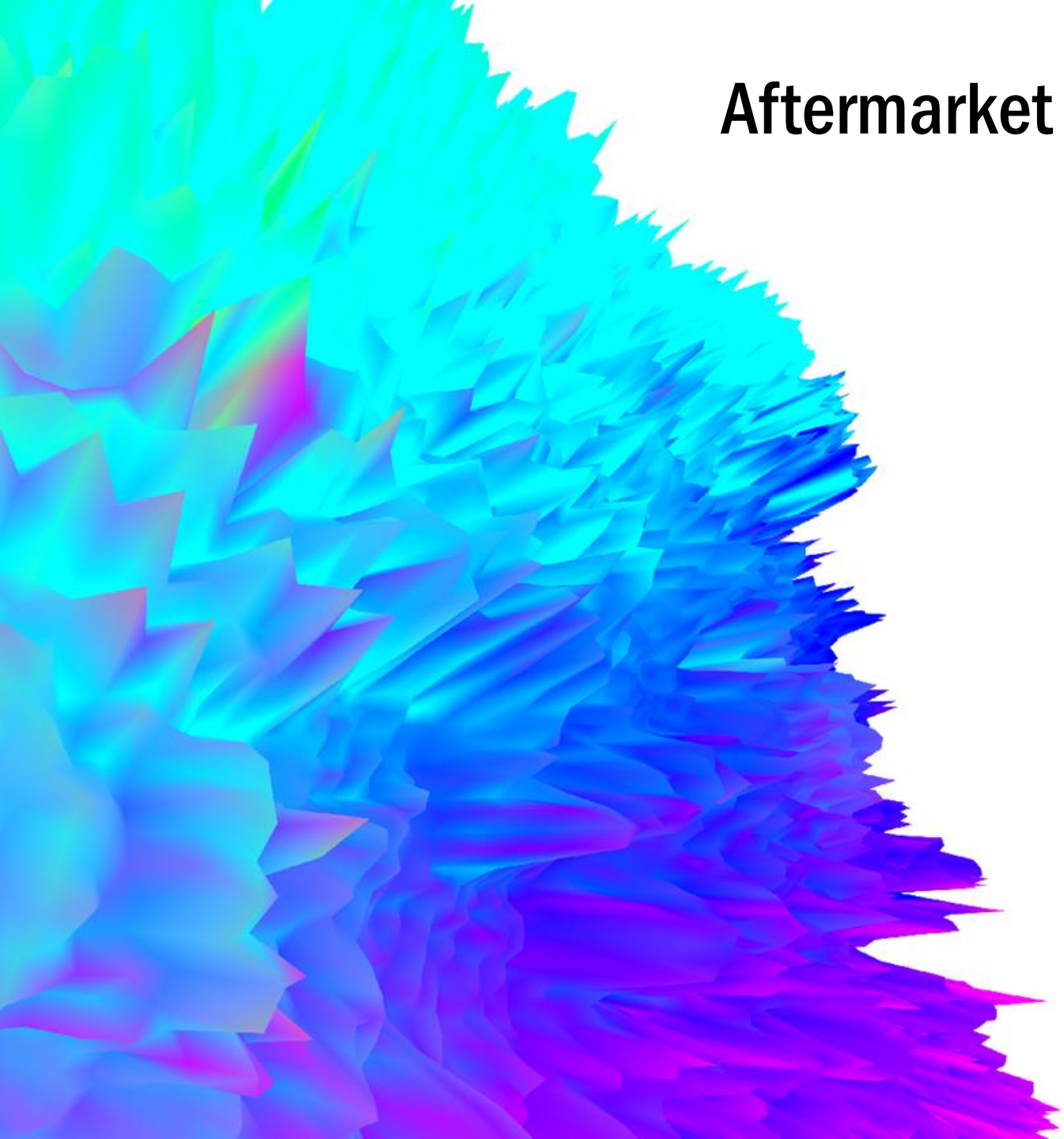


Aftermarket Vehicle Trackers & Immobilizers: Redux

Lachlan “skooch” Temple
Unrestcon
The James Corbin Ministry of Dance

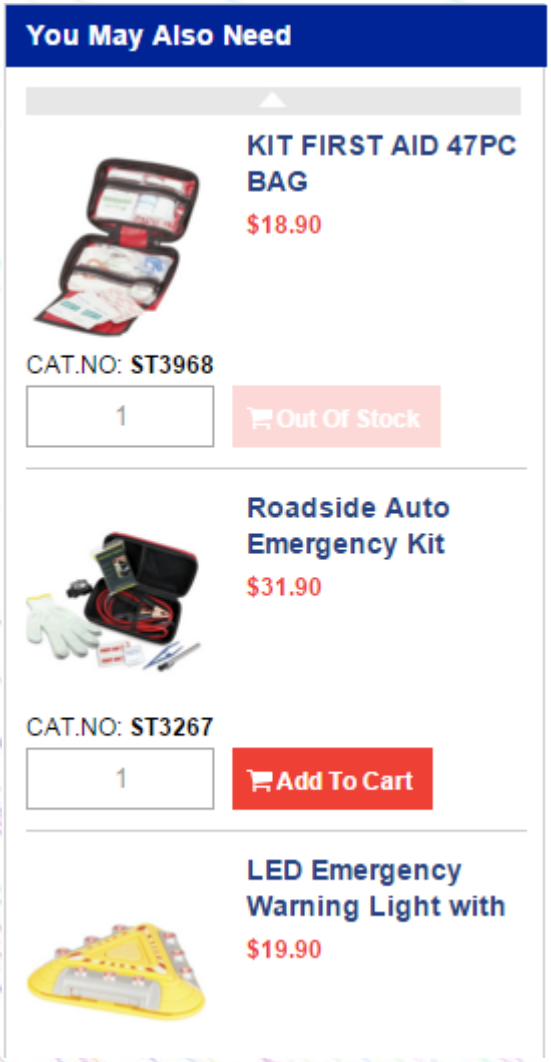
ZX SECURITY

cowsay –f gnu “hi i’m skooch” | wall

- I’m skooch
- Things I like:
  - Annoying my co-worker ss23
  - Music
  - Counter-Strike
  - Swearing at debuggers/IDA
- Straight Outta WGTN
- First time here in Melbourne (yay!)

The “gps thing”

Or rather the “GPS/GSM Tracking Device”



But what is the “gps thing” really?

- Tracks your car, indeed, we are truly entering the pinnacle of the technology era and 21st century
- Made in China, and probably rebranded and sold around the globe
- I know this because I can buy it at Jaycar (electronics retailer) and on Aliexpress (wholesale). Guess which is cheaper?
- Costs around $135USD ($200NZD) from retail or around $35USD on Aliexpress.

Why would you buy this?

- Stop crims from stealing/jacking your car
  - Deterrent stickers help! (said no-one ever)
  - Watch your car go to the chop shop
  - Have location information for LEO
  - Luckily it was only a $500 civic you picked up in Frankston
- To track the use of your car for statistics
  - Fleet management, roast your employees
  - Which route did I take yesterday?
  - Where did I park my car (again)?
- If you're a cool hacker (like me)

What does it do though?

- GPS Location, Coordinates, Speed, Compass, Accelerometer etc.
- GSM/GPRS with a SIM
- Web and Mobile App based management tools
- Panic button (alright I guess)
- Relay control, cut off fuel pump or starter motor to the car (ummm)
- Microphone (Yeah ok, sure, why not??)

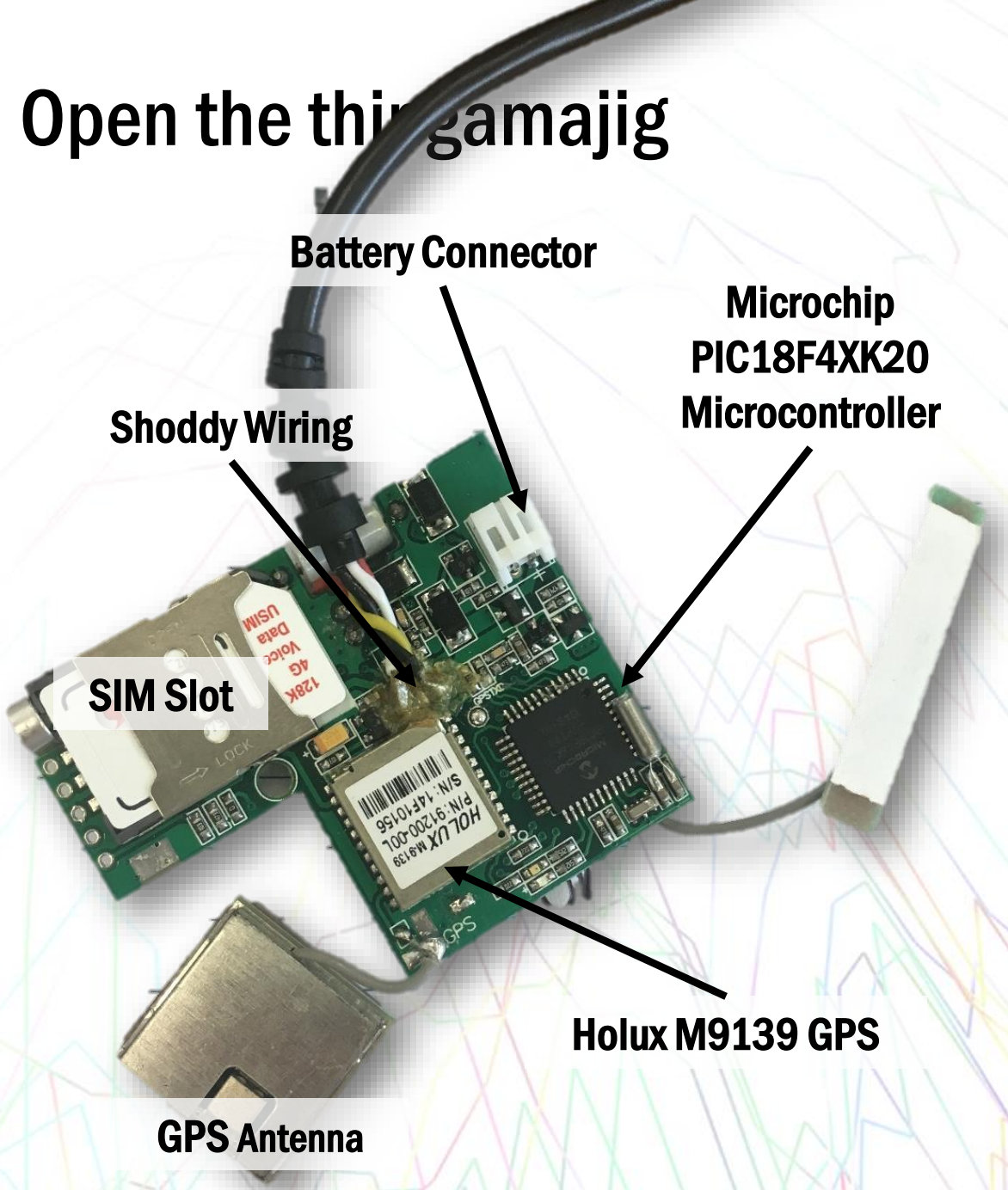

♫You used to call me on my ~~cellphone~~ covert listening and vehicle tracking device♫

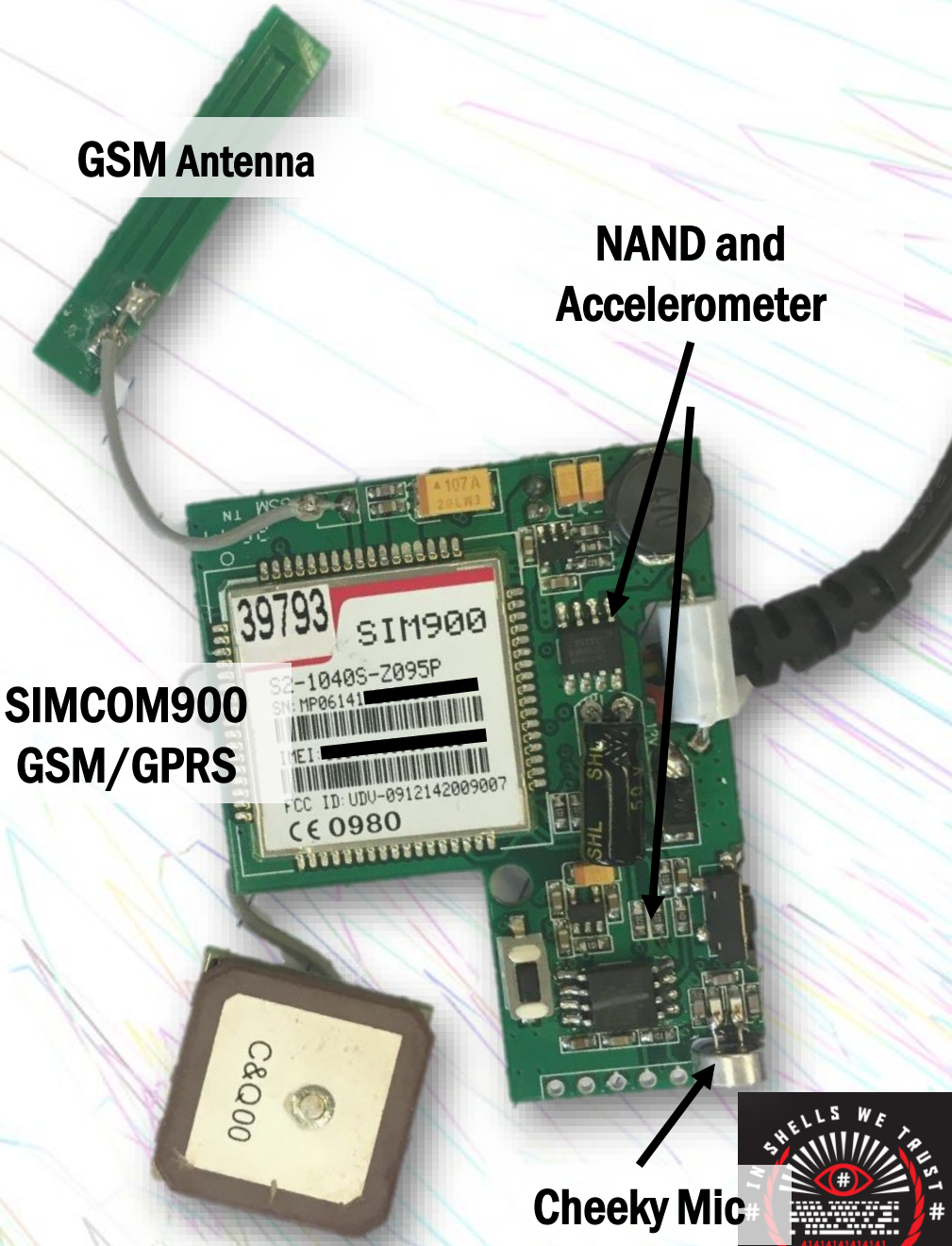
How do we use this “gps thingy” anyway?

- Insert a SIM of your choice in the device
- Text the device from your phone, example: “LINKLOCATE*123456”
- LINKLOCATE being the command
- 123456 being the default code (which yes, you can change)
- You’ll receive a text as a response (in this case containing a google maps link to the location of the device)

- Other command related actions include:
  - LISTEN, will call you back and you can listen through the microphone
  - STOPENGINE, triggers the relay
  - CHECK, returns all settings
  - KEEPONLINE, stops the device from turning off after no movement
  - ADDPHONE, adds your number to the panic button alerts etc

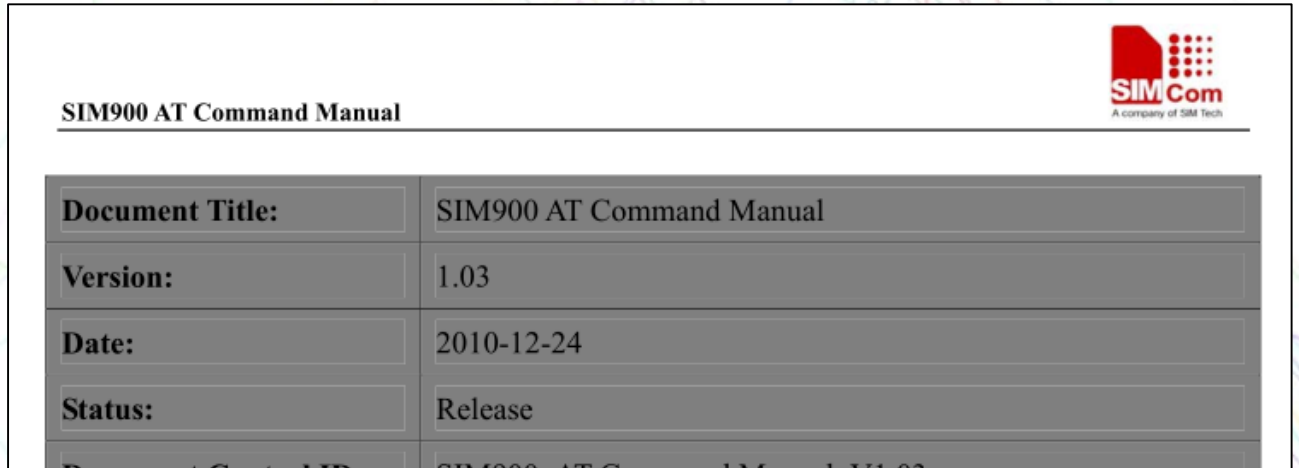
Open the thi gamajig





Datasheet galore

- No end to how common the internals of this device are
- For example: the SIMCOM900 is even used on Arduino GSM shields
- No end to how easily you can find documentation of these chips
- More on this later...



SIM900 AT Command Manual

Document Title:	SIM900 AT Command Manual
Version:	1.03
Date:	2010-12-24
Status:	Release

Internet detective time

- So it’s obviously made in Asia
- Where and by whom though?
- Aliexpress/Alibaba investigation

Shenzhen Thinkrace Technologies Co., Ltd.

Leave Messages | Contact Supplier | Start Order

Business Type:	Manufacturer, Trading Company
✓ Recent Transactions:	16
Main Products:	GPS Tracker,GPS tracking Software,Personal GPS Tracker,Vehicle GPS Tracker,GPS Watch
✓ Location:	Guangdong, China (Mainland)
✓ Year Established:	2006
Year start exporting:	2006
Number Of Employees:	201 - 300 People
Total Annual Sales Volume:	Below US$1 Million

ThinkRace

We are not just provide the hardware but all services for you :

- Manufacturer based in Shenzhen, China
- Make GPS-based equipment and software for commercial and personal situations
- Commercial black-box type stuff for boats and trucks
- Personal vehicle tracking (we know this)
- And personal kid tracking? Alrighty then.

Right! Enough of that!

- In conclusion, it's a cheap chinese-manufactured gps/gsm car bug
- Time for the application stuff
- This is provided to us in the manual in the form of a link and an app I should "search for on the play store"
- I don't really have high expectations from the sort of screenshots I'm seeing in the little booklet, as pretty as they are.

Take a deep breath...

GPS Tracking Platform

Safety Make Better Life

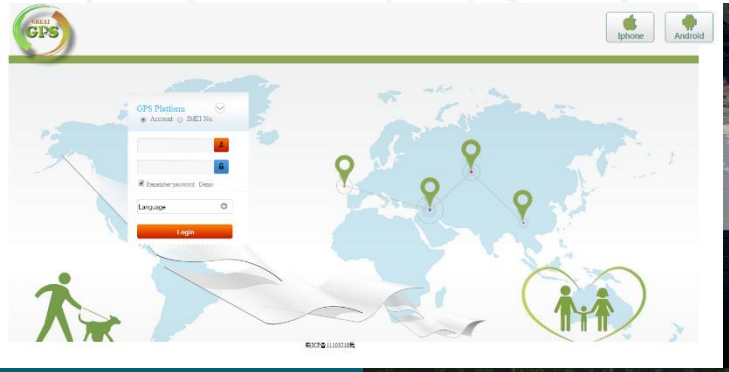
>tfw nikto finds something

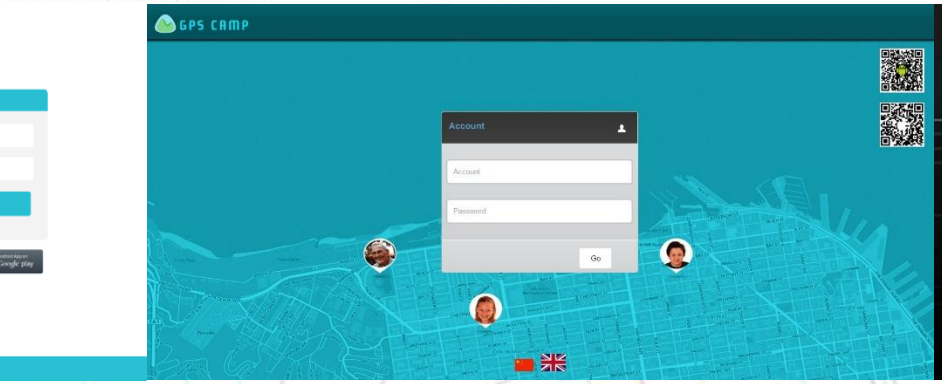
- This already looks GREAT!! (In a masochistic kind of way)
- Nikto.pl says
  - IIS, ASP.NET
  - /log – nice SQLExceptions there buddy
  - /lib – js with API keys embedded in anyone?
  - We'll come back to this
- Hosted in China (of course)
- Remember that rebranding stuff? Well…

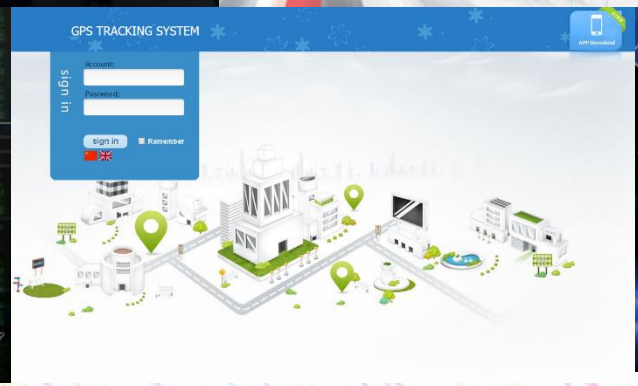
```
user@ubuntu:~/Downloads/nikto/program$ ./nikto.pl -hos
- Nikto v2.1.6
---------------------------------------------------------
+ Target IP:          [redacted]
+ Target Hostname:    [redacted]
+ Target Port:        80
+ Start Time:         [redacted] 17:26:22 (GMT13)
---------------------------------------------------------
+ Server: Microsoft-IIS/7.5
+ Retrieved x-aspnet-version header: 4.0.30319
+ Retrieved x-powered-by header: ASP.NET
+ The anti-clickjacking X-Frame-Options header is not
+ The X-XSS-Protection header is not defined. This hea
+ The X-Content-Type-Options header is not set. This c
+ No CGI Directories found (use '-C all' to force chec
+ Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, POS
+ Public HTTP Methods: OPTIONS, TRACE, GET, HEAD, POST
+ OSVDB-3092: /img/: This might be interesting...
+ OSVDB-3092: /lib/: This might be interesting...
+ OSVDB-3092: /log/: Ahh...log information...fun!
+ OSVDB-3092: /test.aspx: This might be interesting...
+ 7702 requests: 0 error(s) and 11 item(s) reported on
+ End Time:           [redacted] 17:51:34 (GMT13) (151
---------------------------------------------------------
+ 1 host(s) tested
```

I change brands everyday like I change socks

- Bing IP Search plus Google dorks equals what?





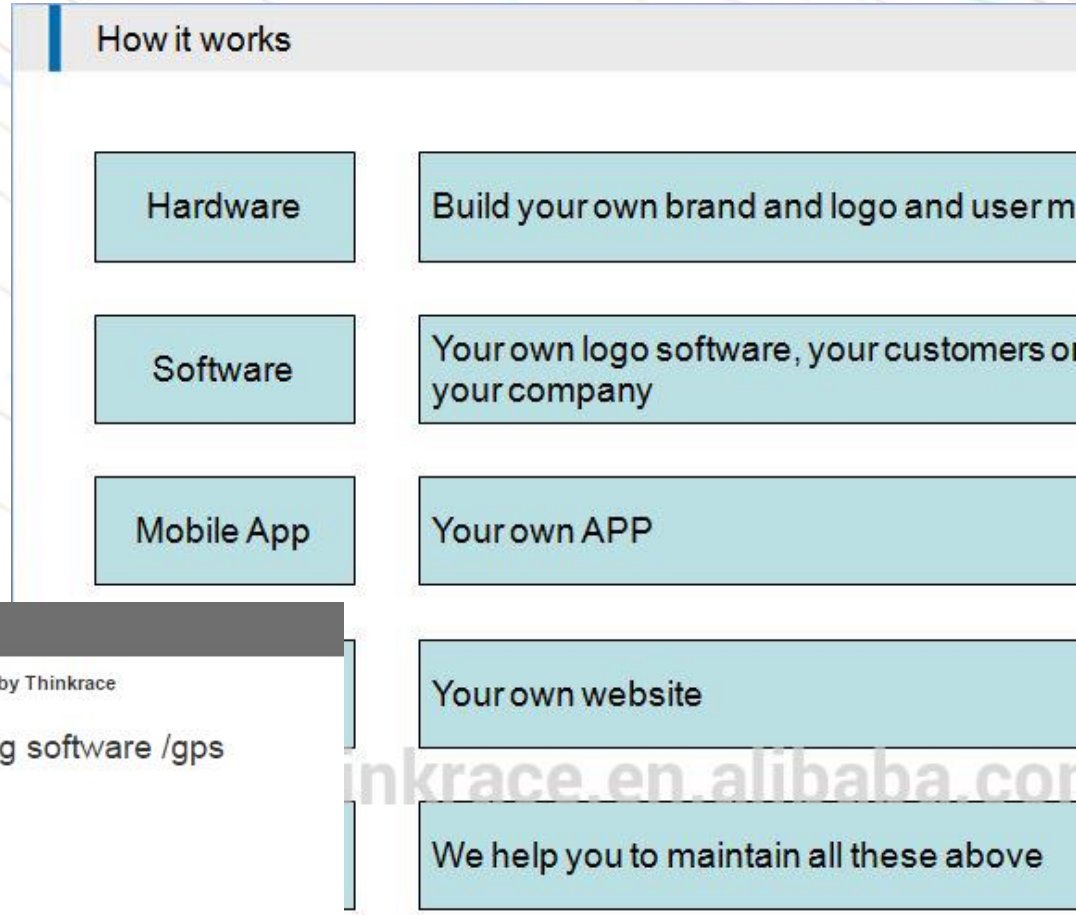


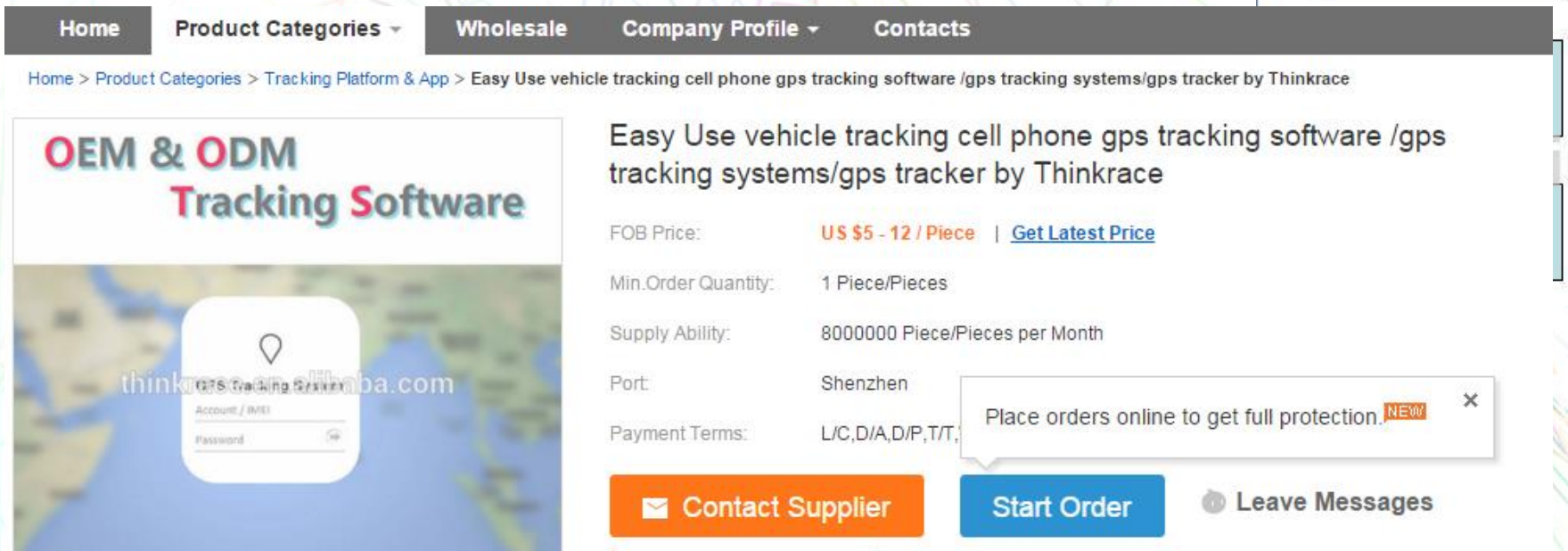
- There are over 50+ rebrands of this same application


Satellite
SKYCOP
www.skycop.my
Satellite
112
KEGEMASAN
Hakcipta Terpelihara Skycop 2015

Why use a host, when you can license?

- Looking further into the Alibaba page…
- It looks like, you too can be a lucky licensee of this web app.
- Fun for the whole family!
- (Batteries not included)





Heyyyyy bu

- Emailed the
- They can hos
  obviously we
- Looking at a
- Unfortunate
  for such a pr
- But we can c
- Lets see wha

ding professional
tware solutions, we

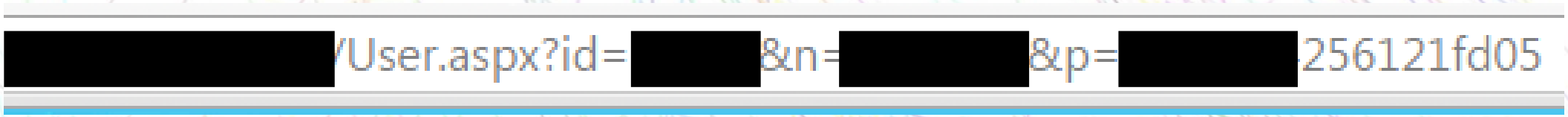
plain to you

own server or rent

one.

Authenticate!!! Human!!!

- According to the manual:
- Your login is the last seven digits of your serial number
- Which is on the device of course, but then your password is uh...
- Also the last seven digits of your serial number
- Nice one, lets go ahead an login shall we?
- Cleartext password submission, great stuff!



GPS [redacted]

[redacted] Hello Message(0) Change password Exit

Monitor Statistics More▼

[redacted]

[redacted])

Select : Please input name/IMEI No.

All(1) Online (0) Offline (1)

+Add Group

Default(1)

[redacted] Offline

Google Map ▼ Target name

Map Sat 30 Refresh after seconds!

[MUFFLED "AYY LMAO" IN THE DISTANCE]

Canada United States Mexico Greenland North Atlantic Ocean Venezuela Colombia Brazil Peru Bolivia Chile Argentina South Pacific Ocean

Safety Make Better Life

Device D

“Hopefully it’s not complete shit”

- So coming back to what nikto found
  - /log contains custom logs of ASP.NET exceptions, hostname, and application routes
  - /lib and /js have some really terrible Javascript files, a few of which have private API keys in them
- Poking around with Burp and other tools reveal things like
  - XSS on a few things, nothing stored unfortunately
  - No CSRF protection, no anti clickjacking, or fancy headers
- You can change the password and other details on the “demo” user, meaning nobody can use it anymore (hehehe)
- WSDL exposes all route information, this is pretty great, everything is easy

“Hopefully it’s not complete shit” II: Electric Boogaloo

- So after poking through the app and changing various target values it turns out that:
- **Requesting data from a user ID that is not yours, requires no authentication.**
- What does this mean?
- We can **access everyone’s information** on that app, so just to remind you…

Oh god everything is terrible

- View information including:
  - Where the device is
  - Speed/distance/travel log
  - If the device is online/offline, and last time it was in contact
  - Command history
  - User information
  - OBD2 information if the device supports
  - IMEI/IMSI
  - Panic status
- Perform actions on the device like:
  - Query latest location
  - Set a “geo-fence” with txt alerts
  - Send commands (like the phone ones)
  - Change user details (passwords, device labels, etc)
  - Change logging settings
  - But now that we can access this between users, what can we do with it?

Oh dios todo es terrible

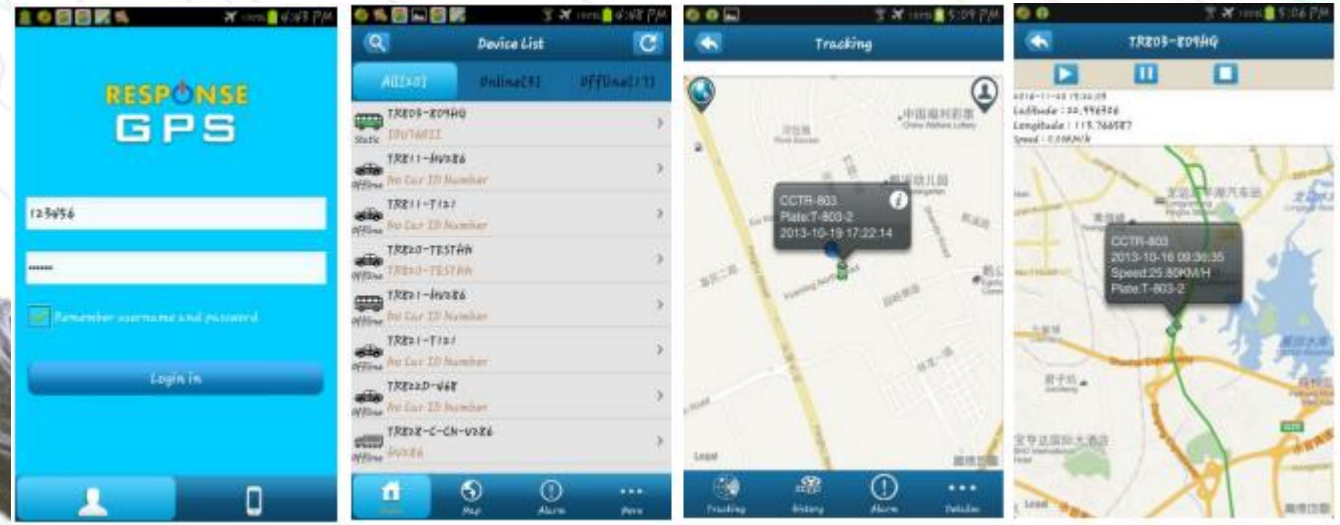
- So how does this flaw work?
- And more importantly
- How do we exploit it?
- The ASP.NET app
  - Has view routes that get JSON information, but we're interested in the actual JSON returning ones, most of which are .asmx
  - We can use WSDL to discover the details of each route, then use Burp to change the variables
- In this case, we change the user ID, and boom, we get their information instead of ours
- This is a very trivial flaw
- We can also iterate through every user ID (more on this later)
- Now, we're not actually limited to that surface value of information, lets see what else is possible with this...

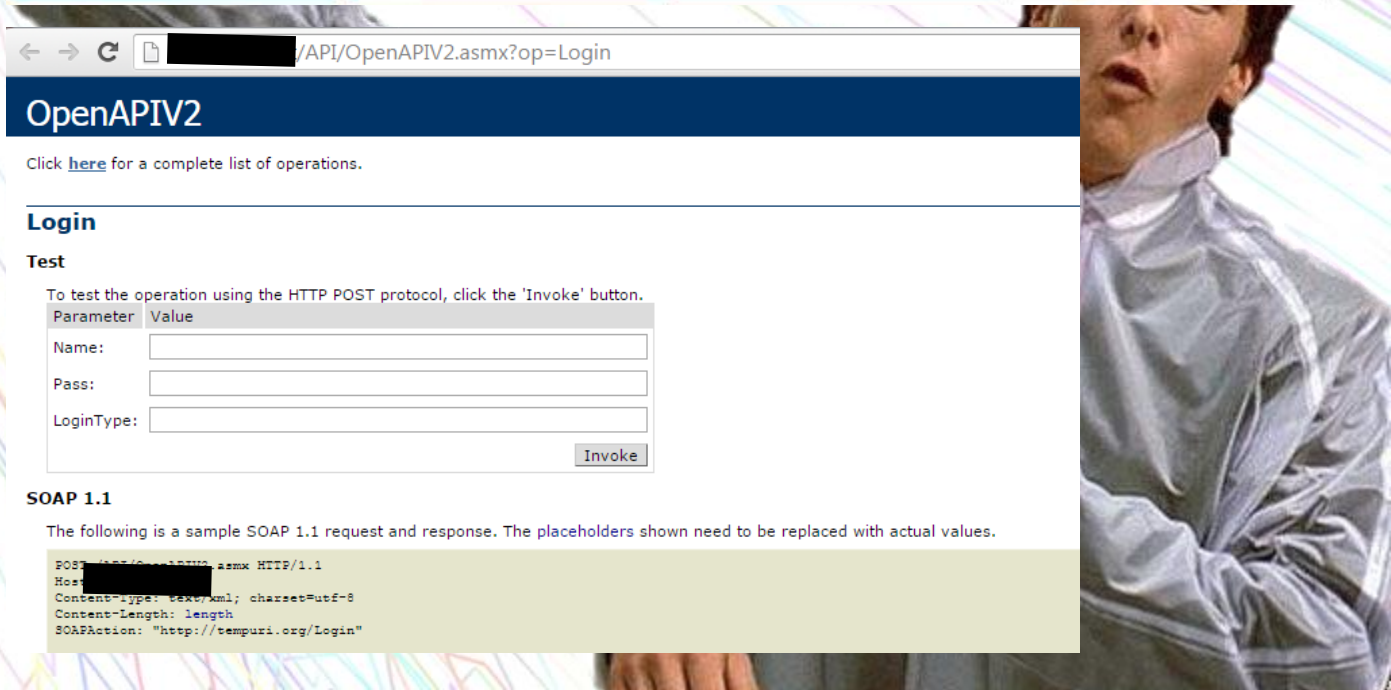
“Hopefully it’s not complete shit” III: More Bugs 4 Free

- That’s not all folks! Other possibilities due to this mother-of-a-flaw include:
- **Disabling someone’s vehicle maliciously, even while they are driving (this is not cool, and very dangerous),** if they use the relay feature
- Using the command log to find their registered phone number, then **registering your own number to the device for malicious purposes**
- After we do that, we could then **listen through the microphone of the device, the user completely oblivious**

We haven't even looked at the mobile app yet

- Horrid UI, akin to the web app as you'd expect, so let's skip all that noise
- Decompilation to .java reveals an API route (similar to the earlier susceptible JSON ones in the web app)
- Is it vulnerable?
- Yes. Of course it is
- It's probably easier to exploit the flaw on this route though

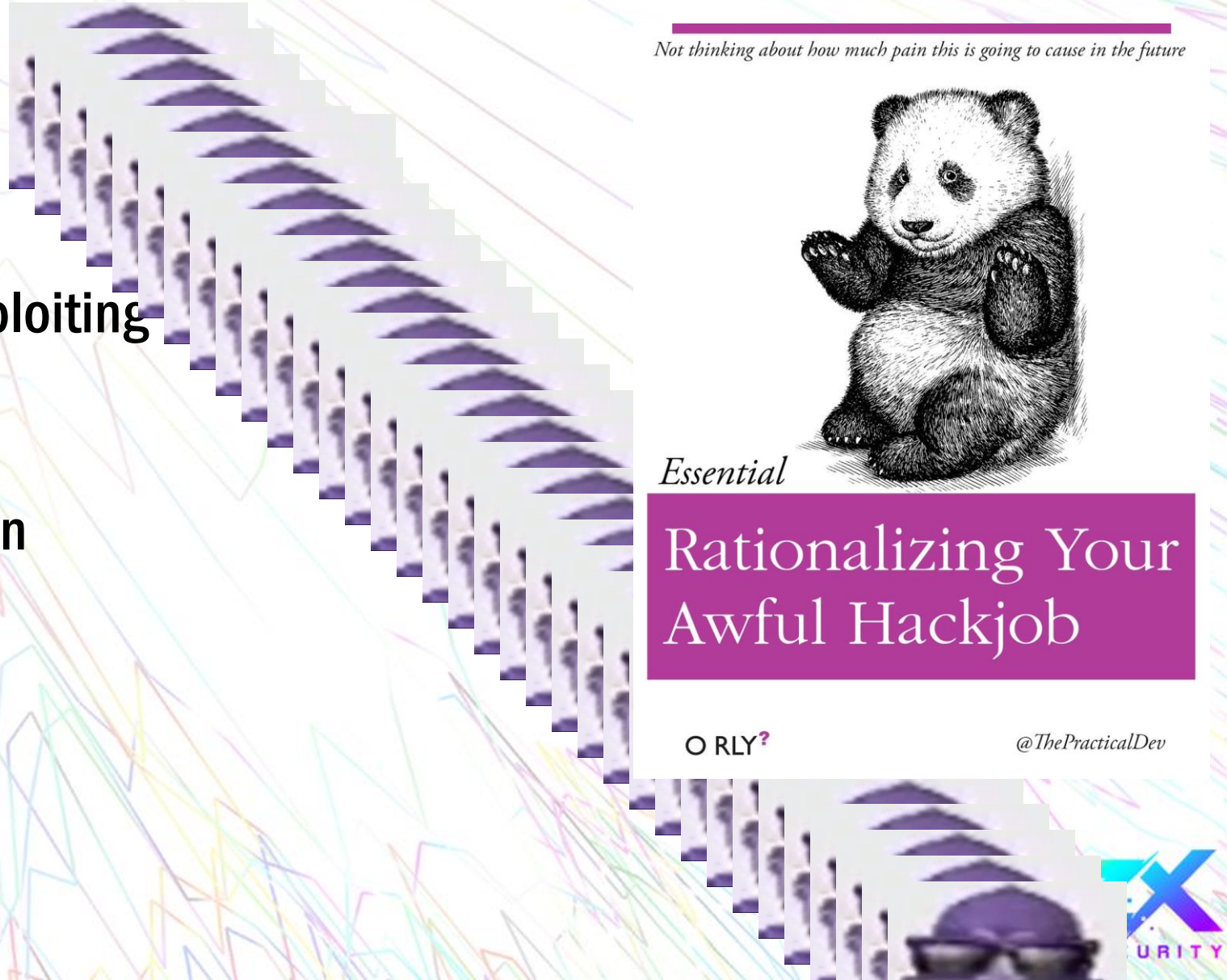




WE INTERRUPT THIS PRESENTATION

Much ado about data

- This is where it gets “cool”
- So what can we do with this vulnerability beyond actually exploiting it?
- Well we can retool it! With python magic!
- But what’s the goal?



gpscrape.py

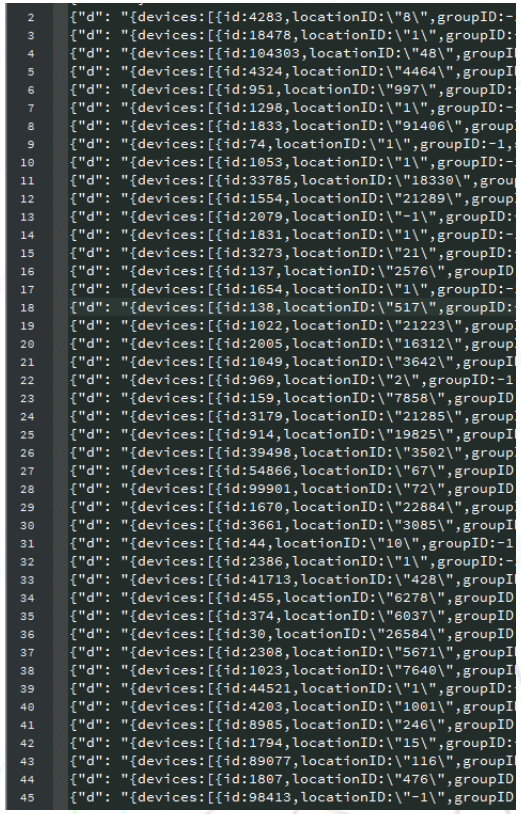
- Find a host (easy to do with google dorks)
- Automatic dumping of data including:
  - Where the device is
  - Speed/distance/travel log
  - If the device is online/offline, and last time it was in contact
  - Etc, we've been through this before
  - Everything, all entries too, we want ALL THE DATA!!
- But once we have all the data what do we do with it?

```
import requests
from scrapy.selector import Selector
import demjson
import json
import argparse
import re
import time
import inspect

_DOMAINS = ['test1', 'test2']
_LOGINS = ['1234', '0039793', 'test', '1234', '0000', '000', '000
_TARGET = ''
_ROUTES = {'Login' : '/Login.aspx', 'GetDevicesByUserID' : '/Ajax
_ARGS = {}
_SESSION = requests.Session()
_USER = {'id' : 0}
_PROXIES= {'http' : '127.0.0.1:8080'}
_TIMEZONE = 'UTC+12'

def initParser():
    parser = argparse.ArgumentParser(description='this is gpscrap
    parser.add_argument('domain', nargs='?', default='track.solut
    parser.add_argument('proxy', nargs='?', default='')
    global _ARGS
    global _TARGET
    global _PROXIES
    _ARGS = parser.parse_args()
    _TARGET = 'http://' + _ARGS.domain
    if _ARGS.proxy != '':
        _PROXIES = { 'http' : _ARGS.proxy, 'https' : _ARGS.proxy
    return True
```

More about gpscrape.py

- Uses the Requests library for EZ HTTP management, then Scrapy's selector tools to pull specific information out.
- Can also iterate through IDs and look for valid logins, and find common logins (1111, 1234, etc)
- Will also operate through a proxy like BuRP so you can capture specific requests etc
- Was planning to add auto-enumeration of hosts through google dorking but never got around to it
- My boss says I shouldn't release it…
- …but buy me a beer at the bar if you're interested.

RAW JSON



An average instance dump is around 40mb of text json data

CO-ORDINATES

(and metadata)

LAT -24.008690

LNG -42.008690

Some databases contain over 90,000 co-ordinates

ANALYSIS

(and storage)

Parsing 90k co-ords in google maps hurts my soul

90k data points for over 30 hosts.
Imagine that on a map.

Google Map ▾ | Target name

Search | 7 Refresh after seconds! | Traffic | Map

AMAR(70/70)

ice List(52/70) | Online

e input name/IMEI No.

ault(2) | +Add Group

26854	Stop	Tracking | Playback More ▼
2013	Stop	Tracking | Playback More ▼
AR (24)		
2650	Offline	Tracking | Playback More ▼
86046	Stop	Tracking | Playback More ▼
5441	Stop	Tracking | Playback More ▼
8332	Stop	Tracking | Playback More ▼
34776	Stop	Tracking | Playback More ▼
14298	Stop	Tracking | Playback More ▼
1574	Stop	Tracking | Playback More ▼
15999	Stop	Tracking | Playback More ▼
42076	Stop	Tracking | Playback More ▼
62931	Offline	Tracking | Playback More ▼

e Detail List

Elfaki Hashim
الفكى هاشم
Ombada
أمبدة
DarDooG
دردوق
Green Valy
الوادي الأخضر
EAST NILE
شرق النيل
الصفوة
Umm Dawm
أم دوم
مرابيع
الشريف
Abu Groon
أبوقرون
Tayba
Alhasanab
طيبة الحسناب
Alosaylat
albu-wayla
White Nile
Blue Nile River

عمار فستو 869
عمار كاوس 5441
عمار كليك 1949
عمار اكسدت 34776
كليك خالد يحيى
12189 علي
26854 ي
1599
كليك م.سعد
8221 علي
3470 فستو
عمار كليك 24246
عمار كليك 27104
كليك م.عثمان
كليك كركاب
كورولا 40540
كورولا 26540
711 كليك
كليك 9974
عمار فستو 804
عمار برايم 1574
سوتي 22158
عمار كليك 13018
تمساح فستو 29226
عمار فستو 30050
تمساح فيستو 2863
32693 علي
خالد يحي 14209

Alarm Overview | Alarm sound on

Target Name	IMEI Number	Alarm Type	Alarm Time	last update	Typ
14209 خالد يحي		GEO-fence In (الخرطوم)	2016/04/30 03:58	2016/04/30 03:58	GT0
5441 عماراوس		Offline	2016/04/30 01:50	2016/04/30 01:50	GT0
14209 خالد يحي		GEO-fence Out (الخرطوم)	2016/04/30 01:31	2016/04/30 01:31	GT0
14209 خالد يحي		GEO-fence In (الخرطوم)	2016/04/30 01:25	2016/04/30 01:25	GT0

.
@skooooch

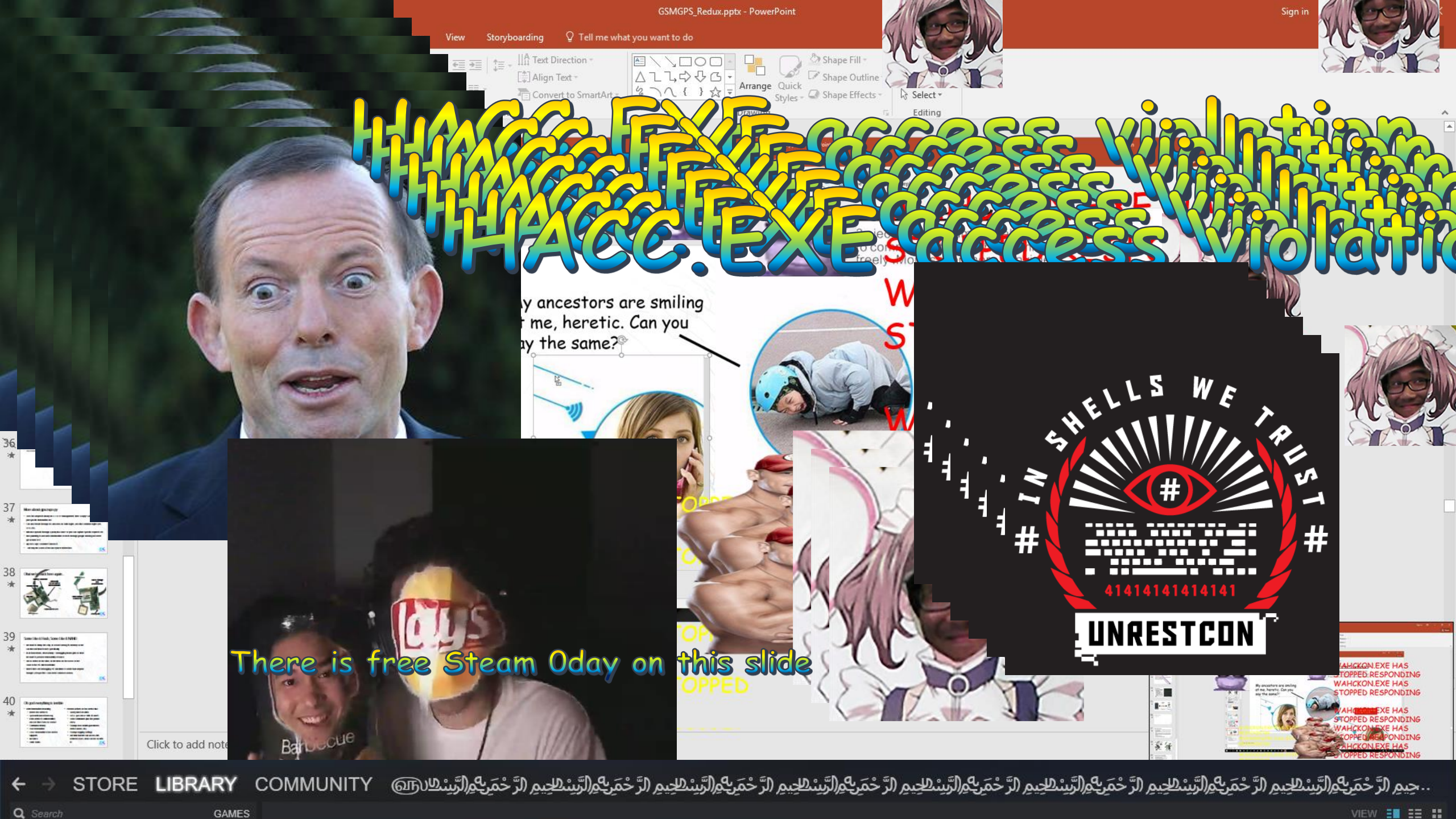
@thegrugq is there a name for intelligence acquired by compromisation of an unaware or neutral party?

8:19 PM - 13 Apr 2016

Reply to @thegrugq

the grugq @thegrugq · Apr 13
@skooooch nothing springs to mind

1


HACC.EXE access violation
HACC.EXE access violation
HACC.EXE access violation
GSMGPS_Redux.pptx - PowerPoint
View
Storyboarding
Tell me what you want to do
Sign in
Text Direction
Align Text
Convert to SmartArt
Arrange
Quick Styles
Shape Fill
Shape Outline
Shape Effects
Select
Editing
ancestors are smiling
me, heretic. Can you
the same?
There is free Steam Oday on this slide
IN SHELLS WE TRUST
41414141414141
UNRESTCON
WAHCKON.EXE HAS STOPPED RESPONDING
STORE
LIBRARY
COMMUNITY
Search
GAMES
VIEW

Ohai we're back here again...

Some Like it Flash, Some Like It NAND

- We want to dump this chip, or at least debug its memory so we can find out what it does specifically
- In an ideal world, disassembly + debugging would give us what we want to perform vulnerability research
- Do we work on the NAND or the Flash of the PIC microcontroller?
- Well it turns out debugging PIC hardware is easier than anyone thought. (Perspective: I had never soldered or touch a multimeter before in my life)
- You can do this too

PIC a chip, any chip...

- What is PIC?
- The PIC series of microcontrollers are made by a company called (funnily enough) Microchip Technology
- These MCUs (microcontroller units) have been around since 1993
- Our target is a PIC18F46K
- Model being PIC18, with 46K of address space (well, almost)

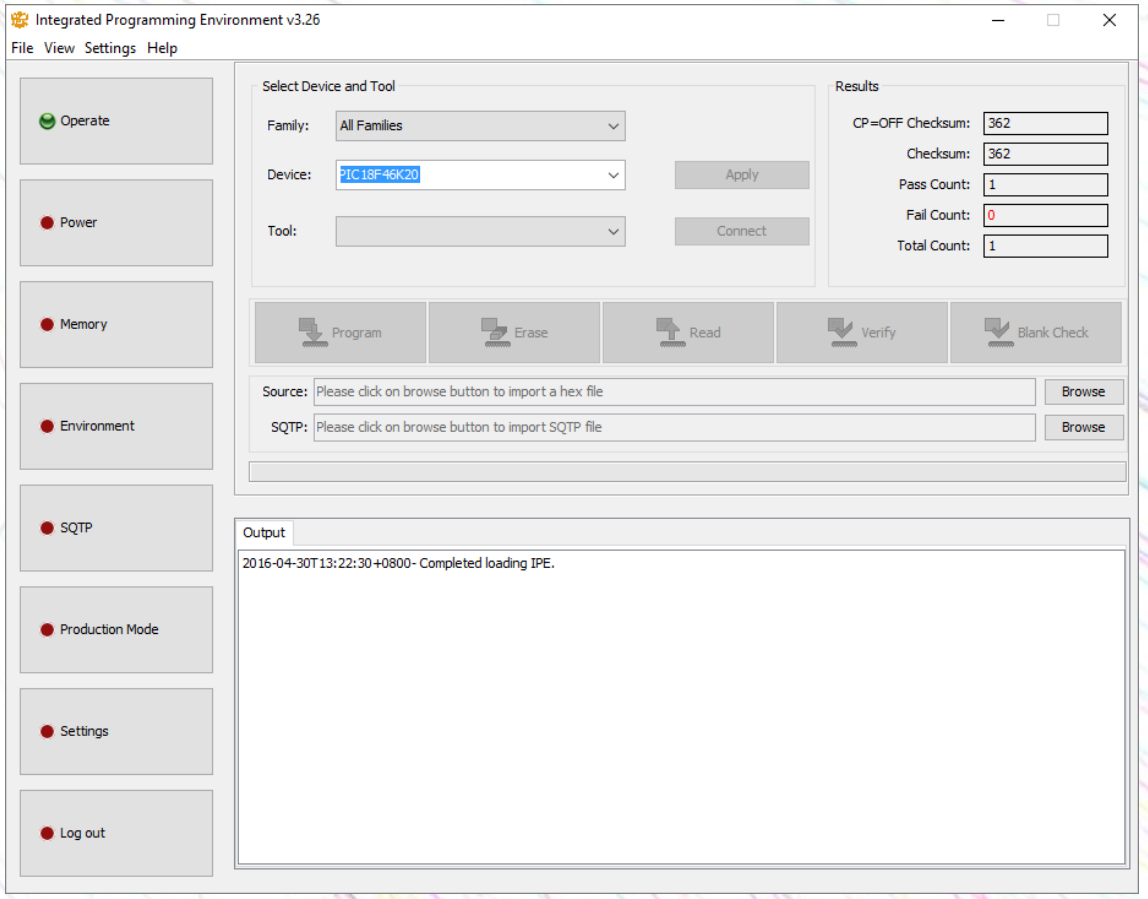
MICROCHIP

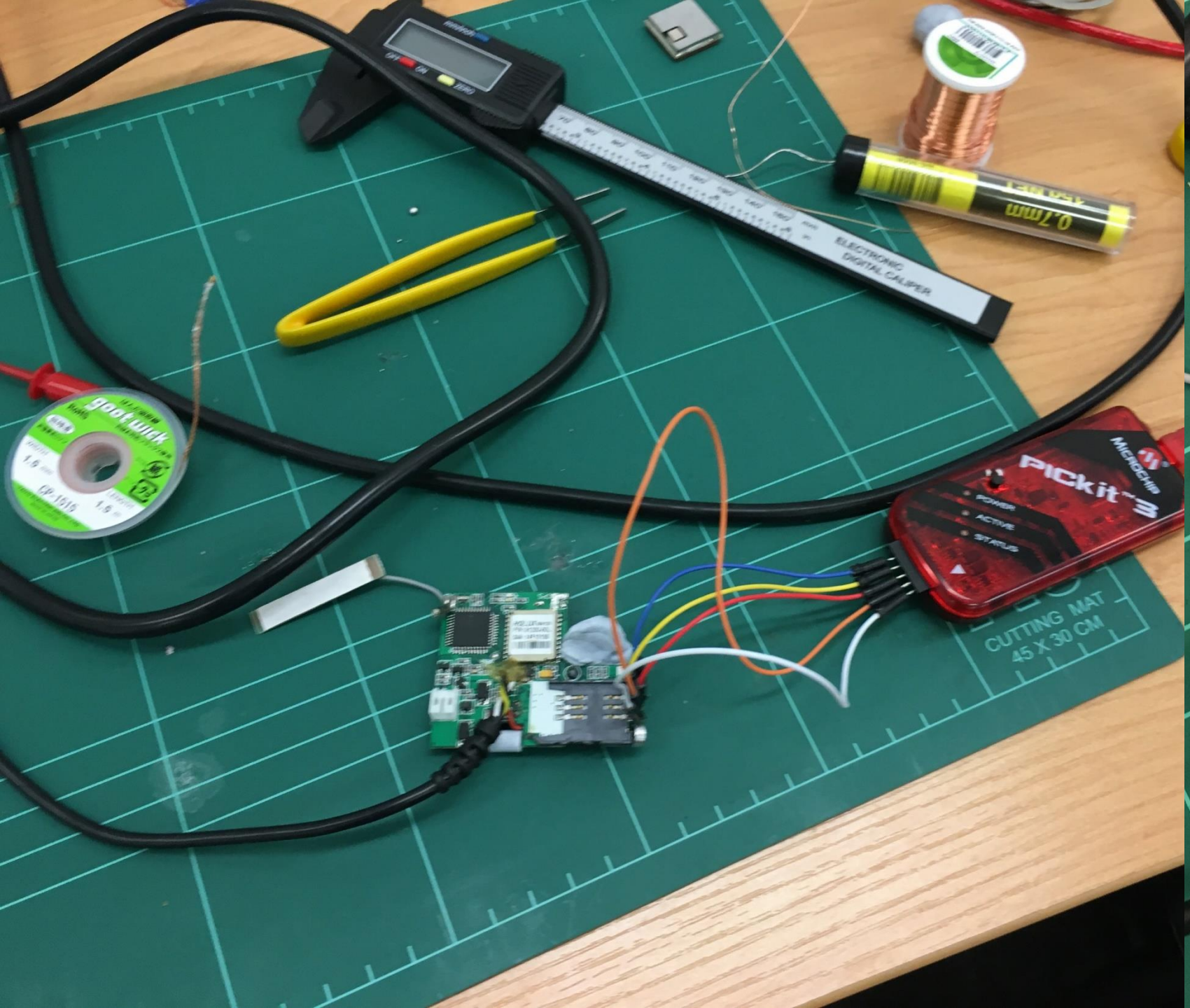
To debug, or not to debug

- Initially I thought I needed something JTAG wise, so I went to dangerousprototypes and got a Bus Blaster
- The Bus Blaster is a really cool open-source JTAG/SWD debugger, and can be mainupulated to debug other things.
- However it turns out nobody has written a driver for Microchip's proprietary ICSP (In Circuit Serial Programming) below the PIC32
- But what does Microchip offer officially?

PICkit


MICROCHIP
PICkit 3
POWER
ACTIVE
STATUS


Integrated Programming Environment v3.26
File View Settings Help
Operate
Power
Memory
Environment
SQTP
Production Mode
Settings
Log out
Select Device and Tool
Family: All Families
Device: PIC18F46K20
Tool:
Apply
Connect
Results
CP=OFF Checksum: 362
Checksum: 362
Pass Count: 1
Fail Count: 0
Total Count: 1
Program
Erase
Read
Verify
Blank Check
Source: Please click on browse button to import a hex file
SQTP: Please click on browse button to import SQTP file
Browse
Browse
Output
2016-04-30T13:22:30+0800- Completed loading IPE.


MICROCHIP
PICkit 3
POWER
ACTIVE
STATUS
CUTTING MAT
45 X 30 CM


HOLUX M-9139
P/N: 91200-00L
S/N: 14F10156

How do we use the PICkit?

- Download
- Solder hea
- Connect th
- Export the
- The IPE too atures
- Looks like

2016-04-30T13:34:06+0800- Hex

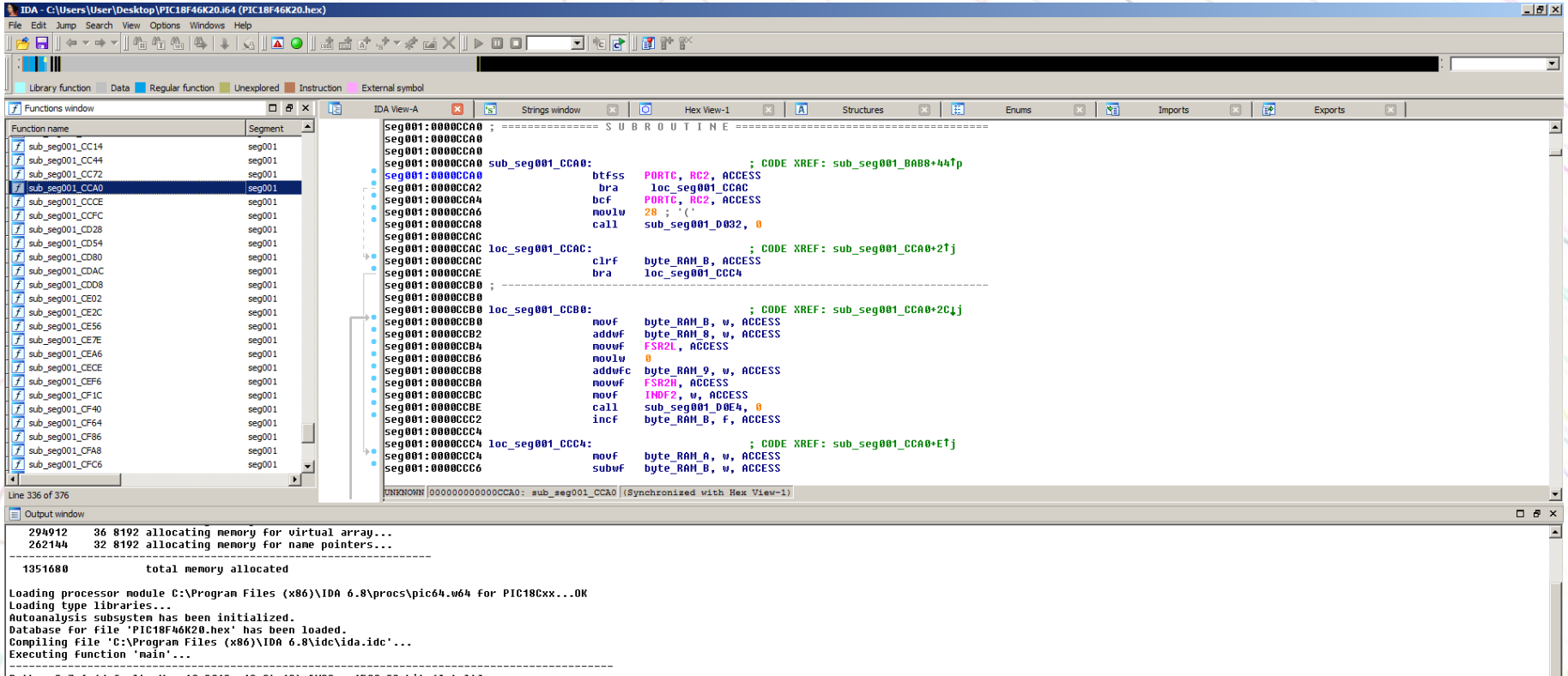
C000h-00FFFFh) not write-prote
ion registers (300000-3000FFh) r
(000000-0007FFh) not write-pro
OM not write-protected

Memory View

e	Value	Field	Option	Category	Setting
		EBTR1	OFF	Table Read Protection Block 1	Block 1 (004000-007FFFh) not protected fr
		EBTR2	OFF	Table Read Protection Block 2	Block 2 (008000-00BFFFh) not protected fr
		EBTR3	OFF	Table Read Protection Block 3	Block 3 (00C000-00FFFFh) not protected fr
FIG7H	40	EBTRB	OFF	Boot Block Table Read Protection bit	Boot Block (000000-0007FFh) not protected

Lettuce reverse

- Originally I spent lots of time looking for a PIC specific disassembler but then realized that
- IDA supports PIC dissassembly



I’m not actually very good at assembler

- This is really good, but I can’t read this yet
- IDA refuses to give me flow graphs for this processor type too, meaning I can’t even get a visual resource
- Oh but wait Google just bought zynamics so BinNavi is free
- Cheers.

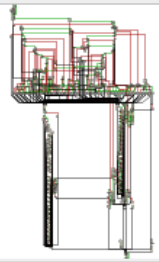
sub_AEE - PIC18F46K20.hex - null - BinNavi

View Graph Selection Search Plugins Window

sub_17A sub_AEE

Address Search

Overview

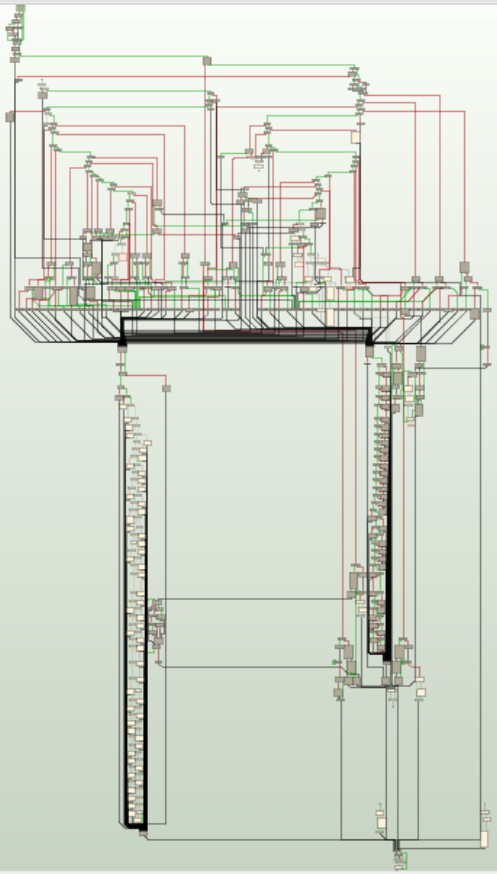


Graph Nodes

In	Out	Node	Color
0	2	00000AEE	
1	2	00000B10	
1	2	00000B22	
1	1	00000B38	
1	2	00000B40	
1	1	00000B56	
2	1	00000B5C	
4	2	00000B5E	
1	1	00000B64	
2	2	00000B78	
1	1	00000B7C	
1	2	00000B96	
1	2	00000BBA	
1	2	00000B...	
1	2	00000BD2	
1	1	00000BDE	
1	1	00000BEA	
1	2	00000BEC	
1	2	00000BF0	
1	1	00000C04	
2	2	00000C08	
1	1	00000C0E	
1	2	00000C12	
1	1	00000C16	
1	1	00000C1C	

Selection History

Selection History



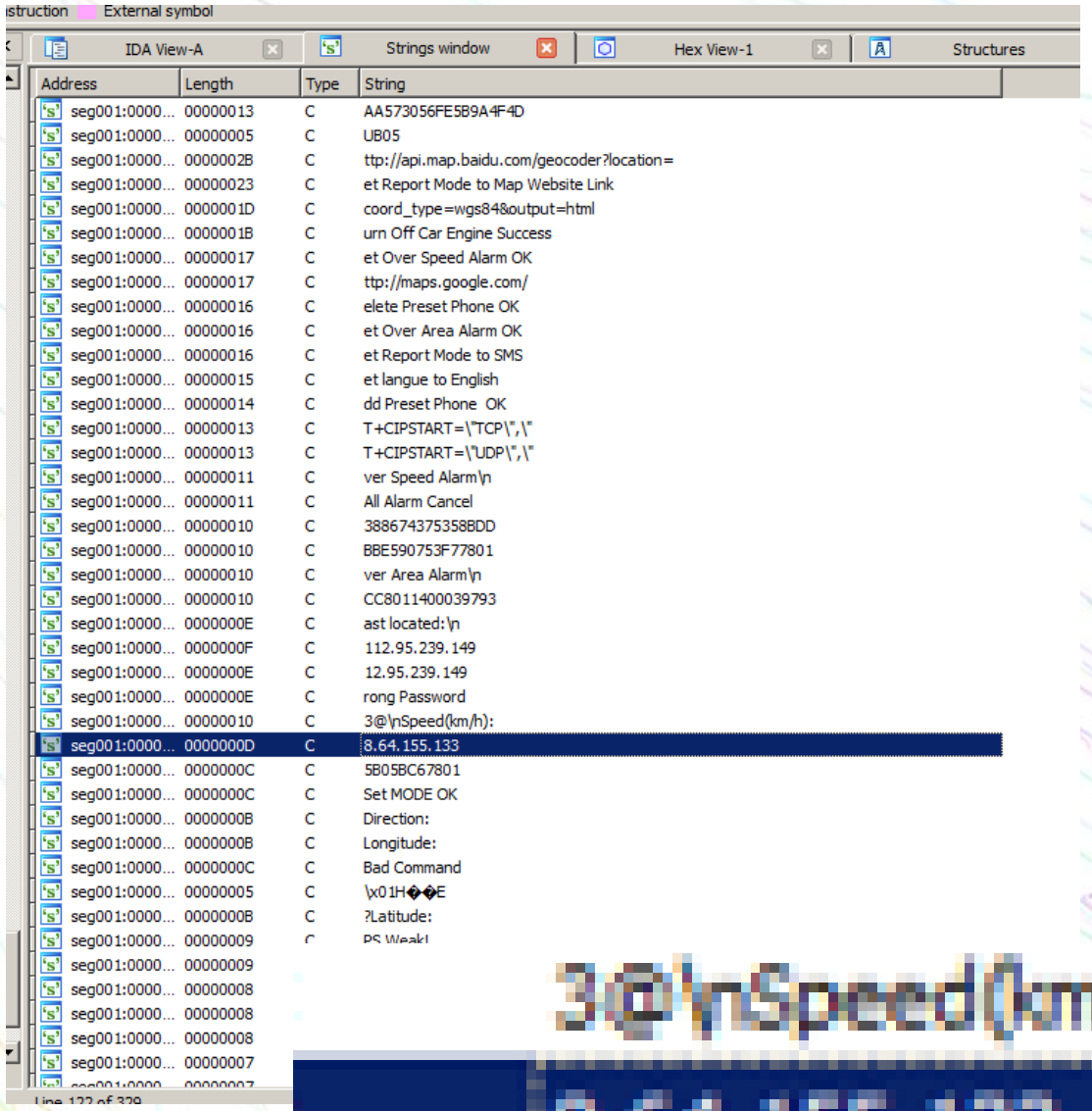
Variables Calling Functions Register Tracking Special Instructions Code Bookmarks

Tagg Proto Stack Type

Start

Interesting things

- We can now search for key subroutines
- ThinkRace left the gates wide open on this… again
- I wish I had more experience in reversing, but time is aplenty and data is forever
- Oh but guess what I did find in there?



Places to go and things to do

- Learn the PIC-specific assembler and do some vulnerability research
- Can we reflash the chip with our own firmware?
- There's a firmware update server and we can remotely trigger it
- More endpoints
- More devices

But what's happened since last time?

- In December of 2015 I gave a talk about this device at Kiwicon 9 in Wellington, New Zealand
- What's different about this one is that I've now done some more stuff with data, and also plenty of hardware hacking
- And then I also gave that talk at Wahckon 3 a couple months ago
- But what's actually happened with the devices or the vendor?

Nothing.

Nothing has changed, the vendor still manufactures and sells vulnerable products. And the resellers keep selling them.

This fucking sucks! (possible understatement)

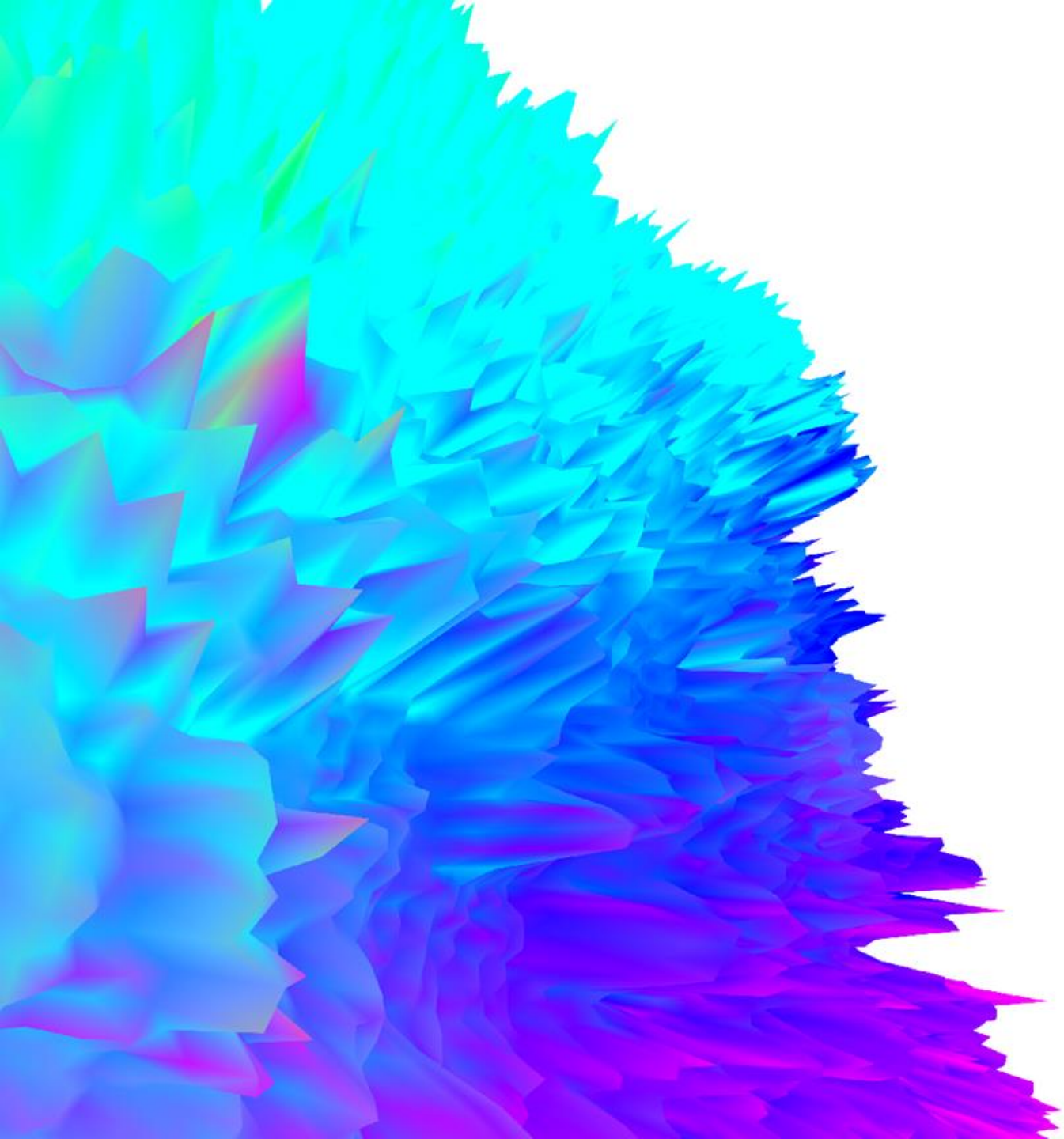
- Considering these are sold in retail to consumers, and online to more personal users across the world, and the severity of this trivial flaw, this is shockingly bad. But for some reason I'm not surprised or shocked.
- There's a lot of these devices

So if you think you may be using this device...

- **DO NOT**
- Uninstall it from your vehicle, and from your life. You should also probably wash your hands.
- Delete ~~System32~~ all your data from the web app
- Throw it away or remove the SIM from it so it can no longer continually compromise your privacy

In closing...

- You really pay for what you get
- Daily reminder that people are reselling this everywhere, apparently even some mechanics outfits will install these for you
- Cool generic gadget, pity that the software behind it is utter trash



Thank you!

Special thanks to:
The Ministers of Unrest
Bogan, Dave and Fabio @ ZX
Jayji, Zeh Matt, Nanomebia, (not) ss23

@skoooooch on twitter
ltmp@ltmp.me if you want to email me
http://ltmp.me/ for more information + slides
See me after and lets chat!