leveraging private APNs for mobile network traffic analysis

2024-08-09 | DEF CON 32 | Aapo Oksman

aapo (oksman)

Founder @ Juurin Oy

- IoT Cybersecurity consulting
- Security research
  - IoT / Devices
  - Cryptography
  - Network protocols

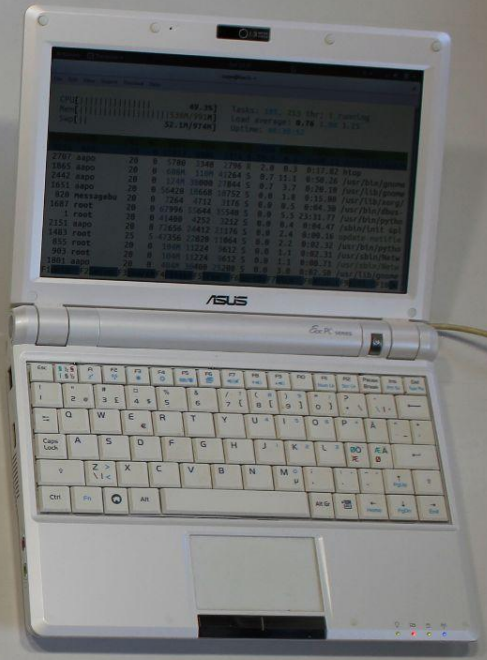
Bug Bounty

- aapo @ HackerOne/Bugcrowd/Intigriti

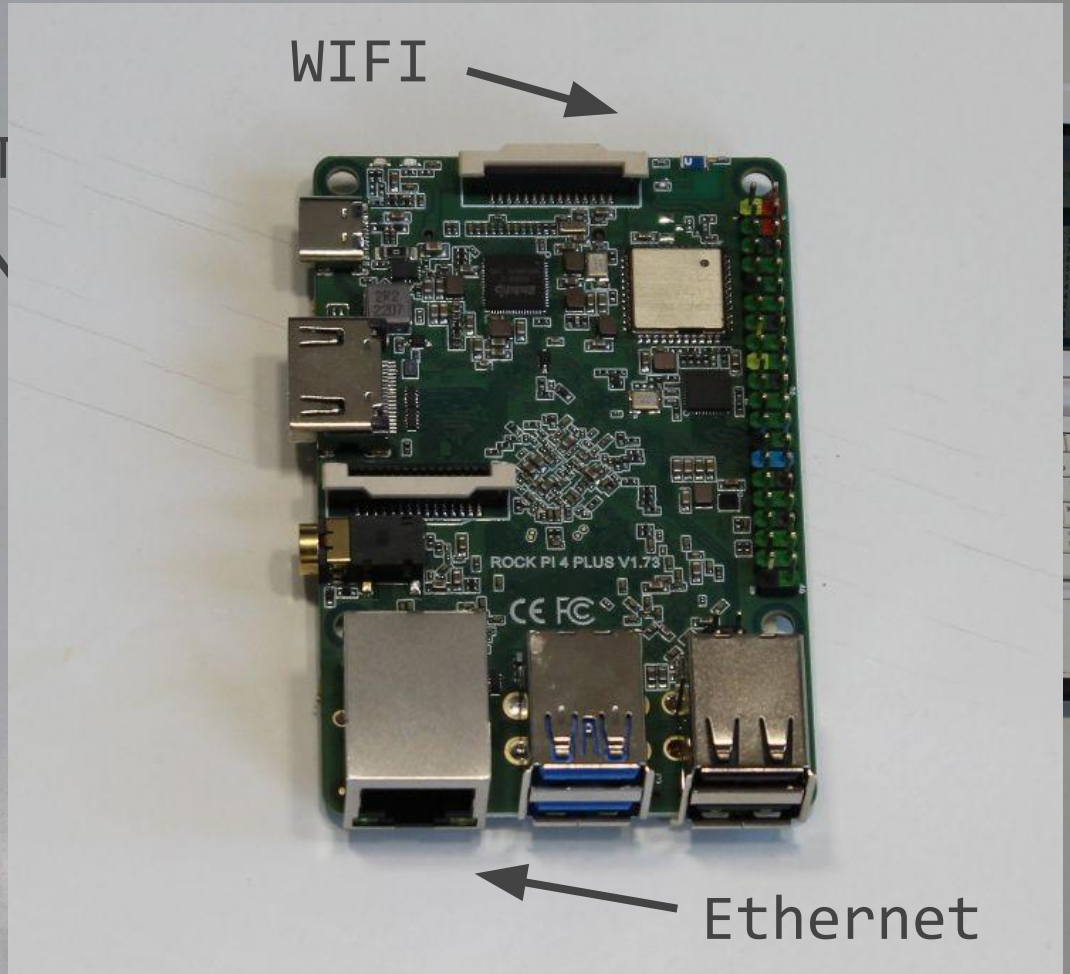
ECSC Team Finland Coach

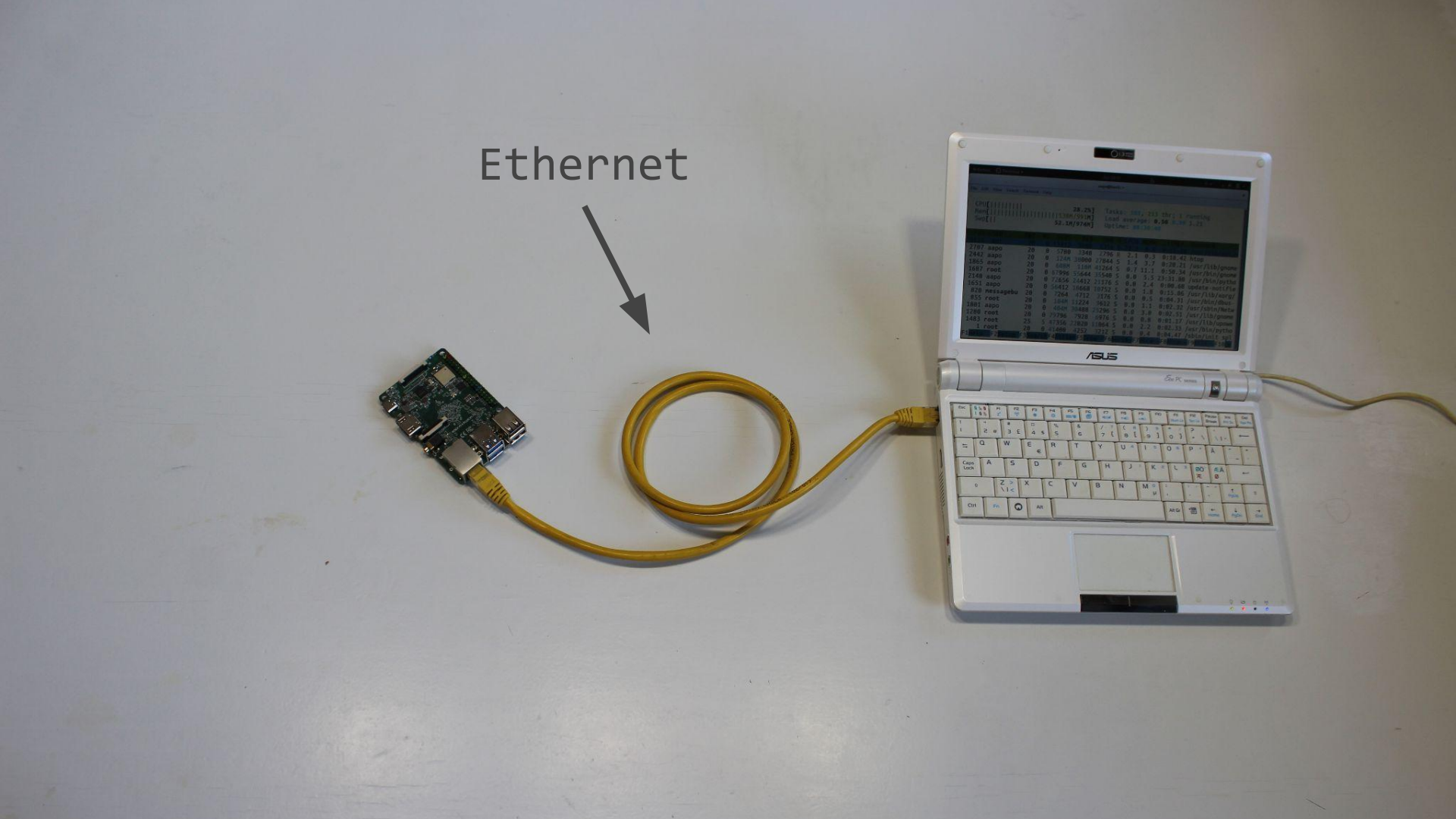
IoT

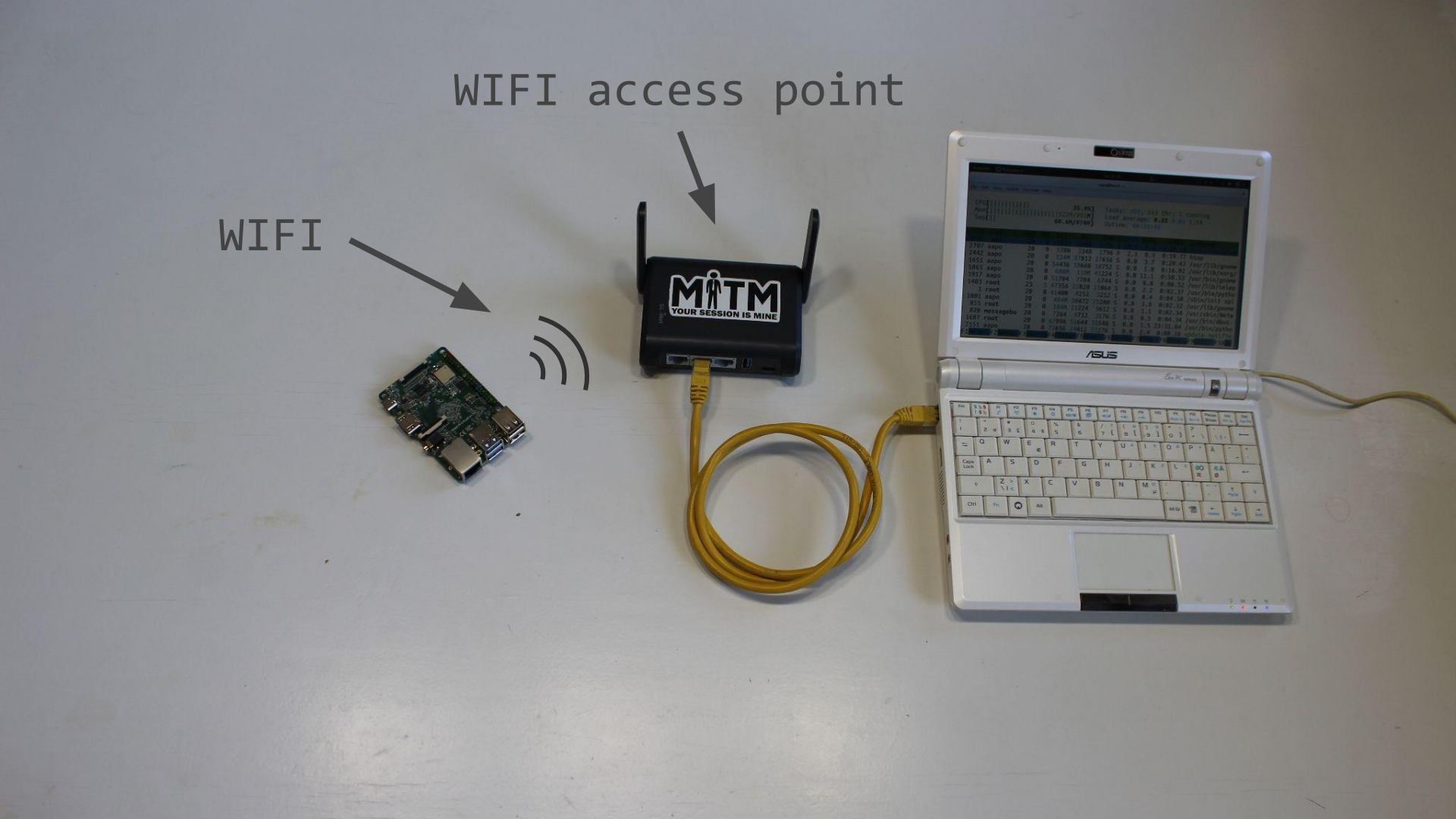
me



IoT



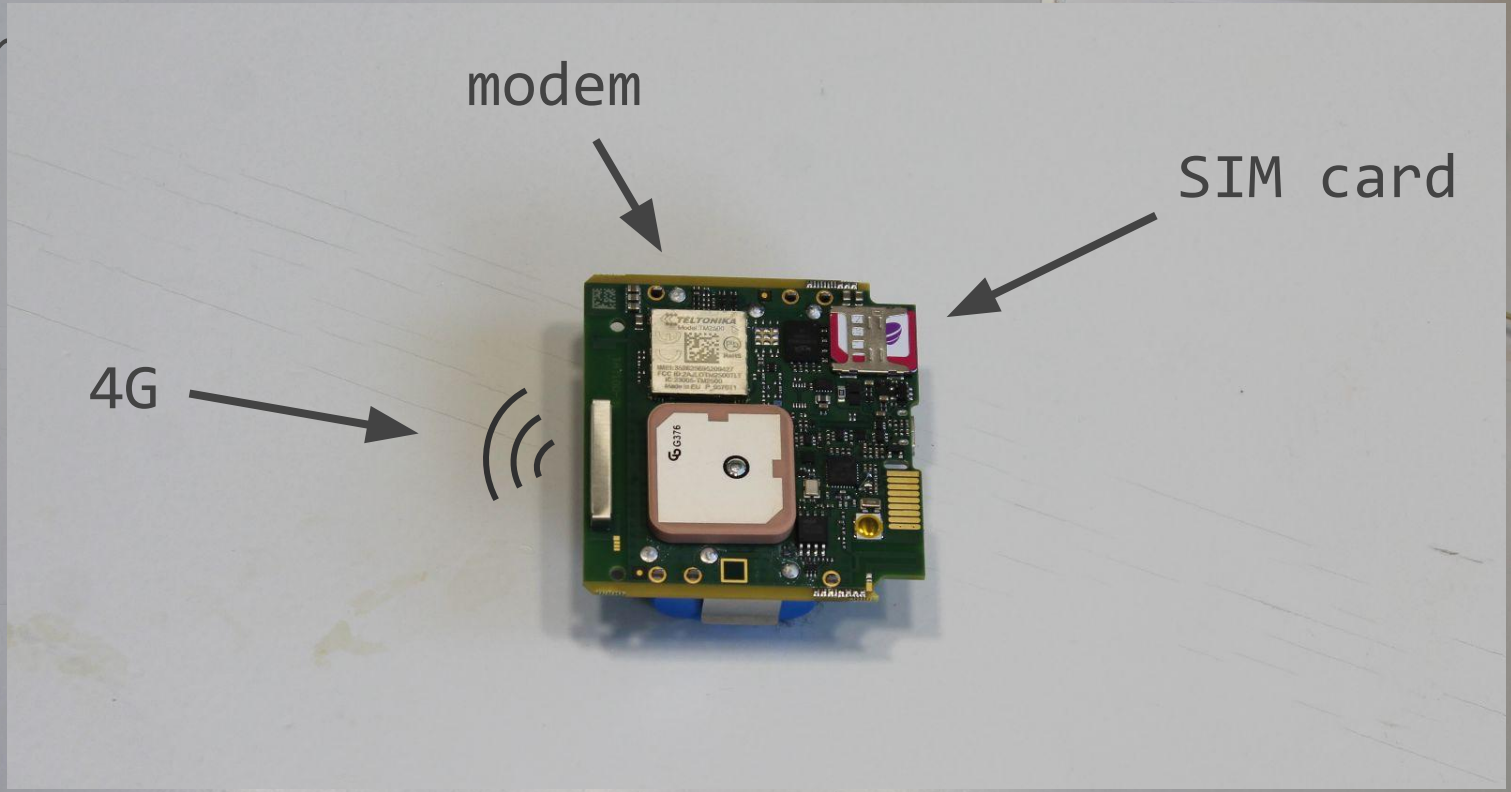

Ethernet


WIFI access point
WIFI
MiTM
YOUR SESSION IS MINE
ASUS

Industrial IoT (IIoT)

me

Ir



is there traffic over 5G as well?

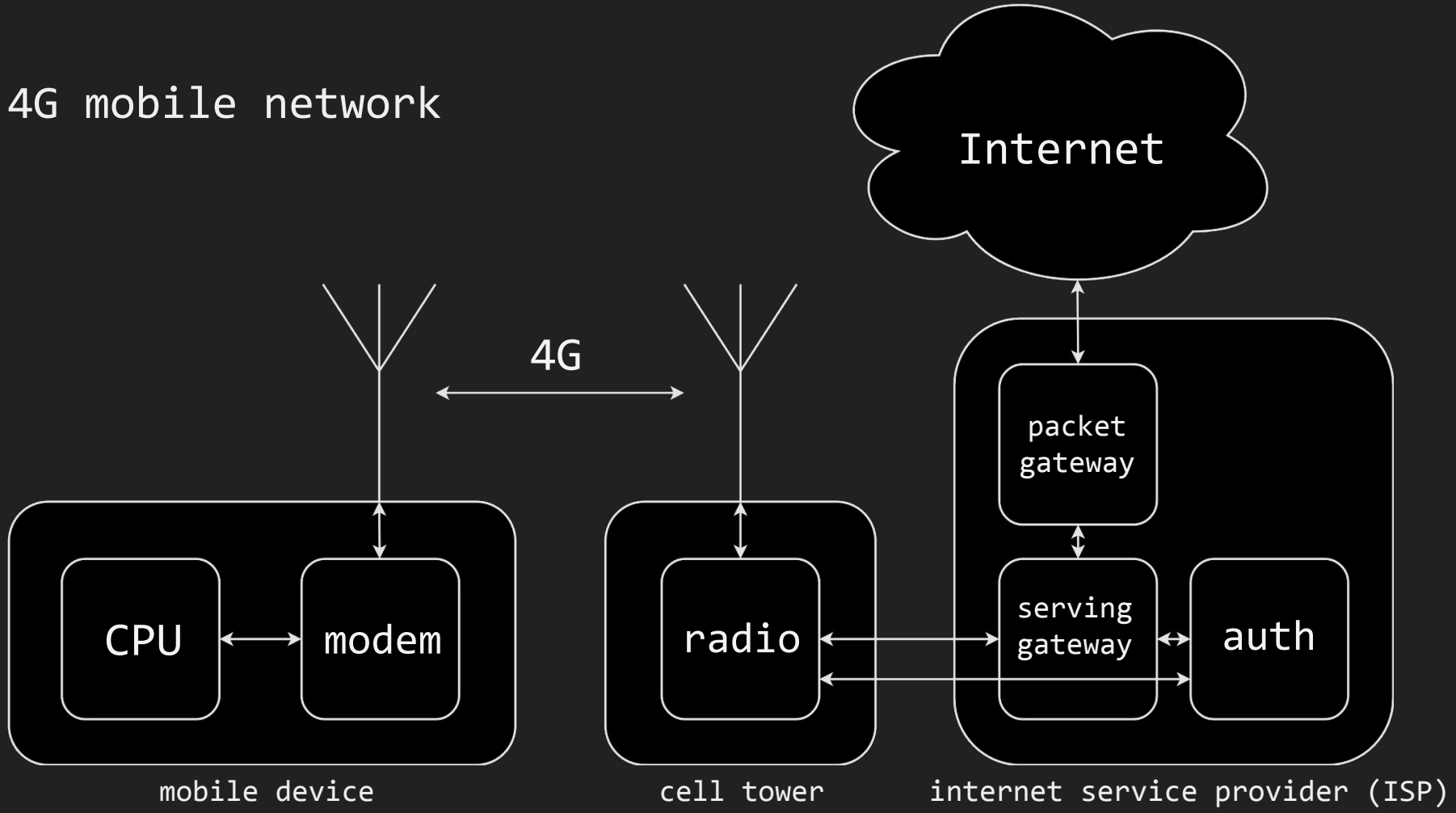
why look into mobile network traffic?

- Curiosity and privacy
  - where do my devices talk to?
- Offensive security
  - can we tamper with the traffic and find vulnerabilities?
- Defensive security
  - can we detect malicious traffic or filter unwanted traffic?

how do mobile networks work?

- different flavors
  - 2G, 3G, 4G (LTE, NB-IoT), 5G, etc.
  - multiple different frequencies and special radios for each
- ISP operated mobile networks
  - massive amount of base stations covering wide areas
  - SIM cards for authentication
- used to route IP traffic from devices to the Internet
- implemented on devices as a separate HW module

4G mobile network



intercepting mobile network traffic

0) intercept the traffic on the device

- simply tcpdump the traffic

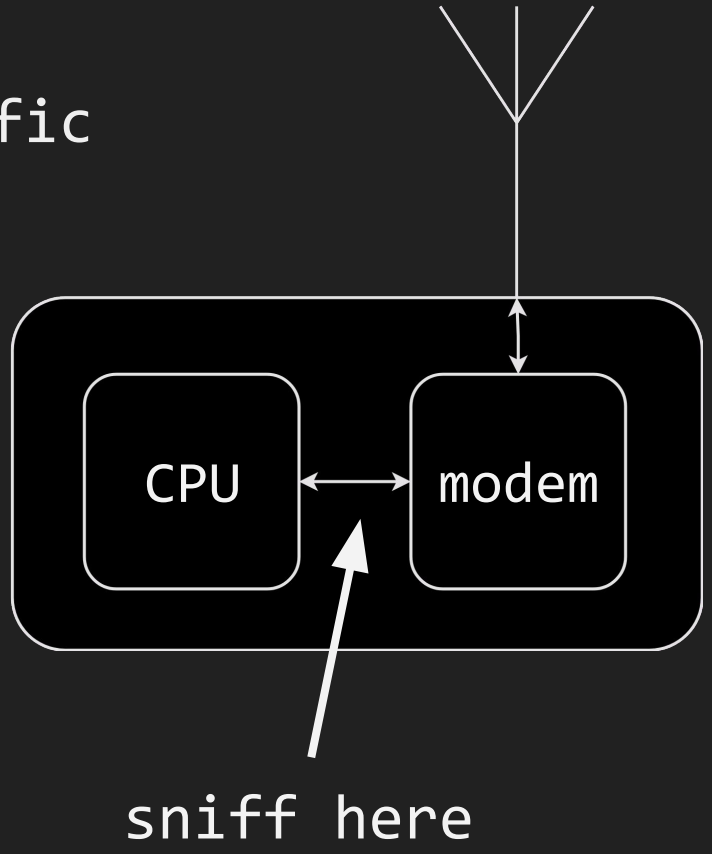
- requires root access to the device
- does not show modems own traffic

```
# id
uid=0(root) gid=0(root) groups=0(root)
# tcpdump -n -i ens3
tcpdump: verbose output suppressed, use -v[v]... f
or full protocol decode
listening on ens3, link-type EN10MB (Ethernet), sn
apshot length 262144 bytes
16:49:23.687056 IP 10.30.45.231.22 > 10.30.45.189.
34614: Flags [P.], seq 2172549464:2172549644, ack
3661018362, win 501, options [nop,nop,TS val 78503
0353 ecr 722622630], length 180
16:49:23.687110 IP 10.30.45.189.34614 > 10.30.45.2
31.22: Flags [.], ack 180, win 1841, options [nop,
nop,TS val 722623260 ecr 785030353], length 0
16:49:23.688019 IP 10.30.45.231.22 > 10.30.45.189.
34614: Flags [P.], seq 180:248, ack 1, win 501, op
tions [nop,nop,TS val 785030354 ecr 722622630], le
ngth 68
16:49:23.688019 IP 10.30.45.231.22 > 10.30.45.189.
34614: Flags [P.], seq 248:548, ack 1, win 501, op
tions [nop,nop,TS val 785030354 ecr 722622630], le
ngth 300
16:49:23.688041 IP 10.30.45.189.34614 > 10.30.45.2
31.22: Flags [.], ack 248, win 1841, options [nop,
```

1) intercept CPU to modem traffic

- AT commands over serial
  - “make connection 1 to ‘google.com’ port 80”
  - “send ‘GET / HTTP/1.1’ to connection 1’
  - “connection 1 received data ‘HTTP/1.1 200 OK’”
- decode the data from serial traffic or replace the modem with a software based simulator

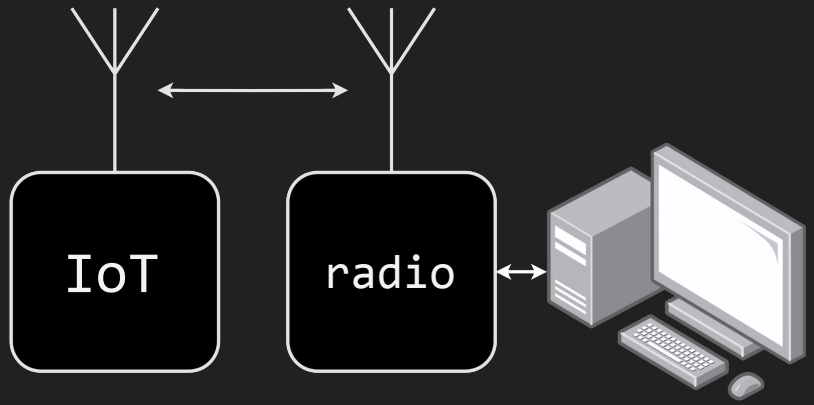
- requires HW reversing and soldering
- some modems require complex setup
- does not show modems own traffic



ref: https://github.com/juanmitaboada/modemsimul

2) run your own base station

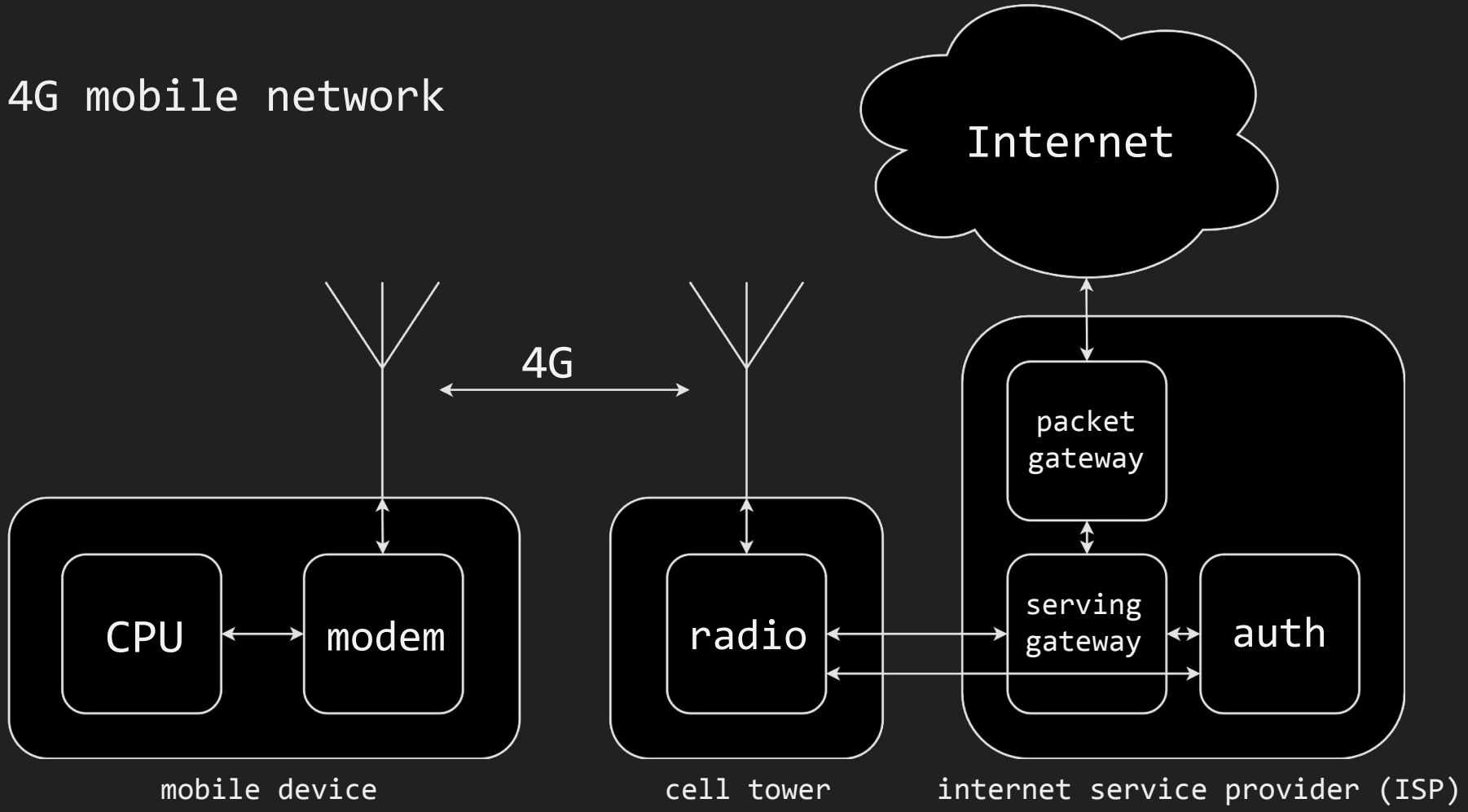
- buy/build a base station
- software defined radios (SDR) are relatively cheap and open source software exists



- basic setup is around $1000 and a week of work to get running
- commercial solutions are _really_ expensive
- illegal to run without a Faraday cage
  - some frequency bands can be licensed
- tied to one physical location

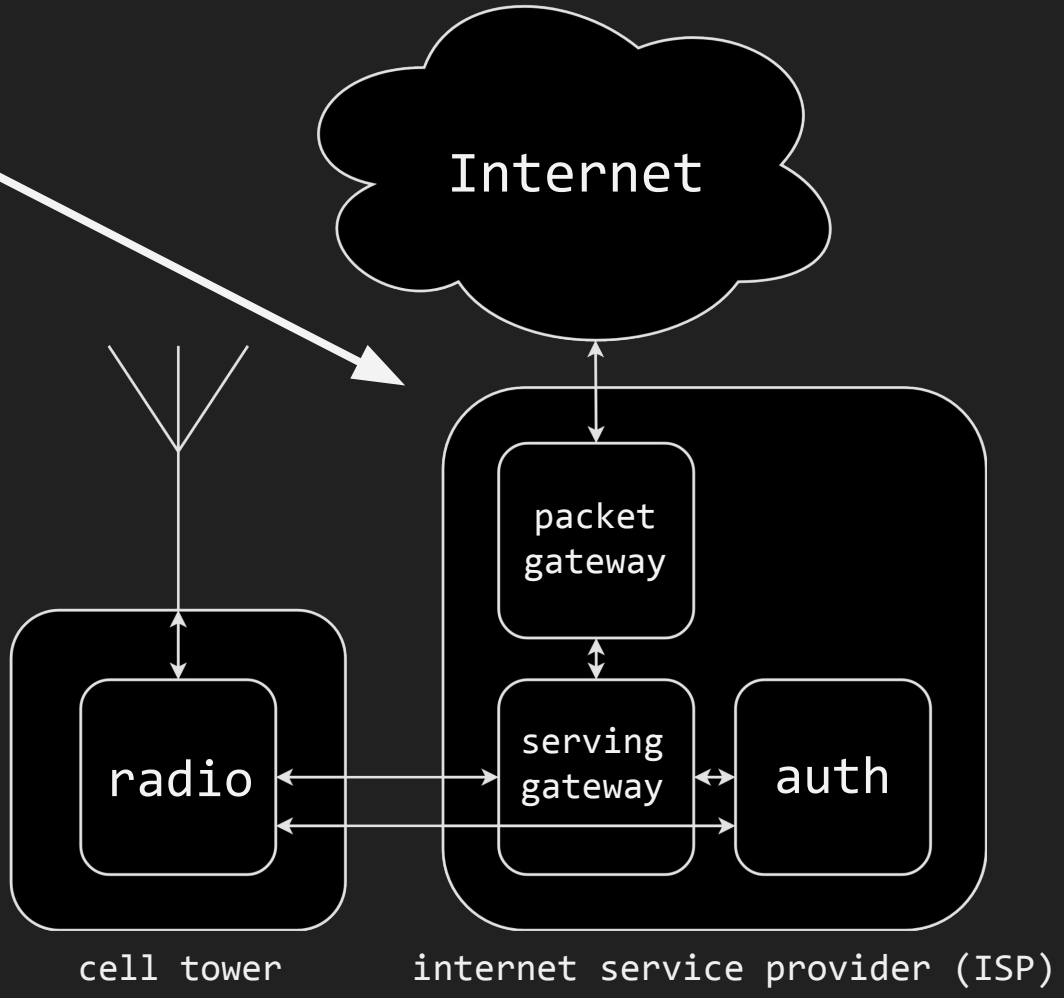
ref: https://librecellular.org

4G mobile network



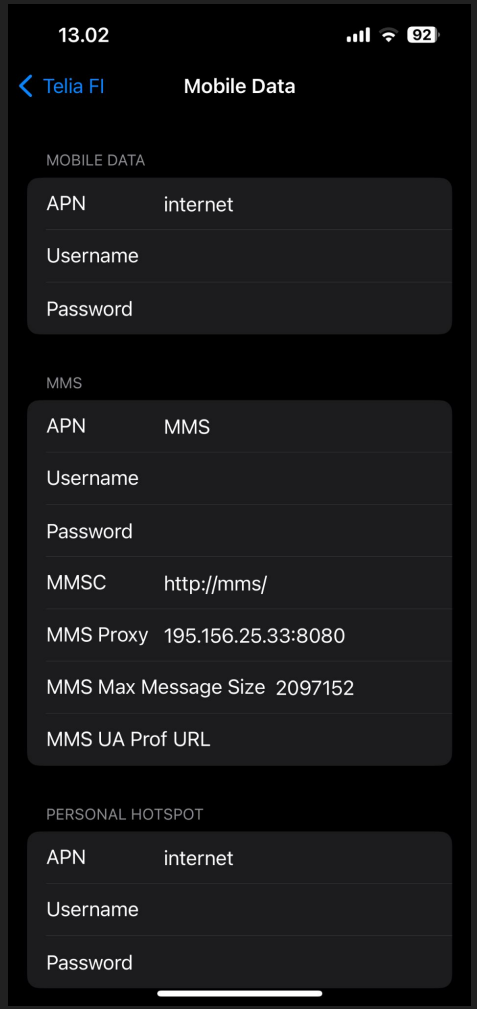
what happens there?

- device authentication with SIM cards
- packet filtering
  - “lawful interception”
- policy enforcement
- billing calculation
- packet routing
  - packets can be routed also internally!
  - APNs!



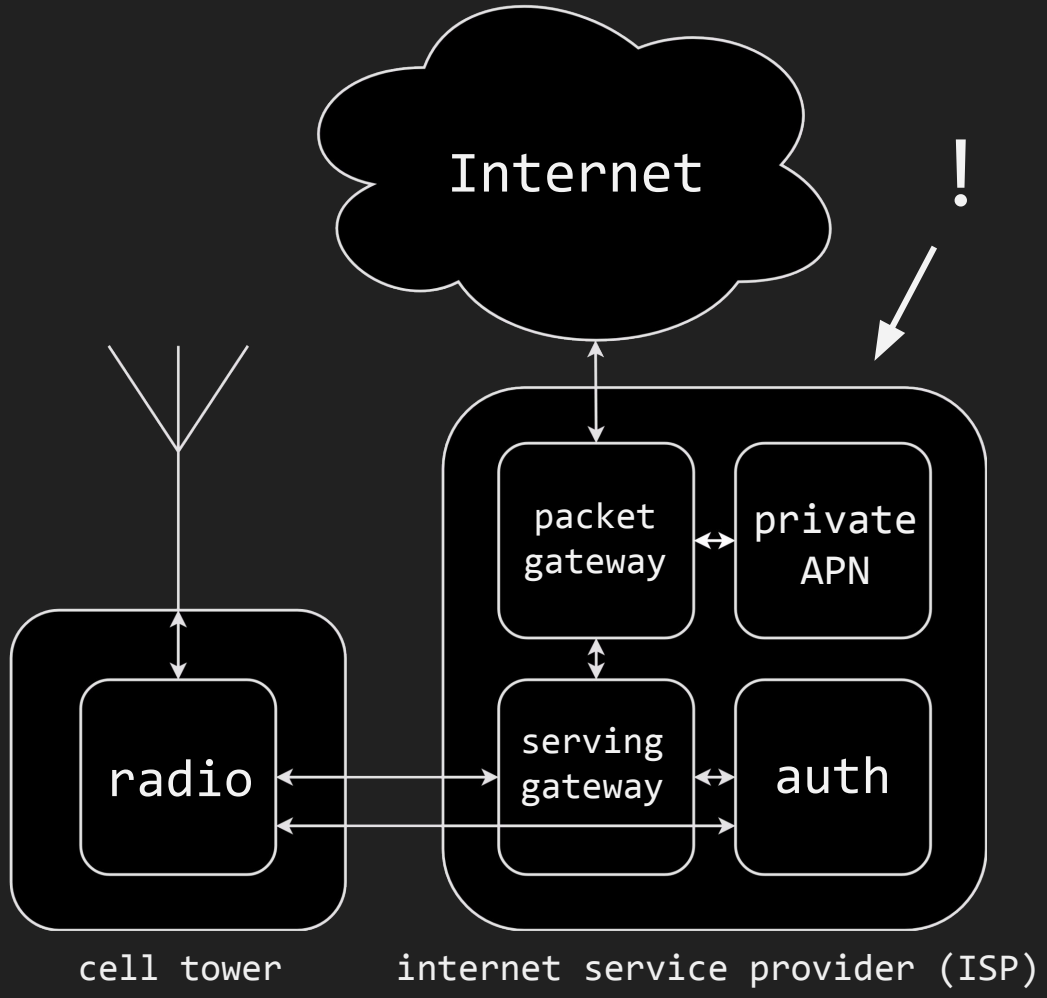
access point names (APNs)

- tells the ISP how to route your packets
- can be pushed to the device from ISP
- manual configuration possible on the device
- device APN setting might not be respected by the ISP



private APNs

- offered by ISPs for connecting mobile devices to private networks
- routing and filtering is configurable
  - allows for direct connections between devices
  - does not filter traffic by default
  - can be configured to route to the Internet or somewhere else



could I get a private APN?

could I get a private APN?

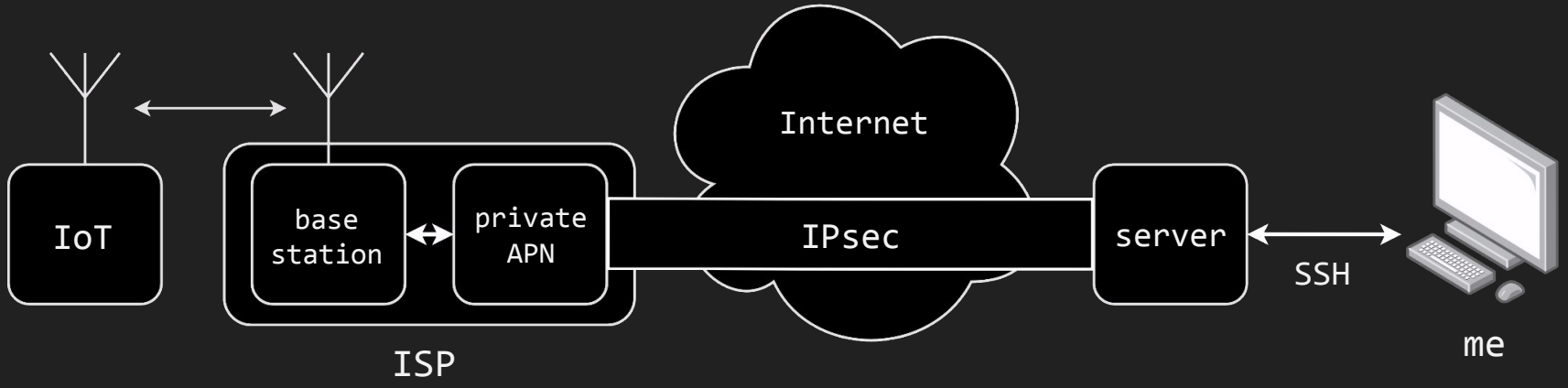
- huge variance in price and usability between ISPs
  - “contact us for pricing”
    - “$3000 engineering fee and $500 monthly fee”
  - “can be activated from our self service portal”
    - “$100 setup fee and $150 a month”
      - $250 a day/week/month, $1900 for a year
    - “$10 setup fee and $0.75 per hour”
      - $30 for a day, $100 a week, $6580 for a year
- differences in global/US/EU coverage
- differences in available data plans
  - (you still have to pay for your data subscriptions)

configuring a private APN

- (disable traffic filtering)
- disable routing to the Internet
- site-to-site VPN between the private APN and a cloud server
- cloud server as the default gateway for the network
- add mobile devices to the private APN
  - some ISPs require you to set the APN settings on the device
  - some ISPs can force the device to join the private APN

- profit?

POC

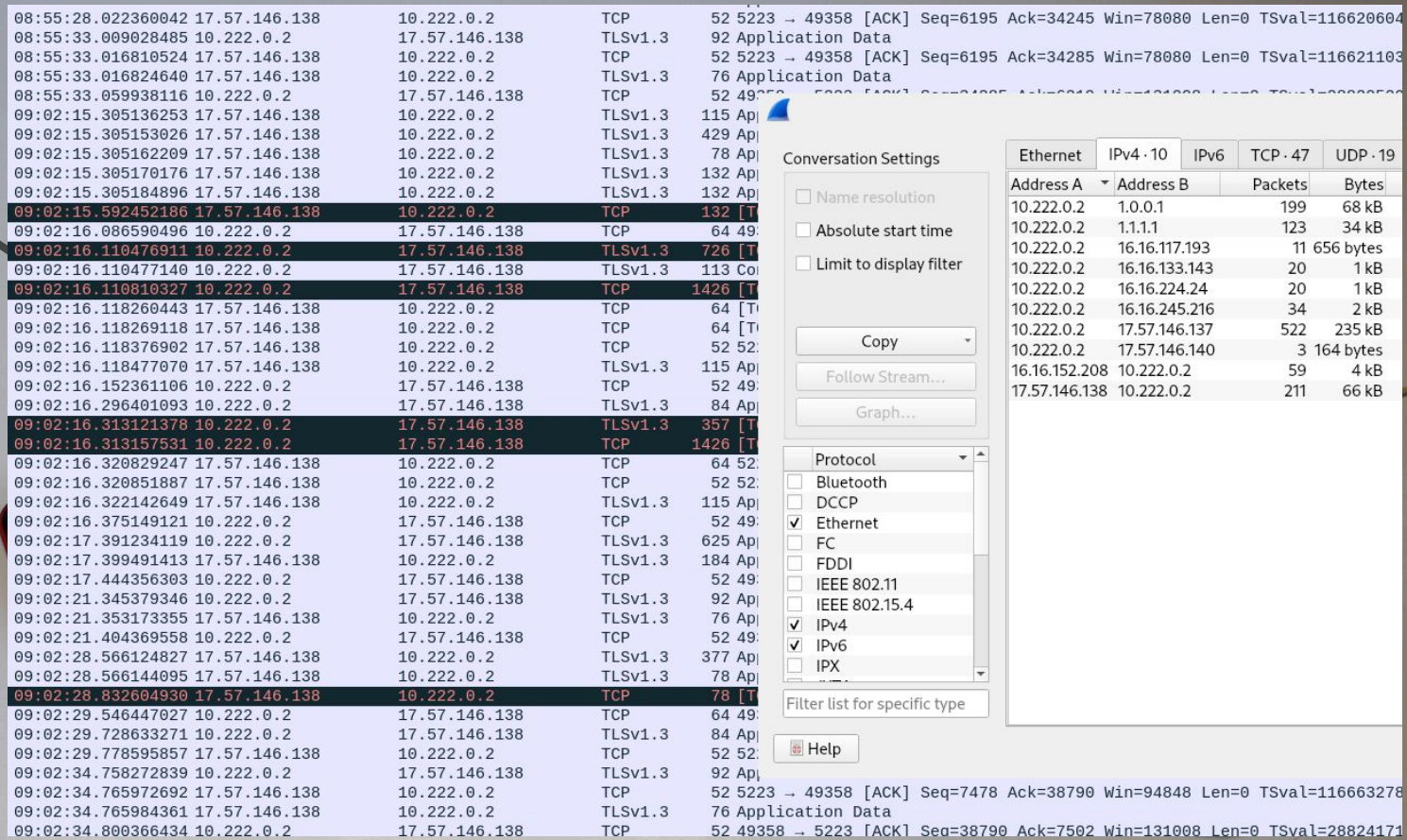

IoT
base station
private APN
ISP
Internet
IPsec
server
SSH
me

demo

is there traffic over 5G as well?

WIFI

?

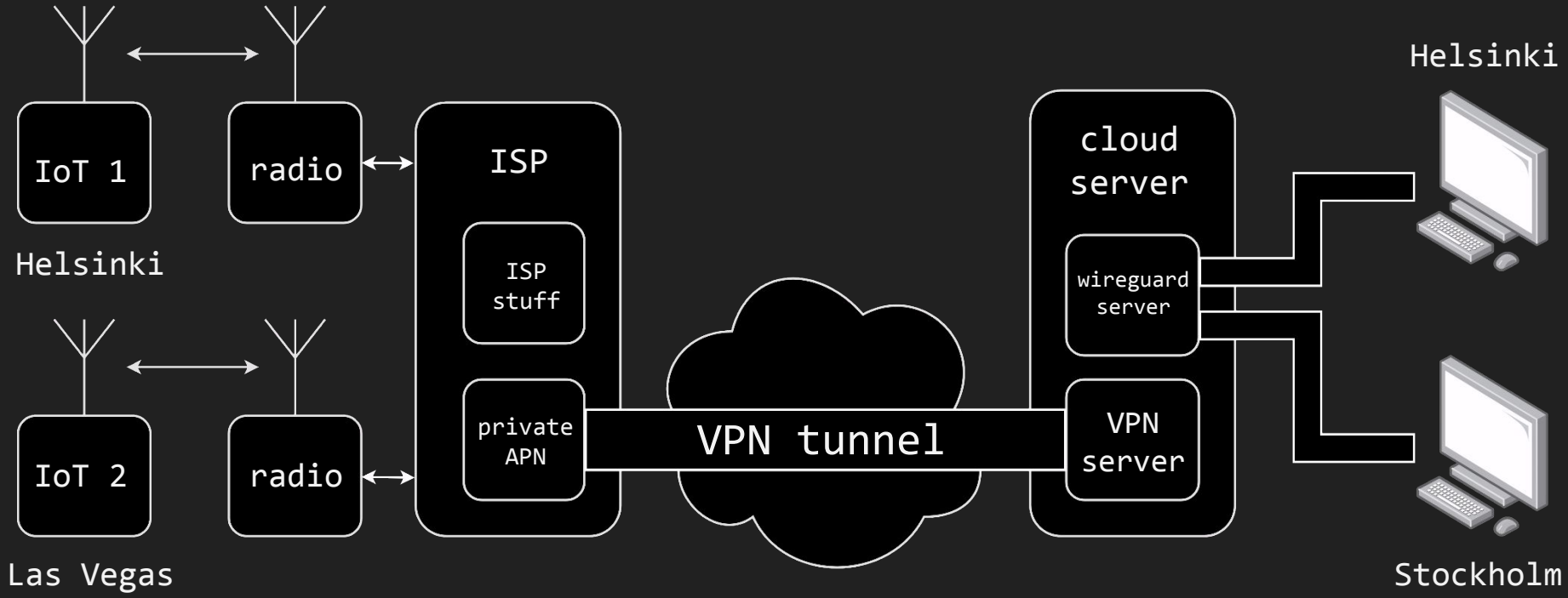


is there traffic over 5G as well?

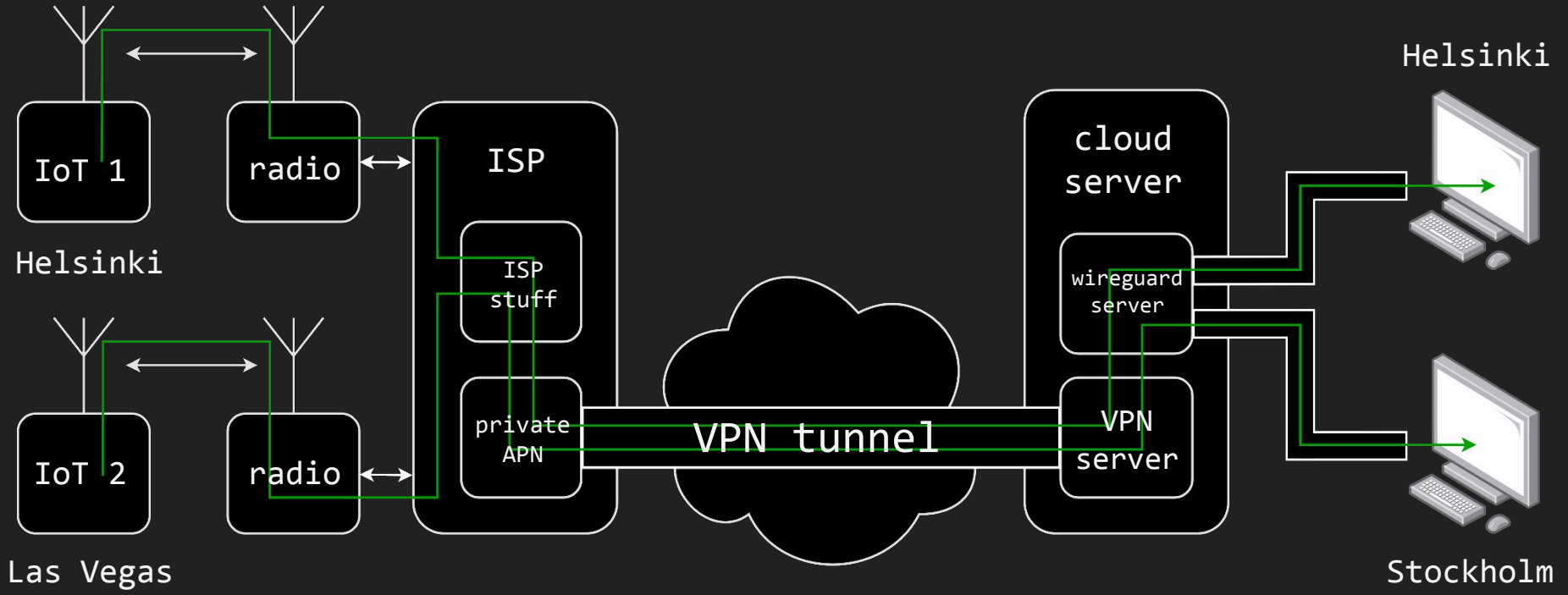
from POC to project

- collaborating with IoT security experts
  - others have had the same exact problems
- looking into the US, EU and global ISPs
  - many ISPs and companies offer affordable private APNs
- creating a platform to share up-to-date information on how to set up this setup in your country
  - https://github.com/AapoOksman/PrivateAPN

https://github.com/AapoOksman/PrivateAPN



https://github.com/AapoOksman/PrivateAPN



https://github.com/AapoOksman/PrivateAPN

Private APNs

Mobile devices connect to the Internet using mobile networks provided by Internet Service Providers (ISPs). The devices connect to the ISP mobile networks with Access Point Names (APNs) that is usually just "Internet" and just connects the device directly to the Internet.

Many ISPs have begun offering private APNs to allow you to have a private network inside the ISP infrastructure. By renting a private APN and redirecting all device traffic to your own server, you can easily intercept and tamper with mobile device network traffic.

This repository has instructions and tools on how to do this.

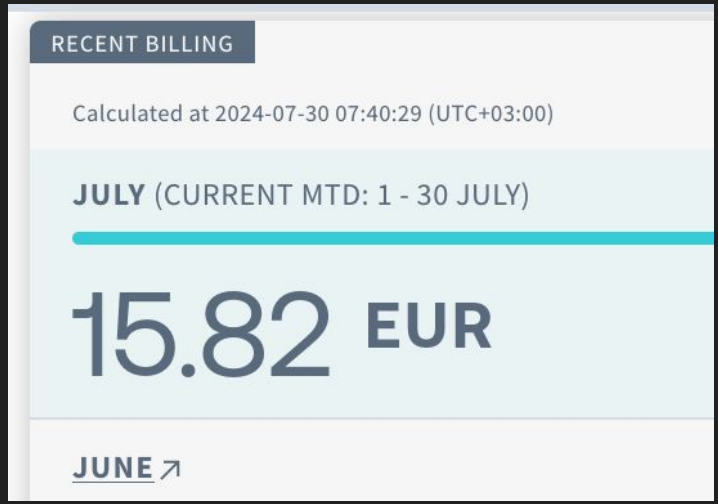
Private APNs offered by ISPs

ISP	Private APN cost	Country	Data cost	Network operator	Can force APN settings?	Notes
Telia	100€ setup + 140€/month	EU(/Global)	???	???	No, APN settings must be set on SIM/device	Not thoroughly tested outside Finland
Telia	100€ setup + 140€/month	Finland	5€/month for slow, 1.5€/day when used for fast	Telia	Yes, if set on the private APN configuration	
Soracom	$10 setup + $0.75/hour	Global	Soracom carriers & pricing	Soracom carriers & pricing	No, APN settings must be set on SIM/device	Some network operators don't seem to need proper APN settings, See "Soracom Finland". Not thoroughly tested outside

wrapping up

Curiosity & privacy

- "where do my devices talk to?”
- 50$ for couple days of tinkering on a device is not a bad deal for anyone
- at $150 a month hackerspaces and even tiny penetration testing companies can get access to mobile network traffic



Offensive security

- “can we tamper with the traffic and find vulnerabilities?”
- a must for any penetration testing company and IoT researcher
  - $2000 a year vs. a possibly illegal setup that requires a week to get working
- devices communicating over mobile networks are everywhere and they have got away with less scrutiny in the past
  - maybe even some new attack vectors for high security devices?

Defensive security

- “can we detect malicious traffic or filter traffic?”
- the private APN can be connected to an existing firewall
- can be affordably scaled to thousands of devices
- mobile phone malware infections might not communicate at all over VPN or WIFI
  - analyzing the mobile network traffic is a must for companies and entities targeted by advanced malware

aapo (oksman)

find the project details @

https://github.com/AapoOksman/PrivateAPN

find me @

- DEF CON
- aapo.oksman@juurin.fi
- linkedin.com/in/AapoOksman
- aapo @ bug bounty