Hacking Wireless Networks For Fun And Profit.

or HWNFFAP

@juicebox

Agenda

- Good Lord why ?
- Dear God how ?
- OMG Hax !! (Can I stop these shenanigans ?)
- Q&A
- Cake

torsdag 9. mai 13

This is all old stuff. It's been talked about plenty. But I like talking about stuff that's been talked about before.

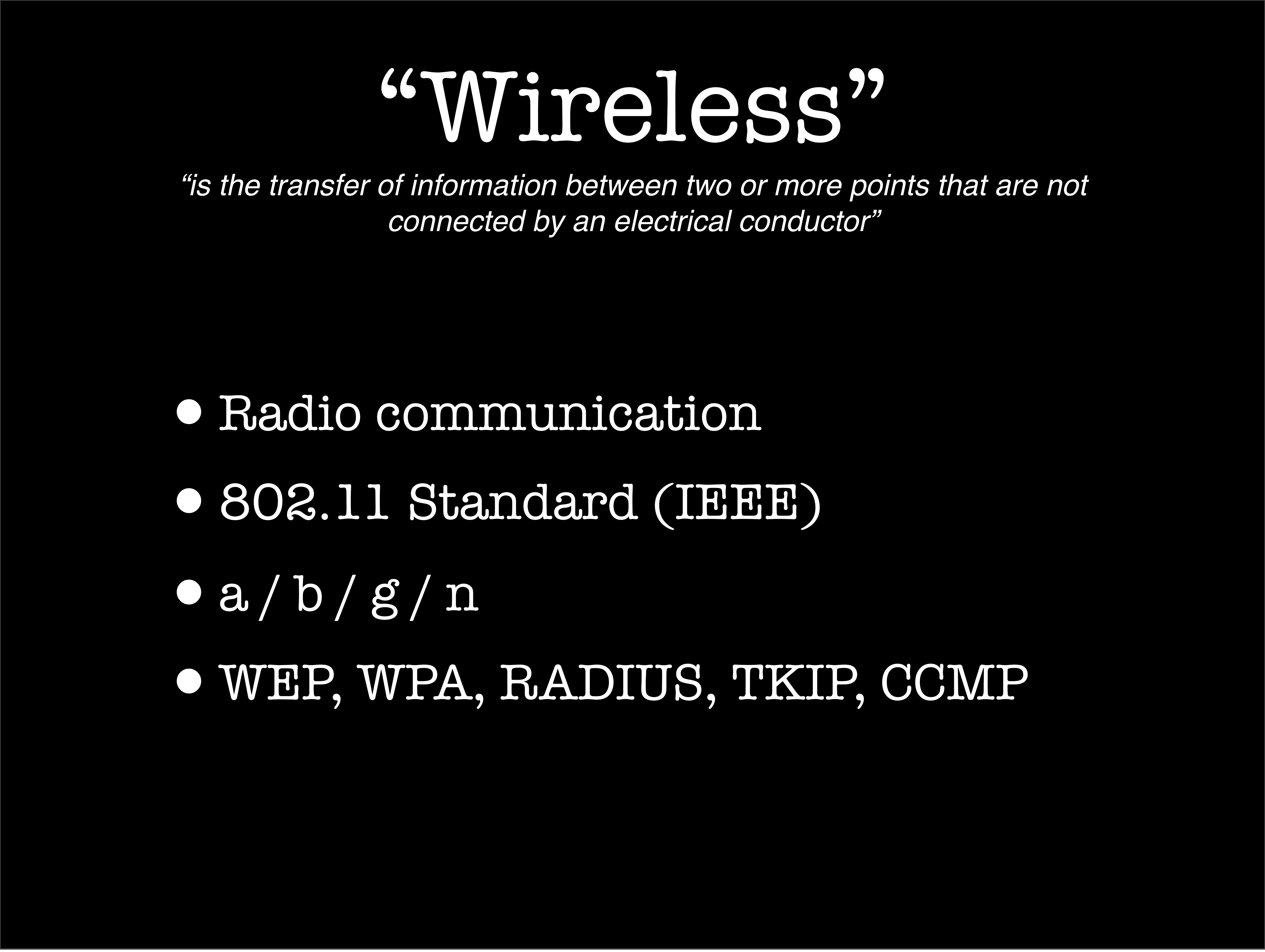
Good Lord why ?

torsdag 9. mai 13

Why would you want to do this ?
Do you want to learn more about the protocols / security involved ?
Or do you just want to jump on your neighbours wireless (and possibly get owned)

The boring stuff

But first we need to go through some boring stuff.



“Wireless”

“is the transfer of information between two or more points that are not connected by an electrical conductor”

- Radio communication
- 802.11 Standard (IEEE)
- a / b / g / n
- WEP, WPA, RADIUS, TKIP, CCMP

source: http://en.wikipedia.org/wiki/Wireless

What we’re most interested in here is the WEP and WPA bits. The rest are just pieces of the puzzle and can be researched in your own time.

Stations

clients...laptops, phones, tablets...anything that you use to connect to a wireless network

Access Points

torsdag 9. mai 13

“servers” Usually act as routers (will likely have a wired connection to the LAN)...you connect to these from your stations.

No security == clear text

torsdag 9. mai 13

clear text is bad. We (as attackers) like clear text as it means we don’t have to do any man in the middle attacks which could out us to our victims.

clear text can be sniffed. Passwords, session cookies etc....all of this can be pulled from the wire.

source: google image search...my bad

WEP && WPA

Our two main targets....

WEP: Wired Equivalent Privacy (easy peasy, lemon squeezy)
WPA: Wifi Protected Access   (a little more difficult)

Dear God how ?

How would you do this ?

Old School: WEP

Cracking WEP

Weak ass crypto

source: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

RC4

source: http://en.wikipedia.org/wiki/RC4

64bit and 128bit keys

initialization vectors

This is where our “problem” comes in with WEP.

24 bits !!!

torsdag 9. mai 13

24 bit IV’s ...this means your 64bit and 128bit keys aren’t quite as tough as you thought. They’ve become a 40bit and 104bit key...

torsdag 9. mai 13

weak

torsdag 9. mai 13

ass :D

crypto

Yes you can use 10 hexadecimal characters (0-9 and A-F)

Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets

source: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

Because RC4 is a stream cipher, the same traffic key must never be used twice. The purpose of an IV, which is transmitted as plain text, is to prevent any repetition, but a 24-bit IV is not long enough to ensure this on a busy network. The way the IV was used also opened WEP to a related key attack. For a 24-bit IV, there is a 50% probability the same IV will repeat after 5000 packets

source: http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

which is transmitted as plain text

You just need “data”

weapon of choice:

aircrack-ng suite

http://www.aircrack-ng.org/

Attack

- Start the wireless interface in monitor mode on the specific AP channel
- Use aireplay-ng to do a fake authentication with the access point
- Start airodump-ng on AP channel with a bssid filter to collect the new IVs
- Start aireplay-ng in ARP request replay mode to inject packets
- Run aircrack-ng to crack key using the IVs collected
- ???
- Profit

source: http://www.aircrack-ng.org/doku.php?id=simple_wep_crack

Demonstration

New School: WPA(2)

torsdag 9. mai 13

Cracking WPA

A little more complicated,

but not much.

Offline Attack

Handshakes, they’re important

Discuss and show the 4 way handshake

Wordlists,
important as well

This will take time, but it’s the easiest way

weapon(s) of choice:

aircrack-ng suite

cowpatty

john the ripper

Tools:

http://www.aircrack-ng.org/
http://www.willhackforsushi.com/Cowpatty.html
http://www.openwall.com/john/

Rainbow tables,
they’re probably
also important

This will save you time (maybe) but it will cost you

~~Rainbow tables, they’re probably also important~~

Sorry..I didn’t have much time to go through this :(

Honourable Mention:

WPS

Tool to highlight: Reaver

https://code.google.com/p/reaver-wps/

whitepaper:

http://sviehb.files.wordpress.com/
2011/12/viehboeck_wps.pdf

or

http://bit.ly/tBMolm

“computing standard that attempts to allow easy establishment of a secure wireless home network”

source: http://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup

WPS

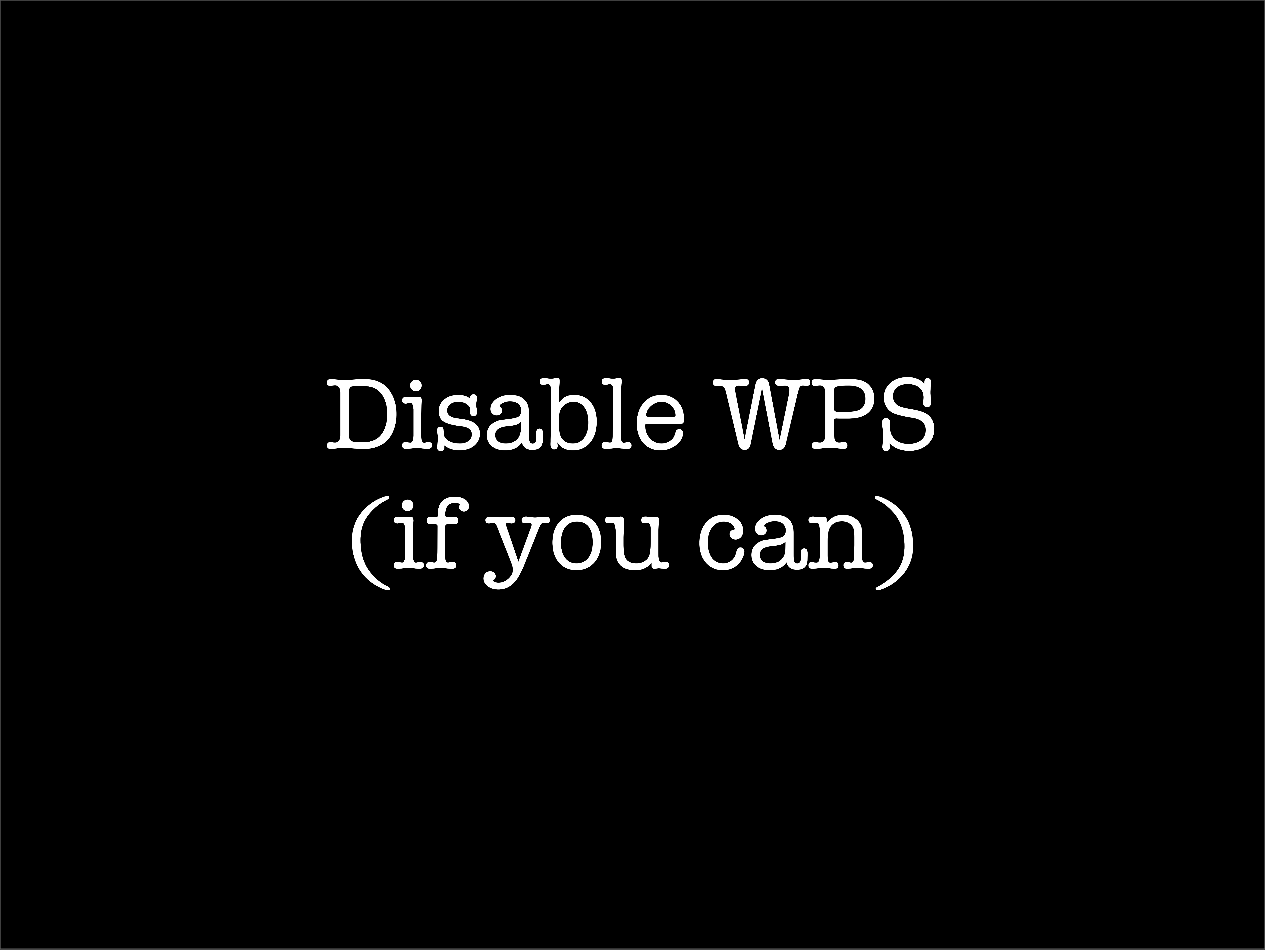
- 8 digit pin
- but the last digit is a checksum
- validation process splits 8 digits in two
- 4 digits = 10 000 possibilties
- 3 digits = 1000 possibilities

weapon of choice:
Reaver

torsdag 9. mai 13

Tool highlight: Reaver

https://code.google.com/p/reaver-wps/



Disable WPS
(if you can)

Difficult as there are a lot of routers that say they will disable it, but don't.
Others don't even offer you the possibility to disable WPS :(
#fail

torsdag 9. mai 13

This means you’re going to have a bad day at some point.

OMG Hax !!

torsdag 9. mai 13

Detect and prevent

Detection ?

torsdag 9. mai 13

Detection ? Can you detect that bad things are happening ?

torsdag 9. mai 13

Not really...it’s difficult. Kind of like looking for a needle in a haystack.

Prevention

torsdag 9. mai 13

Prevention ? Can you prevent bad stuff from happening ?

MAC Locking

I’ve heard you can do MAC locking to prevent people from logging onto your AP ?

~~MAC Locking~~

Nope. All I will do is do a little passive sniffing, grab a MAC address from a working / authenticated client and use that on my machine. I can then knock him off the network, and I'll be able to connect just fine.

There's a neat little tutorial here:
https://wiki.archlinux.org/index.php/MAC_Address_Spoofing

“Spoofing”

RADIUS authentication

Encrypt EVERYTHING

Encrypt all your traffic. Tunnel stuff over ssh, fire up a VPN (OpenVPN is a good one)..just don’t let your traffic go unprotected.

In summary

- WEP is useless, don’t use it
- WPA(2) is also pretty useless
- Drunk 4 year olds could perform these attacks
- Encrypt all the things
- ???
- Profit

So in summary :)

README.txt

- Hacking Exposed: Wireless http://amzn.to/159BnFh
- Basquillions of whitepapers

God stuff to read.

Q&A

Cake

the cake is a lie!

torsdag 9. mai 13

boobies :D

source: internet somewhere...