GPS ankle monitor hacking

How I got stalked by people from the Arab Emirates

Introduction

- Not a security researcher
- Software engineer at a bank: Rabobank
- Stumbled into this by accident, I'm innocent I swear
- Messing around with code and hardware for a long long time
- https://coredump.ws/index.php?dir=code&post=Myrope_support_and_mch2022

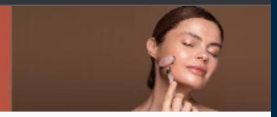
Contents of presentation

1. Beginnings.
2. Let’s laugh at a CVE
3. How did I get all of this information
4. JIMI/Concox based trackers.
5. Concox protocol
6. Megastek trackers
7. Megastek protocol
8. Xexun trackers
9. Xexun protocol[s]
10. Thinkrace/myrope/others
11. Vulnerabilities
12. Public information/accessible servers

How it started

nl.aliexpress.com/item/32349089748.html?spm=a2g0o.detail.1000014.2.63f17591bop6ag&gps-id=pcDetailBottomMoreOtherSeller&scm=1

DISCOVERY Schoonheidsitems voor u



Sell on AliExpress | Privacy-instellingen | Help | Kopersbescherming | mobiele | / Nether

AliExpress

Tracker Room Store

93.9% Positieve feedback

+ Volgen

806 Volgers

Ik winkel voor...

Winkel Home | Producten | Verkoop Artikelen | Bestverkopende | Nieuw Binnen | Feedback

Gps Tracker Voor Gevangene Enkelband Key Locker En Moni

★★★★★ 5.0 1 Recensie 24 bestellingen

€ 149,02 ~~€ 175,33~~ -15%

Price includes VAT

Kleur: no box

with box | no box

Aantal:

1 476 stukken beschikbaar

Wordt verzonden naar Netherlands

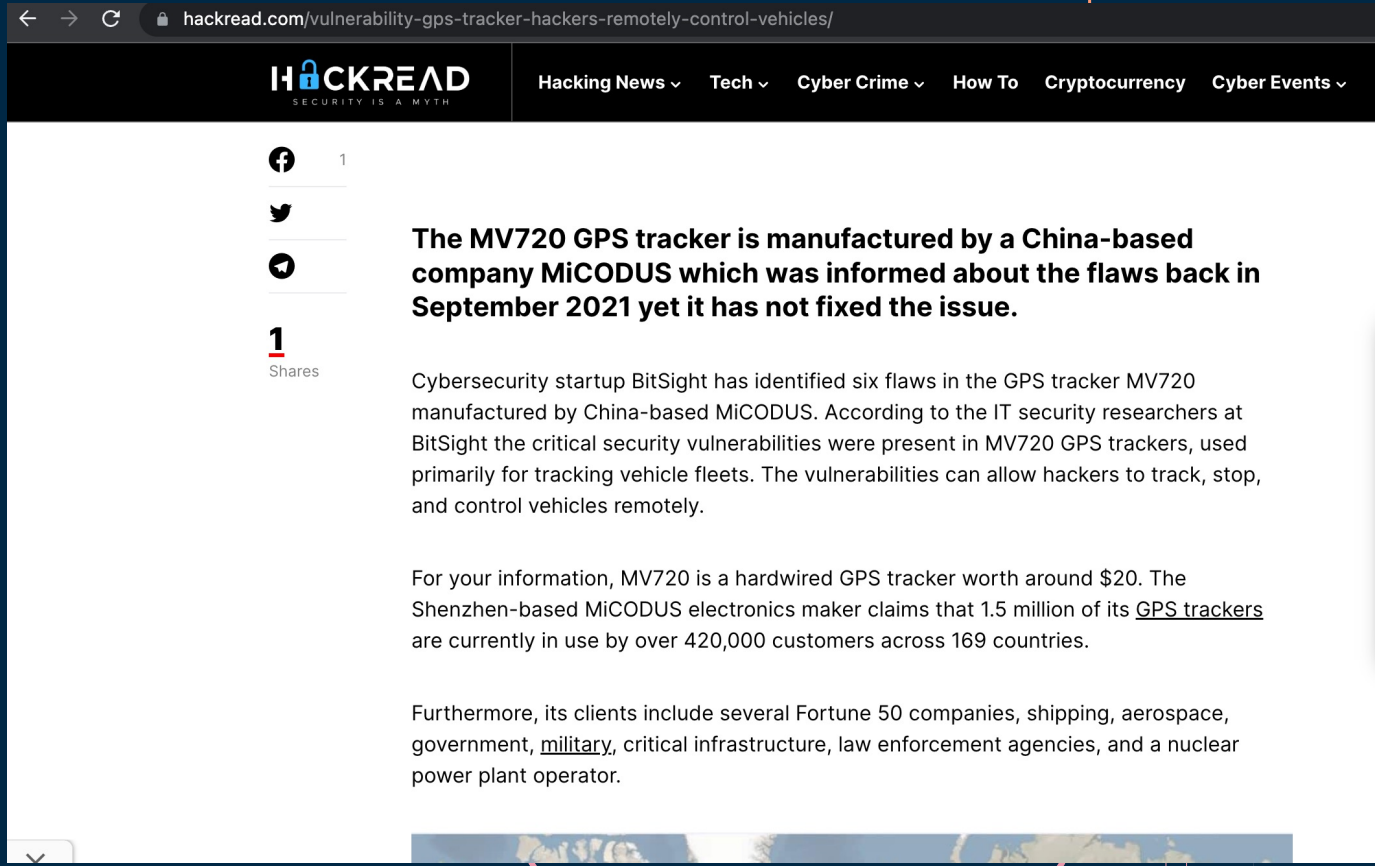
Verzending: € 15,46

Van China naar Netherlands via AliExpress Standard Shipping

Geschatte levering op 18 aug

How it’s going

It’s like that, but much much worse



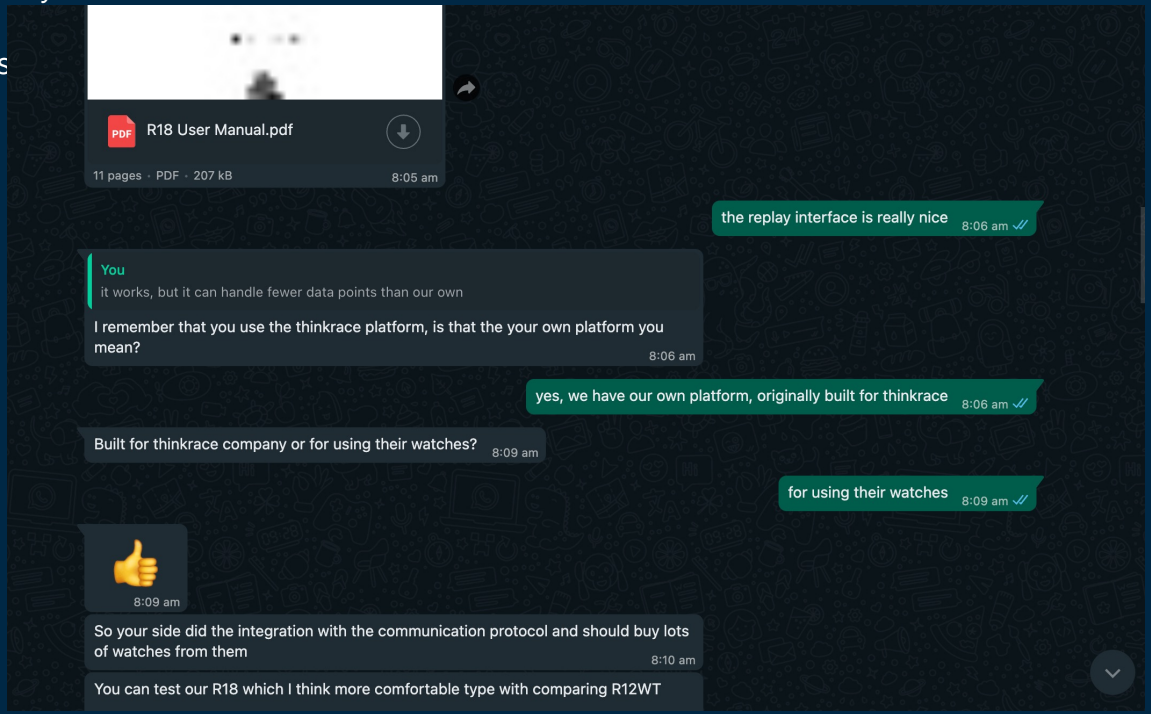
How much?

gps123.org/log2/20220719/GateWayLog07.txt

```
2022/7/19 7:00:08,2104255041,Str:*HQ,2104255041,LINK,230010,0,0,79,0,0,180722,FFE7FBFF#

2022/7/19 7:00:08,353327022929780,HEX:78780A1346060400000479A7780D0A78781F12160712163A39CD0093643E006BB5210ADC400264050029008254047A86FF0D0A

2022/7/19 7:00:08,1403158206,Str:[3G*1403158206*0009*LK,0,0,67]

2022/7/19 7:00:08,9705079035,Str:[3G*9705079035*0009*LK,0,0,51]

2022/7/19 7:00:08,353327022917264,HEX:78780A1345060400000062C6240D0A

2022/7/19 7:00:08,2104245378,Str:[3G*2104245378*0009*LK,0,0,10]

2022/7/19 7:00:08,353327022496996,HEX:78780A13440604000000067CD30D0A

2022/7/19 7:00:08,2717007573,Str:[3G*2717007573*000A*LK,0,0,100]

2022/7/19 7:00:08,353327022938211,HEX:78780A13440604000003F6A1340D0A

2022/7/19 7:00:08,2104258431,Str:*HQ,2104258431,V1,230010,A,5356.5482,N,03252.8591,E,000.0,024,180722,FFFFFBFF#

2022/7/19 7:00:08,353327023250657,HEX:78780A1344060400000CB889860D0A

2022/7/19 7:00:08,2104021546,Str:[3G*2104021546*000A*LK,8,0,100]

2022/7/19 7:00:08,353327023273287,HEX:78780A134606030000011BA9080D0A

deviceToken:,userToken:

2022/7/19 7:00:08,6430030191,Str:*HQ,6430030191,LINK,084355,60,0,96,0,0,241021,FEFFFFFF#

2022/7/19 7:00:08,2104282365,Str:*HQ,2104282365,LINK,230010,52,0,52,0,0,180722,FFE7FBFF#

2022/7/19 7:00:08,9705034877,Str:[3G*9705034877*0009*LK,0,0,43]

2022/7/19 7:00:08,353327023270036,HEX:78780A13040604000000DCB16440D0A

2022/7/19 7:00:08,9705021032,Str:[3G*9705021032*0009*LK,0,0,18]

2022/7/19 7:00:08,353327022928758,HEX:78780A13060604000000B3B82A00D0A

2022/7/19 7:00:08,2104109520,Str:
[3G*2104109520*00CD*UD,180722,230010,A,34.125977,N,112.0712233,E,0.00,160.9,0.0,7,95,60,0,0,00000010,7,1,460,0,14512,2021,142,14512,2022,144,14512,7973,128,14336,20823,126,14512,20572,125,145
12,2023,124,14512,20832,123,0,18.9]

2022/7/19 7:00:08,2104052871,Str:*HQ,2104052871,LINK,-10011,100,0,100,0,0,190722,FFE7FBFF#

2022/7/19 7:00:08,353327023448756,HEX:78780A1344060400000209B7940D0A
```

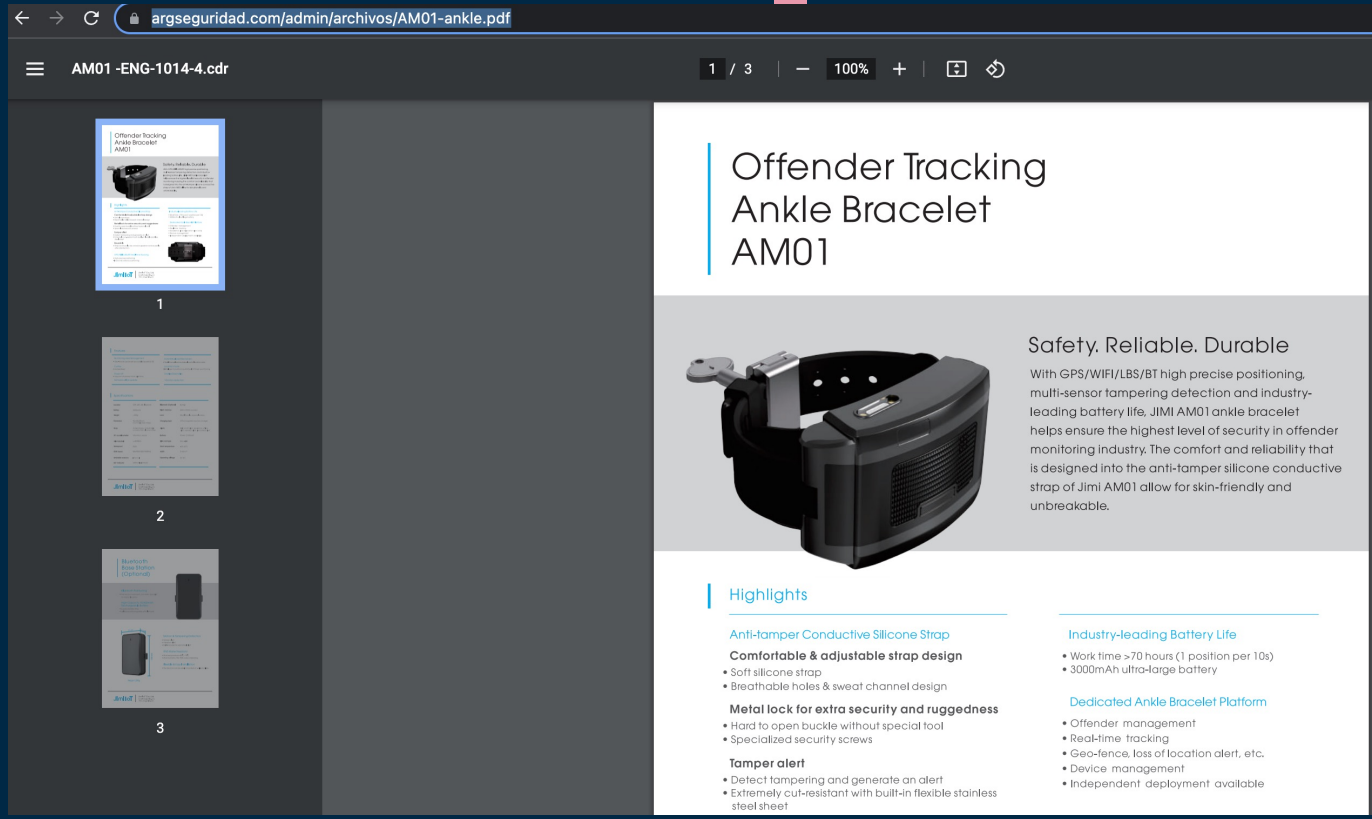
How did I get this information

1. Just ask, really
2. Pretend to be a big enough company
3. Google can teach you a lot
4. Car trackers with similar protocols



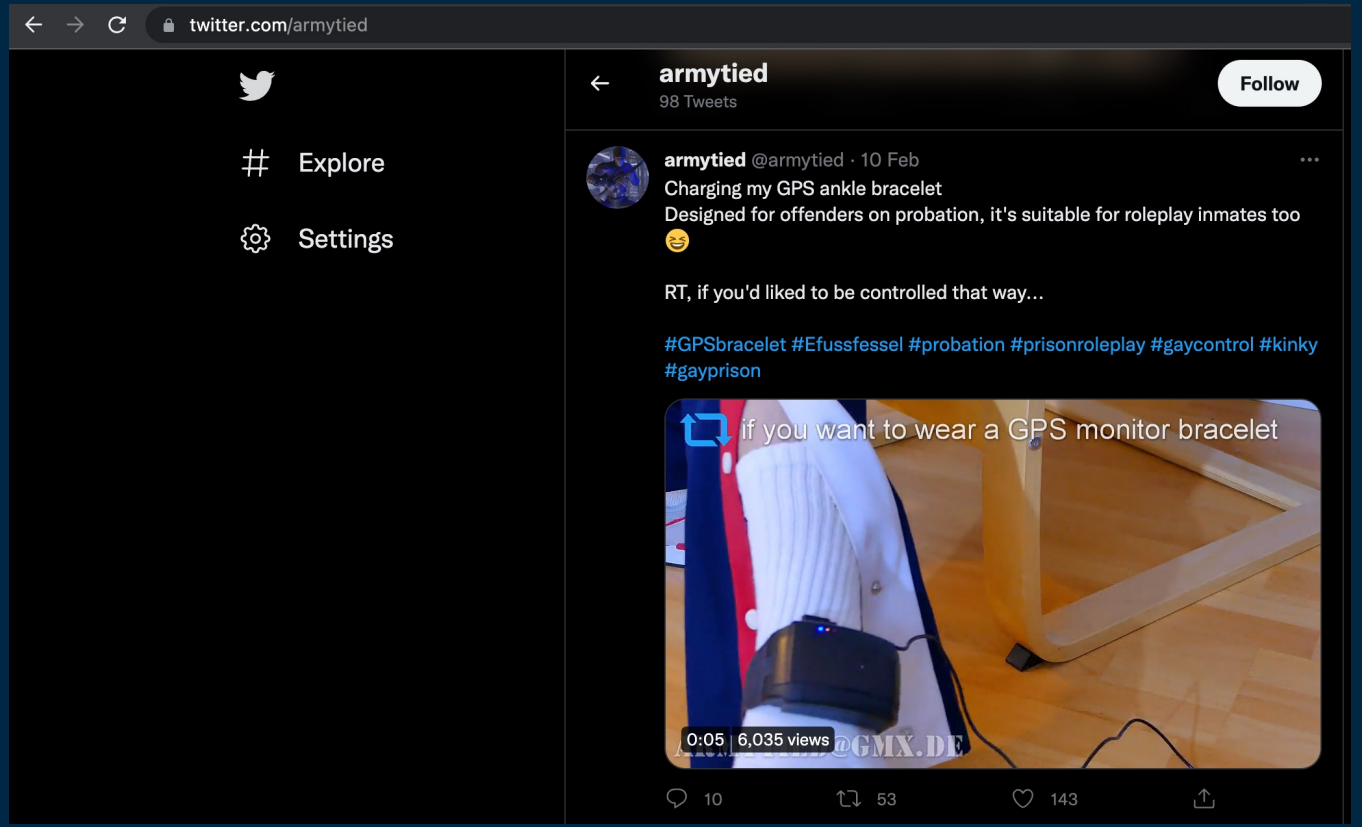
Jimi/concox based trackers

1. Based on vehicle trackers
2. Decent/good useability
3. Rather poor waterproofing



Jimi/concox based trackers

1. So I took your people tracker
2. And made it a gay thing
3. Sorry, not sorry 🤣



Concox protocol

1. Better documentation [but not implementation for personel tracking] in traccar
2. Manuals included
3. Binary protocol
4. No encryption of any sort
5. Show command manual/protocol manual

Megastek trackers

1. Many more models
2. Lots of versions
3. Much more widely used

Not Secure | trackingtheworld.com/products/

CAT-65 4G

- 4G LTE, 3G dual band UMTS/HSDPA, quad band GSM/GPRS
- Log data when there is no GSM signal
- Belt-off alarm
- Waterproof, IP67 compliant
- FCC and CE certified

70 x 42 x 25 mm

CAT-110

- 2G quad band GSM/GPRS
- Log data when there is no GSM signal
- Belt-off alarm
- Waterproof, IP67 compliant
- CE certified

61 x 49 x 22 mm

CAT-200X 4G

- 4G LTE, 3G dual band UMTS/HSDPA, quad band GSM/GPRS
- Log data when there is no GSM signal
- Belt-off alarm
- Waterproof, IP68 compliant
- FCC and CE certified

70 x 64 x 20 mm

CAT-200X

- 3G dual band UMTS/HSDPA, quad band GSM/GPRS
- Log data when there is no GSM signal
- Belt-off alarm
- Waterproof, IP67 compliant
- FCC and CE certified

70 x 64 x 20 mm

Original? Think not.

MEDIA ROOM

SCRAM Systems and Upstreem enter a strategic partnership to bring a GPS locking smartwatch to the United States market

January 25, 2022

Megastek trackers

1. Show protocol/device
2. Much more secure hardware wise
3. Not so much software wise
4. Multiple anti tamper mechanism options

Thinkrace trackers

JT **Julie tale**
Hi Arno, please add me to your LinkedIn network
To: Arno Pol

Inbox - Mail 25 January 2022 at 07:48

Arno Pol

Hi Arno, I'd like to join your LinkedIn network.

Julie tale
Digital Specialist at siliconapp

View profile Accept

Unsubscribe | Help

You are receiving Invitation emails.

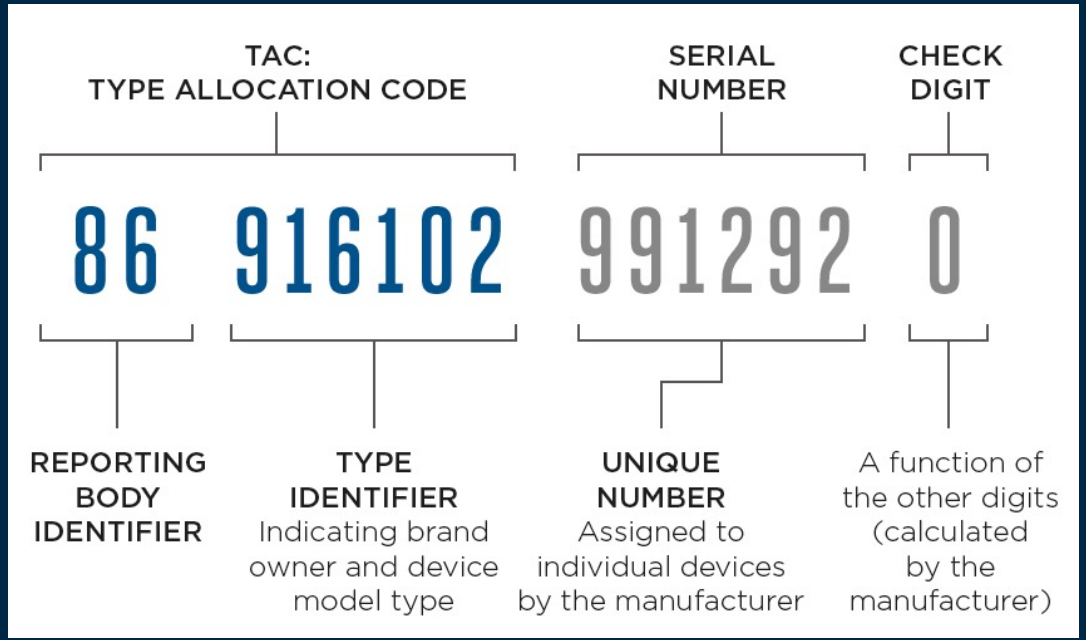
This email was intended for Arno Pol (Software Engineer (Msc)).
Learn why we included this.

LinkedIn

1. They also monitor people going on the haj.. Interesting to our spooks?

Thinkrace trackers

1. Show protocol/commands
2. What would happen if we send a lot of SMS messages to the UAE
3. IMEI numbers are incremental
4. https://decoded.avast.io/martinhron/the-secret-life-of-gps-trackers/ avast did this before, but for children. And just for one brand.. This presentation is a bit bigger than that :P



Xexun trackers

1. Binary protocol
2. Kind of more widely used
3. Ankle bracelet factor not very ergonomic but..
4. Maybe I should avoid China too for now.. Spooks feel free to give me advice on this.

Our Customers

- Shanghai community correction Bureau
- Qinghai community correction Bureau
- Xinjiang community correction Bureau
- Sichuan community correction Bureau
- Guangdong Community Correction Bureau
- Heilongjiang Public Security Department
- Qianxinan Judicial Bureau
- Tianjin Community Correction Bureau
- Ningxia community correction Bureau
- Liaoning community correction Bureau
- Yunnan Community Correction Bureau
- Wuhan Community Correction Bureau
- Kezhou Public Security Bureau
- Qiandongnan Judicial Bureau

- Hunan Power Grid
- Jibei Power Grid
- Beijing Power Grid
- Xining prison
- Caidamu prison
- Anhui Power Grid
- Henan Power Grid
- Menyuan prison
- Xichuan prison
- Jiulong prison

Tracking methods

1. LBS single/multiple
2. Bluetooth
3. WiFi (thanks Arch linux)
4. GPS

Security details

1. Can cross-reference like they do with SCRAM
2. Jamming is possible, so is downgrading to 2g
3. WiFi for xexun devices can be used to avoid transmitting GPS info
4. But it’s still possible to force GPS location

LBS tracking

1. Local base station
2. MNC: 1 byte
3. MCC: 2 bytes
4. LAC: 2 bytes
5. Cell ID: 4 bytes
6. These attributes are all binary -> we can just radix sort

7. OpenCellID and other databases
8. Google database

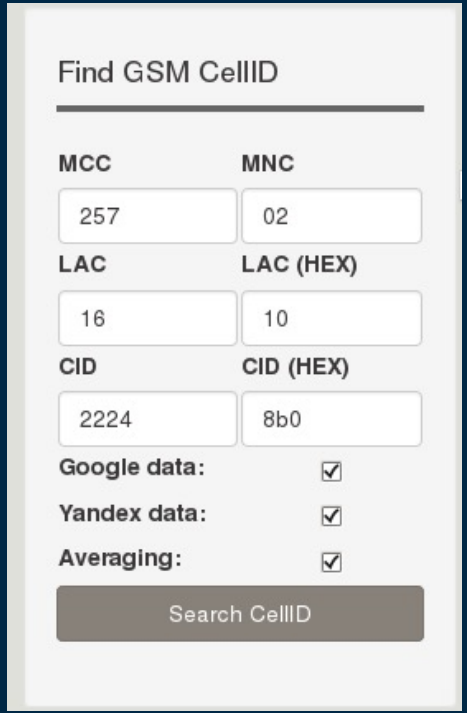


Image from: https://cellidfinder.com/articles/how-to-find-cellid-location-with-mcc-mnc-lac-i-cellid-cid

LBS tracking

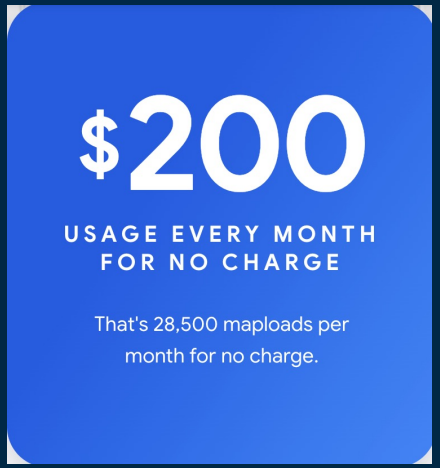
1. Interpolate between points
2. Naïve implementation, divide the space between towers into squares – and use the signal strength as distance estimate
3. Quick, dirty and good enough
4. When we have just one cell tower, accuracy is not great

WiFi tracking

1. Send a list of networks to google
2. Google responds with a location

3. Concessions made: no signal strength sent
4. Save/cache lists of wifi networks with location. Use a hash based lookup to find them.
5. When we cannot find a set of networks in the list – try finding a match where the current set is a subset of it. If that fails – find it via the google API and cache it.

6. I'm not that rich, so thanks Arch ^^
7. Fallback to here geolocate API because it's cheaper.



Security details.. continued

1. Fiber injection is possible, not just tapping.
2. Remember the NSA?
3. If prohibitively expensive you can always nuke the device and continue with spoofed transmissions
4. Debug cables. Lots of debug cables
5. They're basically smartphones everyone!
6. This might or might not include western devices as well.

High-efficiency light injection and extraction using fiber bending

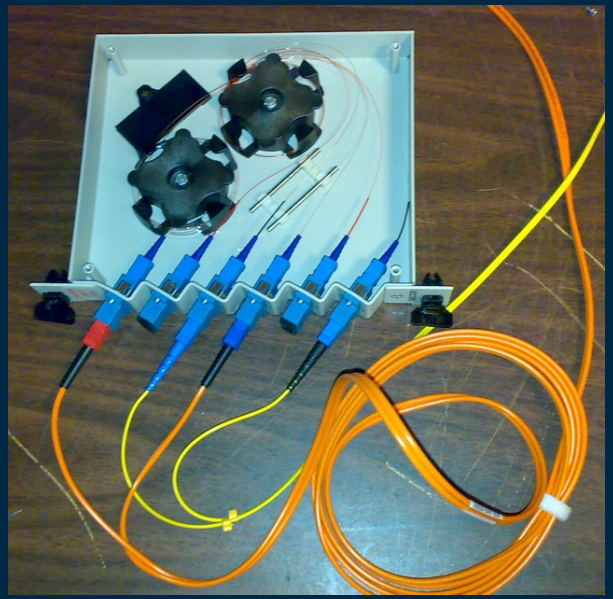
Takui Uematsu, Takanori Kiyokura, Hidenobu Hirota, Tomohiro Kawano, and Tetsuya Manabe

Author Information ▾ Find other works by these authors ▾

Get PDF | Email | Share ▾ | Get Citation ▾ | Citation alert | Save article

Abstract

We achieve a temporary optical coupler that injects/extracts light into/from a fiber with high efficiency by using fiber bending. We demonstrate experimentally that extraction efficiency is improved by using a double-clad fiber.



Security details.. continued

1. Open servers
2. You can all access this
3. https://www.gps123.org/log2/20220723/GateWayLog07.txt
4. Live demo of software

Do you have any questions?

apol@mail.com
coredump.ws

Or talk to me later outside the tent

THANKS