A GLANCE INTO WIFI NETWORK SECURITY AND PRIVACY

AMINDA SUOMALAINEN

2024-10-08

For those struggling to find the balance between Environment, Privacy and Security.
You aren’t alone.

Contents

0.1 Foreword

I have said it multiple times during planning and whoever listens to me, but since this begins the final document, I am going to repeat myself and say that writing about Wi-Fi is difficult.

Wireless networks are everywhere, they are impossible to avoid entirely, even if they were only signs on a public wall saying that wherever you are provides one. Everyone who has used a ”smart” device has used one and knows what it is, but do they really?

This document attempts to be what I have wanted to read about Wi-Fi for a decade or longer within one cover, but the subject is so vast that I don’t know whether I can collect it all or whether I end up covering nearly enough of what I really want to say.

Hopefully you will also begin questioning your WiFi network and its configuration and leave it in a better state than you found it in.

Oh and I am also aiming to graduate by showing that I have some sort of an idea on what is a cybersecurity and how to maintain it.

Later in the document I will also discuss WiFi positioning services, which make the subject even more challenging than it already was. So few people know and understand that the SSID (simplifiedly network name) can easily be turned into a position where the access point is located and the MAC address is even more identifiable that way.

While I attempt to [redacted] information exposing other people, I am leaving mine visible so there is something to show and there is no guarantee that it’s not translatable to my location. Thus I request that you will not try whether or not `_nomap` protects me since there is always some service not respecting it and telling you all about my access points regardless.

0.2 Introductionary case study: Huawei K562

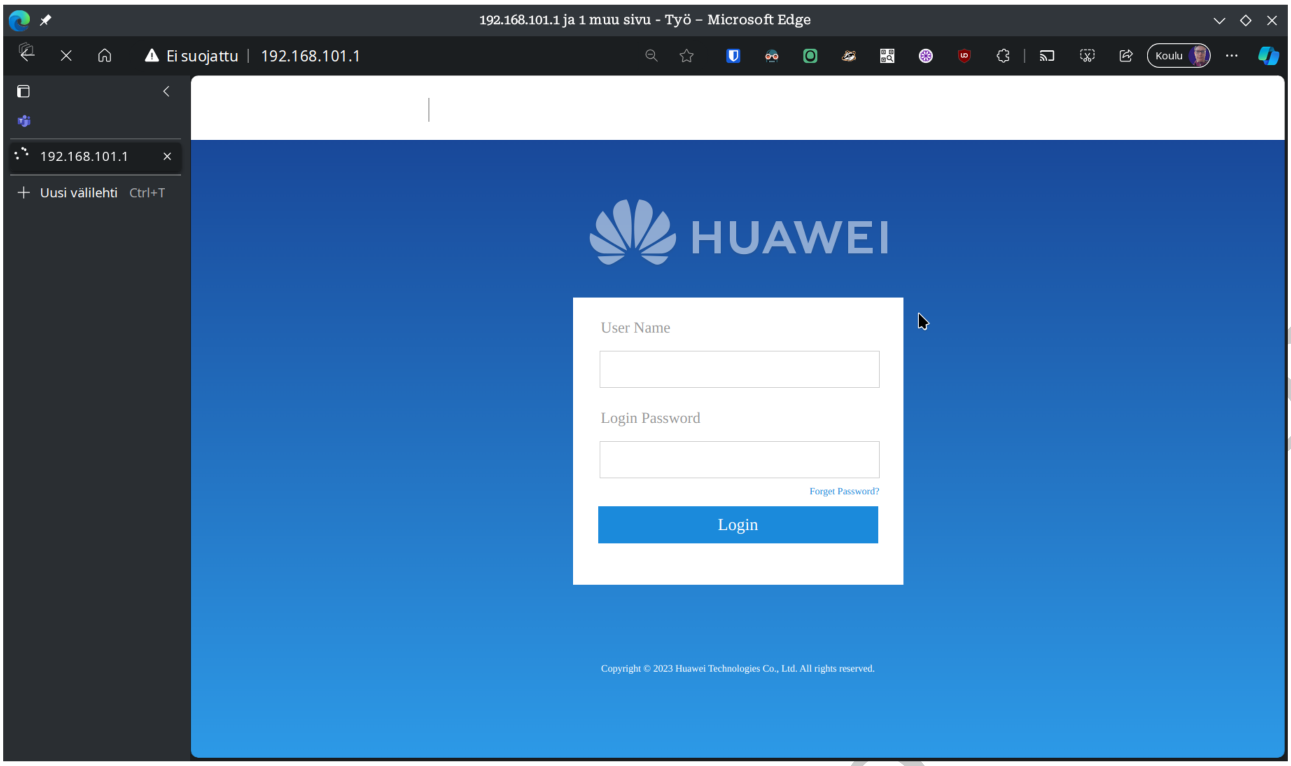
Also known as *OptiXstar K562 Ethernet Terminal*, *DNA Mesh WiFi -modem K562* and *Valoo WiFi 6 Mesh -router*. First we factory reset it, then we will go through all the settings to see how everything is wrong.

0.2.1 Fresh from the factory

I was trying to perform the setup using an ethernet cable, but since that is very slow for some reason, I am laxing from information security a bit by connecting to the device wirelessly.

The default credentials read on the bottom of the device and luckily either Huawei or DNA has included a QR code there, so first we use an Android to open network settings and scan the code. Next we select the new network and share the connection, so we can see the password without having to take photos or think of other hacks.

The control panel is located in `192.168.101.1` with the username being `admin` and password `1234`.


192.168.101.1 ja 1 muu sivu - Työ – Microsoft Edge
Ei suojattu | 192.168.101.1
Koulu
192.168.101.1
Uusi välilehti Ctrl+T
HUAWEI

User Name

Login Password

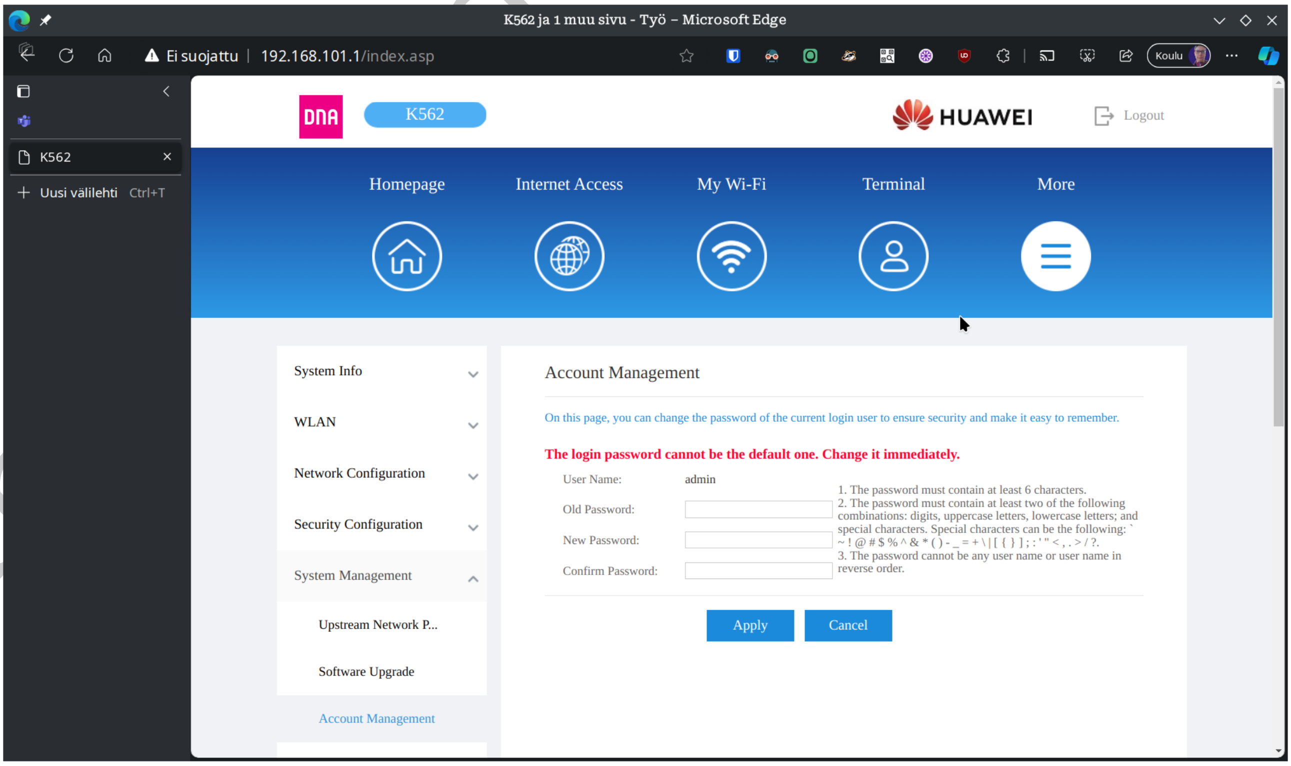
Forget Password?

Login

Copyright © 2023 Huawei Technologies Co., Ltd. All rights reserved.

Admin password

Now if security was a priority, we would be forced to change the login password immediately. However as they don't, we have to navigate More, System Management, Account Management by ourselves to see this prompt.



Account Management

On this page, you can change the password of the current login user to ensure security and make it easy to remember.

The login password cannot be the default one. Change it immediately.

User Name: admin

Old Password:

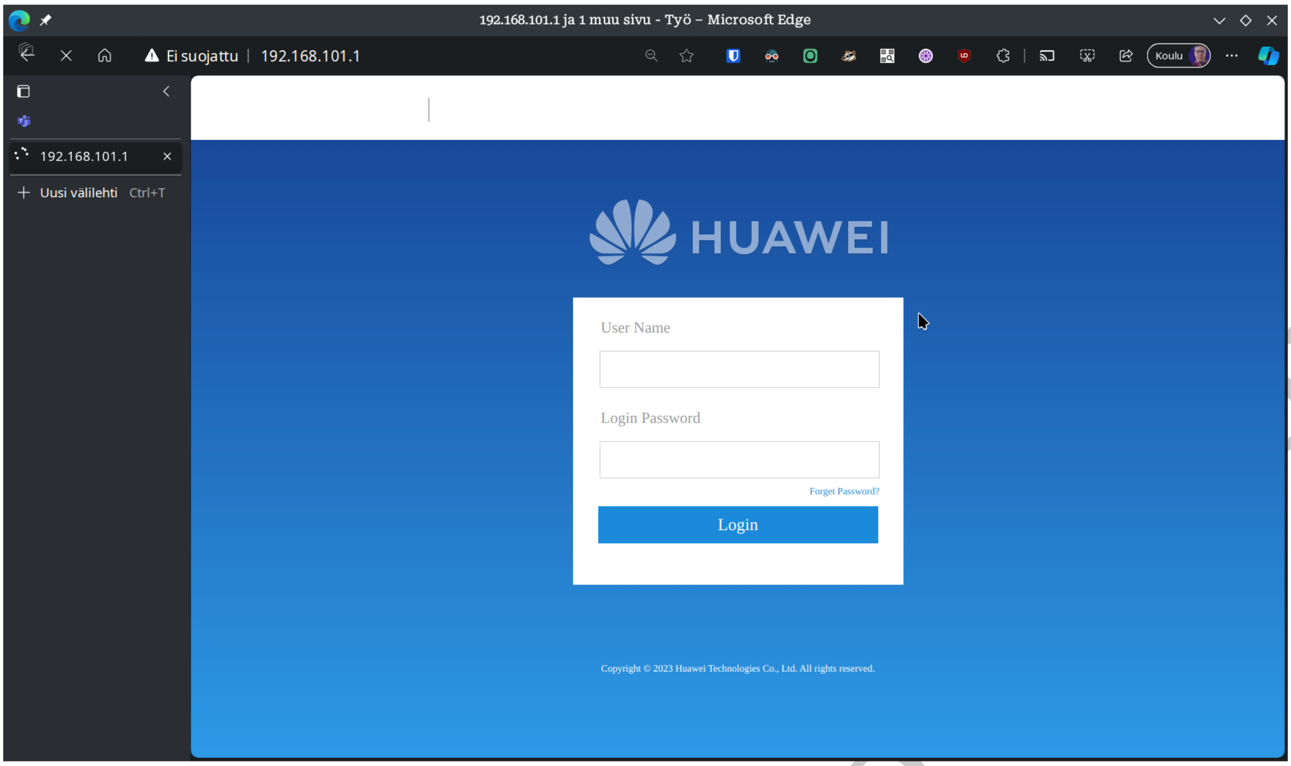
New Password:

Confirm Password:

1. The password must contain at least 6 characters.
2. The password must contain at least two of the following combinations: digits, uppercase letters, lowercase letters; and special characters. Special characters can be the following: ` ~ ! @ # $ % ^ & * ( ) - _ = + \ | [{ }] ; : ' " < , . > / ?.
3. The password cannot be any user name or user name in reverse order.

Apply Cancel

We are thrown back to the login screen displayed previously.


192.168.101.1 ja 1 muu sivu - Työ – Microsoft Edge
Ei suojattu
192.168.101.1
Koulu
192.168.101.1
Uusi välilehti Ctrl+T
HUAWEI
User Name
Login Password
Forget Password?
Login
Copyright © 2023 Huawei Technologies Co., Ltd. All rights reserved.

Default SSID

For some reason this device shíps with one 2.4 GHz SSID enabled, DNA-WIFI-[redacted], and two 5 GHz ones, DNA-WIFI-[redacted]and DNA-WIFI-5Ghz-[redacted]. As the defaults are insecure, we change them immediately (which will also permit my devices to reconnect after the factory reset).

We have to navigate to WLAN and there both 2.4 GHz and 5 GHz settings separately.

We also have to disable WPS by ourselves by disabling the checkbox (on both frequencies).

Next the same for WiFi 5, where note the existence of a duplicate SSID!

Off-screen I have also visited Network Configuration, LAN Settings, which is irrelevant for this work, but my devices have static network configuration that is not compatible with Huihai defaults.

0.2.2 My WiFi

Now that our basics are in order, we are ready to start moving through all the menus. Homepage and Internet Access have nothing terribly interesting, but our first issue is My WiFi where we can see a *WiFi Power Mode*, which is set to *Through-wall (high power, better signal)*.

Now, is this a reasonable option? I am living in a studio apartment and I have a single room (the kitchen closet has its removed) and I don't use WiFi or anything else in the bathroom.

Remember that WiFi is a semi-duplex radio, so all access points sharing the same channel distrupt each other due to sharing airtime assuming they can hear each other. We are also turning all radios connecting to the access point to maximum power since there is an assumption that if server with maximum power is heard, so will be the client with equal power, so there may also be a question of electricity and green ICT perspective. On the security side, do we want the network to be connectable from far beyond the closest set of walls? [2]

We change it to *Sleep (low power, weak signal)* and receive a scary warning **You are advised to use the through-wall mode. The signal in this mode is better.Wi-Fi power modification takes effect, causing a short interruption of Wi-Fi.**

0.2.3 WLAN Advanced Configuration

Here we see that our device is configured to use

Channel: automatic Channel width: automatic 20/40 MHz Mode: 802.11b/g/n/ax Airtime fairness

Channel: automatic Channel width: automatic 20/40/80/160 MHz Mode: 802.11a/n/ac/ax Airtime fairness

The device again repeats **You are advised to set it to 11b/g/n/ax.**

2.4G Wi-Fi all wrong

2,4 G frequencies are a limited resource, one that our access points share with microwave ovens, bluetooth and everything. If we want to live in peace without disturbing others, we have three channels, that is if everyone uses 20 MHz channel width, but no, a lot of devices decide to use 40 MHz.

As per Apple's recommendation we switch to channel width 20 MHz.[5]

Now, the mode. While generally backwards compatibility is good, we are using the valuable shared airtime and by being backwards compatible, we make sacrifices including in speed (and possibly energy consumption). [1]

802.11n, nowadays also known as Wi-Fi 4 was adopted in 2009 and remains the most common version of 2.4G Wi-Fi today. 802.11g (Wi-Fi 3) is from 2003 and 802.11b (Wi-Fi 1) from 1999 [6]. Do we really need backwards compatibility so far back?

The only Wi-Fi device incapable of WiFi N that I can name is Nokia E63 running Symbian. Thus we switch to 802.11n-only.

Interlude: WiFi DFS channels and Location Aware Routing

The automatic channel selection of 5 GHz sounds great in theory, but in practice we are following European regulation and thus can only use channels 36 to 64 if we cannot detect weather radars (100-144) [4] and who knows what are channels 149-177 for (TODO).

Our devices should be aware of what country we are in, but commonly consumer devices don't allow configuring that explicitly so we end up in Germany if we are even in Europe. This can be seen through `iw reg get` for our current NIC when using Linux:

```
global
country FI: DFS-ETSI
...

phy#0 (self-managed)
country FI: DFS-UNSET
...
```

Redacted are the regulations our WiFi network interface card recognises. Luckily at the time of writing, we are correctly detected to be in Finland, but that is often not the case, and generally all access points broadcast being in Germany.

However note that DFS is unset, thus we are avoiding DFS channels out of the box and have to configure our device manually to have free channel.

DFS stands for Dynamic Frequency Selection and means that when booting, our access point scans around for weather radars for 10 minutes before beginning broadcasting and WiFi starting to work.

We can also see what the nearby access points broadcast:

```
sudo iw wlan0 scan | grep -E "SSID:|Country:" | less
```

```
SSID: LocationServices_nomap
Country: FI     Environment: bogus
SSID: LocationServices_nomap
Country: FI     Environment: bogus
```

All of the more presumably recent DNA devices appear to be advertising being setup in Finland, but in invalid environment, while the older models advertise being setup in Germany Indoor/Outdoor meaning the access points don't know are they setup indoors or outdoors, which again furter restricts the frequency options.

Back to 5G configuration

In order to not share channel with all 14 other networks that are present at the time of writing, we must configure the 5G channel by hand. As the regulatory domain says DFS is unset, everyone keeps avoiding those channels and we should check where the weather radars are. I mostly spend my time in Helsinki and Kotka and happen to know that the closest weather radars to those share the channel 128 and are located in Vantaa and Anjalankoski [3]. Thus we are free to pick any other channel.

I have once observed a TP-Link device on channel 100 at my home, so I am using the channel 112 which will not overlap the 128 which would cause a distruption whenever the weather radar activates.

Thus we again see Huwaei telling us **You are advised to set the channel to Automatic.**, since they seem to be having incorrect assumption of access point being configured properly. Perhaps they expect to be a minority and rely on the majority to have proper configuration for Location Address Networking.

When applying this, Huawei once again gives us a warning **Due to frequency regulation, if you select this channel, you need to wait for 10 minutes until the Wi-Fi network is available.**, but that we already knew, even if otherwise it might have been helpful.

Next would be *Wi-Fi Coverage Management*, which doesn't refer to the transmit power discussed previously, but mesh networking and I am going to just disable this due to the small size of my apartment.

Automatic Wi-Fi Shutdown is also irrelevant and as I only have this Huawei router I don't need to switch from router to bridge mode either.

0.2.4 LAN Settings

I visited here before and the Apple recommendation is 8 hours for private networks, one for public hotspots and guest networks.[5]

We can no longer reliably identify devices based on the MAC address and that affects routers as well, since modern mobile devices have MAC address randomisation with unpredictable interval. In case of Android, there is a developer mode option to always change MAC address.

0.2.5 IPv6 and DHCPv6 Server Configuration

IPv6 itself is a toggle whether it's enabled or not, and we are going to leave it enabled, since most of Finland already has IPv6 available and IPv4 addresses ran out ages ago.

In DHCPv6 settings, we could change DNS Information to benefit from DNS Over TLS opportunistic mode.

I choose `2620:fe::fe` and `2620:fe::9` which are Quad9 with ECS and increase client security by DNS level filtering of bad domains. More on ECS later.

We could also enable ULA in automatic mode. ULA starts for Unique Local Address and is the successor of the old class A/B/C internal networks from IPv4.

The final option of `Network Configuration` would be `UPnP` which for security should be disabled since it could allow potentially unwanted applications to connect to the internet through our router firewall, but I run firewalls on all client devices where possible and utilise applications relying on UPnP such as Syncthing synchronising my files between my devices without other people's computers, so I am leaving it enabled.

0.2.6 Security configuration

The router admin panel would begin at MAC address filtering, but as mentioned before, mobile devices are constantly changing their MAC addresses and besides as discussed in the upcoming Aircrack subsection, the MAC addresses or BSSIDs are visible really easily and thus MAC address filtering is entirely pointless. Otherwise there isn't really much to say about security configuration and unlike everything before, the defaults seem reasonable.

The next subsection would be *System Management*, where the only relevant thing would be *Account Management*, which was already handled.

Chapter references

[1] David Coleman. *Backward Compatibility: The Double-Edged Sword of Wi-Fi Performance and Connectivity?* `https://www.extremenetworks.com/resources/blogs/backward-compatibility-the-double-edged-sword-of-wi-fi-performance-and-connectivity`. [Online; accessed 19-August-2024]. 2022.

[2] Petri Riihikallio. *8 reasons to turn down the transmit power of your Wi-Fi*. `https://metis.fi/en/2017/10/txpower/`. [Online; accessed 19-August-2024]. 2017.

[3] Petri Riihikallio. *Weather radars in Finland*. `https://metis.fi/en/2017/01/weather-radars/`. [Online; accessed 19-August-2024]. 2017.

[4] Petri Riihikallio. *What are WiFi DFS frequencies and should I care?* `https://metis.fi/en/2017/08/dfs-en/`. [Online; accessed 19-August-2024]. 2017.

[5] Apple Support. *Recommended settings for Wi-Fi routers and access points*. `https://support.apple.com/en-us/102766`. [Online; accessed 26-August-2024]. 2024.

[6] Wikipedia contributors. *Wi-Fi 6 — Wikipedia, The Free Encyclopedia*. `https://en.wikipedia.org/w/index.php?title=Wi-Fi_6&oldid=1242032750`. [Online; accessed 26-August-2024]. 2024.

0.3 WiFi Monitoring mode

As previously discussed, the first step is switching the NIC to monitoring mode so we can observe the WiFi traffic around us. In case of Tails, this means three simple steps.

1. Open the `root terminal` application
2. Stop wpa_supplicant so it won't interfere by running `systemctl stop wpa_supplicant`. Note that this will cut our wireless connection.
3. Actually switch to the monitoring mode by `airmon-ng start wlan0`

0.3.1 aircrack-ng

Still staying in the root terminal, we execute `airodump-ng wlan0` and we should now see all the networks around us alongside client devices (stations) requesting connection to BSSIDs and immediately learn that security is a lie.

Based on short observation, I know someone around me has visited both `Finlandia_public` and `Datapaja`. I also know that a neighbor named [redacted] who likely lives in `Koti_`[redacted] and they own an iPhone 13 Pro Max.

Thus we have confirmed that hidden SSIDs ("`<length: 0>`") are harmful for your privacy and won't stop us from knowing them anyway.

0.4 Attacks against WiFi

0.4.1 Theory

0.4.2 Attacking our own AP

0.4.3 Mitigating attacks / securing management frames

0.5 WiFi positioning services

0.5.1 WiFi Privacy isn't only between your client and AP

Since the advent of GPS personal navigation technology has been becoming increasingly common and in addition to cars, smartphones and even smartwatches or smart rings may come with a GPS nowadays.

However the traditional positioning systems may not function well when the client is located between high buildings, indoors or even tunnels and at some point, businesses decided to start collecting WiFi Access Point MAC addresses and locations for reliable positioning anywhere with a WiFi access.

The largest of these databases likely belong to Google and Apple considering how with default settings their operating systems Android and iOS contribute into them.

0.5.2 Google

When an Android phone is first booted, there is an setup wizard that amongst Google account credentials asks whether to enable Google's Location Services. Later in settings there is also a toggle on whether WiFi network scanning is allowed even when WiFi is disabled.

Should the user answer yes, which they likely will, all networks the phone sees are transmitted to Google both for locating the device now, and in the future.

Chapter references

[1] David Coleman. *Backward Compatibility: The Double-Edged Sword of Wi-Fi Performance and Connectivity?* `https://www.extremenetworks.com/resources/blogs/backward-compatibility-the-double-edged-sword-of-wi-fi-performance-and-connectivity`. [Online; accessed 19-August-2024]. 2022.

[2] Petri Riihikallio. *8 reasons to turn down the transmit power of your Wi-Fi*. `https://metis.fi/en/2017/10/txpower/`. [Online; accessed 19-August-2024]. 2017.

[3] Petri Riihikallio. *Weather radars in Finland*. `https://metis.fi/en/2017/01/weather-radars/`. [Online; accessed 19-August-2024]. 2017.

[4] Petri Riihikallio. *What are WiFi DFS frequencies and should I care?* `https://metis.fi/en/2017/08/dfs-en/`. [Online; accessed 19-August-2024]. 2017.

[5] Apple Support. *Recommended settings for Wi-Fi routers and access points*. `https://support.apple.com/en-us/102766`. [Online; accessed 26-August-2024]. 2024.

[6] Wikipedia contributors. *Wi-Fi 6 — Wikipedia, The Free Encyclopedia*. `https://en.wikipedia.org/w/index.php?title=Wi-Fi_6&oldid=1242032750`. [Online; accessed 26-August-2024]. 2024.

0.6 Taking action

If everything older than WPA3 is broken and we make ourselves vulnerable through backwards compatibility, perhaps we should run guest networks usable by everyone as the precense of open network is easier for anyone to confirm than someone breaking into the network through captured four way handshake.

0.6.1 Open Wireless Networks

Also known as unprotected or insecure networks although that may be inaccurate with WPA3 also bringing Open Wireless Enhanced which provides encryption between the access point and client, while downgrade attacks and evil twin attacks still exist.

That may sound scary, but ...

Combating climate change

When considering the carbon footprint of Information Technology and the internet in general, researchers end up to conclusions that include mobile networks being more energy-intensive than static ones. Thus having an open guest network transfer data instead of connecting 4G BBS may be better for climate.

Our WiFi access point is going to consume electricity whether or not we are using it or even present. If it was open, maybe this would help reduce our carbon footprint.

Reducing carbon footprint and improving cybersecurity both work in layers, small steps cumulate and become more impactful when put together.

Helping those who just need access

Have you ever needed access to a WiFi network in the middle of habitation with a lot of closed networks available, without any open ones? What is the easiest thing to do in this case?

Opening Router Keygen by YoloSec, selecting a SSID with default configuration and seeing possible passwords to it, problem solved.

Of course that isn't legal (unless the access point belongs to your confused partner who tells you to show them and resulting to reconfiguration of said access point for security reasons), but will a blackhat who just needs internet access care about that?

Encountering a blackhat in such a situation may be bad luck, but if there was an open network, they would have less incentive for attacking us or neighbouring networks and hopefully they might pay it forwards by opening their network too.

Reducing Radio Frequency pollution

This paper repeats it a lot, but many networks come with default configuration that uses maximum transmit power, maximum channel width and crowded channels. Would open networks help with that, especially with less radios having been active for communicating with mobile BBS? Maybe it would at least reduce the amount of Wi-Fi tethering.

0.6.2 Staying safe

I believe the zero trust approach can be adapted here. If we treat every network as possibly compromised, as a result we will take actions against the router and potential attacker and thus it doesn't matter where our devices are.

- Encrypt everything. DNS encryption is supported by current versions of all major operating systems and can be enforced system wide e.g. through group policy and similarly https-only mode can be enabled.
- Firewall everything and consider carefully what to let through the firewall.
- Reject passwords, embrace stronger authentication methods. Especially in remote control, such as SSH, the best practices include `PasswordAuthentication no`, and using keys instead. Thus even if SSH is exposed in firewall, it's hardened against casual bruteforce attackers.