

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

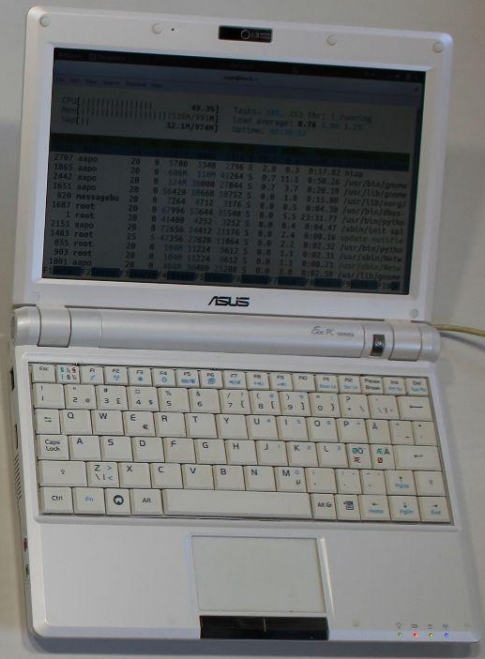
ECSC Team Finland Coach



IoT



me



IoT

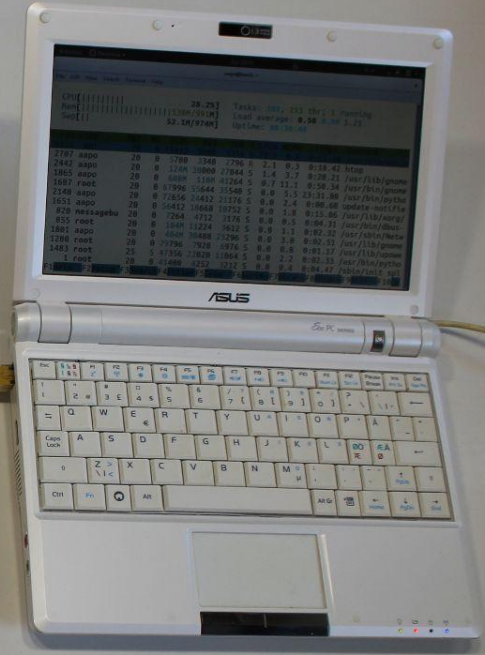
WIFI



Ethernet



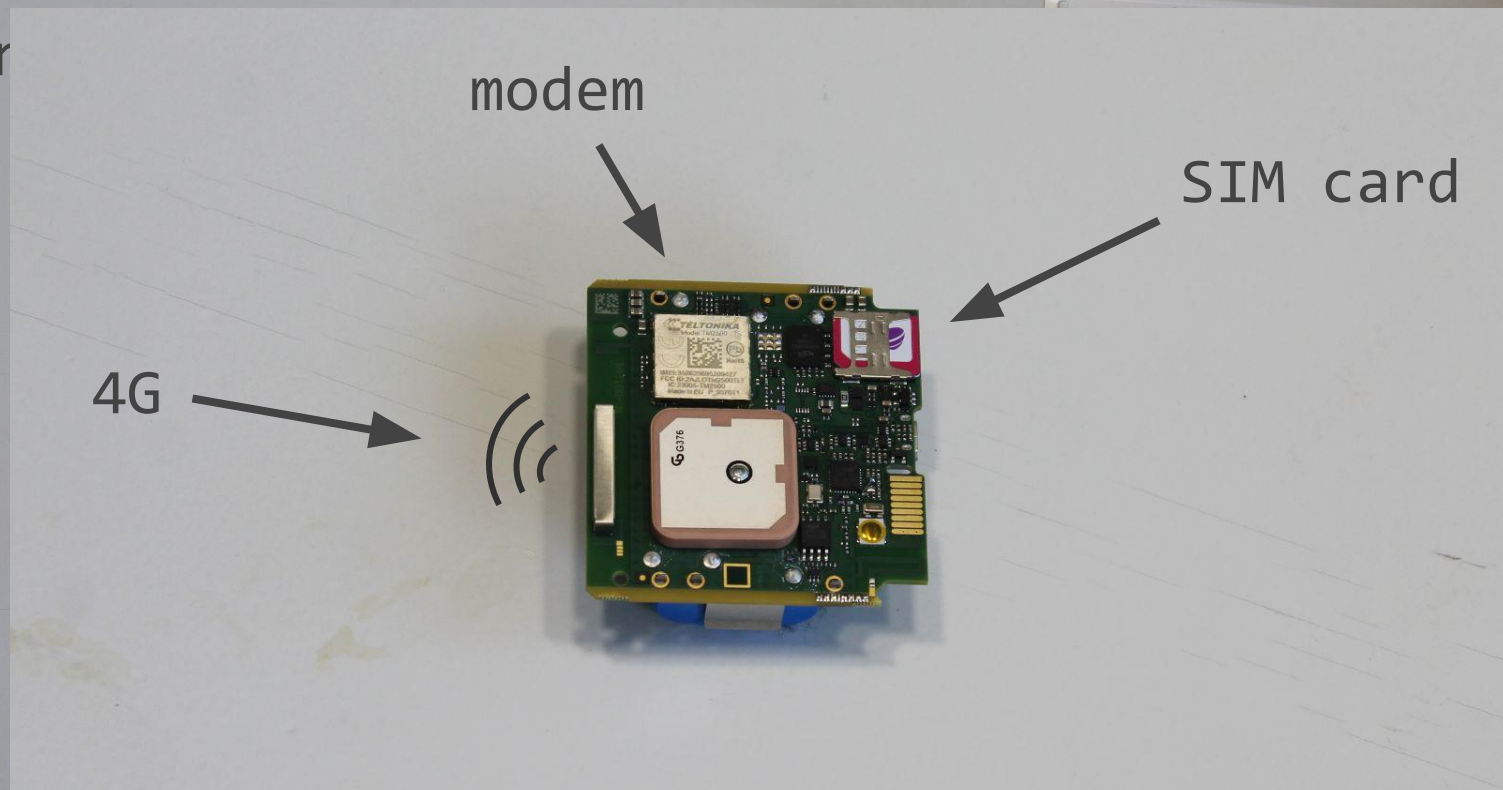
Ethernet







Ir



WIFI



?



is there traffic over 5G as well?

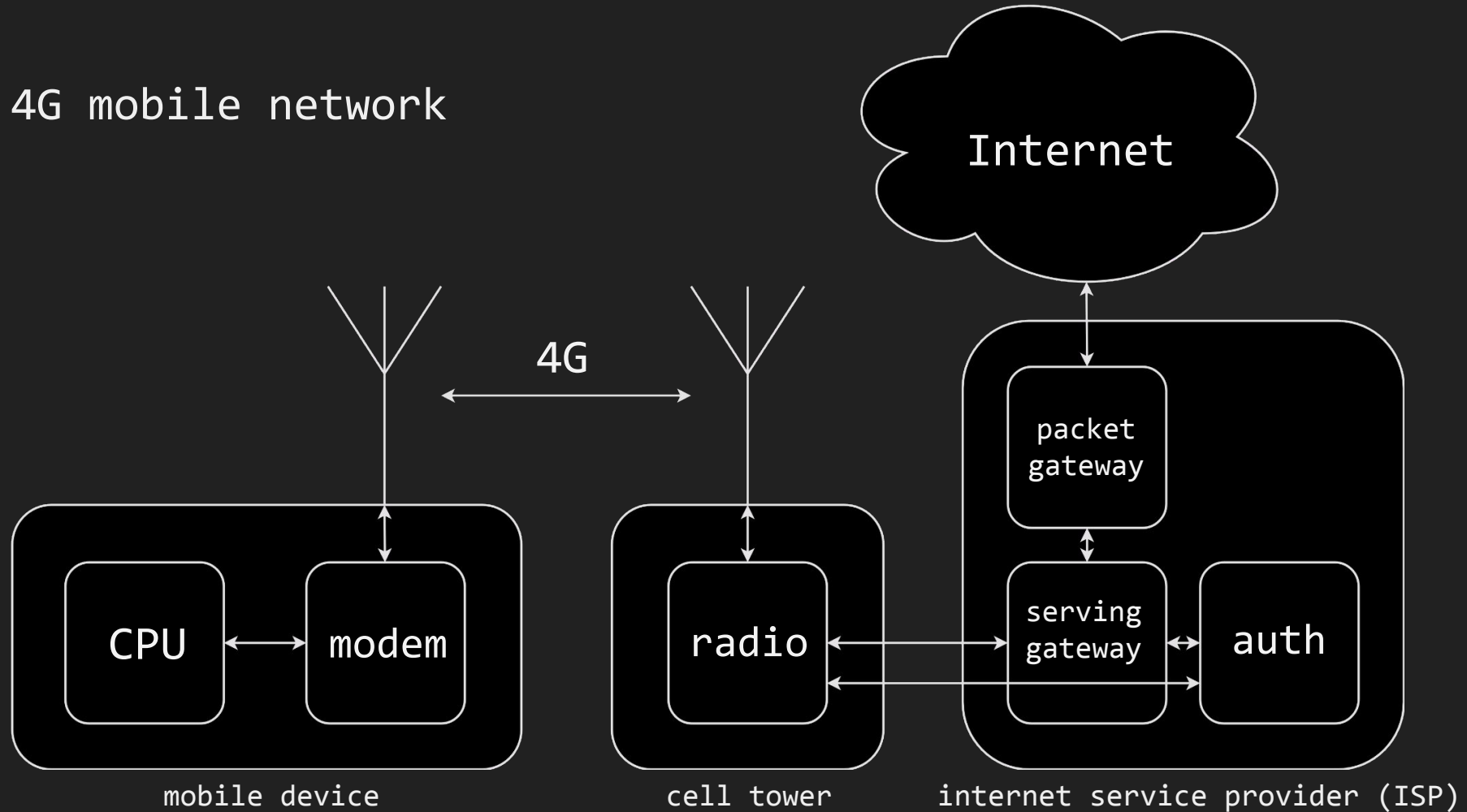
why look into mobile network traffic?

- 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

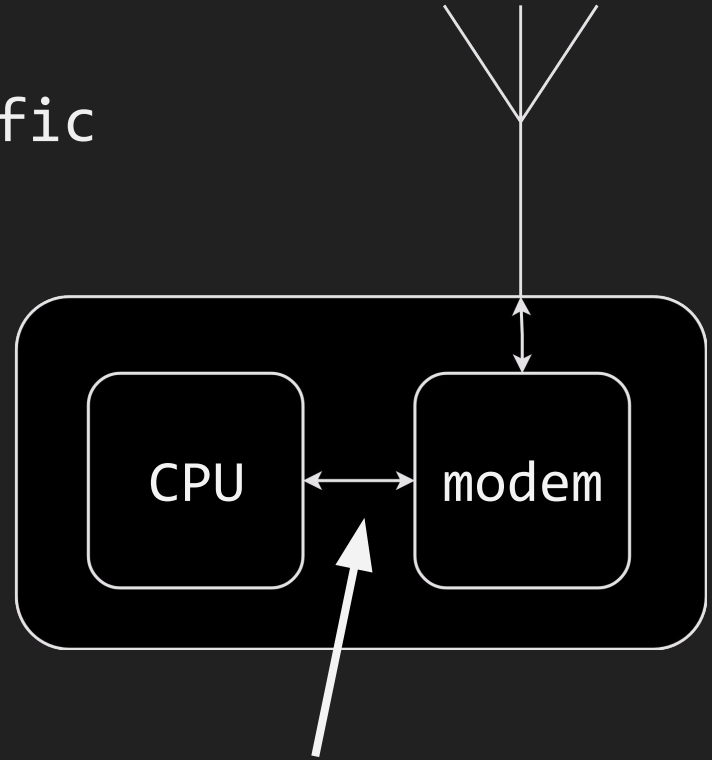
0) intercept the traffic on the device

- 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

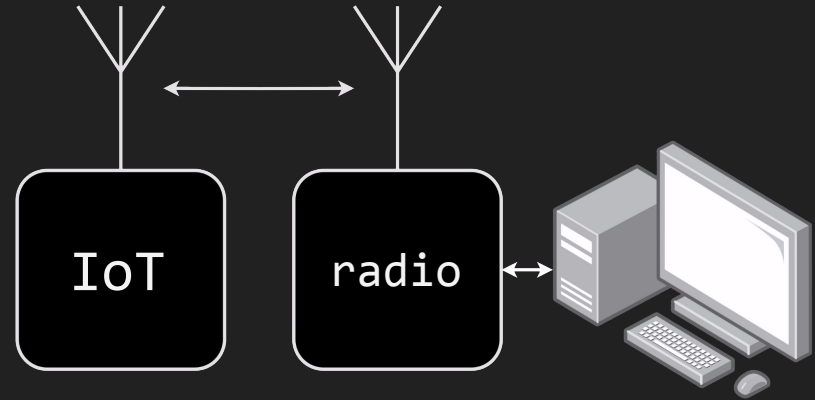


sniff here

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

2) run your own base station

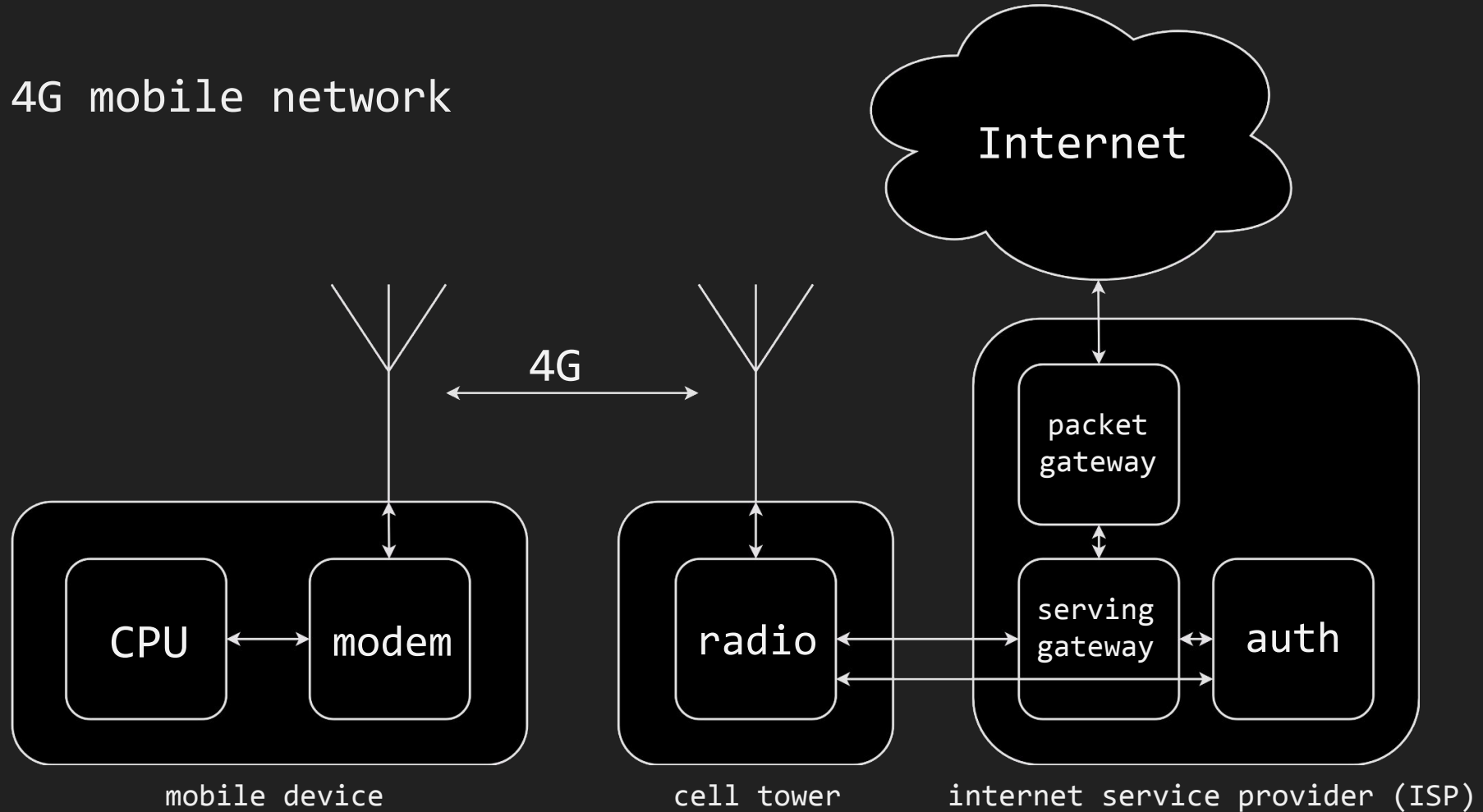
- buy/build a base station
- software defined radios (SDR) are relatively cheap and open source software exists



- 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

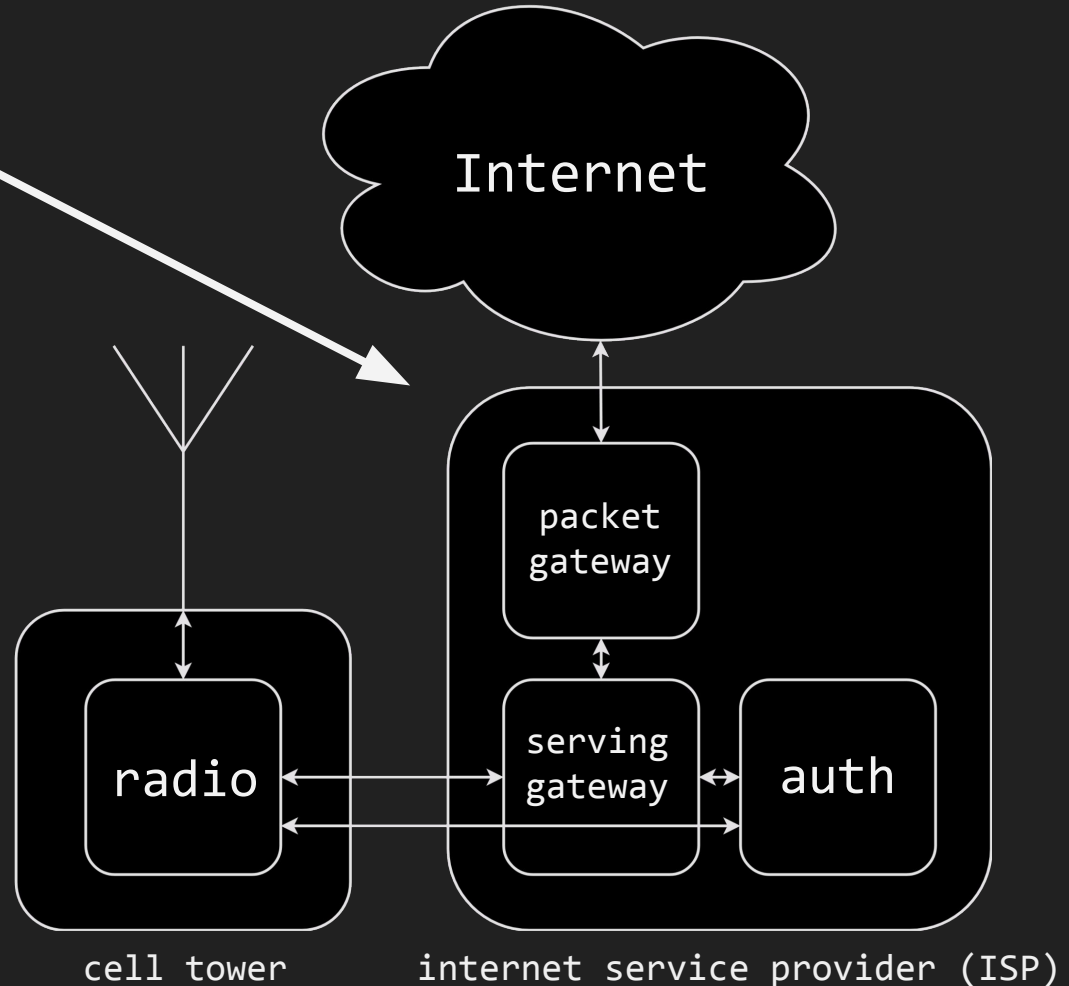
ref: <https://librecellular.org>

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

13.02 📶 🔋 92

[← Telia FI](#) Mobile Data

MOBILE DATA

APN	internet
Username	
Password	

MMS

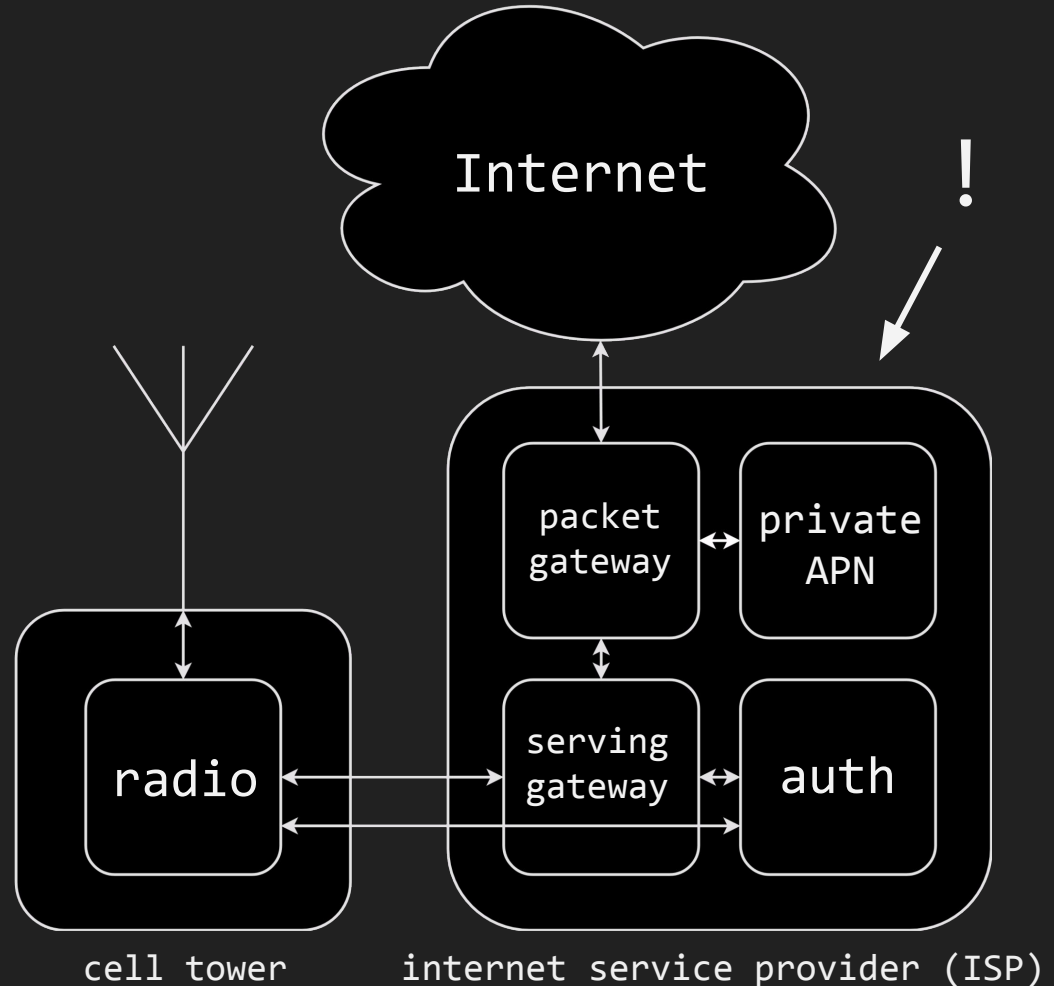
APN	MMS
Username	
Password	
MMSC	http://mms/
MMS Proxy	195.156.25.33:8080
MMS Max Message Size	2097152
MMS UA Prof URL	

PERSONAL HOTSPOT

APN	internet
Username	
Password	

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?

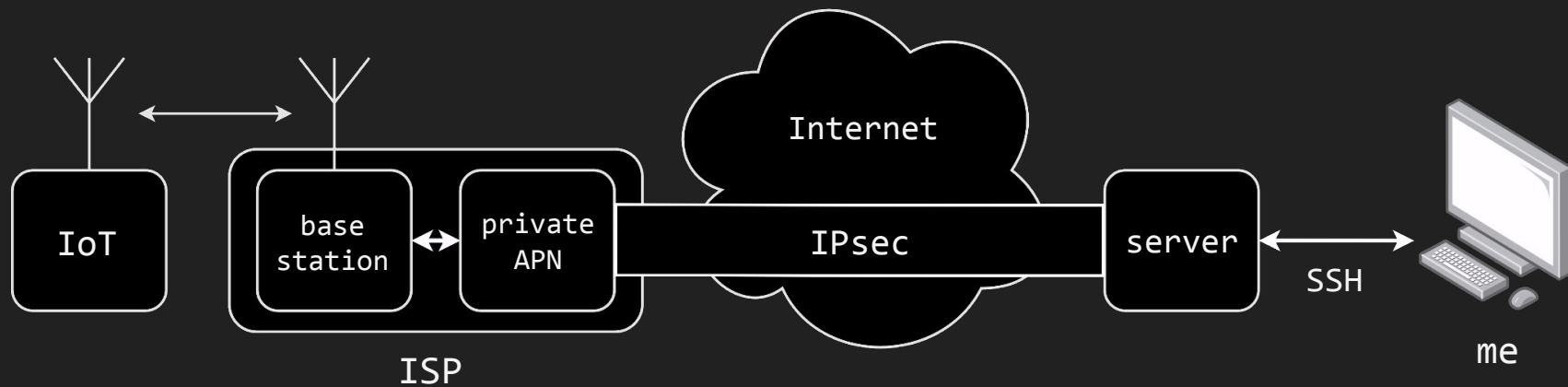
could I get a private APN?

- 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

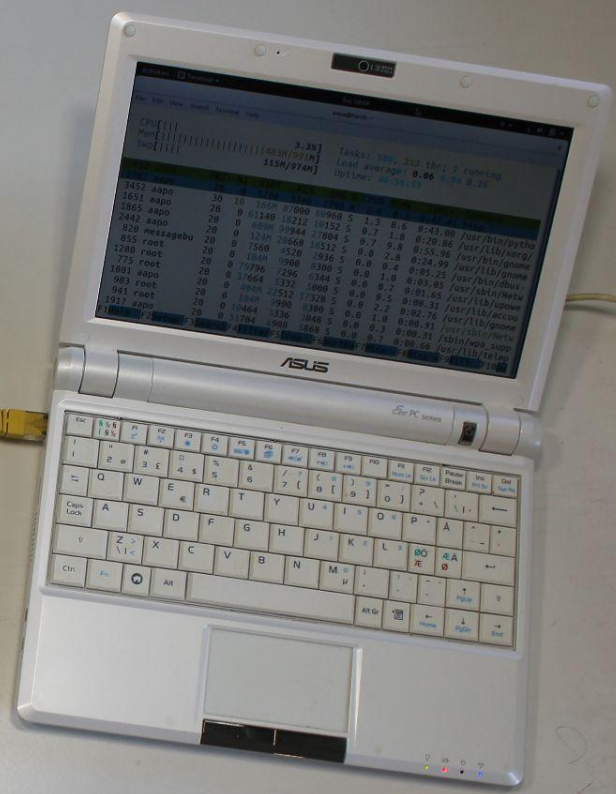


demo

WIFI



?



is there traffic over 5G as well?

WIFI

?



08:55:28.022360042	17.57.146.138	10.222.0.2	TCP	52 5223 → 49358 [ACK] Seq=6195 Ack=34245 Win=78080 Len=0 TSval=116620604
08:55:33.009028485	10.222.0.2	17.57.146.138	TLSv1.3	92 Application Data
08:55:33.016810524	17.57.146.138	10.222.0.2	TCP	52 5223 → 49358 [ACK] Seq=6195 Ack=34285 Win=78080 Len=0 TSval=116621103
08:55:33.016824640	17.57.146.138	10.222.0.2	TLSv1.3	76 Application Data
08:55:33.059938116	10.222.0.2	17.57.146.138	TCP	52 49358 → 5223 [ACK] Seq=38790 Ack=5223 Win=131008 Len=0 TSval=28824171
09:02:15.305136253	17.57.146.138	10.222.0.2	TLSv1.3	115 Application Data
09:02:15.305153026	17.57.146.138	10.222.0.2	TLSv1.3	429 Application Data
09:02:15.305162209	17.57.146.138	10.222.0.2	TLSv1.3	78 Application Data
09:02:15.305170176	17.57.146.138	10.222.0.2	TLSv1.3	132 Application Data
09:02:15.305184896	17.57.146.138	10.222.0.2	TLSv1.3	132 Application Data
09:02:15.592452186	17.57.146.138	10.222.0.2	TCP	132 [T]
09:02:16.086590496	10.222.0.2	17.57.146.138	TCP	64 49358 → 5223 [ACK] Seq=38790 Ack=5223 Win=131008 Len=0 TSval=28824171
09:02:16.110476911	10.222.0.2	17.57.146.138	TLSv1.3	726 [T]
09:02:16.110477140	10.222.0.2	17.57.146.138	TLSv1.3	113 Connection Refused
09:02:16.110810327	10.222.0.2	17.57.146.138	TCP	1426 [T]
09:02:16.118260443	17.57.146.138	10.222.0.2	TCP	64 [T]
09:02:16.118269118	17.57.146.138	10.222.0.2	TCP	64 [T]
09:02:16.118376902	17.57.146.138	10.222.0.2	TCP	52 5223 → 49358 [ACK] Seq=6195 Ack=34245 Win=78080 Len=0 TSval=116620604
09:02:16.118477070	17.57.146.138	10.222.0.2	TLSv1.3	115 Application Data
09:02:16.152361106	10.222.0.2	17.57.146.138	TCP	52 49358 → 5223 [ACK] Seq=38790 Ack=5223 Win=131008 Len=0 TSval=28824171
09:02:16.296401093	10.222.0.2	17.57.146.138	TLSv1.3	84 Application Data
09:02:16.313121378	10.222.0.2	17.57.146.138	TLSv1.3	357 [T]
09:02:16.313157531	10.222.0.2	17.57.146.138	TCP	1426 [T]
09:02:16.320829247	17.57.146.138	10.222.0.2	TCP	64 5223 → 49358 [ACK] Seq=6195 Ack=34245 Win=78080 Len=0 TSval=116620604
09:02:16.320851887	17.57.146.138	10.222.0.2	TCP	52 5223 → 49358 [ACK] Seq=6195 Ack=34285 Win=78080 Len=0 TSval=116621103
09:02:16.322142649	17.57.146.138	10.222.0.2	TLSv1.3	115 Application Data
09:02:16.375149121	10.222.0.2	17.57.146.138	TCP	52 49358 → 5223 [ACK] Seq=38790 Ack=5223 Win=131008 Len=0 TSval=28824171
09:02:17.391234119	10.222.0.2	17.57.146.138	TLSv1.3	625 Application Data
09:02:17.399491413	17.57.146.138	10.222.0.2	TLSv1.3	184 Application Data
09:02:17.444356303	10.222.0.2	17.57.146.138	TCP	52 49358 → 5223 [ACK] Seq=38790 Ack=5223 Win=131008 Len=0 TSval=28824171
09:02:21.345379346	10.222.0.2	17.57.146.138	TLSv1.3	92 Application Data
09:02:21.353173355	17.57.146.138	10.222.0.2	TLSv1.3	76 Application Data
09:02:21.404369558	10.222.0.2	17.57.146.138	TCP	52 49358 → 5223 [ACK] Seq=38790 Ack=5223 Win=131008 Len=0 TSval=28824171
09:02:28.566124827	17.57.146.138	10.222.0.2	TLSv1.3	377 Application Data
09:02:28.566144095	17.57.146.138	10.222.0.2	TLSv1.3	78 Application Data
09:02:28.832604930	17.57.146.138	10.222.0.2	TCP	78 [T]
09:02:29.546447027	10.222.0.2	17.57.146.138	TCP	64 49358 → 5223 [ACK] Seq=38790 Ack=5223 Win=131008 Len=0 TSval=28824171
09:02:29.728633271	10.222.0.2	17.57.146.138	TLSv1.3	84 Application Data
09:02:29.778595857	17.57.146.138	10.222.0.2	TCP	52 5223 → 49358 [ACK] Seq=6195 Ack=34245 Win=78080 Len=0 TSval=116620604
09:02:34.758272839	10.222.0.2	17.57.146.138	TLSv1.3	92 Application Data
09:02:34.765972692	17.57.146.138	10.222.0.2	TCP	52 5223 → 49358 [ACK] Seq=6195 Ack=34285 Win=78080 Len=0 TSval=116621103
09:02:34.765984361	17.57.146.138	10.222.0.2	TLSv1.3	76 Application Data
09:02:34.800366434	10.222.0.2	17.57.146.138	TCP	52 49358 → 5223 [ACK] Seq=38790 Ack=5223 Win=131008 Len=0 TSval=28824171

Conversation Settings

- ☐ Name resolution
- ☐ Absolute start time
- ☐ Limit to display filter

Copy

Follow Stream...

Graph...

Protocol

- ☐ Bluetooth
- ☐ DCCP
- ☒ Ethernet
- ☐ FC
- ☐ FDDI
- ☐ IEEE 802.11
- ☐ IEEE 802.15.4
- ☒ IPv4
- ☒ IPv6
- ☐ IPX

Filter list for specific type

Help

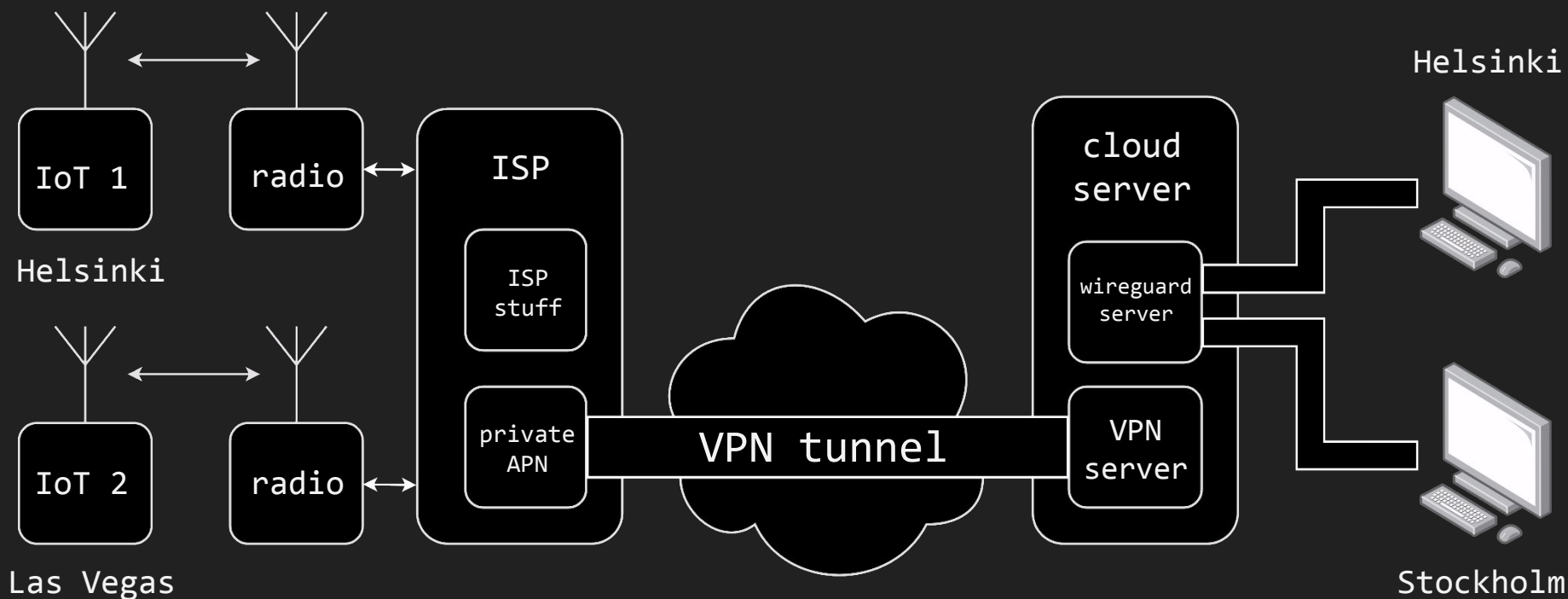
Ethernet	IPv4 · 10	IPv6	TCP · 47	UDP · 19
Address A	Address B	Packets	Bytes	
10.222.0.2	1.0.0.1	199	68 kB	
10.222.0.2	1.1.1.1	123	34 kB	
10.222.0.2	16.16.117.193	11	656 bytes	
10.222.0.2	16.16.133.143	20	1 kB	
10.222.0.2	16.16.224.24	20	1 kB	
10.222.0.2	16.16.245.216	34	2 kB	
10.222.0.2	17.57.146.137	522	235 kB	
10.222.0.2	17.57.146.140	3	164 bytes	
16.16.152.208	10.222.0.2	59	4 kB	
17.57.146.138	10.222.0.2	211	66 kB	

is there traffic over 5G as well?

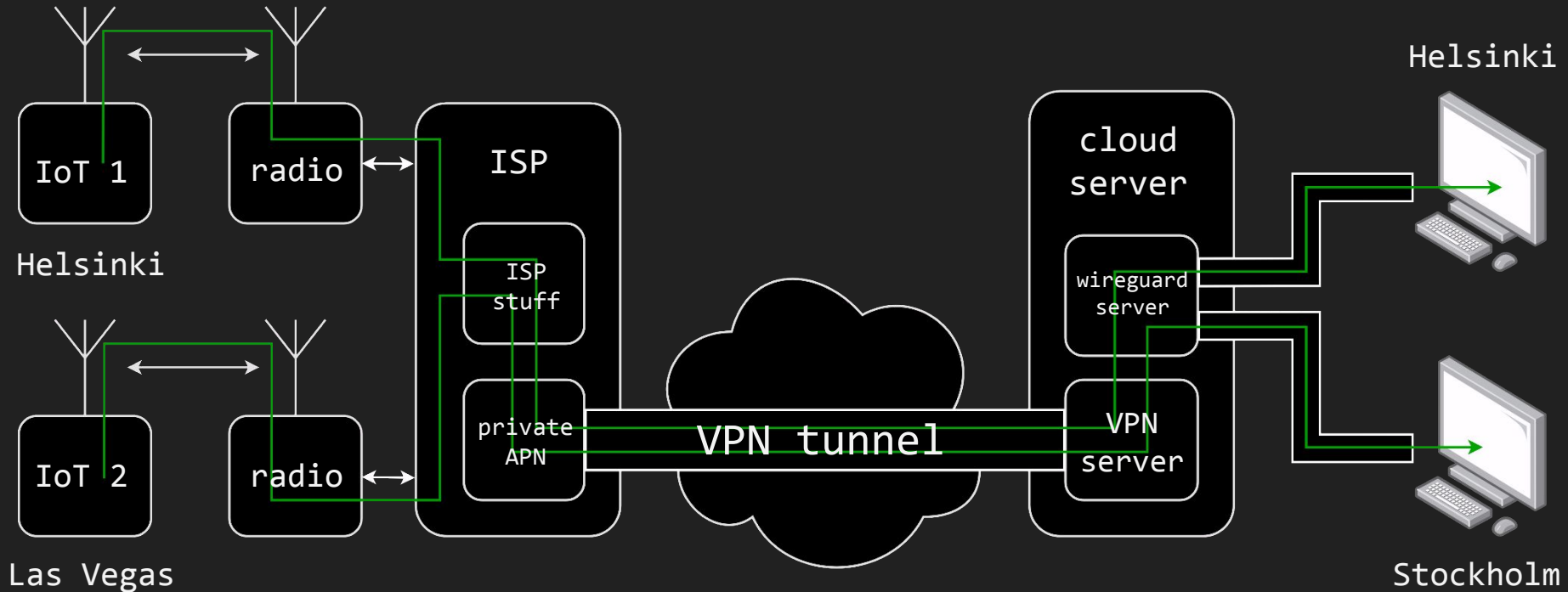
from POC to project

- 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.

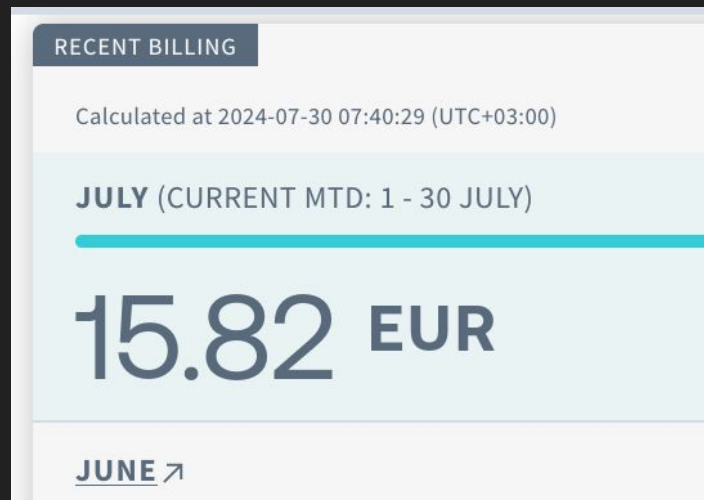
Private APNs offered by ISPs

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](https://www.linkedin.com/in/AapoOksman)
- aapo @ bug bounty