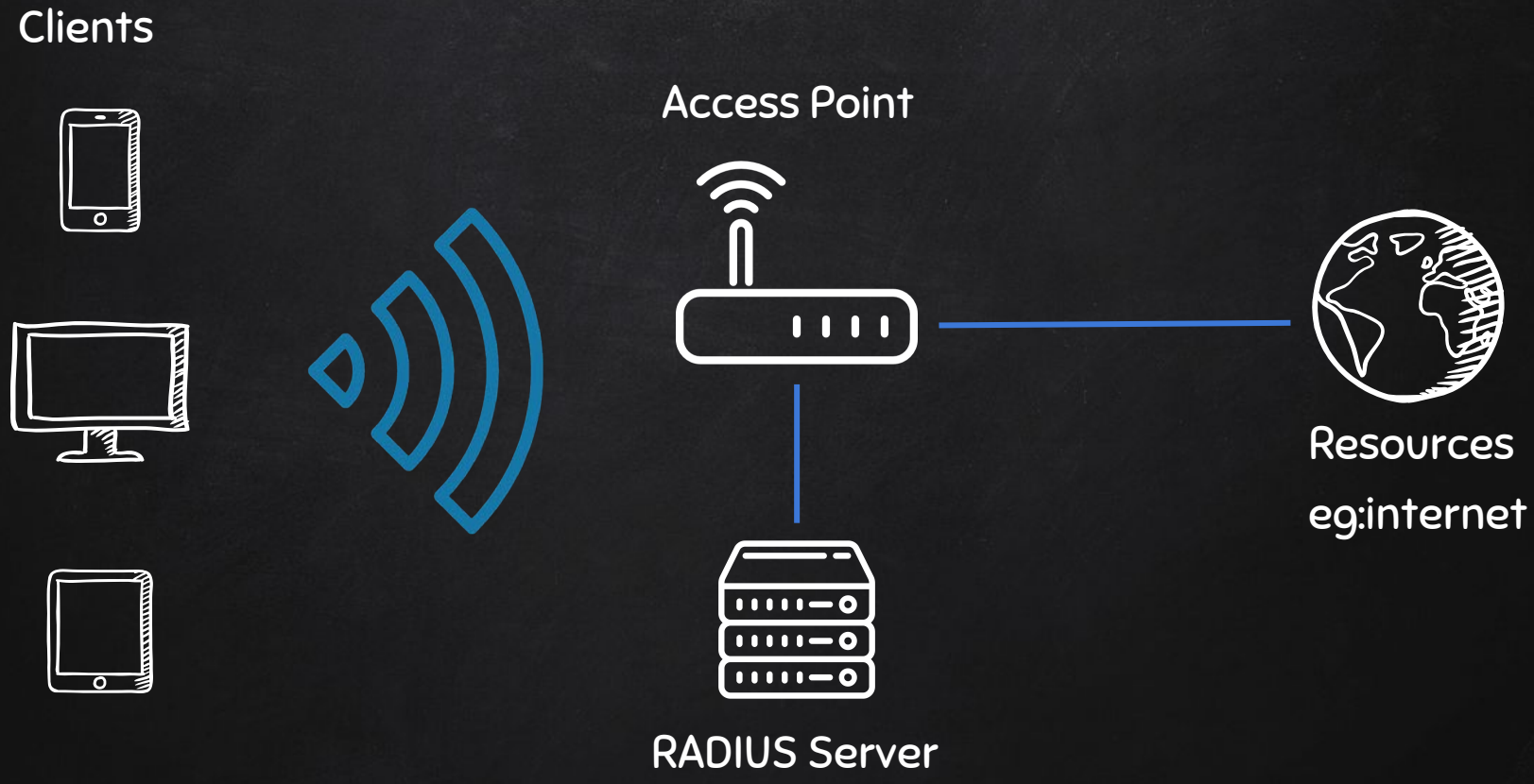
WPA Enterprise

- All WPA/WPA2 networks we seen so far use PSK authentication.
- A shared key is used to authenticate users.
- One key per network.
- Router manages authentication.

- WPA Enterprise is another form of authentication.
- Each user get their own key to connect to the network.
- Authentication is managed through a central server (RADIUS Server).

WPA Enterprise



Hacking WPA Enterprise

Problems:

1. Encryption is used, so can't sniff credentials in monitor mode.
2. Can't use ARP spoofing because we need to connect first.

The only solution is to run an evil twin attack, 2 ideas:

1. Using the traditional method, just use a page that looks like login box.
2. Create a fake AP that uses WPA enterprise.

Hacking WPA Enterprise

Using Traditional Fake AP

Drawbacks:

1. Has to be an open network when users know their network use WPA/WPA2.
2. They have to enter password in a web page.

Advantages:

- Password is sent in plain text.
- No need to decrypt it.

Hacking WPA Enterprise

Using a Fake WPA Enterprise AP

Drawbacks:

- Captured password will be encrypted.

Advantages:

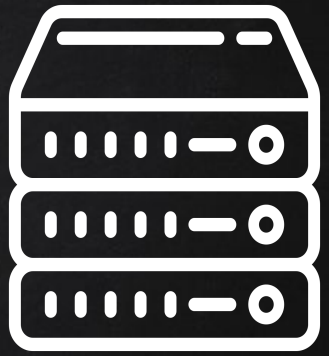
- Looks and behaves exactly like a real WPA-Enterprise network.

Challenge Response Authentication

I want to connect

Solve this challenge XXX

Response



RADIUS Server

Security

Security

1. Captive Portals

- Open networks.
- No encryption is used.
- Lots of ways to get in.

Solution:

- Do not use captive portals.
- Use WPA/WPA2 enterprise instead.

Security

2. WEP

- Lots of methods to crack it.
- Even SKA networks can be cracked.

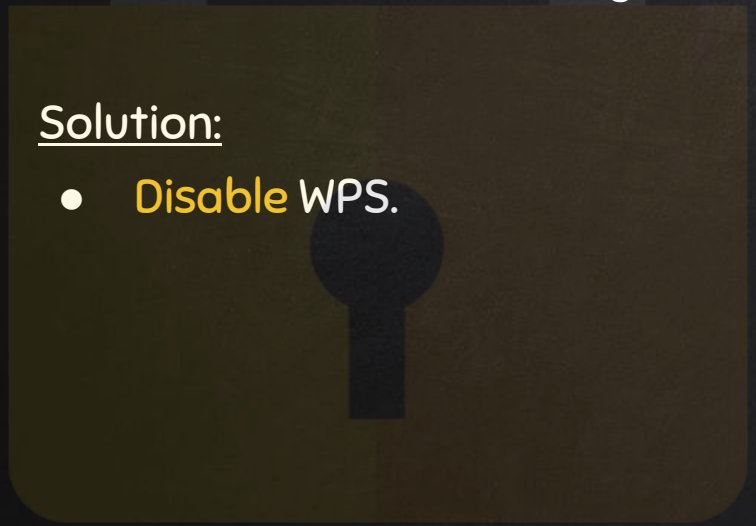
Solution:

- DO NOT USE WEP.

Security

3. WPS

- WPS pin is only 8 digits.
- Can be brute-forced even if the router locks.
- Then it can be used to get the WPA/WPA2 key.



Solution:

- Disable WPS.

Security

4. Advanced Wordlist attacks

- Work against all networks.
- Password can be cracked as long as it's in the wordlist.

Solution:

- Use long complex password of letters, numbers and symbols.

Security

5. Evil-Twin Attacks

- Exploit the users.
- Work against all networks.

Solution:

- Educate the users.
  - Always connect to the right AP.
  - Never enter password in a web interface.

Security

Summary

1. Do not use captive portals.
2. Never Use WEP.
3. Disable WPS.
4. Use WPA/WPA2 with a long complex password.
5. Educate users