Boat electronics hacking

•••

for 33C3

Lasse Karstensen
@lkarsten / “scn”

Who am I

- Varnish Cache developer
- Racing sail boats in Oslo, Norway.
- Active in Oslo hackerspace Hackeriet (https://hackeriet.no/)


One-Design Class

Why hack boat electronics?

Mostly greenfield

Industry haven’t caught up with the times.

Wifi-bridges and satcom becoming more commonplace. (attack_surface++)

Odd platform archeology, there are 15-25 year old machines in use.

Everything is expensive, DIY makes sense.

We can make better software for these units. (if we want to)

To be clear:

I do not want anyone to run any ships aground.

Attacks

- Flood the communication bus, taking everything offline.
- Collide frames from a specific sensors. (compass, GPS position)
- Impersonate a sensor.
- Destroy units
  - bricking software updates
  - burn pumps by running them while dry
- On large ships with trim/balance tanks ..... (Hackers movie!)

Security concerns

- 1990s era systems. Should be fun.
- Are software updates over NMEA2000 really unauthenticated?
- Protocol stacks are probably fragile. Have they ever been fuzzed?
- Wifi bridges based on old OpenWRT/dd-wrt with default passwords? (vyacht)

Approach

- understand the problem domain (70-90% done)
- understand the protocols
- break out of the stupid vendor lock in
- win more regattas/races.
- (score internet points/likes)
- own entertainment

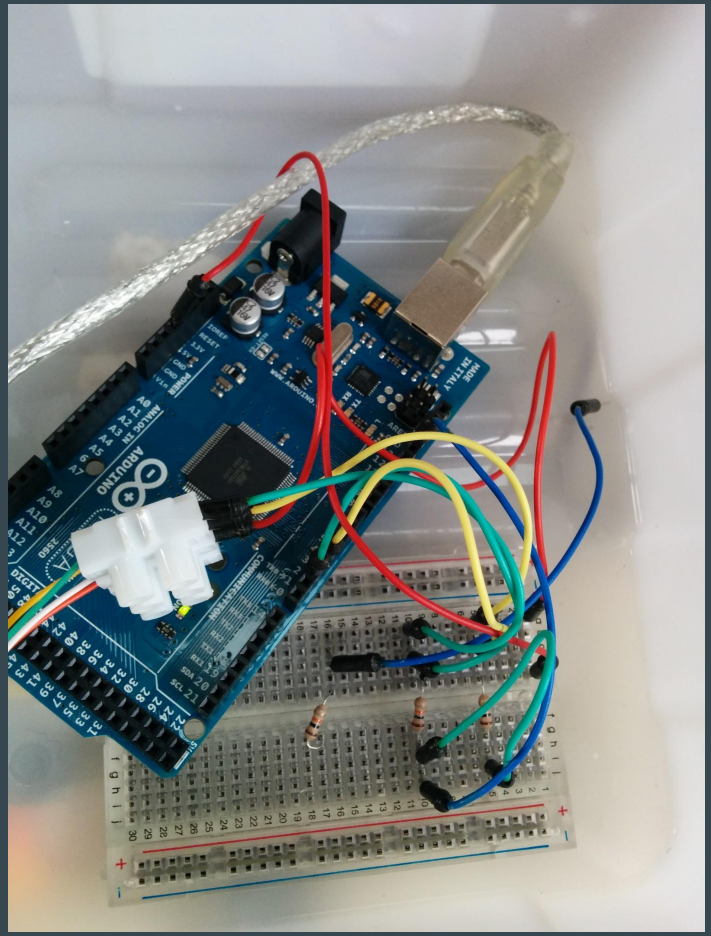
Initial attempts

Robert Huitema's Freeboard

Arduino interface for the wind sensor.

Limited success, too many "moving" parts.

Lesson learned: not a whole lot of fun to find sensor calibration coefficients. Let someone else handle the very basics.



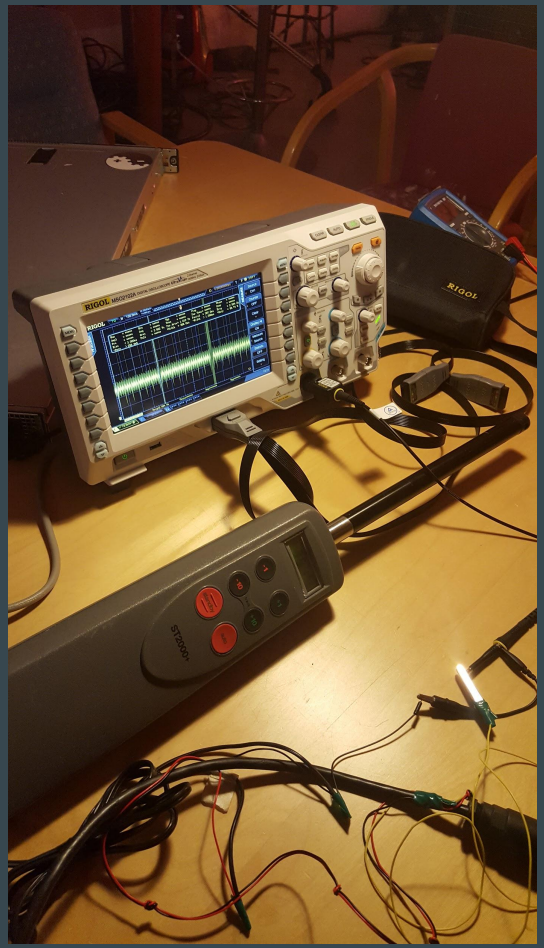
Buy lab equipment on Ebay

Project: Garmin GND10 decoder

- Garmin GND10 is a network bridge/converter. NMEA2000, USB and Nexus FDX.
- GND10read.git parse the FDX output on the USB port and make it readable as json or nmea0183.
- I think this is the only FDX decoder available for free. Actually done!

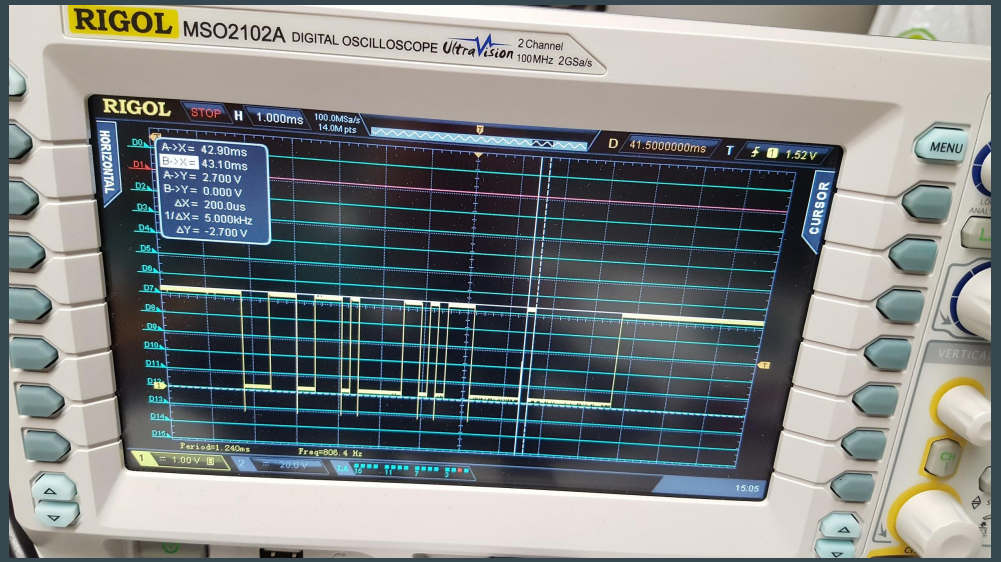
Project: Autopilot interfacing

- Raymarine ST2000+ tiller pilot. Hooks onto the stearing tiller, moving it back and forth.
- Seatalk and basic NMEA0183 protocols.
- Converters units available online (100EUR ++)
- I want to play with the raw protocol.
- Idea: Arduino shield/reference design, have some fun.



Project: Autopilot interfacing (II)

- Seatalk is a 4800baud, 9bit (!!) TTL serial bus.
- Idea: Arduino shield/reference design, have some fun.
- End goals: steer by wind direction, send course changes, write configurator software.



Project: B&G units

B&G H5000 is considered as a high-end racing gear.

Sensors, displays, “central CPU”, autopilot.

About half of the boats on the ongoing Vendee Globe single handed around the world race is using B&G.

B&G (II)

The H5000 series runs Linux on Freescale i.Mx ARM SoCs.

Software images are ubifs. Extracting works with a bit of effort.

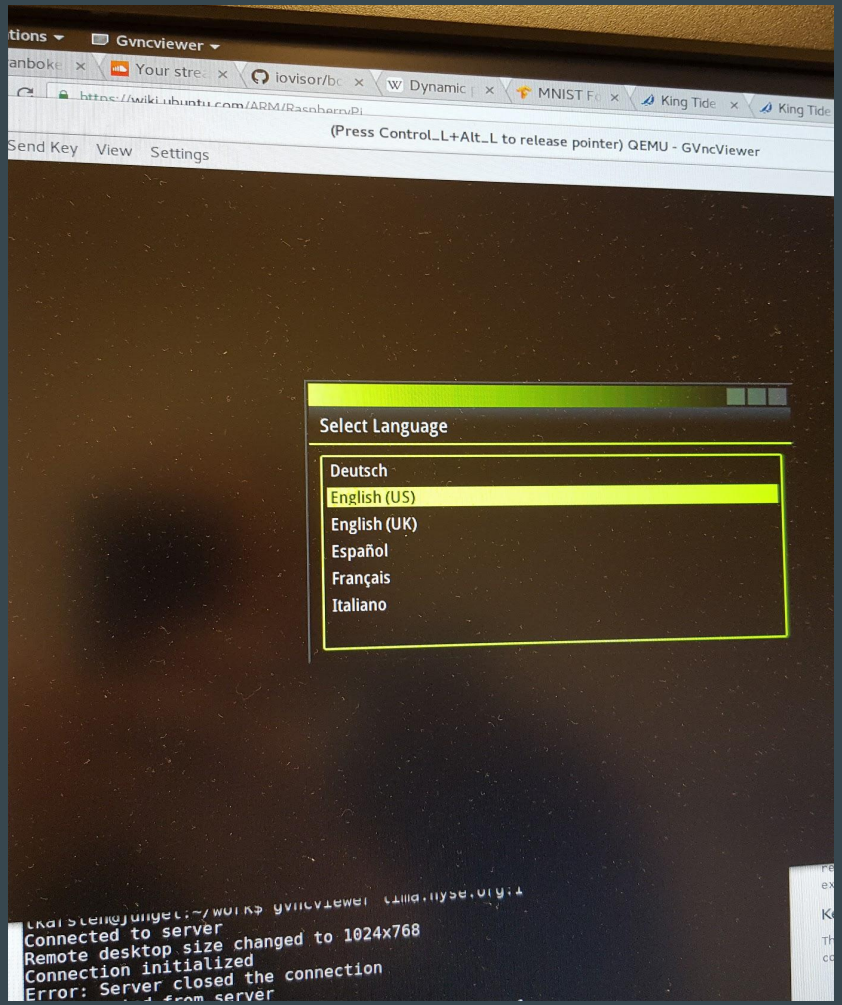
Hashes in /etc/shadow ...

B&G (III)

With a standard debian kernel, it boots in qemu!

Both H5000 “CPU” and display (“MFD”) software running.

(image is the initial setup dialog, since settings file is missing ..)



B&G (IV)

Next up:

- get CANbus networking into the qemu environment
- get input to work reliably. (convince the QT5 application there to accept mouse events)
- B&G sensors (I think) are MSP430, would be fun to get the “intelligent” of those running as well.

Help appreciated!

Project: Garmin units

Garmin has a suite of “smart” displays and sensors.

I think most of the new ones are ARMv5.

Software updates are bundled in “GUPDATE.GCD”. 600MB undocumented blob.

First goal: Extract the different firmwares from the GCD file. Help appreciated!

Why run the images standalone?

- Interoperability testing
- Training. The B&G and NKE platforms are expensive and hard to get to
- (and of course it makes fuzzing and similar efforts easier)

(comparable to what dynamips did for Cisco IOS training)

Not covered

SignalK stuff. I don’t want to pick on it right now. :-)

Autopilot software. Scary. Interesting math?

openracebox project (Use IMU to correct GPS and wind measurements)

Setting up a community

- Coordinate and show off our work.
- Cool and more tangible stuff to show off next year.

I suggest: #hacking on the http://slack-invite.signalk.org/

- other chat room? email list? wiki somewhere?

Contact

lasse.karstensen@gmail.com is simplest.

@lkarsten on the twitters

@lasse on signalk-dev slack team

scn on #oslohackerspace on freenode