Hands-on with wifi security

OWASP Göteborg Security Tapas

2015-10-20

Anders Rosdahl

OWASP

Open Web Application Security Project

#whoami

- Avarage security enthusiast
- No bleeding edge research, no wall of fames, no cve's
- Actually, this is me...

@rosdahl

Agenda

Wifi overview

Authentication and encryption

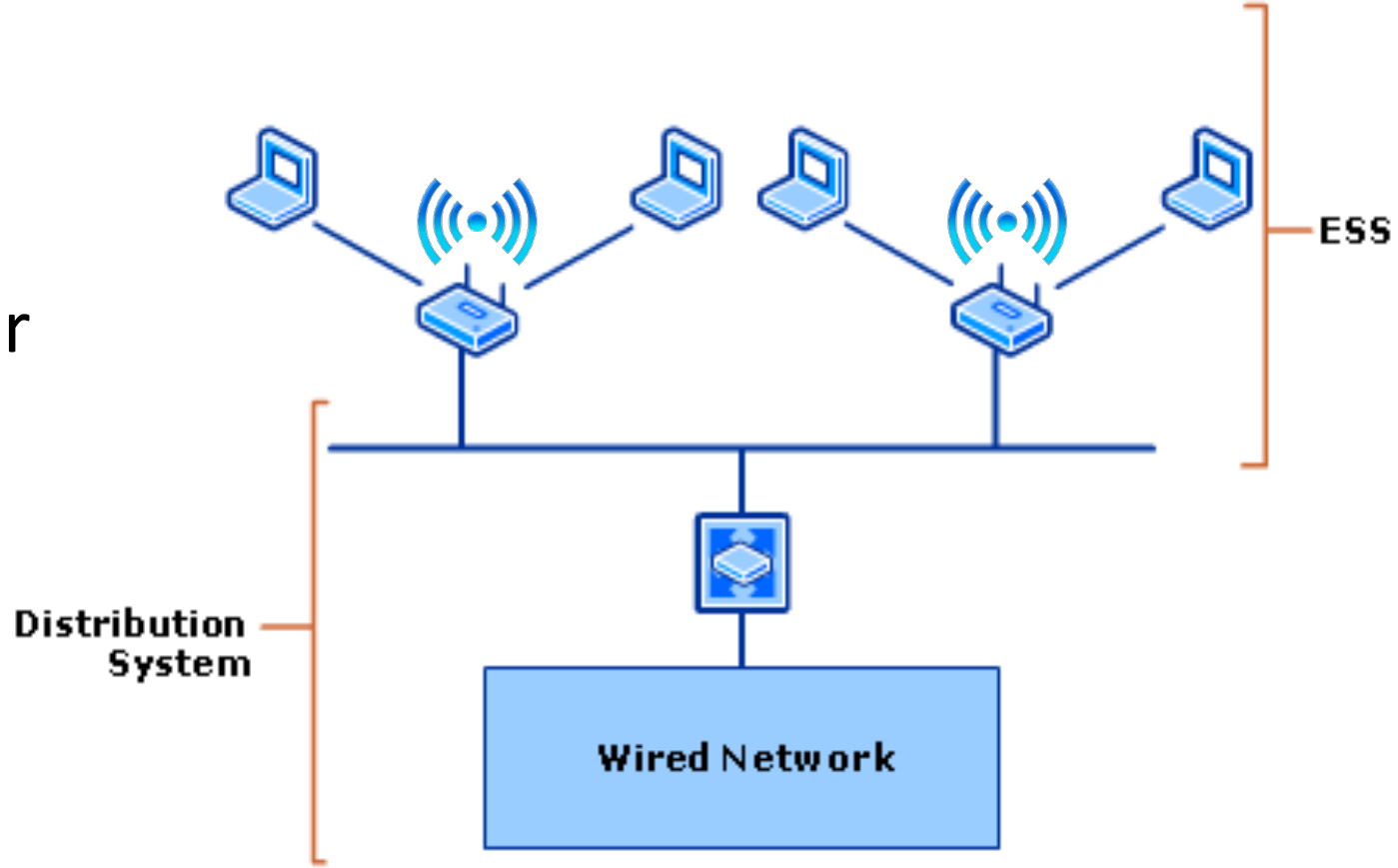
Attacks

Defence

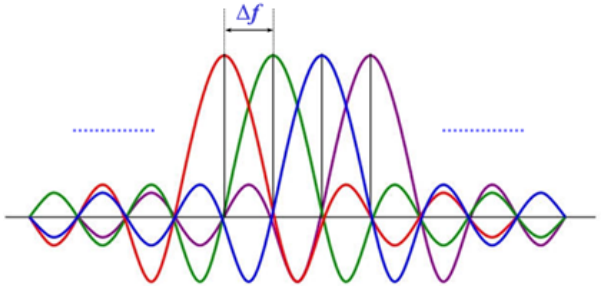
Demo / lab

Wifi overview

- **Access points** continuously send **beacons** to announce themselves
- **Clients** continously **probe** for access points
- **Authentication**
- **Association**



Bands, channels and frequencies



802.11	Release year	Frequency (GHz)	Max data transfer rate (Mbit/s)	Bandwidth (MHz)
a	1999	5 / (3.7)	54	20
b	1999	2.4	11	22
g	2003	2.4	54	20
n	2009	2.4 / 5	72/150 (per MIMO stream)	20/40
ac	2013	5	96/200/433/866 (per MIMO stream)	20/40/80/160
there's more...				

Wireless Modes

Each wireless device/inteface can be in one of the following modes. Definitions vary.

- **Station** – also referred to as Client mode or Managed mode
- **Master** – also referred to as Access Point or Infrastructure mode
- **Ad hoc** – for mesh wifi networks
- **Monitor** – also referred to as RFMON (Radio Frequency MONitor). Used to silently listen to wifi traffic. An interface in this mode can capture traffic without connecting to any network.

Not all combination of wifi cards/drivers/OS support all modes..

Authentication and encryption

WEP

- Based on the RC4 stream cipher, which is effectively broken

WPA/WPA2

- WPA – intermediate solution while waiting for WPA2, which would fix all that was broken with WEP. Designed by crytographers.
- PSK or asymmetric key pairs/certificates
- TKIP-RC4 (WPA) / CCMP-AES (WPA2)

WPS

- Provides WPA/WPA2 password to client requiring only a PIN code
- Two modes:
  - Push-Button-Connect
  - 4/8 digit PIN code

Attacks

- WPA/WPA2
  1. Deauthenticate connected client(s) with traffic injection
  2. Capture re-authentication handshake
  3. Offline word-list or rule-based brute force attack on recorded handshake

- WPS
  - Brute force WPS PIN. In 2012 several deficiencies in WPS were disclosed. E.g. only max 11k vs 10M tries is needed since AP acks/nacks first 4 digits.
  - WPS backoff/timeout timeout prevents bruteforcing. Was not ubiquitous 2012.

- WEP
  - RC4 ...
  - Offline brute force attack similar to WPA above

Defence – hot security tips for hotspots

- Use long and strong WPA2 passwords!
- Disable WPS on your router
- Don’t use WEP – obviously...
- Use VPN when connected to public access points – anyone can listen
- Be careful about auto-connect features of devices to avoid connecting to rouge access points

Demo/lab

- Alfa cards for loan!