OPSEC considerations when using wifi

Suspicious_Actions 1 April 18, 2022, 11:09am

Here is a list of stuff with wifi that leads to deanonymization and some other trivia on information leaks with this technology. No wifi hacking tho.

All of those attacks only work if your adversary is in range of your wifi. It can be extended with directional antennas, LNAs and all of this is applying to **management packets**. Those are modulated differently to allow for more range at the cost of bandwidth compared to normal data packets.

Mac Addresses

Your wifi card has a permanent hardware serial number that is used as its address on OSI layer 2, the **MAC address**. It is send unencrypted with every packet and can be read by anyone in range. This number is of the following format: “FF:FF:FF:AA:AA:AA”,
where the first 3x2 hex digits are the manufacturers prefix, and the last part the unique identifier within that address space.

Here is a list of all manufacturer prefixes.

If you see a MAC address that is for example `00:20:91:AB:0C:13` you can figure out that this wifi card was build by the National Security Agency.

Everybody in range can passively log MAC addresses with minimal ($2) hardware.

Mitigations

Turn on MAC randomization and hostname randomization. I wrote a setup script if somebody wants to copy my (very simple and auditable) bashcode into dom0.

Caveat! Some wifi firmwares are shitty. You can change your MAC address in software, but some chipsets will answer to packets that are addressed at their real MAC address, enabling an adversary to perform an active confirmation attack.

Wifi probes

Wifi probes are a bitch, so you probably want to mitigate those.

The APs (the thing that makes your wifi network) does send out beacon frames periodically, basically saying “Hi, i am network_a!”. This is enough for your devices to connect to it, but to speed up this process and to aid in roaming wifi probes are used.

Those are unencrypted packets send out by your devices whenever wifi is enabled to interrogate every known APs.

You wifi cards constantly sends out “hey home network, are you there? Hey network of my mate, are you there?” for every network you where connected at one time, resulting in a pretty unique used AP list that leaks astonishing metadata like where you where on vacation in some scenarios (“trump hotel guest wifi”) and so on… More a threat to smartphones, but of course also applies to laptops.

Wifi probe fingerprinters are in active deployment by corpos to track if customers return to their

store and measure engagement by deploying one on billboards and one in the store… Those things are cheap ($2).

Mitigation

Only activate wifi if you really need it.
Delete old networks you won't use anymore.
In qubes you could create one *sys-wifi-networkname* that is used as the netvm for *sys-net* for every network you connect and only start the one you want, or selectively only expose the configuration of needed networks to your *sys-net* dynamically.

Hardware imperfections

If your adversary is technically a bit more skilled, ones wifi card can be uniquely finerprinted by its **hardware imperfections**. Despite the fanciness of thid attack the needed hardware has gotten quite cheap (~20$). I am not aware of ready to go open source solutions for this attack **If you are: Please send me a link!**

Mitigations

None.

As you cannot mitigate your hardware imperfections in software, the only way to stay "anonymous" is to simply buy more hardware.

Assume that every wifi device can be uniquely identified by an skilled and motivated adversary.

You can compartmentalize with hardware, like use only one physical wifi device for one single network, this would at least make your adversary unable to link together different networks you use.

You adversary will still be able to recognize that the same device is connected to the same network again, but there is nothing one can do about that that would scale good enough to be practical, but to not use wifi.

Other stuff

There is much wrong with wifi, i will not go into the attacks on the crypto here.

But even without attacking the crypto an passive adversary can monitor network traffic metadata (timings, size of packets) and leverage that knowledge with other deanonymization techniques.

Oh and you can **look through walls** with wifi. Pretty neat. LE has this in active deployment for years now.

Threat model is everything

This all may sound scary, and arguably it is. Assuming the most powerful adversary is a common mistake new ppl make in OPSEC so carefully evaluate what attacks your specific adversary is capable of/willing to execute.

Here is my assesment:
Mac address deanonymication: Active deployment, cheap easy. Everybody can do this and corpos do this already.

Wifi probe deanonymization: Active deployment, cheap, easy. Everybody can do this and corpos do this already.

Hardware imperfections: No known deployment in an industrial setting. I would say this is more private investigator and higher adversary stuff.

Looking through walls:
Batshit sci-fi crazy. LE stuff. If you have an open source project you know of, pls let me know!

Closing notes

If you have more ideas/info on how to deanonymize or fingerprint with wifi, please let me know!
More fun trivia about wifi welcome!
Did i miss something important or made a mistake? Pls tell me!

3 Likes

Preventing Active WiFi Probing

Most secure solution(s) for wireless capabilities with Qubes

Benefits/drawbacks of a travel router alongside QubesOS for those on the move

After reboot wifi password forgotten

After reboot wifi password forgotten

KarlinQubes 2 April 18, 2022, 12:21pm

Fantastic post.

I had never heard about Wifi probes, but this makes total sense as a massive leak of metadata.
Thank you for bringing this to my attention.

2 Likes

---

oijawyuh 3 April 18, 2022, 1:16pm

> Suspicious_Actions:
>
> Only activate wifi if you really need it.

To disable wifi by default on boot, one option is to add a command to rc.local to disable it.

Run in sys-net terminal the following:
`sudo gedit /rw/config/rc.local`

If sys-net is disposable, then run the command in the Disposable Template (the underlying template for sys-net). If `gedit` is not installed, use another editor such as `nano`.

Then add the following text to `rc.local` and save:

```
sudo nmcli radio wifi off
```

This will disable the wifi on boot. It can be enabled easily via the Network Manager (check box).

4 Likes

*****débutant*** quelque problème préliminaire à régler**

Johnboy 4 April 18, 2022, 3:04pm

Randomizing your hostname is also a nice feature, not just for wifi:

Qubes-Community/Contents/blob/master/docs/privacy/anonymizing-your-mac-address.md

```
Anonymizing your MAC Address
============================

Although it is not the only metadata broadcast by network hardware, chang
Currently, Qubes OS *does not* automatically "anonymize" or spoof the MAC


## Upgrading and configuring Network Manager in Qubes

Newer versions of Network Manager have options for randomizing MAC addres
In particular, versions 1.4.2 and later should be well suited for Qubes.
However, use of the NetworkManager GUI to set these options is **unreliab
You should check carefully that any settings you make in the GUI are save
If the settings are not saved, you can use the method described below usi


Network Manager 1.4.2 or later is available from the Fedora 25 repository

Check that Network Manager version is now at least 1.4.2:
```

This file has been truncated. **show original**

2 Likes

---

disp-forum-account-q 5 May 4, 2022, 9:13am

With the edits to disp-vm which serves your disp-sys-net:

Do we need to create a new template and edit that to preserve the original state of our original disp-vm of choice?

If we apply Mac randomizations and/or hostname witholding/randomizations to the same disp-

vm which creates all of our disp-app-vms, will there be any sudden networking issues between disp-app-vms and disp-net-vms?

If not, why isn't this an issue? Is there some policy or address translation or whatever that I should get my headaround to understand the qube sinfrastructure better?

Keywords, homework, things to read, please

1 Like

Suspicious_Actions 6 May 4, 2022, 9:28am

> disp-forum-account-q:
>
> Do we need to create a new template and edit that to preserve the original state of our original disp-vm of choice?

It you want, i did that.

> disp-forum-account-q:
>
> If we apply Mac randomizations and/or hostname witholding/randomizations to the same disp-vm which creates all of our disp-app-vms, will there be any sudden networking issues between disp-app-vms and disp-net-vms?

I don't think so, but have not tried this.

> disp-forum-account-q:
>
> If not, why isn't this an issue? Is there some policy or address translation or whatever that I should get my headaround to understand the qube sinfrastructure better?

This would change the mac addresses of your virtual network interfaces and the hostname. Neither of those are really important for the netvm to deliver networking (i think).

1 Like

---

disp-forum-account-q 7 May 4, 2022, 9:46am

So my goal is to create a new *service* qube, specifically 'sys-net-disp-random'.

'sys-net-disp-random' will always randomize MAC address and host names. This will replace sys-net in most instances, but i'd like to maintain sys-net for rare use cases.

For these randomisations to always happen in 'sys-net-disp-random', they need to be spawned from template 'sys-net-random-template' which has the required scripts.

Have successfully created both the above mentioned: 'sys-net-disp-random' & 'sys-net-random-template'.

But I cannot change template vm of ‘sys-net-disp-random’ to ‘sys-net-random-template’.

‘Sys-net-disp-random’ is still bound to ‘debian-11-dvm’.

What do now?

(I tried creating a new topic but i’ve hit my limit for a new user, I still think it’s related to wifi OPSEC: I can’t implement the policies if I can’t make the new template/service qubes work)

1 Like

---

unman 8 May 5, 2022, 11:07am

These are good questions which will get lost in this thread.
Open TWO new threads, one for each question.

1 Like

---

disp-forum-account-q 9 May 6, 2022, 9:27am

Qubes-Community/Contents/blob/master/docs/privacy/anonymizing-your-mac-address.md

```
Anonymizing your MAC Address
============================

Although it is not the only metadata broadcast by network hardware, chang
Currently, Qubes OS *does not* automatically "anonymize" or spoof the MAC


## Upgrading and configuring Network Manager in Qubes

Newer versions of Network Manager have options for randomizing MAC addres
In particular, versions 1.4.2 and later should be well suited for Qubes.
However, use of the NetworkManager GUI to set these options is **unreliab
You should check carefully that any settings you make in the GUI are save
If the settings are not saved, you can use the method described below usi


Network Manager 1.4.2 or later is available from the Fedora 25 repository

Check that Network Manager version is now at least 1.4.2:
```

This file has been truncated. **show original**

Permission Issues when creating .conf file

I appreciate this isn't a qubes specific question, but i'm sure people reading here could benefit from it.

Action: Write the settings to a new file in the `/etc/NetworkManager/conf.d/` directory, such as `00-macrandomize.conf`.

Issue: 'Permission Denied'

Question: Why am I having permissions issues in a templatevm with passwordless root? Isn't that sorta the point of passwordless root? Do I need to set about creating a user in my template just to work around this and assign permissions to that user?

Posted above question to new topic

1 Like

Suspicious_Actions 10 May 6, 2022, 9:46am

Iam happy to help you with this problem, but please create another topic for this.

This topic is about OPSEC considerations when using wifi.

1 Like

---

uesqoho998 11 November 4, 2022, 11:15pm

I've got a question related to this, I made it in its own topic.

> **Preventing Active WiFi Probing**
>
> This is a follow up to this great post **OPSEC considerations when using wifi** I am trying to confirm that using a disposable sys-net will avoid this active WiFi probing from happening. Being a disposable I don't need to worry about NetworkManager storing SSIDs to perform the active probing, but my biggest concern is the possibility that the WiFi chip/physical device would ever cache SSIDs on the hardware itself. I can't find much information on this, is it something that is possible or do WiFi c…

Please answer if you area able to.

Quben 12 November 5, 2022, 12:27am

Imagine not using a $5 usb-to-ethernet dongle from amazon

1 Like

uesqoho998 13 November 5, 2022, 4:48am

Imagine thinking $5 hardware is secure.

1 Like

Karrie 14 April 18, 2023, 8:56pm

I didn't even know about some of this. Seeing through walls is some intense stuff right there. More reasons why I use Ethernet whenever possible. WiFi is so convenient, but that's part of why it's dangerous. Encrypt all network traffic (Whonix or VPN depending on task) and then your attacker has to either be your ISP (or friendly with them) or in your router. Even then, they're getting usage metadata. Sure, that's not great. But we can't do much about it.

A bit off topic, but that's why I don't like router-level encryption. At least, I don't like relying on that alone. Unless you check in on it all the time and know how to detect a compromise, you're pwnd.