

# Wireless Security – Principles & Tools

Network Startup Resource Center  
[www.nsrc.org](http://www.nsrc.org)



These materials are licensed under the Creative Commons Attribution-NonCommercial 4.0 International license  
(<http://creativecommons.org/licenses/by-nc/4.0/>)

# This talk

Security is a very complex and controversial theme.

We will therefore make a few opening

**1. remarks about network and information security in general,**

but then we will focus specifically on

**2. wireless security aspects**  
and

**3. tools for security auditing.**

# General Security: CIA

- 1. "Preservation of **confidentiality, integrity and availability** of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009)[1]
- 2. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide **confidentiality, integrity, and availability.**" (CNSS, 2010)[2]
- 3. "Ensures that only authorized users (confidentiality) have access to **accurate and complete information (integrity) when required (availability)**." (ISACA, 2008)[3]

[1] ISO/IEC 27000:2009 (E) (ISO). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC.

[2] Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009, 26 April 2010.

[3] ISACA. (2008). Glossary of terms, 2008.

All cited via: [https://en.wikipedia.org/wiki/Information\\_security#cite\\_note-4](https://en.wikipedia.org/wiki/Information_security#cite_note-4)

# CIA

- **Confidentiality**

- that information can stay private / limited to those it is for
  - Access
    - that you can get to it

- **Integrity**

- that information can be trusted to stay unchanged
  - Authenticity
    - that it is really what it says it is and that it comes from where it says its from

- **Availability**

- that information is available

# No security without conflicts

Some of these aspects can be in conflict with one another:

- Some people see a security problem in the fact that others can see and read their traffic (Confidentiality)
- Others see a security problem in the fact that they can NOT see and read people's traffic (Ensure Availability)

# More security facts

- No security can be 100%. It is always a trade off process, and **risk management** process.
- Security is connected to **usability** - if a system has near-perfect security but is impossible to use, users will just find other ways.
  - A classic example: if people can not remember or store complicated passwords, they will write them on a post-it note and put it on their screens.

# More security facts

- Most security problems can not be addressed on network level, but by services and servers.
- According to a 2014 study (source), most attacks come from the inside of networks and organizations.[1]
- Google therefore suggests to no longer make a difference between inner and outer network.[2]

[1] “IBM 2015 Cyber Security Intelligence Index” and the “IBM X-Force Threat Intelligence Quarterly – 2Q 2015.” cited by:  
<https://securityintelligence.com/the-threat-is-coming-from-inside-the-network/>

[2] Google BeyondCorp - [static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/43231.pdf](https://static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/43231.pdf)

# Some top security issues on campus networks

- Phishing
- Virus/Malware
  - often leading to spam or broadcast storm activity
- Uncontrolled improper use of networks (file sharing, videos, torrents ?)
- Operating systems spying
- BYOD - leading to completely uncontrolled quality of clients on your network
- Non-availability of (wireless) networks
- Physical security – theft and vandalism
- State sponsored intrusion / espionage / surveillance
  - as revealed by Snowden and others

**Which ones are your top problems?**



# Physical security

- As for all other technical equipment, don't forget to think about physical security – for example
  - Cables - Hidden and fastened
  - Switches, Routers - in locked cabinets
  - Power -locked in cabinets
  - Water protection - equipment at least 30cm above ground
  - Outdoor equipment on secured masts

# Physical security



# Now let us talk about **wireless**

- The main difference between wired and wireless networks is:  
**wireless access is not strictly bound to a physical location.**
- We can keep people away from a certain network drop, but it is almost impossible to keep them away from our radio signal.
- This is the reason why we typically do not implement authentication on wired networks (although 802.1x was made for wired networks!).

# What can we do for **wireless security**?

A healthy way of looking at security on the network level:

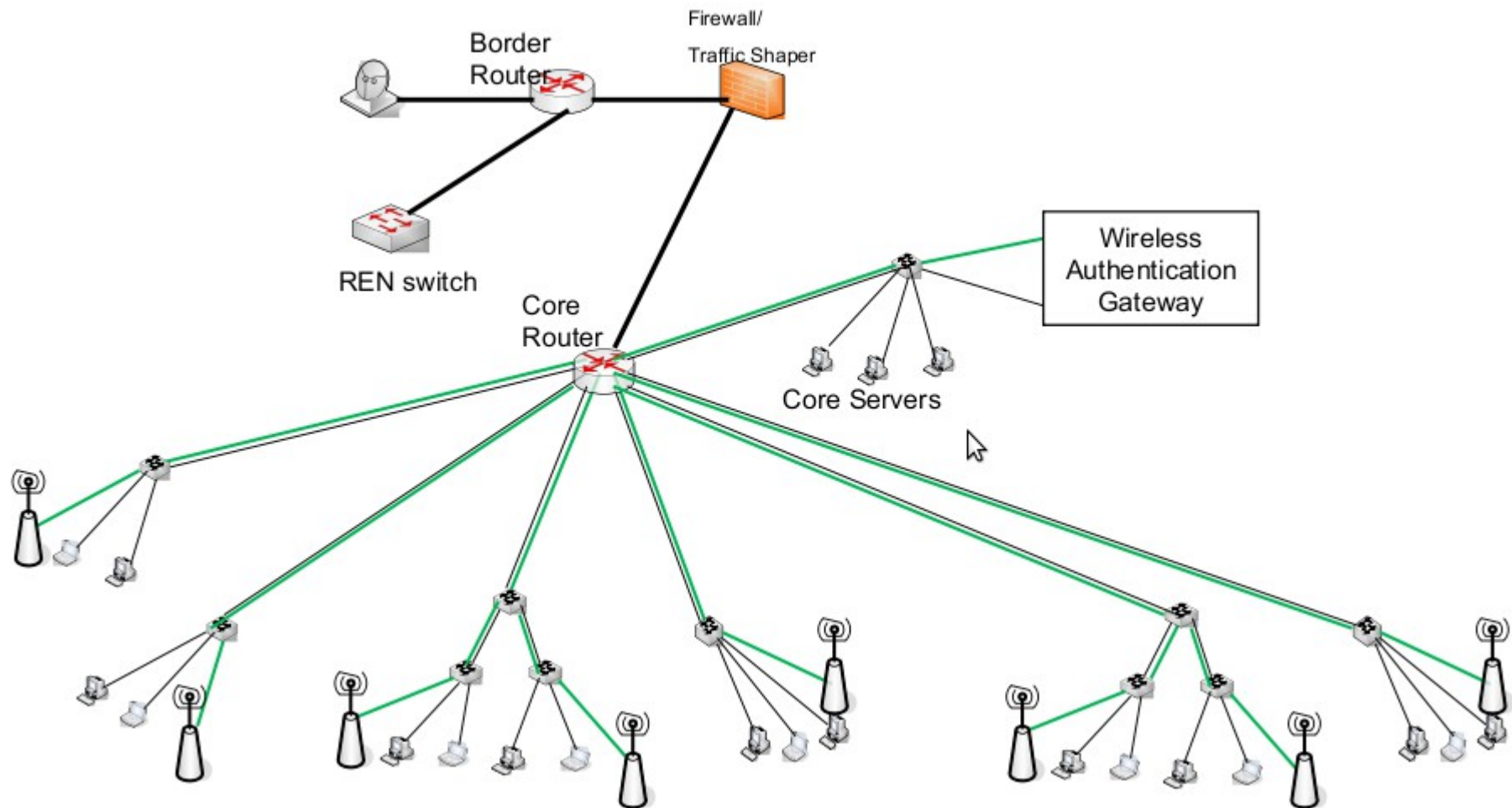
- The network is our streets and roads.
- Many people and vehicles travel on these roads.
- Streets and roads are open, or mostly open – we don't lock people into their houses.
- If we need to transport money from A to B – we use a protected vehicle (= “end-to-end security”).
- **We will do our best to keep unwanted drivers off the road, but it will never be perfect.**

# Authentication on wireless networks

## **Authentication via**

- captive portal or
- **802.1x (recommended)**
- This should happen via centralized servers on your core network (Radius, AD/LDAP), **not** on the edge access points

# Authentication on wireless networks



# 802.1x/WPA2 Enterprise on the AP

## WPA2-AES

To secure your wireless network, select **WPA2-AES**, which is WPA2 (Wi-Fi Protected Access 2) security mode with AES (Advanced Encryption Standard) support only. AES is also known as CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), which uses the AES algorithm.



The image shows a 'Wireless Security' configuration window. It contains three fields: 'Security:' with a dropdown menu set to 'WPA2-AES', 'WPA Authentication:' with a dropdown menu set to 'PSK', and 'WPA Preshared Key:' with a text input field and a 'SHOW' button to its right.

WPA2-AES currently is the only recommended security mode. WPA1 and WEP are no longer secure.

Source: AirOs7 User Guide / Ubiquiti - <http://ubnt.com>

# 802.1x/WPA2 Enterprise on the AP

**WPA Authentication** Specify one of the following WPA key selection methods:

- **PSK** Pre-shared Key method (selected by default).
- **EAP** EAP (Extensible Authentication Protocol) IEEE 802.1x authentication method. This method is commonly used in enterprise networks.

PSK is for one shared passkey for all users or devices,  
**EAP (802.1x) is for personal user credentials.**

Source: AirOs7 User Guide / Ubiquiti - <http://ubnt.com>



# 802.1x/WPA2 Enterprise on the AP

The important setting is  
the address of your  
**RADIUS server.**

We will discuss details of this  
in the unit on  
**Authentication.**

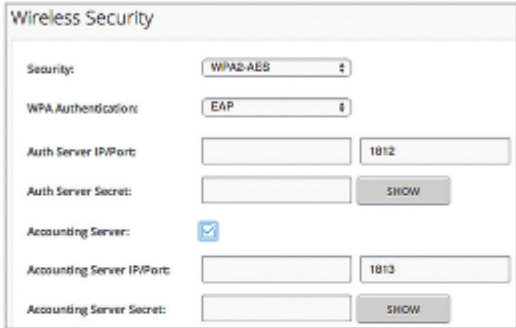
Source: AirOs7 User Guide / Ubiquiti - <http://ubnt.com>

## EAP

Available options depend on the wireless mode, as follows:

### EAP - Access Point PTP or Access Point PTMP Mode

The options below apply in *Access Point PTP* or *Access Point PTMP* mode only.



The image shows a 'Wireless Security' configuration window. It has several fields: 'Security' is set to 'WPA2-AES'; 'WPA Authentication' is set to 'EAP'; 'Auth Server IP/Port' has an empty IP field and a port field set to '1812'; 'Auth Server Secret' has an empty field and a 'SHOW' button; 'Accounting Server' is checked with a blue checkbox; 'Accounting Server IP/Port' has an empty IP field and a port field set to '1813'; and 'Accounting Server Secret' has an empty field and a 'SHOW' button.

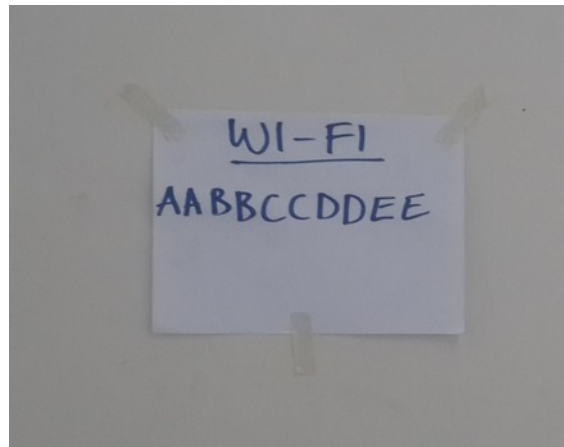
**Auth Server IP/Port** In the first field, enter the IP address of the RADIUS authentication server. RADIUS is a networking protocol providing centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect to and use a network service.

In the second field, enter the UDP port of the RADIUS authentication server. The most commonly used port is 1812, but this may vary depending on the RADIUS server you are using.

**Auth Server Secret** Enter the password. A shared secret is a case-sensitive text string used to validate communication between two RADIUS devices.

# What about ... PSK?

- You may use PSK (pre-shared key) for some tasks, e.g. giving access to devices (Internet of Things!) - but they are not recommended for people, except maybe in a (rather open) internet cafe or such.
- Be aware: PSKs typically get shared very fast, or are pinned on the wall :)



# What about ... MAC?

- MAC address lists are not suitable for user access control
- They identify machines (interfaces), not people.
- In larger organizations, you will cause a lot of work for the helpdesk – updating, removing, adding, ...
- MAC addresses are easily spoofed.
- MAC access control might be useful in infrastructure / p2p links / IoT.

# Security issues of 802.1x

802.1x or WPA2/EAP is the recommended authentication option, but it has a big security problem too:

- Its outer tunnel security relies on TTLS/SSL certificates
- These are vulnerable to man-in-the-middle attacks – if the client device does not properly check the certificate, then it will give its credentials to ANY AP, e.g. rogue APs
- Its inner tunnel encryption is MSCHAP2, which is known to be broken/crackable

# Addressing security issues of 802.1x

Nothing can protect us against client devices with bad certificate check implementations. Many do not check CN or CA\*, but:

- We can enforce the best possible client configuration, for example by using the eduroam CAT tool, see <https://cat.eduroam.org>
- See also security recommendations on <https://wiki.geant.org/>
- These are vulnerable to man-in-the-middle attacks – if the client device does not properly check the certificate, then it will give its credentials to ANY AP, e.g. rogue APs
- Its inner tunnel encryption is MSCHAP2, which is known to be broken/crackable

\* The details are beyond the scope of this talk! Some more info is given in our unit on *Authentication*.

# Tools for wireless security

**Enterprise wireless management systems**  
like Unifi provide tools like  
Rogue detection, traffic analysis, etc

In addition to this, there are tools on

## **Physical layer:**

Spectrum analyzers: airview, wispy

Packet sniffers: kismet – Netstumbler (windows)

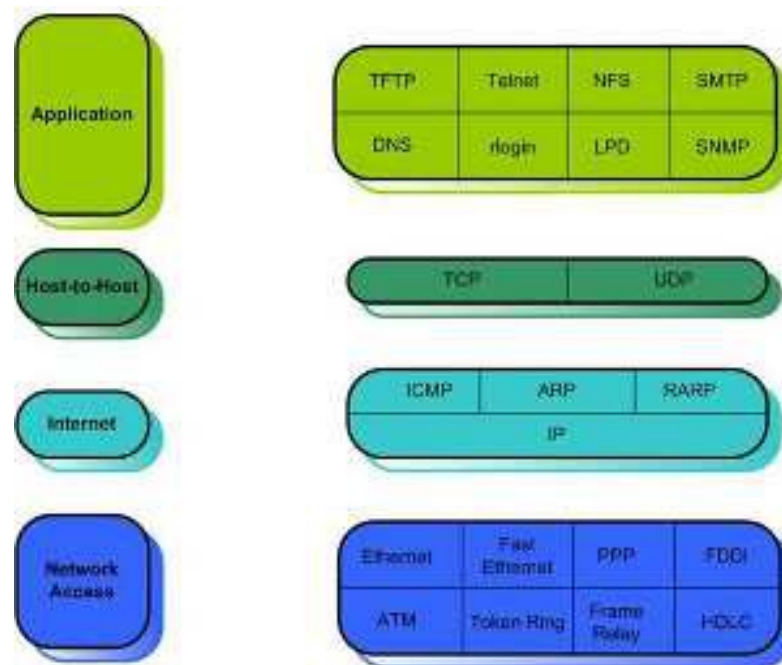
## **Network layer:**

etherape (no admin tool – just quick visual overview)

General networking and management tools: wireshark, ntop, mrtg, rrdtool, nmap, mtr

Tool collections: backtrack

**This is just a quick overview – explore these tools in the Lab!**

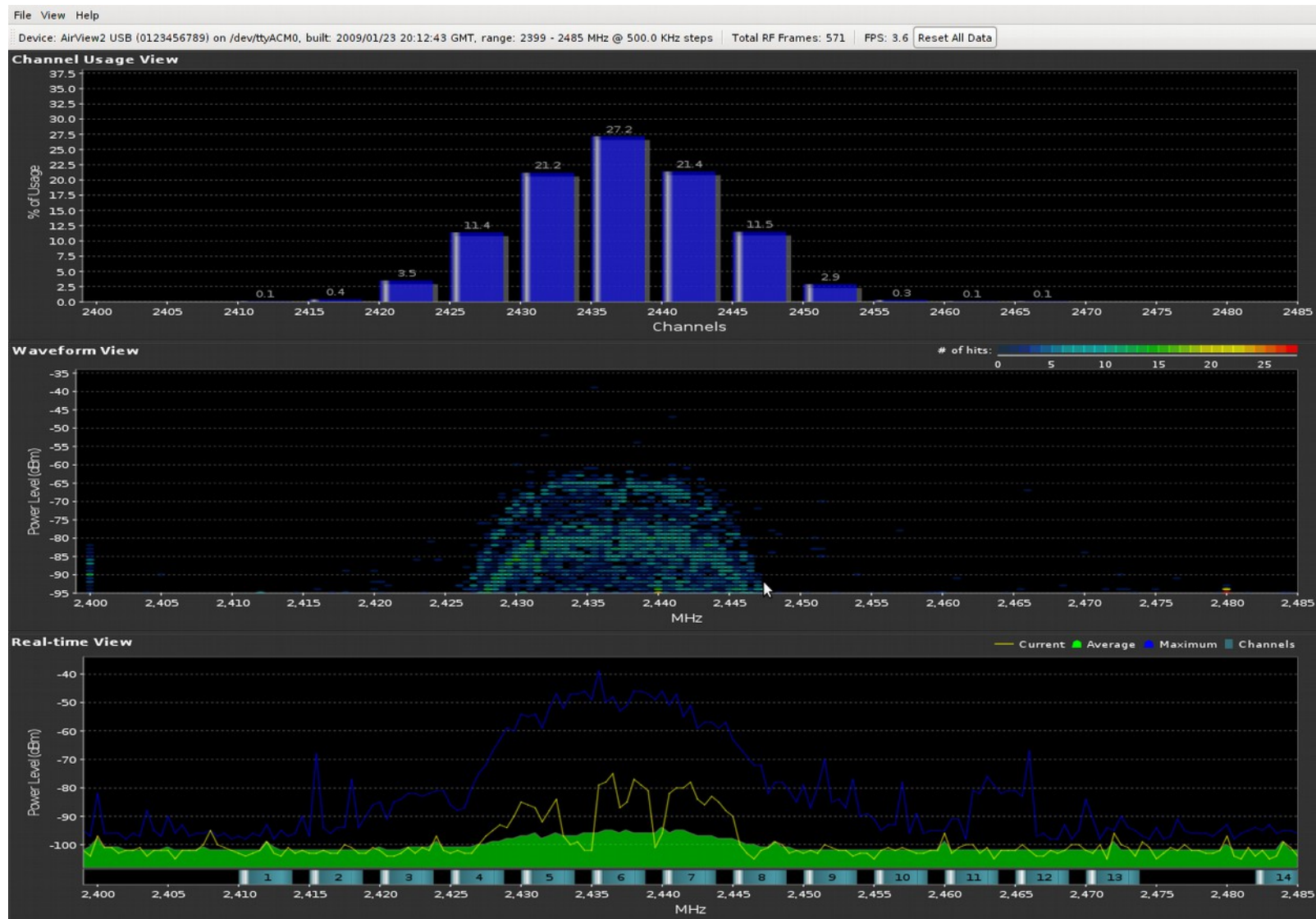


# Spectrum analyzers

- Real spectrum analyzers very expensive, but USB analyzers or RF Explorer are a reasonable compromise
- e.g. AirView (2.4 GHz), WiSpy (2.4 – 5.8 GHz)
- Pure physical layer! They will show you non-WiFi stuff, like microwave ovens, jamming attempts, bluetooth phones, etc

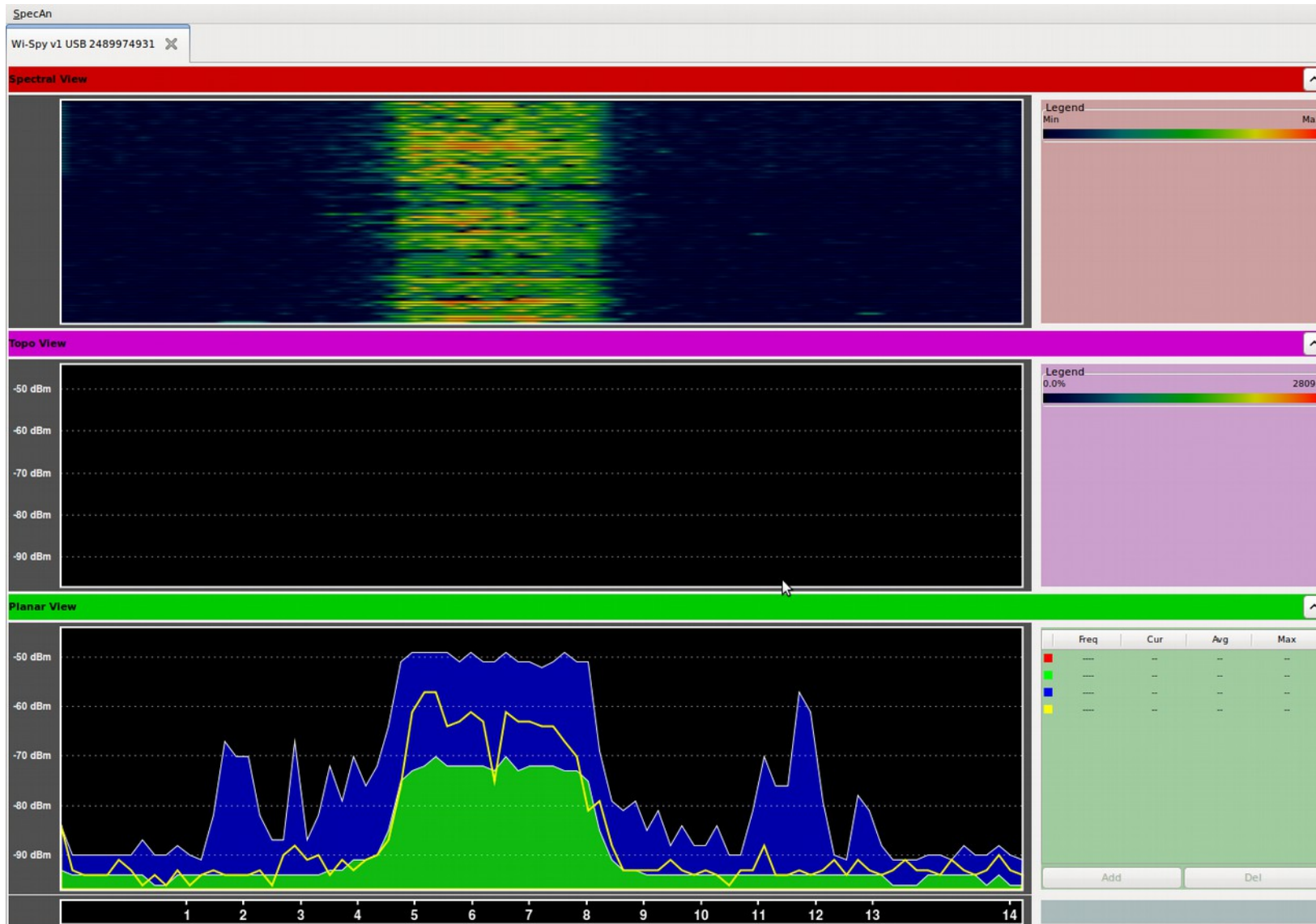


# Spectrum analyzers: Airview

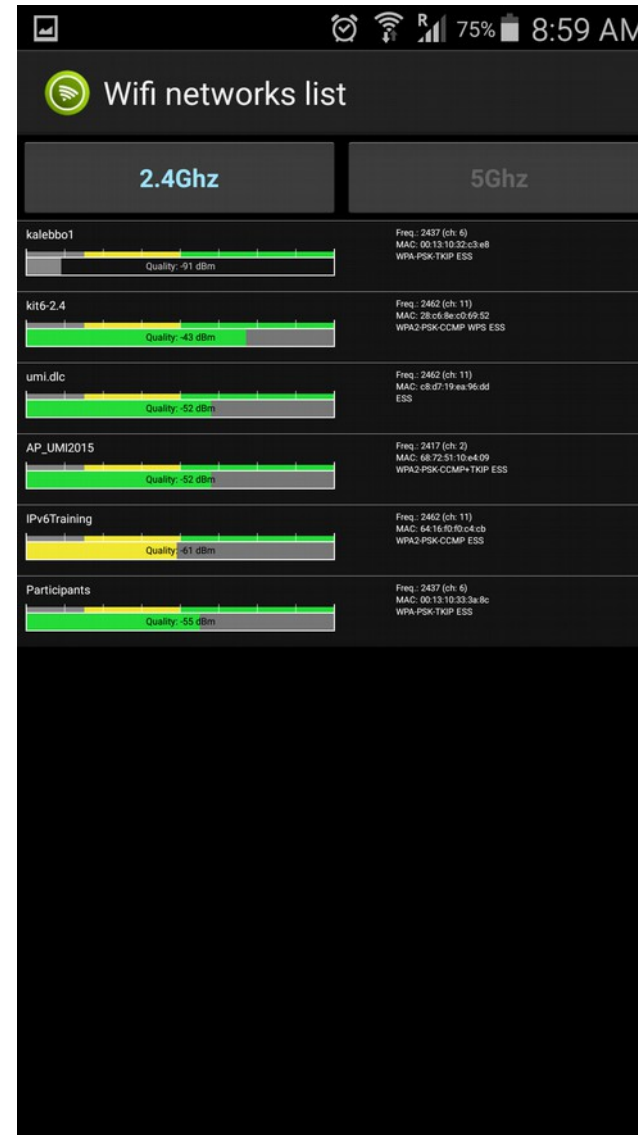
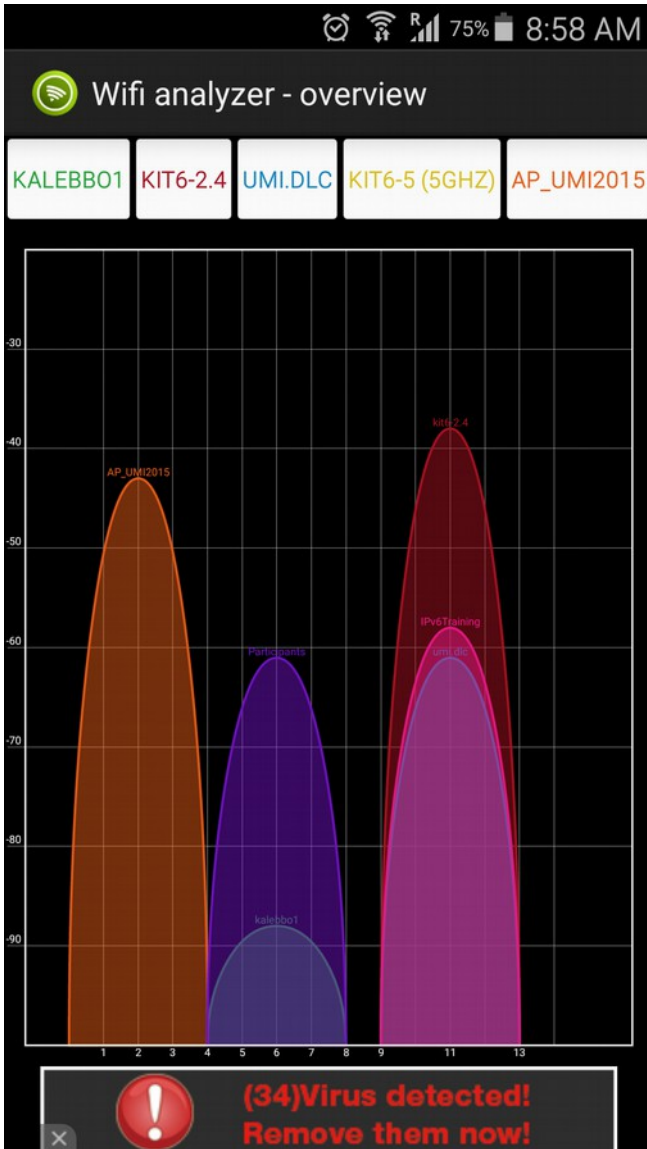




# Spectrum analyzers: WiSpy



# Android WiFi analyzers



# Kismet

- Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.
- Works in raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic.
- It is passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and presence of nonbeaconing networks via data traffic.
- Kismet is powerful - especially when combined with other tools like tcpdump/wireshark, nmap, etc

# Kismet

```

root@wirelessdefence:~
File Edit View Terminal Tabs Help

Network List (Autofit)
Name          T W Ch  Packts  Flags  IP Range
default       A N 006    9 F   192.168.0.1
! iyonder.net A N 005   42 U4  10.254.178.254
! iyonder.net A N 001   22 A3  10.254.178.0
! eurospot    A N 001   19 U4  204.26.5.166
! NETGEAR     A 0 006    5    0.0.0.0
. eurospot    A N 011   14    0.0.0.0
! belkin54g   A Y 011   17    0.0.0.0
! iyonder.net A N 011   16 A3  10.254.178.0
! tsunami     A Y 007   17    0.0.0.0
! <no ssid>   A 0 003   11    0.0.0.0
Probe Networks P N ---    3    0.0.0.0
! iyonder.net A N 008   35    0.0.0.0
. <no ssid>   A Y 011    5    0.0.0.0
NCDT_NET      A Y 006    1    0.0.0.0
<no ssid>     A Y 011    1    0.0.0.0

Info
Ntwrks      16
Pckets      228
Cryptd       4
Weak         0
Noise        0
Discrd       0
Pkts/s       8
Elapsd      00:00:20

Status
Found new probed network "\012\003\031\034\012\013\023\007\027\003\033\033\0
36\011\030\005\023\011\004\022\013\010\027\030\031\001\011\027\003\003\0
bssid 00:0A:8A:A2:C8:7F
Found IP 10.254.178.254 for iyonder.net::00:50:8B:51:17:17 via UDP
Battery: AC 107%
  
```

# Kismet

File Edit View Terminal Help

### Network List (SSID)

| Network Details                      |      | Size | Info        |
|--------------------------------------|------|------|-------------|
| Name : mySecure                      | 0.40 | 80B  | Ntwrks 7    |
| SSID : mySecure                      |      | 0B   | Pckets 1550 |
| Server : localhost:2501              |      | 0B   | Cryptd 58   |
| BSSID : 0A:15:6D:AD:C8:28            |      | 0B   | Weak 0      |
| Carrier : IEEE 802.11b               |      | 8k   | Noise 0     |
| Manuf : Unknown                      | 4.36 | 58k  | Discrd 0    |
| Max Rate: 18.0                       |      |      | Pkts/s 27   |
| BSS Time: a94c87181                  |      |      |             |
| Max Seen: 1000 kbps                  |      |      |             |
| First : Wed Mar 3 21:19:19 2010      |      |      |             |
| Latest : Wed Mar 3 21:21:03 2010     |      |      |             |
| Clients : 0                          |      |      |             |
| Type : Access Point (infrastructure) |      |      |             |
| Info :                               |      |      |             |
| Channel : 5                          |      |      |             |
| Privacy : Yes                        |      |      |             |
| Encrypt : TKIP WPA PSK               |      |      | my_int      |
| Decryptd: No                         |      |      | Ch: 52      |
| Beacon : 25600 (26.214400 sec)       |      |      |             |
| Packets : 391                        |      |      | Elapsd      |
| Data : 0                             |      |      | 00:01:44    |
| LLC : 391                            |      |      |             |
| Crypt : 0                            |      |      |             |
| Weak : 0                             |      |      |             |

75% (+) Down

Battery: AC 99%

:BD via UDP  
:37 via UDP  
:19 via UDP  
57 via ARP

# wireshark

- Wireshark is a free and open-source packet analyzer.
- It is used for network troubleshooting, analysis, software and communications protocol development, and education.
- Filtering for fast identification of problems, e.g. specific protocols (e.g. ARP), IP numbers, or keywords



# wireshark

The image shows the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. The main display area is divided into three panes. The top pane shows a list of captured packets, filtered by 'http contains assword'. The middle pane shows the details of the selected packet (Frame 6039), including Ethernet II, Internet Protocol, Transmission Control Protocol, and Hypertext Transfer Protocol. The bottom pane shows the raw packet data in hexadecimal and ASCII. The packet list shows several HTTP requests, including a POST request to /workshops/2010/garnet-nsrc/login. The details pane for Frame 6039 shows the Hypertext Transfer Protocol section with the text 'Line-based text data: application/x-www-form-urlencoded'. The raw data pane shows the packet data in hexadecimal and ASCII, with the password 'sebastian' visible in the URL.

Filter: http contains assword

| No.   | Time       | Source          | Destination    | Protocol | Info  |
|-------|------------|-----------------|----------------|----------|---|
| 407   | 31.189339  | 128.223.157.19  | 41.74.92.20    | HTTP     | HTTP/1.1 200 OK (text/html)   |
| 488   | 39.798732  | 41.74.92.20     | 128.223.157.19 | HTTP     | POST /workshops/2010/garnet-nsrc/login HTTP/1.1 (application/x-www-form-urlencoded)   |
| 791   | 62.372509  | 41.74.92.20     | 209.35.17.17   | HTTP     | GET /c/a/Administration/Capturing-Packets-with-the-Wireshark-Network-Analyzer/3/ HTTP |
| 813   | 63.970537  | 41.74.92.20     | 209.85.229.101 | HTTP     | GET / utm.gif?utmwmv=1.3&utm=529904867&utmcs=ISO-8859-1&utmsr=1400x1050&utmsc=24-bi   |
| 4874  | 170.723290 | 41.74.92.20     | 209.85.229.100 | HTTP     | GET /complete/search?hl=en&client=serp&expIds=17259,25901,26440&pq=POST&q=password&c  |
| 4879  | 170.856041 | 41.74.92.20     | 173.194.37.104 | HTTP     | GET /search?hl=en&q=password&aq=f&aqi=g10&aql=&oq=&gs_rfai=&fp=bbe94252df21093c HTTP  |
| 5798  | 193.902524 | 128.223.157.19  | 41.74.92.20    | HTTP     | HTTP/1.1 200 OK (text/html)   |
| 6039  | 202.176036 | 41.74.92.20     | 128.223.157.19 | HTTP     | POST /workshops/2010/garnet-nsrc/login HTTP/1.1 (application/x-www-form-urlencoded)   |
| 8899  | 240.562635 | 192.221.115.126 | 41.74.92.54    | HTTP     | HTTP/1.1 200 OK (text/css)  |
| 9930  | 241.864214 | 216.45.19.33    | 41.74.92.54    | HTTP     | HTTP/1.1 200 OK (application/x-javascript)  |
| 11882 | 246.775524 | 209.126.179.3   | 41.74.92.54    | HTTP     | [TCP Previous segment lost] Continuation or non-HTTP traffic                          |
| 11886 | 246.778089 | 209.126.179.3   | 41.74.92.54    | HTTP     | Continuation or non-HTTP traffic  |
| 11887 | 246.779789 | 209.126.179.3   | 41.74.92.54    | HTTP     | Continuation or non-HTTP traffic  |

Frame 6039 (216 bytes on wire, 216 bytes captured)

- Ethernet II, Src: Intel\_05:b6:9b (00:19:d2:05:b6:9b), Dst: D-Link\_bd:d6:76 (00:13:46:bd:d6:76)
  - Destination: D-Link\_bd:d6:76 (00:13:46:bd:d6:76)
  - Source: Intel\_05:b6:9b (00:19:d2:05:b6:9b)
  - Type: IP (0x0800)
- Internet Protocol, Src: 41.74.92.20 (41.74.92.20), Dst: 128.223.157.19 (128.223.157.19)
- Transmission Control Protocol, Src Port: 35262 (35262), Dst Port: http (80), Seq: 2422, Ack: 38609, Len: 150
- [Reassembled TCP Segments (849 bytes): #6038(699), #6039(150)]
- Hypertext Transfer Protocol
- Line-based text data: application/x-www-form-urlencoded
  - \_FORM\_TOKEN=453a6d4a8ac48b906dc366c7&referer=http%3A%2F%2Fnsr.org%2Fworkshops%2F2010%2Fgarnet-nsrc%2Fwiki%2Fagenda&user=sebastian&password=

Frame (216 bytes) Reassembled TCP (849 bytes)

Frame (frame), 216 bytes Packets: 14173 Displayed: 13 Marked: 0 Profile: Default

# wireshark

- Wireshark is a free and open-source packet analyzer.
- It is used for network troubleshooting, analysis, software and communications protocol development, and education.



# Next steps

- Security settings, practice and exercises -  
in the **Lab**
- Unit on **Authentication**

# Questions?

