_2 \oplus RC4(k, IV_2)$ where $IV_1 = IV_2$
     - $C_1 \oplus C_2 = P_1 \oplus P_2$
   - *The more CTs captured with same IV; the less uncertainty of the key.*

Cipher Text ⊕ Cipher Text = Plain Text ⊕ Plain Text

Passive Attacks via Network Sniffing!!!

The WEP: Vulnerabilities

Vulnerabilities: WEP

1. **Vulnerable Authentication Scheme**: *An attacker who is able to monitor the network traffic exactly during an arbitrary authentication to the WLAN, could easily calculate key stream used to encrypt the response and authenticate to the wireless network.*

   Cipher Text $\oplus$ Plain Text $=$ Key Stream

2. **A Small Number of Initialization Vectors**:
   - *24 bit of IVs: 16,777,216 possible combination.*
   - *It is possible to capture a modest number of messages encrypted with the same key stream (IV reuse).*
     - $C_1 = P_1 \oplus RC4(k, IV_1)$ *and* $C_2 = P_2 \oplus RC4(k, IV_2)$ *where* $IV_1 = IV_2$
     - $C_1 \oplus C_2 = P_1 \oplus P_2$
   - *The more CTs captured with same IV; the less uncertainty of the key.*

   Cipher Text $\oplus$ Cipher Text $=$ Plain Text $\oplus$ Plain Text

Passive Attacks via Network Sniffing!!!

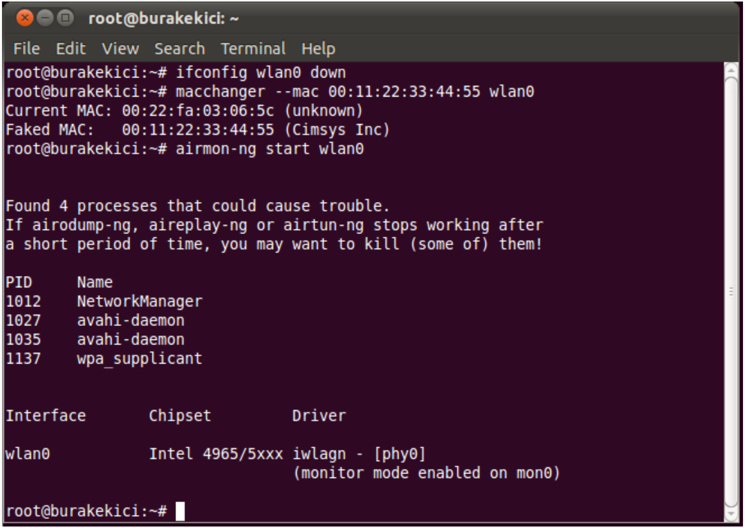


Figure: Phase 1: MAC Changing + Airmon

A Case Study: Airmon + Airodump + Aircrack

```
root@burakekici: ~
File  Edit  View  Search  Terminal  Help

CH  9 ][ Elapsed: 2 mins ][ 2012-04-18 16:58

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

00:1C:A8:90:7E:3D   -1        0        5    0 108  -1   WPA              <length:
00:1C:A8:95:D5:31  -76      183        0    0  11  54   WPA2 CCMP   PSK  Ekici
00:1E:40:65:1E:35  -76      235        0    0  11  54   WPA  TKIP   PSK  as
00:25:12:BD:06:FD  -81      162        0    0   1  54   WPA2 TKIP   PSK  argon
00:1C:A8:96:4B:2A  -79       53        0    0  11  54e. WPA2 CCMP   PSK  zeynep    N
4C:ED:DE:B0:2E:69  -80      124        0    0   1  54e  WPA  TKIP   PSK  Huawei_HG N
00:1A:2A:84:FC:05  -82      108        6    0  11  54   WPA  TKIP   PSK  tuncayoztu
00:1E:40:37:FB:16  -82      126        0    0  11  54   WPA2 CCMP   PSK  Pikatel
00:1A:2A:B2:A3:CE  -81       91        0    0  11  54   WPA  TKIP   PSK  AIRTIES
00:13:A3:79:22:9D  -82       68        0    0  11  54   WPA  TKIP   PSK  speedstrea
00:12:BF:D9:61:22  -84       92        0    0  11  54 . WPA  TKIP   PSK  AIRTIES_RT
00:1F:1F:D0:B3:31  -84      206        0    0   6  54e  WPA2 CCMP   PSK  edimax_0
C8:D5:FE:24:97:DB  -85      103        0    0   1  54e  WPA  TKIP   PSK  Huawei_HG5
00:12:BF:FE:42:67  -85       88       26    0   6  54 . WPA  TKIP   PSK  yener elek
00:23:F8:B1:4D:93  -87       27        5    0   6  54 . WPA2 CCMP   PSK  NnNn
00:1C:A8:68:BB:F8  -87       38        0    0  11  54   WPA  TKIP   PSK  AIRTIES_RT
00:1C:A8:FE:AC:3A  -87       29        0    0   6  54   WEP  WEP         cardak
00:23:F8:B9:7A:F2  -87       37       22    0   6  54 . WPA2 CCMP   PSK  yasemin
00:1C:A8:F6:80:0F  -87        1        1    0   6  54e  WPA2 CCMP   PSK  Sn67aau786
00:1C:A8:15:2A:58  -88       25        3    0  11  54   WPA  TKIP   PSK  yucel
00:1E:40:5F:9E:92  -88        2        0    0  11  54   WPA2 TKIP   PSK  esmeli
00:1D:19:10:8A:FC  -88       25        0    0  11  54   OPN              <length: 1
18:28:61:1C:35:61  -107      80      156    0   6  54e  WPA2 CCMP   PSK  SUPERONLIN
00:1C:A8:19:9F:D4  -84       33        0    0  11  54   WPA  TKIP   PSK  Fat35
18:28:61:04:4D:80   -1        0        1    0 133  -1   WPA              <length:  N
14:DA:E9:7F:48:04  -87       26        0    0   1  54e  WEP  WEP         EOS COMPUTN
00:02:CF:9F:93:D2  -88        2        0    0   6  54   WPA  TKIP   PSK  ZyXEL
14:DA:E9:7F:48:05  -87       27        0    0   1  54e  WEP  WEP         EOS COMPUT
00:1E:40:D9:17:8F  -85       42        0    0  11  54   WPA  TKIP   PSK  ozge
```

Figure: Phase 2: Airodump (for all wireless networks)

A Case Study: Airmon + Airodump + Aircrack

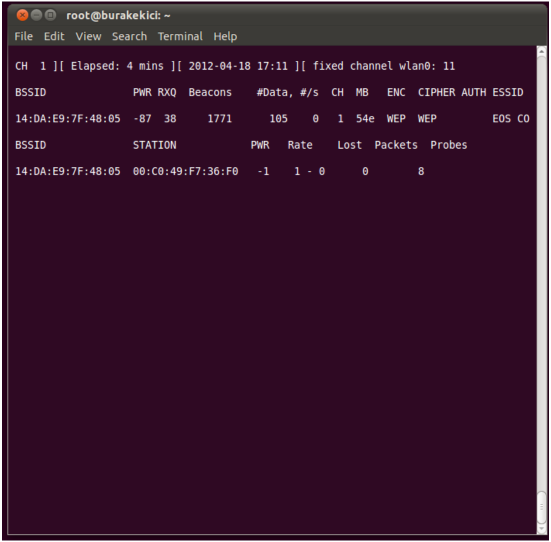


Figure: Phase 3: Airodump (for a specific wireless network)

A Case Study: Airmon + Airodump + Aircrack

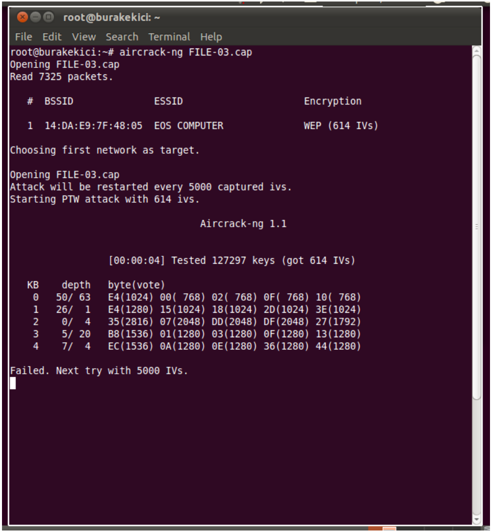


Figure: Phase 4: Aircrack

Cryptographic Approach: The WPA

Definition: What is WPA?

WPA *is another wireless* **security protocol** *which generally aims to close the vulnerabilities of WEP with 48-bit initialization vector and a 128-bit encryption keys.*

Versions of WPA

1. *WPA*
2. *WPA2*

The WPA: Authentication

WPA Authentication Schemes: Both in WPA and WPA2

1. **WPA-PSK (Pre-Shared Key) Authentication**:
   - *performs the same authentication steps with WEP authentication. All clients use the same initial master key but different per-packet keys.*
2. **WPA-EAP (Extensible Authentication Protocol)**:
   - *usage of certificates*
   - *RADIUS server is used for authentication and key distribution*

The WPA: Authentication

WPA Authentication Schemes: Both in WPA and WPA2

1. **WPA-PSK (Pre-Shared Key) Authentication**:
   - *performs the same authentication steps with WEP authentication. All clients use the same initial master key but different per-packet keys.*
2. **WPA-EAP (Extensible Authentication Protocol)**:
   - *usage of certificates*
   - *RADIUS server is used for authentication and key distribution*

The WPA: Authentication

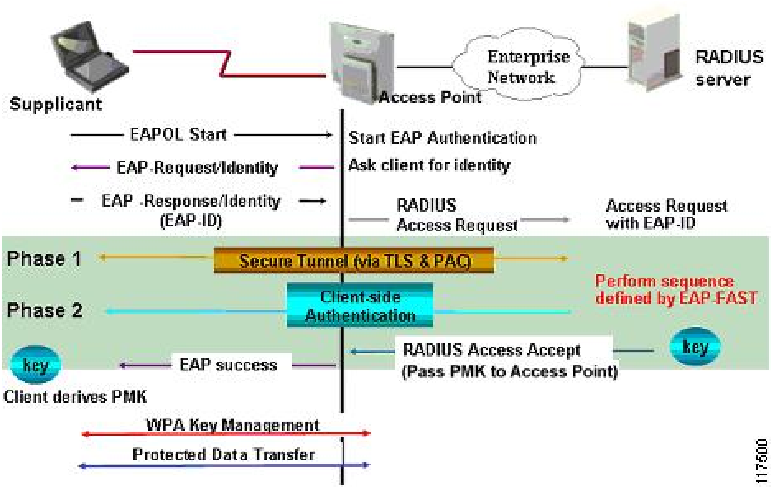


Figure: WPA-EAP Authentication Scheme

The WPA: Encryption & Decryption

WPA Encryption & Decryption Schemes

WPA: *TKIP (temporal key integrity protocol): RC4 + 4 algorithms:*

1. *Message Integrity Code (MIC)*
   - *tagging function (64-bit secret aut. key, msg): message integrity code*
2. *IV sequencing discipline*
   - *packet sequencing numbers (represented by IVs) are performing the synchronization between sender and receiver*
3. *Re-keying Mechanism*
   - *Temporal keys*
   - *Key encryption keys*
   - *Master Keys*
4. *Per-Packet Key Mixing Function*
   - *an intermediate key is created by combining the use of S-boxes and the client's MAC address*
   - *the packet sequence number is encrypted with a small cipher using the intermediate key*

Per Packet Key Mixing Function

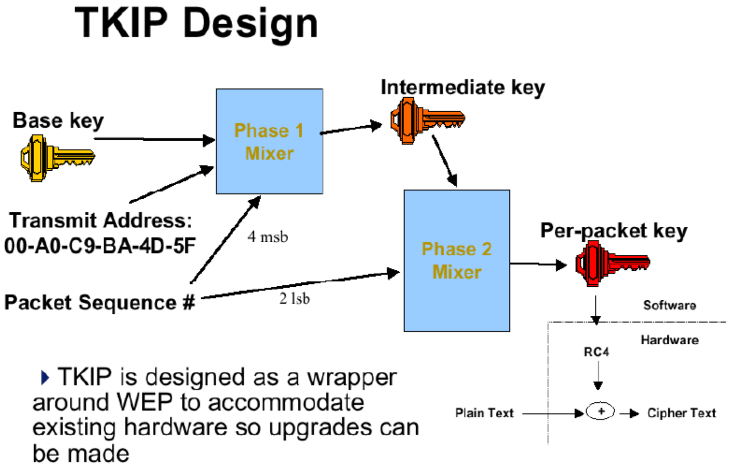


Figure: TKIP: Per Packet Key Mixing

Vulnerabilities: WPA

1. **Vulnerable Authentication Scheme**: *An attacker who is able to monitor the network traffic exactly during an arbitrary authentication to the WLAN, could easily calculate key stream used to encrypt the response and authenticate to the wireless network.*

The Handshake!

Known Issues:

- *Plain Text (Challenge Text)*
- *Cipher Text*
- *Therefore: Per-Packet Key*

Unknown Issue:

- *Base Key*

Dictionary Based Attacks!

The WPA: Vulnerabilities

Vulnerabilities: WPA

1. **Vulnerable Authentication Scheme**: *An attacker who is able to monitor the network traffic exactly during an arbitrary authentication to the WLAN, could easily calculate key stream used to encrypt the response and authenticate to the wireless network.*

The Handshake!

Known Issues:

- *Plain Text (Challenge Text)*
- *Cipher Text*
- *Therefore: Per-Packet Key*

Unknown Issue:

- *Base Key*

Dictionary Based Attacks!

The WPA: Vulnerabilities

Vulnerabilities: WPA

1. **Vulnerable Authentication Scheme**: *An attacker who is able to monitor the network traffic exactly during an arbitrary authentication to the WLAN, could easily calculate key stream used to encrypt the response and authenticate to the wireless network.*

   The Handshake!

   Known Issues:

   - *Plain Text (Challenge Text)*
   - *Cipher Text*
   - *Therefore: Per-Packet Key*

   Unknown Issue:

   - *Base Key*

   Dictionary Based Attacks!

The WPA: Vulnerabilities

Vulnerabilities: WPA

1. **Vulnerable Authentication Scheme**: *An attacker who is able to monitor the network traffic exactly during an arbitrary authentication to the WLAN, could easily calculate key stream used to encrypt the response and authenticate to the wireless network.*

The Handshake!

Known Issues:

- *Plain Text (Challenge Text)*
- *Cipher Text*
- *Therefore: Per-Packet Key*

Unknown Issue:

- *Base Key*

Dictionary Based Attacks!

The WPA: Vulnerabilities

Vulnerabilities: WPA

1. **Vulnerable Authentication Scheme**: *An attacker who is able to monitor the network traffic exactly during an arbitrary authentication to the WLAN, could easily calculate key stream used to encrypt the response and authenticate to the wireless network.*

The Handshake!

Known Issues:

- *Plain Text (Challenge Text)*
- *Cipher Text*
- *Therefore: Per-Packet Key*

Unknown Issue:

- *Base Key*

Dictionary Based Attacks!

A Case Study: Airmon + Airodump

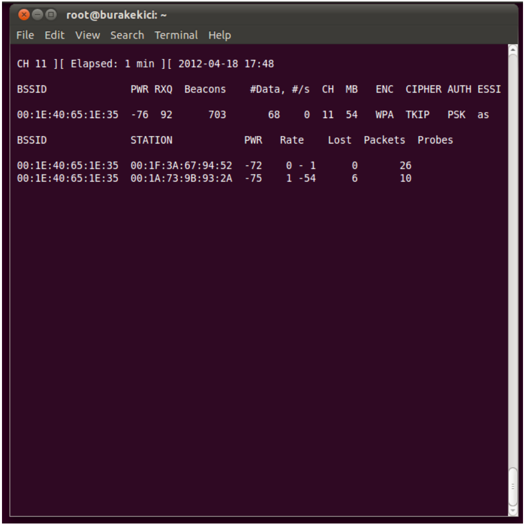


Figure: Phase 2: Airodump (for a specific wireless network without handshake)

A Case Study: Airmon + Airodump

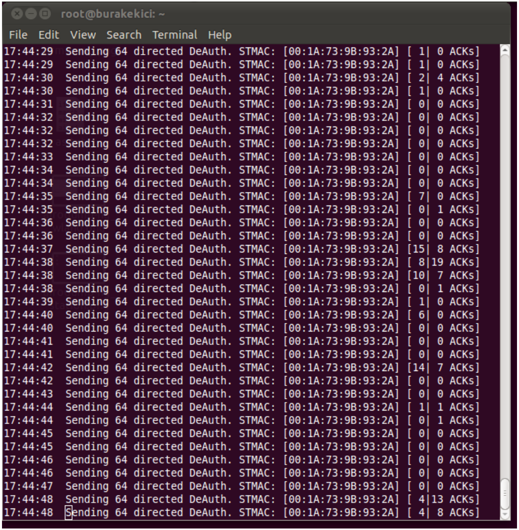


Figure: Phase 3: Aireplay (to implement deauth attack)

A Case Study: Airmon + Airodump

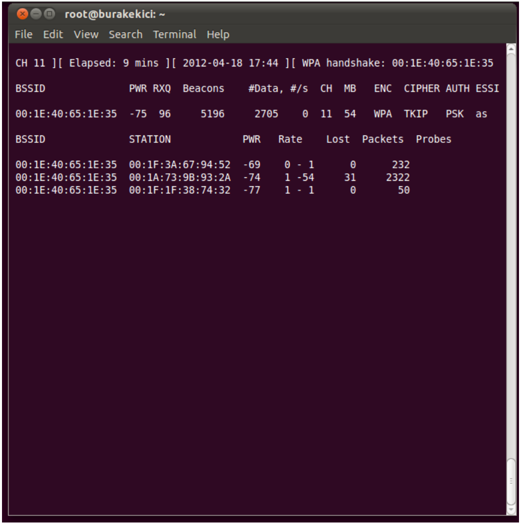


Figure: Phase 4: Airodump (for a specific wireless network with handshake)

A Case Study: Airmon + Airodump

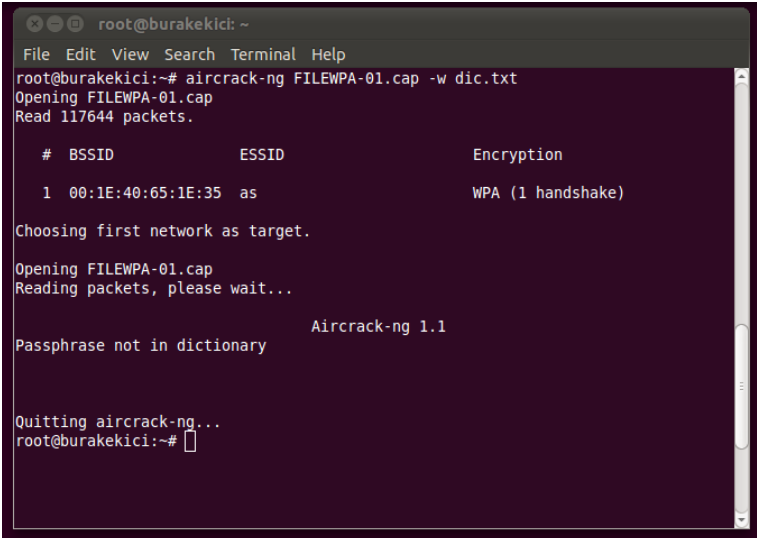


Figure: Phase 5: Aircrack Dictionary Attack

The WPA: Encryption & Decryption

WPA Encryption & Decryption Schemes

WPA2: *Instead of TKIP; CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), a new AES-based encryption/decryption mode with strong security is used.*

- *The most secure one for the current state of art.*
- *To be able to use it; your access point hardware should have the special support.*

General Precautions Should be Taken

General Precautions in Wireless Networking

- *SSID hiding (although it could be seen)*
- *MAC based access control (although MAC duplication could be done)*
- *Usage of Security Protocols (WPA2/WPA/WEP)*
- *Usage of more complex systems like AIRDEFENSE, if your transferred data are critical*

General Precautions Should be Taken

General Precautions in Wireless Networking

- *SSID hiding (although it could be seen)*
- *MAC based access control (although MAC duplication could be done)*
- *Usage of Security Protocols (WPA2/WPA/WEP)*
- *Usage of more complex systems like AIRDEFENSE, if your transferred data are critical*

General Precautions Should be Taken

General Precautions in Wireless Networking

- *SSID hiding (although it could be seen)*
- *MAC based access control (although MAC duplication could be done)*
- *Usage of Security Protocols (WPA2/WPA/WEP)*
- *Usage of more complex systems like AIRDEFENSE, if your transferred data are critical*

General Precautions Should be Taken

General Precautions in Wireless Networking

- *SSID hiding (although it could be seen)*
- *MAC based access control (although MAC duplication could be done)*
- *Usage of Security Protocols (WPA2/WPA/WEP)*
- *Usage of more complex systems like AIRDEFENSE, if your transferred data are critical*

Summary

Summarization:

1. *The notion: WLANs*
2. *Radio Signal Propagation*
3. *Components of WLANs*
4. *Modes of WLANs*
5. *WLAN security issues*
    - *Risks*
    - *Awareness: Wardriving and Warchalking*
    - *Cryptographic Approaches: WEP & WPA*
6. *General Precautions Should be Taken*

Çok Teşekkürler!
Efcharistó Polý!
Muito Obrigado!
Danke Schön!
Bedankt!
Labai Ačiu!
Thanks a Lot!

Burak Ekici
ekcburak@hotmail.com

Feedback

Bugs, Comments, Suggestions and Questions

Please let me know, if you have;

- seen any **Bugs** in the presentation.

Please share, if you have;

- any **Comments** and **Suggestions**.

QUESTIONS?

Feedback

Bugs, Comments, Suggestions and Questions

Please let me know, if you have;

- seen any **Bugs** in the presentation.

Please share, if you have;

- any **Comments** and **Suggestions**.

QUESTIONS?

Bibliography

[Çubukçu2002]
İlkay Çubukçu et al - FSU, Network Security PROTOCOLS group meeting.
Security of the WEP algorithm (Wired Equivalent Privacy).

[Kaya]
Dr. Lami Kaya.
Wireless Network Devices.

[Breeze]
Breeze Wireless Communications Ltd.
Radio Signal Propagation.

[Machta2003]
Demian Machta
Securing WLAN: From WEP to WPA.