ROSEN Digital Business Solutions

Swimming IoT
or how to hack yachts

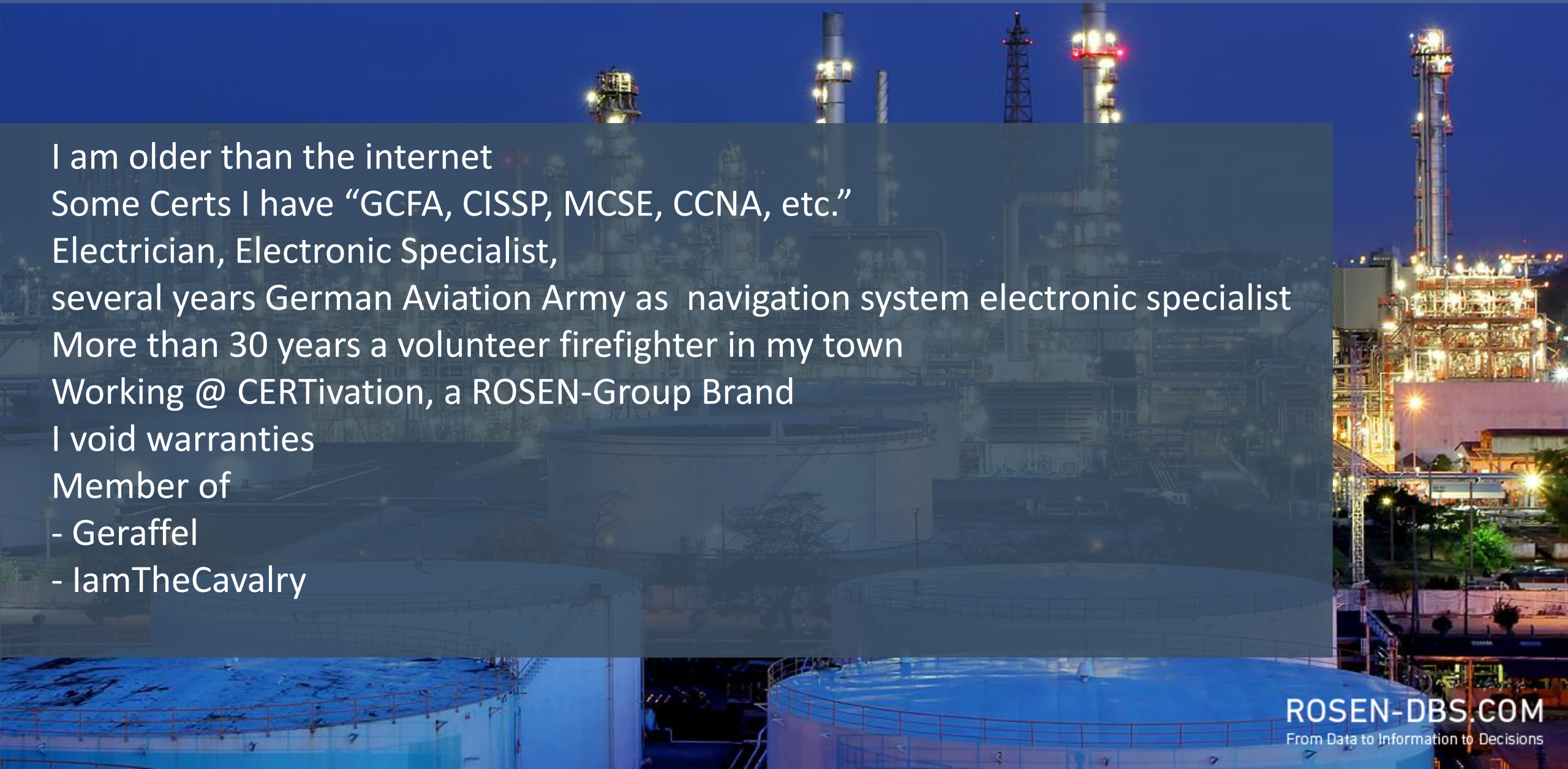
ROSEN-DBS.COM
From Data to Information to Decisions


FANDANGO
MOVIECLIPS

Agenda

- Who am I
- Yachts and ships
- Marine 1x1
- Different attack vectors
- How to look up your target
- Security bugs in a marine router

@ObiWan666



I am older than the internet
Some Certs I have “GCFA, CISSP, MCSE, CCNA, etc.”
Electrician, Electronic Specialist,
several years German Aviation Army as navigation system electronic specialist
More than 30 years a volunteer firefighter in my town
Working @ CERTivation, a ROSEN-Group Brand
I void warranties
Member of
- Geraffel
- IamTheCavalry

Business segments of ROSEN

- Through our business activities, we help customers to avoid leaks and spills by inspecting facilities, pipelines and tanks
- We have inspected billions of square meters of Oil- and Gas-Pipelines with ultrasound, eddy current, magnetic flux leakage, optical and acoustic technologies, worldwide.
- We focused on safety and security of humans and environment
- ROSEN not only serves the oil and gas industry but also aerospace, marine, transportation and security

Accidents in 2017

Februar:	Containervessel 10h without access to Navigationsystem
18. Sep	Norwegian: GPS Jamming from eastern direction

US Navy involved in 4 collisions in eastern pacific

- Februar — USS Antietam in Bay of Tokios grounded
- Mai — USS Lake Champlain: collision with trawler
- 17. Juni — USS Fitzgerald: collision with freighter
- 21. August — USS John S. McCain: collision with Tanker

BBC NEWS

Sign in | News | Sport | Entertainment & Arts

Home | Video | World | UK | Business | Tech | Science | Magazine

THE DISRUPTORS

How will we shop in the future?

DISCOVER

Technology

How hackers are targeting the shipping industry

Share

digitalpresent.tagesspiegel.de/h

DIGITAL PRESEN

123456 war das häufigste Passwort, das User benutzten, um sich auf eine

Hacker kapert Yacht per Laptop

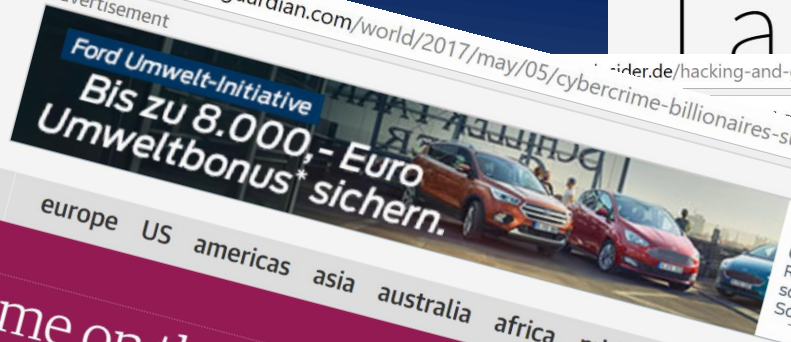
& CYBER, SEA

Was The Merchant Ship Hacked? McCain Collision Is First Run For Navy Investigators Cyber

By SYDNEY J. FREEDBERG JR.
on September 14, 2017 at 12:56 PM
36 Comments

Sicher | https://www.theguardian.com/world/2017/may/05/cybercrime-billionaires-superyacht-owners-hacking

Advertisement



home › world

europe | US | americas | asia | australia | africa | middle east | cities | development

Water transport

Cybercrime on the high seas: the new threat facing billionaire superyacht owners

Buyers at London superyacht conference shown the ease with which hackers can take control of vessels – and even procure private photos

ider.de/hacking-and-gps-spoofing-involved-in-navy-accidents-2017-8?r=US&IR=T

internal issues, as well as high operational tempos in
at could be related to the mishaps.

rships in the western Pacific —
nas stirred concern that outside
crews.

Capt. Peter Nilsen, commander of guided-missile cruiser USS Philippine Sea, on the ship's bridge, June 14, 2017.

h Hackerangriffe.

F-22 gefä

Süddeutsche Zeitung

SZ.de | Zeitung | Magazin

Wirtschaft | Panorama | Sport | München | Bayern | Kultur | Gesellschaft | Wissen | Digital | Karriere | Reise | Auto

Tip

IT-Sicherheit > IT-Sicherheit bei Schiffen: Auf falschem Kurs

6. September 2017, 05:50 Uhr Hacker und Schiffe

Wenn die Yacht wie von Geisterhand den Kurs ändert

Vessels, Yachts and ships

Overview

A **yacht** is a recreational boat or ship.

The term originates from the Dutch word jacht, which means "hunt"

It was originally defined as a light fast sailing vessel used by the Dutch navy to pursue pirates and other transgressors around and into the shallow waters of the Low Countries.

Size matters

Boot	up to 7m (20ft.)
Yacht	>= 10m (33 Fuß)
Super Yacht	bigger than 24m (79 ft.)
mega yacht	any yacht over 50 meters (164 ft.)

Superyacht

Indigo Star
Length 38,8m
Beam 7,7m

Swimming IoT

Modern vessels becomming swimming IoT devices

- Vessel Traffic Service (VTS)
- Automatic identification system (AIS)
- Autopilot
- GPS
- Radar
- Camera‘s, including Thermal imaging
- Engine control and monitoring (some now cloud based)
- Internet Access
- Entertainmentsystems

NMEA

NMEA 0183 (National Marine Electronics Association)

A combined electrical and data specification for communication between marine electronic devices, 4800 Baud speed

- echo sounder
- Sonars
- Anemometer
- Gyrocompass
- Autopilot
- GPS receivers

and many other types of instruments

NMEA

NMEA 2000

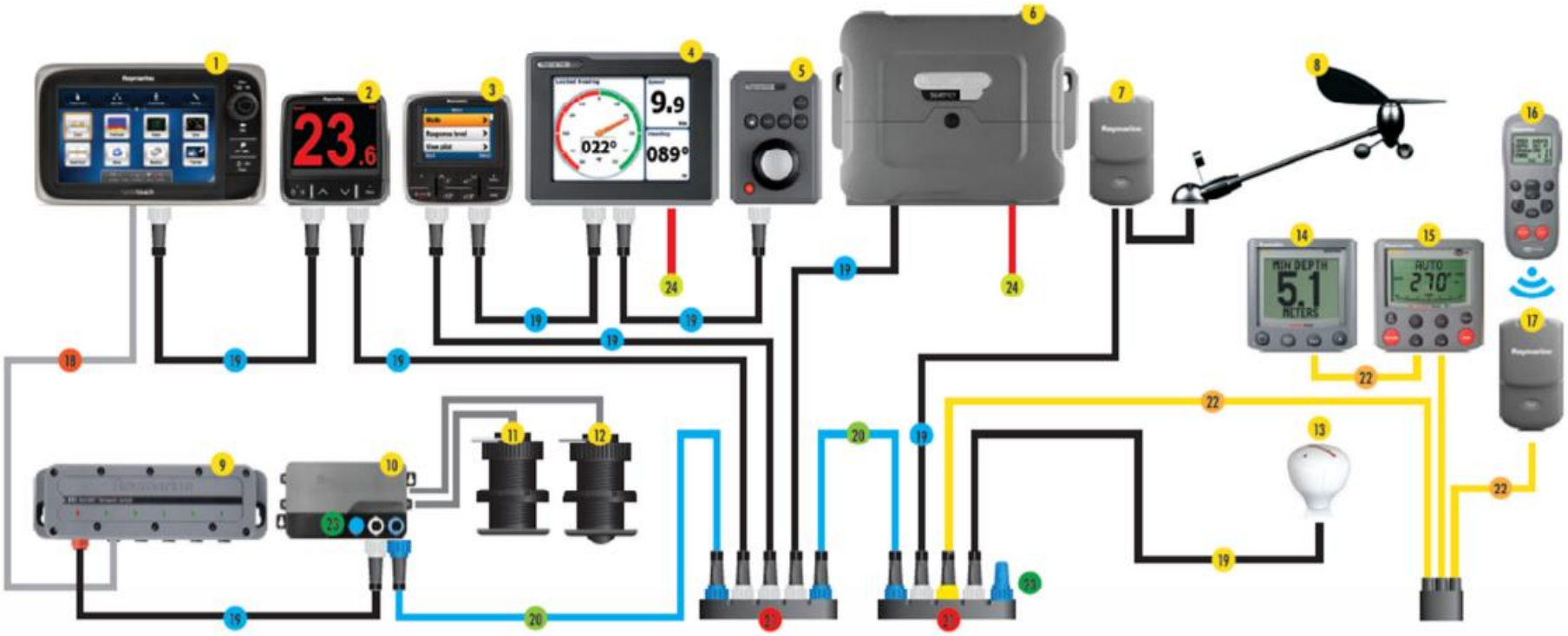
bandwidth capacities of less than 1Mbit/s

connects devices using Controller Area Network (CAN) technology originally developed for the auto industry.

NMEA 2000 network is not electrically compatible with an NMEA 0183 network

NMEA

SeaTalk*ng*



Note: Imagery for illustrative purposes only. Product images shown in suggested system diagrams are not to scale

Typical Basic SeaTalk^{ng} System:

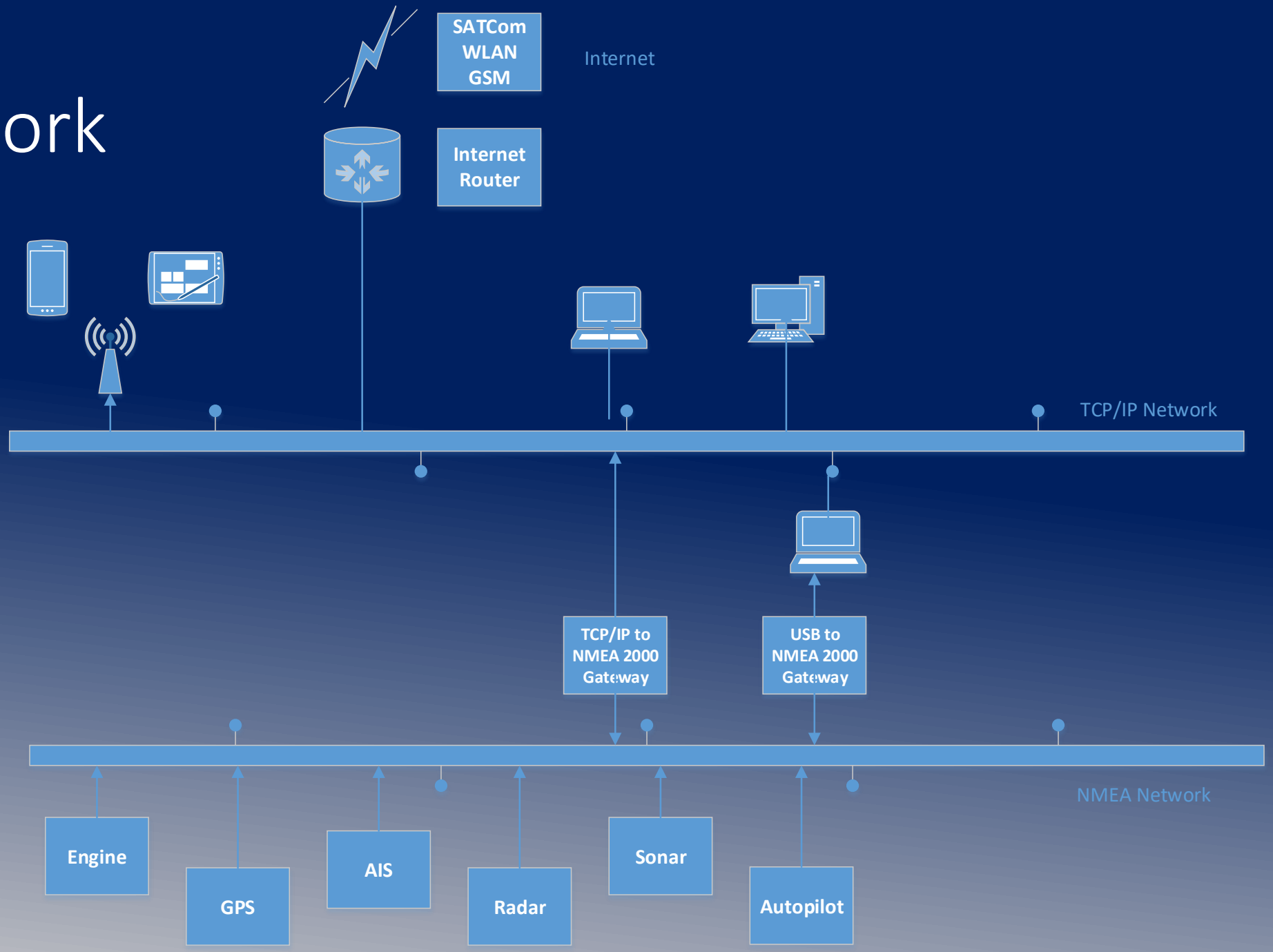
1. New e Series **2.** i70 Instrument **3.** p70/p70R Autopilot **4.** ST70 Plus Instrument **5.** ST70 Plus Autopilot Keypad **6.** SPX Course Computer **7.** Pod **8.** Wind Transducer **9.** Network Switch **10.** iTC-5 **11.** Speed Transducer **12.** Depth Transducer **13.** RS130 GPS Sensor **14.** ST60+ Instrument **15.** ST6002 Autopilot **16.** SmartController **17.** Pod **18.** RayNet Cable **19.** SeaTalk^{ng} Spur **20.** SeaTalk^{ng} Backbone **21.** 5-Way SeaTalk^{ng} Connector **22.** SeaTalk **23.** Terminator **24.** Power Supply

http://www.raymarine.de/uploadedFiles/Products/Networking/SeaTalk/SeaTalkng.pdf

SeaTalk^{hs}

http://www.raymarine.de/uploadedImages/Products/Networking/HS%20with%20HS5%20switch.jpg

Network


SATCom
WLAN
GSM
Internet
Internet
Router
TCP/IP Network
TCP/IP to
NMEA 2000
Gateway
USB to
NMEA 2000
Gateway
NMEA Network
Engine
GPS
AIS
Radar
Sonar
Autopilot

Marine Electronic

Vessel Traffic Service (VTS)

Automatic identification system (AIS)

Electronic Chart Display and Information System (ECDIS)

Autopilot

Internet Access

Vessel traffic service

A vessel traffic service (VTS) is a marine traffic monitoring system established by harbour or port authorities, similar to air traffic control for aircraft.

VTS systems use

- Radar
- closed-circuit television (CCTV)
- VHF radiotelephony
- automatic identification system

Automatic identification system (AIS)

AIS is an automatic tracking system used

- on ships and
- by vessel traffic services (VTS).

Satellite-AIS (S-AIS)

- satellites are used to detect AIS signatures

Automatic identification system (AIS)

AIS information supplements marine radar,

- similar to GPS in Aircrafts –

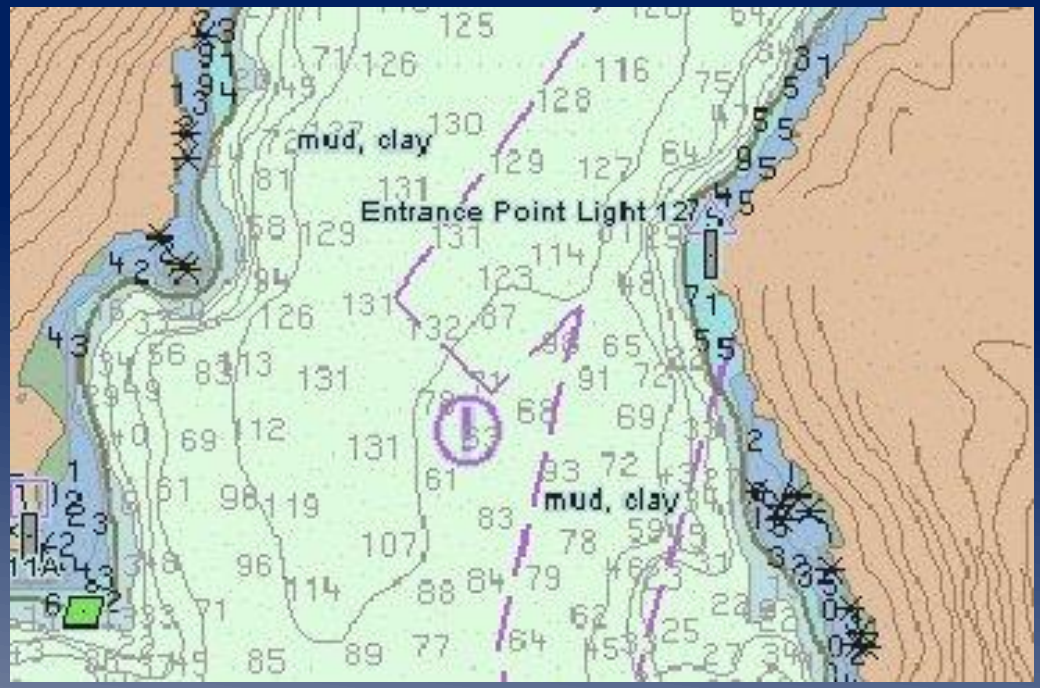
which continues to be the primary method of collision avoidance for water transport.

Electronic Chart Display and Information System (ECDIS)

ECDIS is a geographic information system used for nautical navigation

displays information from:

- Electronic Navigational Charts (ENC)
- or Digital Nautical Charts (DNC)



integrates position information

- Position
- Heading
- speed

sensors which could interface with an ECDIS are radar, Navtex, Automatic Identification Systems (AIS), and depth sounders.

IT Equipment on Board

Internet Access

- GSM
- WiFi
- SAT (Inmarsat, VSAT, Iridium, etc.)

On Board

- Entertainment Systems
- WiFi (Crew, Guest/Owner)
- VoIP

IT equipment on Board

10 Smart TV & Sat Receiver

1 Chart PC

14 VoIP Telephones

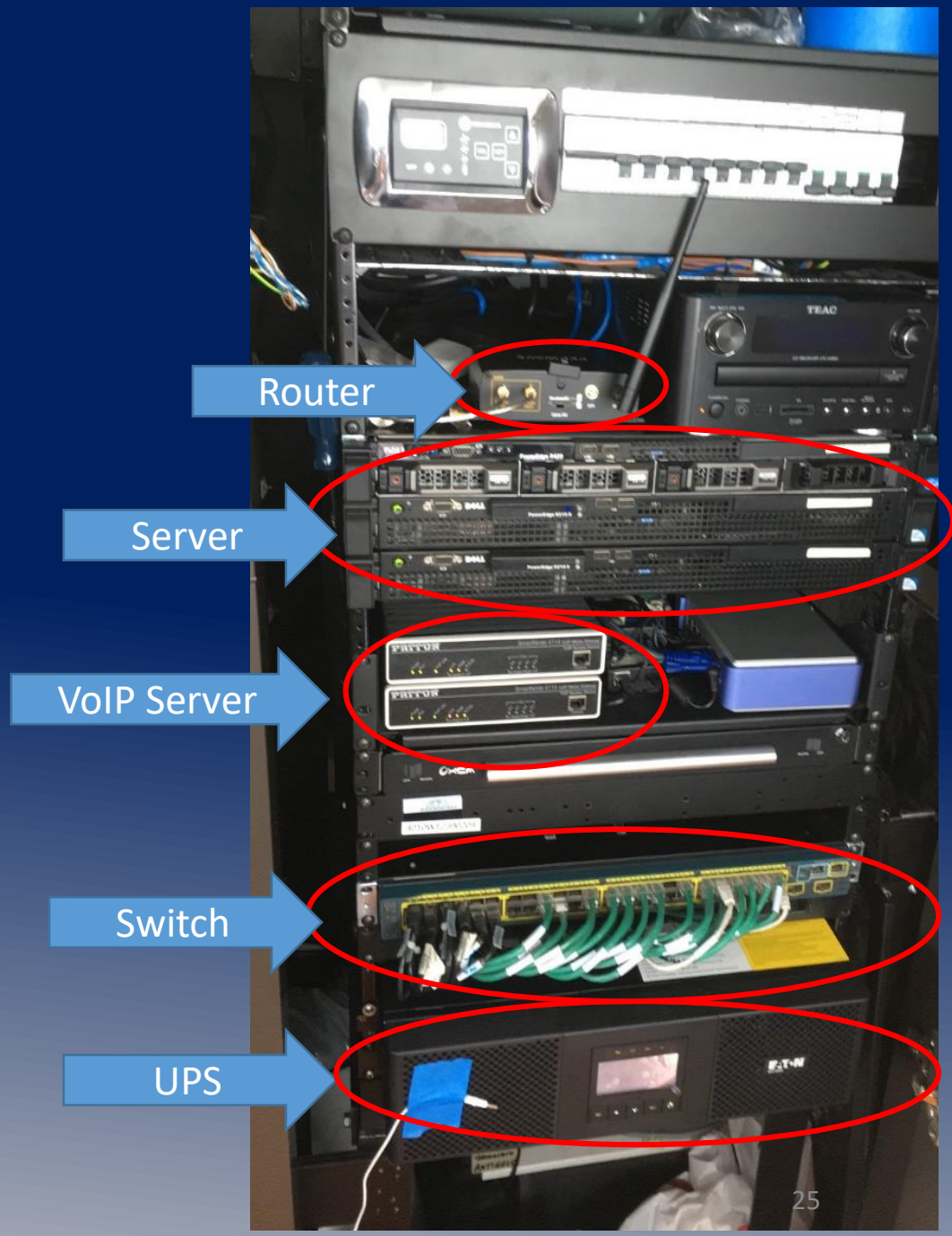
1 Internet Router (GSM, WiFi, SAT)

1 rack mounted Switch (48ports)

1 UPS

4 WiFi Access Point

(Crew, Guest/Owner)



Smart Ships

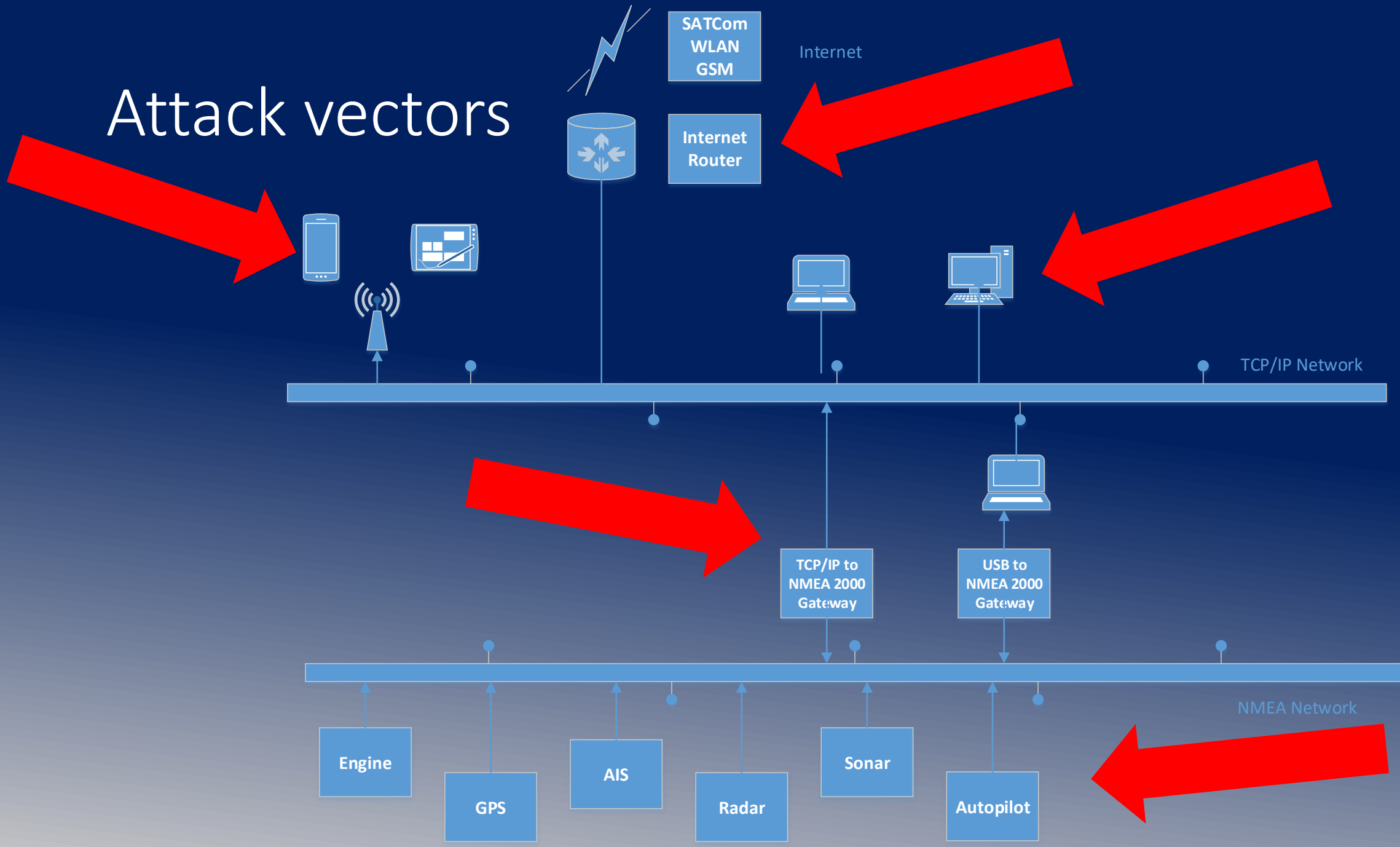
Audio & Video Streaming

iPhone/iPad remote control of

- Lights
- Electric curtains
- Engine monitor

Etc.

Attack vectors



Attack vectors

- GPS
- AIS
- Autopilot
- IT equipment on Board
- Cloud based services

GPS

Spoofing GPS signal is not that easy

Minimum 3 different Satellite signal has to be spoofed

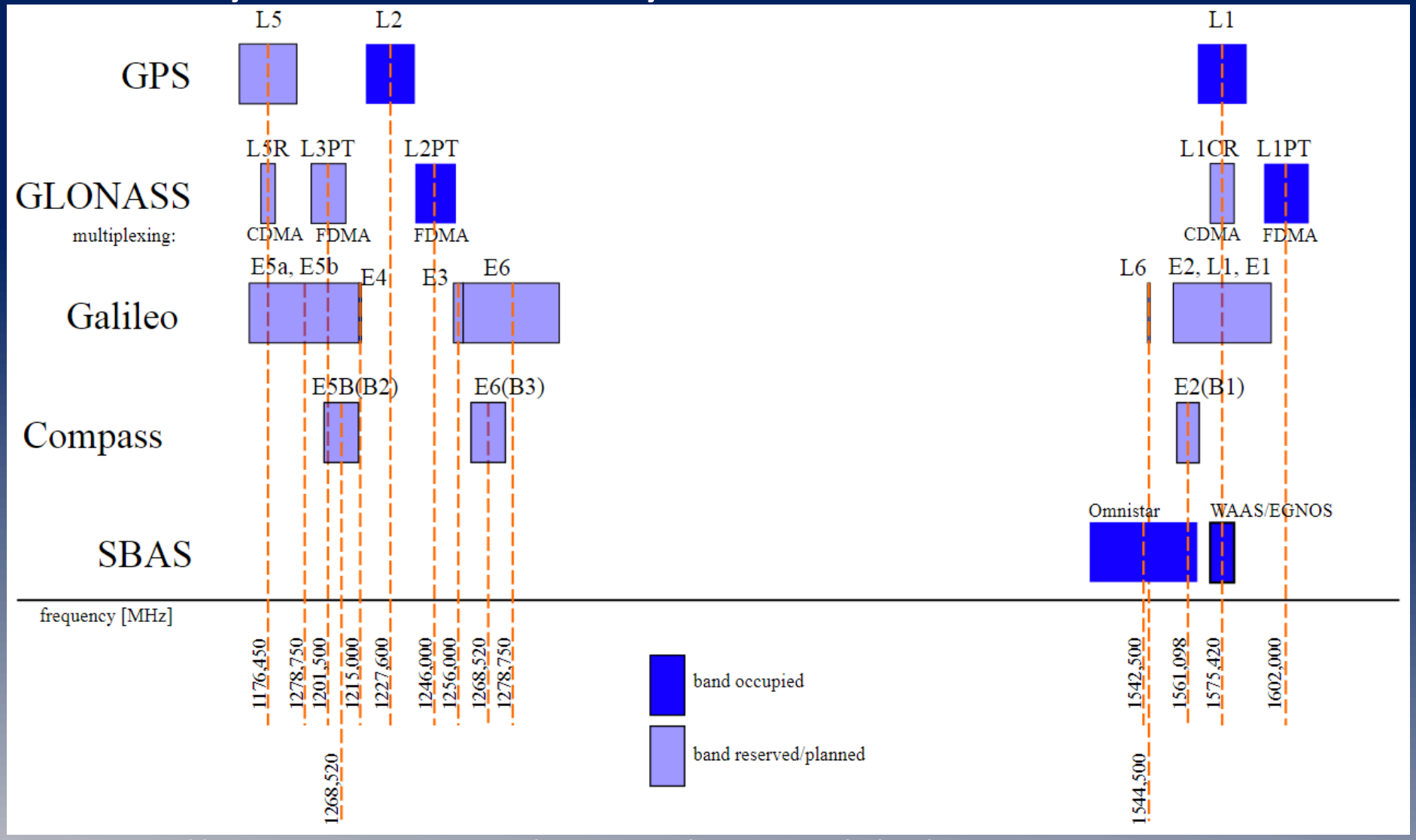
It’s easier to fake the NMEA data of the GPS Sensor

GPS – many different systems

GNSS (global Navigation satellite system)

- NAVSTAR GPS (United Staates of America)
- GLONASS (Russian Föderation)
- Galileo (Europe Union)
- Beidou (China)

GPS – many different systems



https://upload.wikimedia.org/wikipedia/commons/9/9a/Gnss_bandwidth.svg

GPS

2 Scenarios are possible

- jamming
- spoofing

complexibility:

Jamming = quite simple

Spoofing = complex – feasible for under1000 Euro

GPS

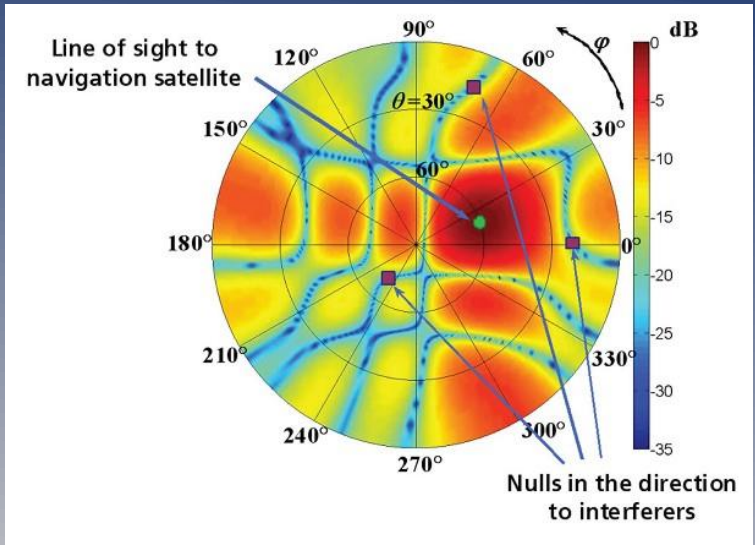
Eastern Pacific reports more and more GPS anomalies

- Juni, week 25 – more than 20 reports – north east black see
- NATO Troops maneuver at same time there
- Sept. Norway reports anomalies in a height >2000ft
- https://rntfnd.org/wp-content/uploads/Norway-Comms-Auth-Report-GPS-Jamming-Sept-2017.pdf

Securing GPS?

Research Project – „Galant“ by DLR – Institute of communications and navigation

- 2x2 active antenna array
- Beamforming & array processing



http://www.dlr.de/kn/en/desktopdefault.aspx/tabid-4306/6938_read-9224/

Automatic identification system (#1)

Following Data a AIS transceiver sends every 2 to 10 seconds while underway,
and every 3 minutes while a vessel is at anchor:

- Maritime Mobile Service Identity (MMSI) – a unique nine digit identification number.
- Navigation status – "at anchor", "under way using engine(s)", "not under command", etc.
- Rate of turn – right or left, from 0 to 720 degrees per minute
- Speed over ground – 0.1-knot (0.19 km/h) resolution from 0 to 102 knots (189 km/h)
- Positional accuracy: Longitude & Latitude – to 0.0001 minutes
- Course over ground – relative to true north to 0.1°
- True heading – 0 to 359 degrees (for example from a gyro compass)
- True bearing at own position. 0 to 359 degrees
- UTC Seconds

Automatic identification system

IMO: **8979142**
MMSI: **248311000**
Call Sign: **9HA4604**
Flag: **Malta [MT]**
AIS Vessel Type: **Pleasure Craft**

Gross Tonnage: **310**
Deadweight: **-**
Length Overall x Breadth Extreme: **38m × 7.7m**
Year Built: **1995**
Status: **Active**

Position Received: **2017-10-31 08:10 UTC**
Vessel's Time Zone: **UTC +1**
Area: **WMED - Ligurean Sea**
Latitude / Longitude: **43.85978° / 10.24154°**
Status: **Moored**
Speed/Course: **0.0kn / -**
AIS Source: **3406**

Automatic identification system (#1)

Following Data a AIS transceiver sends every 2 to 10 seconds while underway,
and every 3 minutes while a vessel is at anchor:

- Maritime Mobile Service Identity (MMSI) – a unique nine digit identification number.
- Navigation status – "at anchor", "under way using engine(s)", "not under command", etc.
- Rate of turn – right or left, from 0 to 720 degrees per minute
- Speed over ground – 0.1-knot (0.19 km/h) resolution from 0 to 102 knots (189 km/h)
- Positional accuracy: Longitude & Latitude – to 0.0001 minutes
- Course over ground – relative to true north to 0.1°
- True heading – 0 to 359 degrees (for example from a gyro compass)
- True bearing at own position. 0 to 359 degrees
- UTC Seconds

Automatic identification system (#2)

following data are broadcast every 6 minutes:

- IMO ship identification number – a seven digit number that remains unchanged
- Radio call sign – international radio call sign,
- Name – 20 characters to represent the name of the vessel
- Type of ship/cargo
- Dimensions of ship – to nearest meter
- Location of positioning system's (e.g., GPS) antenna on board the vessel - in meters aft of bow and meters port or starboard
- Type of positioning system – such as GPS, DGPS or LORAN-C.
- Draught of ship – 0.1 meter to 25.5 meters
- Destination – max. 20 characters
- ETA (estimated time of arrival) at destination – UTC month/date hour:minute

optional : high precision time request, a vessel can request other vessels provide a high precision UTC time and datestamp

AIS RF part

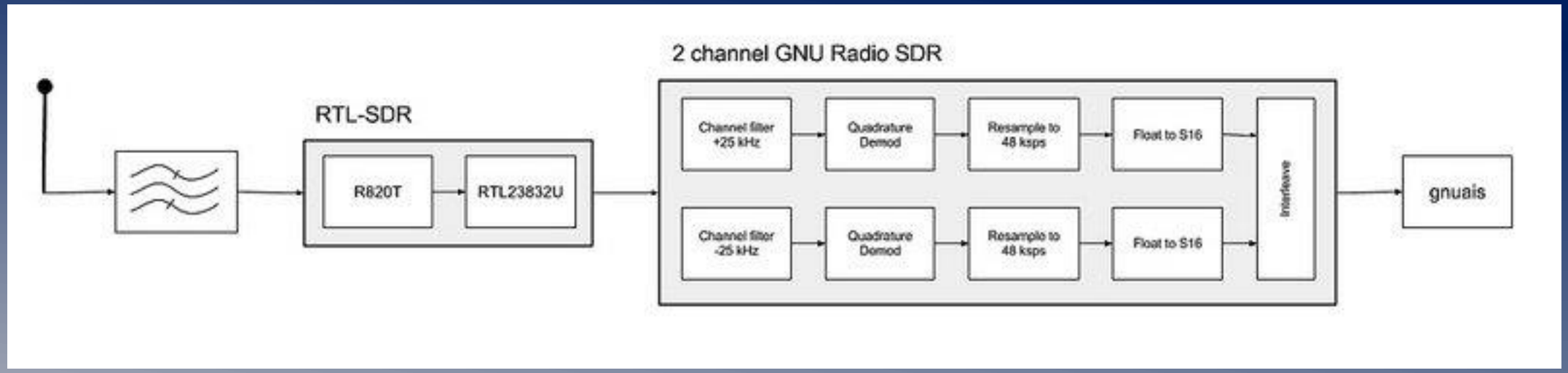
AIS uses the globally allocated Marine Band channels 87 & 88.

AIS uses the high side of the duplex from VHF radio "channels" (87B) & (88B)

- Channel A 161.975 MHz (87B)
- Channel B 162.025 MHz (88B)
- Before being transmitted, AIS messages must be NRZI encoded.
- AIS messages are GMSK modulated.
- transmission bit rate is 9600bit/s

AIS hacking

2-CHANNEL AIS RECEIVER WITH RTL-SDR AND GNUAIS



https://www.rtl-sdr.com/2-channel-ais-receiver-rtl-sdr-gnuais/

Autopilot

Raymarine S100 wireless Remote Control

The compact Raymarine S100 remote control gives you basic, onboard wireless control of any Raymarine SeaTalk autopilot, even if you're below deck and out of sight of your autopilot.

Key Features

- Two lines of text
- Signal strength indicator
- Out of range of base station warning

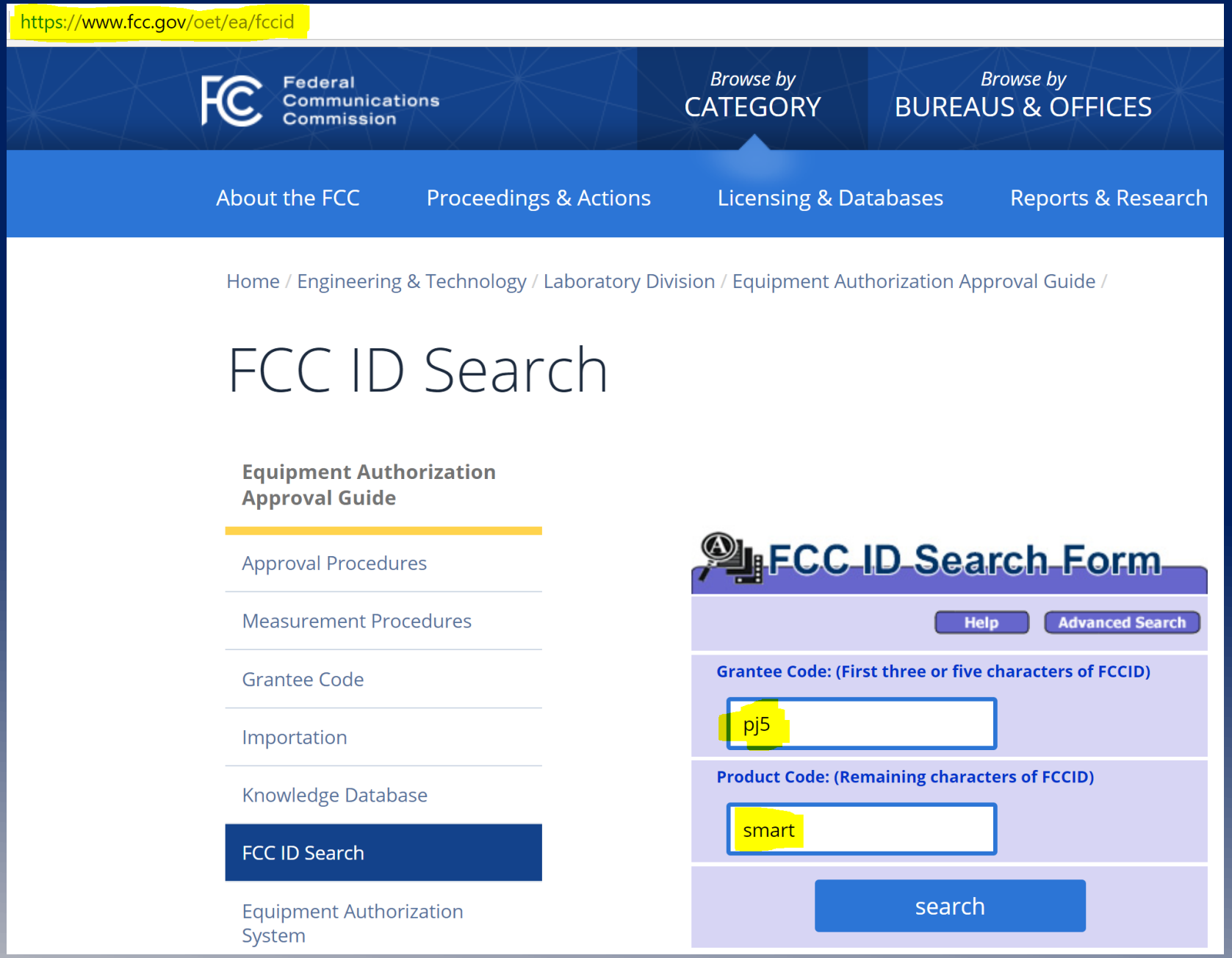
Autopilot

A sailor gave me a hint

Remote control for heading & speed !

Autopilot

FCC ID search



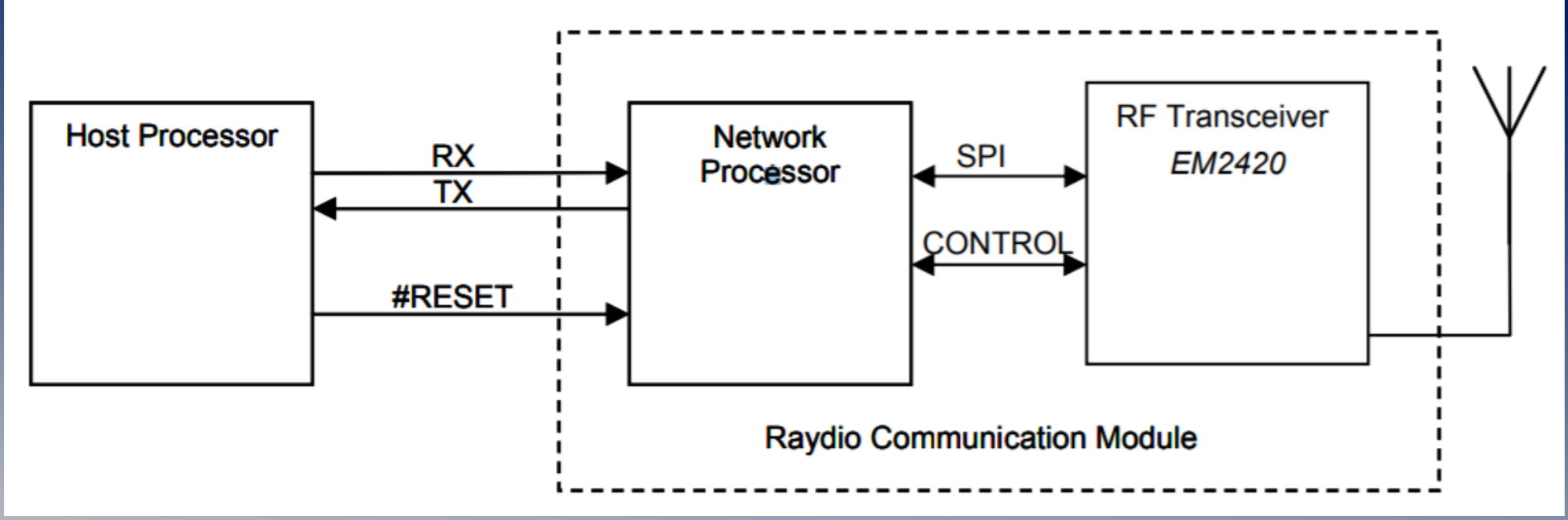
Autopilot

Raymarine Autopilot S100 Handheld

- FCC ID PJ5Smart
- Communicates with the S1000 Autopilot
- Operates wireless on 2.45GHz
- Is not WiFi

Autopilot

RCM is based upon Ember's EM2420 2.45GHz RF transceiver
connected to an ATMEGA64 microprocessor
runs on Emberstack



Yacht Router hacking

Locomarine

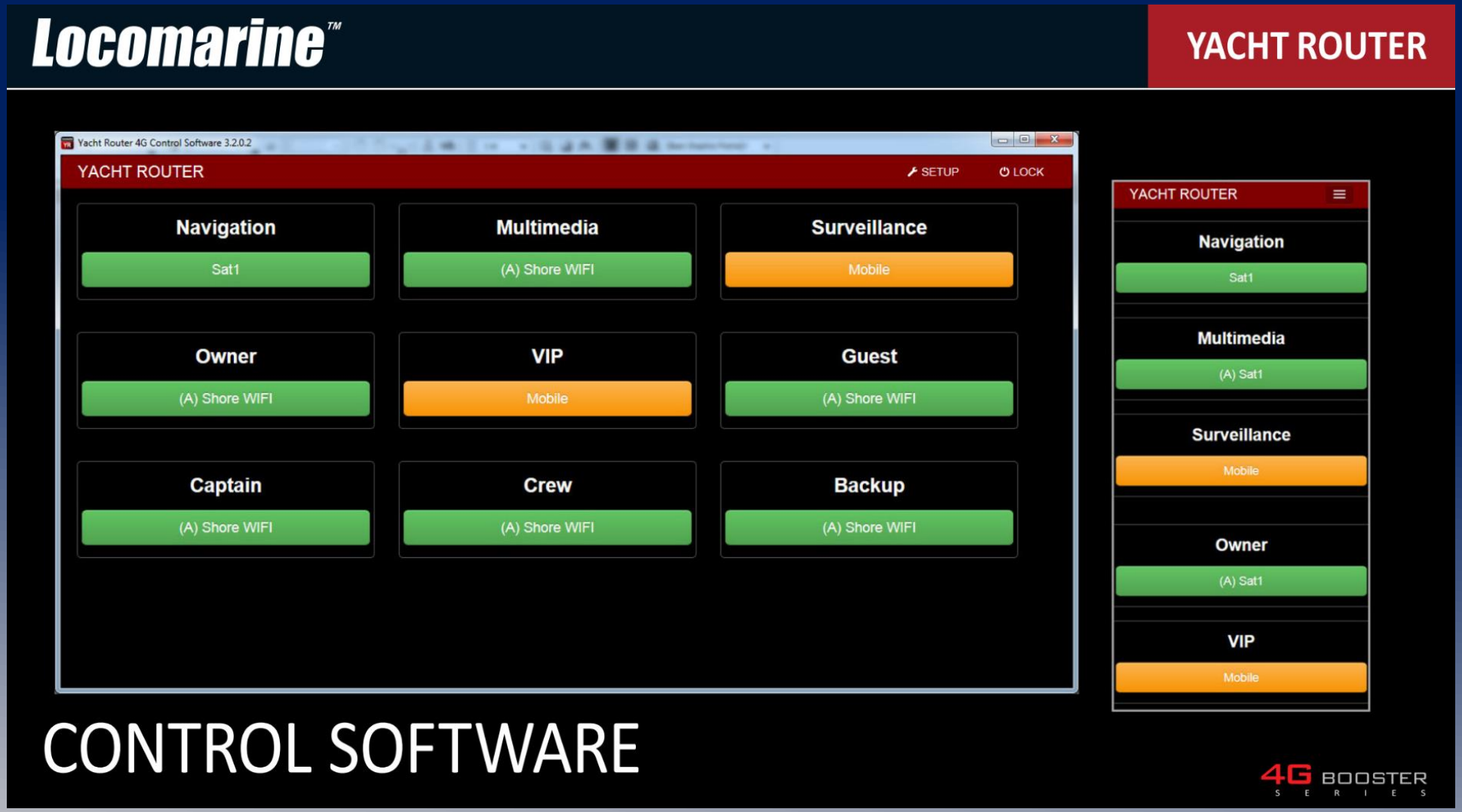
Yachtrouter

Yacht Router hacking

Locomarine Yachtrouter

- High power WIFI Booster for long distance connectivity (15+ NM)
- High power 4G/3G/2G module (30+ Nautical miles)

Issue #1 – The control software



Issue #1 – The control software

- FTP connect to router
- Download “YachtRouterGen3.xml
- The APP changes settings in the XML
- Uploaded to the Router

Issue #1 – The control software

- FTP is clear text
- Hardcoded credentials used !!!
- …xml file contains WLAN SSID and Password (clear text)

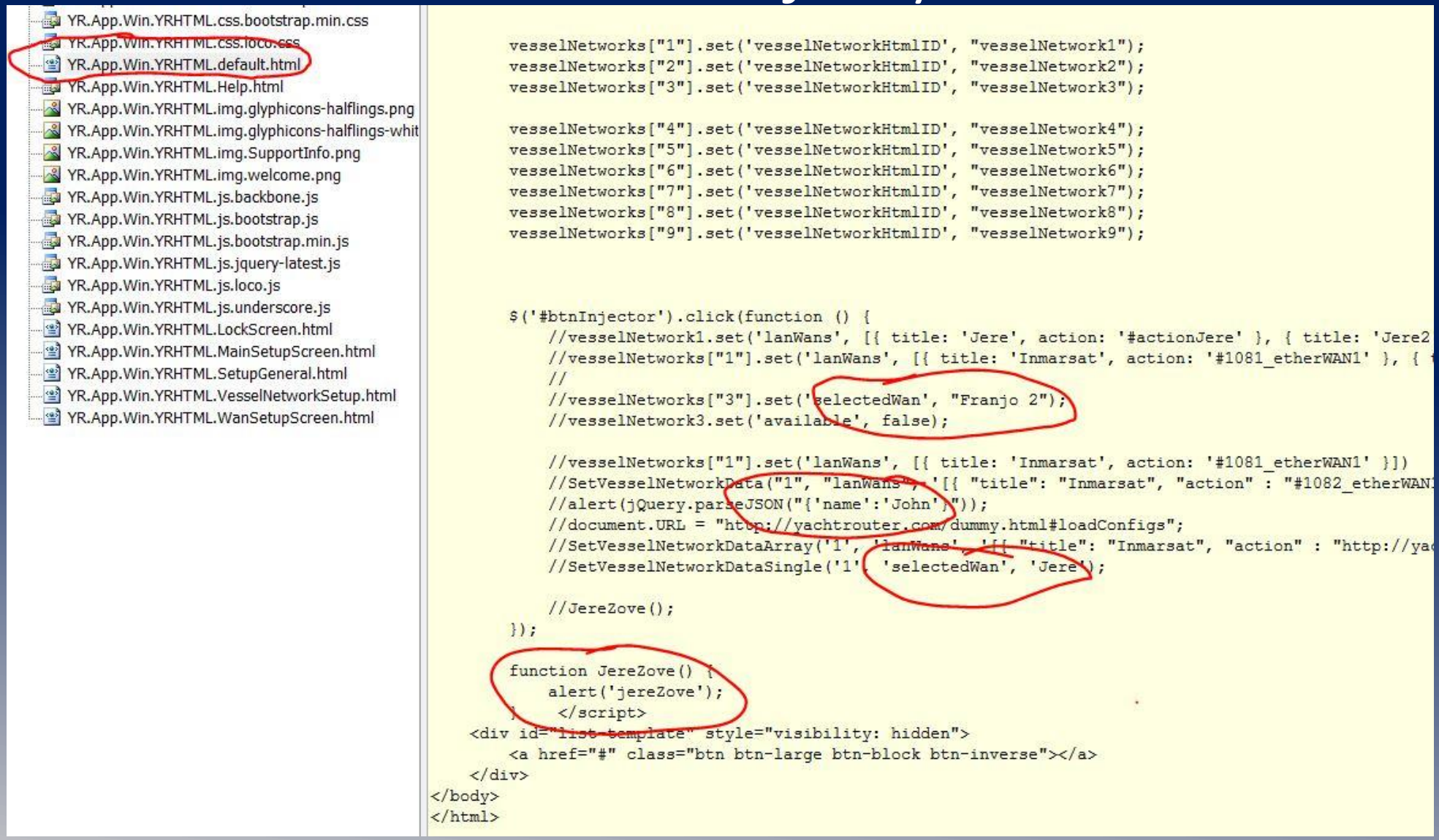
344	98.416854	10.80.0.1	10.81.255.254	F
345	98.418233	10.81.255.254	10.80.0.1	F
346	98.418601	10.80.0.1	10.81.255.254	T
347	98.418976	10.80.0.1	10.81.255.254	F
348	98.419067	10.81.255.254	10.80.0.1	F
349	98.451857	10.80.0.1	10.81.255.254	T

Wireshark · Follow TCP Stream (tcp.stream eq 0) · locomarine-next try

```
220 YachtRouterMiniB FTP server (MikroTik 6.24) ready
USER loco
331 Password required for loco
PASS
230 User loco logged in
OPTS utf8 on
500 'OPTS': command not understood
PWD
257 "/" is current directory
TYPE I
200 Type set to I
PASV
227 Entering Passive Mode (10,80,0,1,148,225).
RETR YachtRouterGen3.xml
150 Opening BINARY mode data connection for /YachtRouterGen3.xml (11104 bytes)
226 BINARY transfer complete
```

secret

Issue #2 – code contains juicy informations



Issue #2 – code contains juicy informations

```
static yrEngine()
{
  yrEngine.RouterConfig_Username = "
  yrEngine.RouterConfig_Password = "                    ser";
  yrEngine.RouterConfig_FtpPath = "ftp://10.80.0.1/YachtRouterGen3.xml";
  yrEngine.RouterSupportInfo_FtpPath = "ftp://10.80.0.1/SupportInfo.png";
  yrEngine.extenderIdentity = "YR_WIFI_EXTENDER";
  yrEngine.rootExtenderDHCPServer = "dhcpBACKBONE";
  yrEngine.bridgePrefix = "bridgeEoip_";
  yrEngine.routingMarkPrefix = "markAlwaysON_";
  yrEngine.virtualApPrefix = "wifiAlwaysON_";
  yrEngine.virtualApSecurityProfilePrefix = "SecurityProfile_";
  yrEngine.eoipTunnelPrefix = "eoipTunnel_";
  yrEngine.shipPhysicalWifiInterface = "shipPhysical";
  yrEngine.defaultPassword = "12345678";
  yrEngine.rootIpAddress = "10.90.";
```

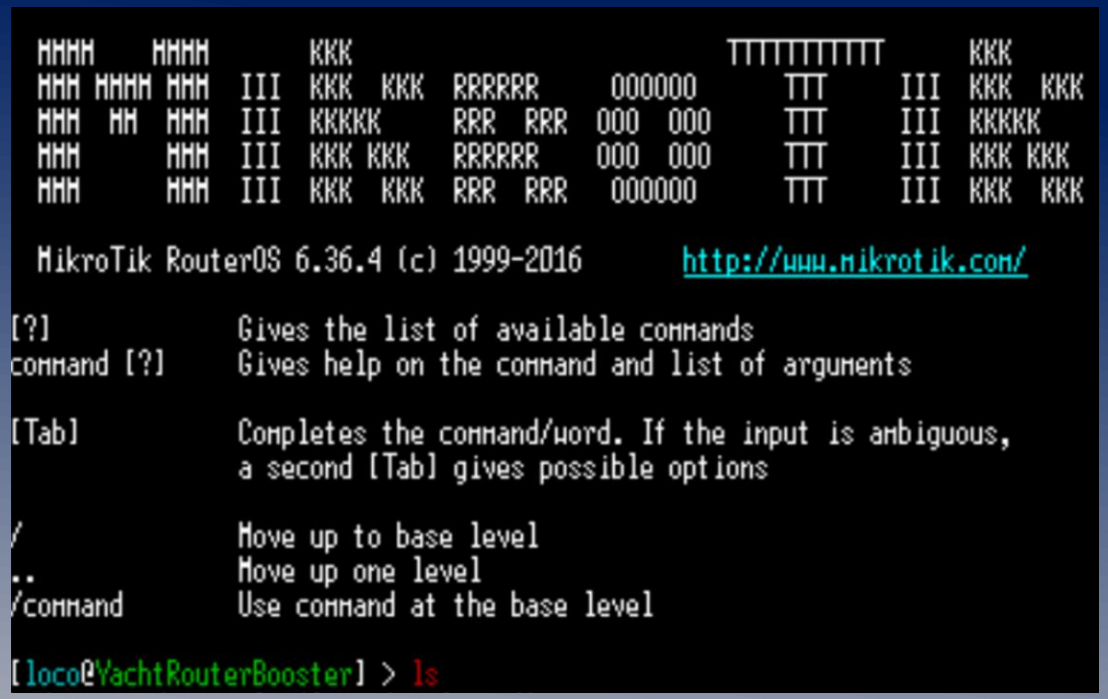
secret

Issue #3 - no firewall

NMAP scan on the puplic IP

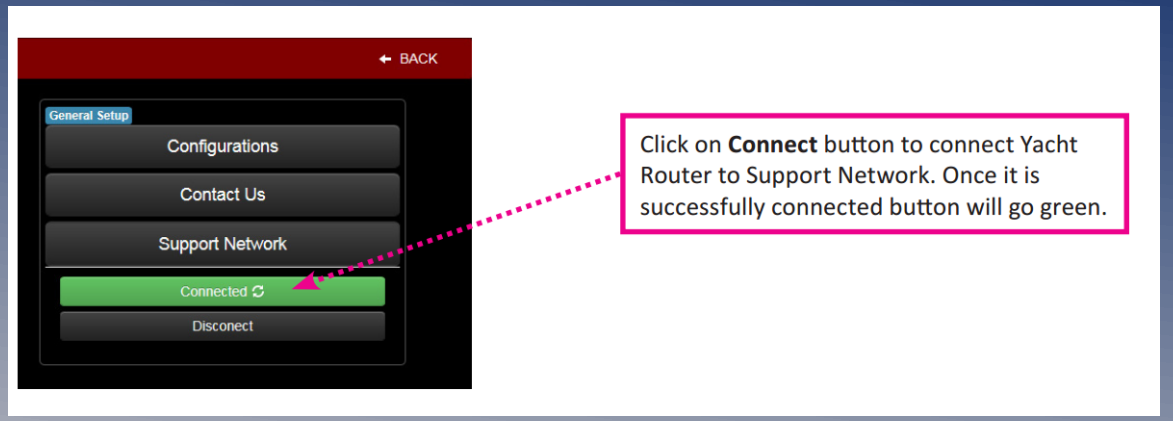
- Router os= Mikrotik Router OS
- Winbox Management 8291/TCP
- API access of the Yachtrouter exe 8728/TCP (API)

- Portscan from Internet:
- PORT STATE SERVICE
- 21/tcp open ftp
- 22/tcp open ssh
- 53/tcp open domain
- 2000/tcp open cisco-sccp
- 8291/tcp open unknown



Issue #4 - Remote support

- **9.1. Remote Support**
  Each Yacht Router is equipped with Remote Support feature that gives our Technical Support ability to connect remotely over the Internet to your Yacht Router. You can use Remote Support
  in various situatons like remote setup, diagnostcs or Cloud Service actvaton.
-
  To establish Remote Support please send an e-mail to support@locomarine.com with following details:
  - Contact details (name, e-mail, phone number)
  - Yacht Router model
  - Yacht Router serial number
  - Descripton of the problem
  - Suggested best time (minimum one)



Issue #4 - Remote support

Yacht Router model & serial number ?

How do they know the IP address?

Issue #4 - Remote support

```
ror=0
..!done../ping.=address=5.10.88.130.=count=5
ket-loss=100..!re.=seq=1.=status=no route to
 host.=sent=3.=received=0.=packet-loss=100..
```

Whois IP 5.10.88.130

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '5.10.88.128 - 5.10.88.135'

% Abuse contact for '5.10.88.128 - 5.10.88.135' is 'abuse@softlayer.com

inetnum:        5.10.88.128 - 5.10.88.135
netname:        NETBLK-SOFTLAYER-RIPE-CUST-BO1663-RIPE
descr:          LOCOMARINE DOO
country:        HR
admin-c:        BO1663-RIPE
tech-c:         BO1663-RIPE
status:         ASSIGNED PA
mnt-by:         MAINT-SOFTLAYER-RIPE
created:        2013-07-25T18:27:47Z
last-modified:  2013-07-25T18:27:47Z
source:         RIPE
```

Issue #3 - Remote support

Remember the Portscan ?

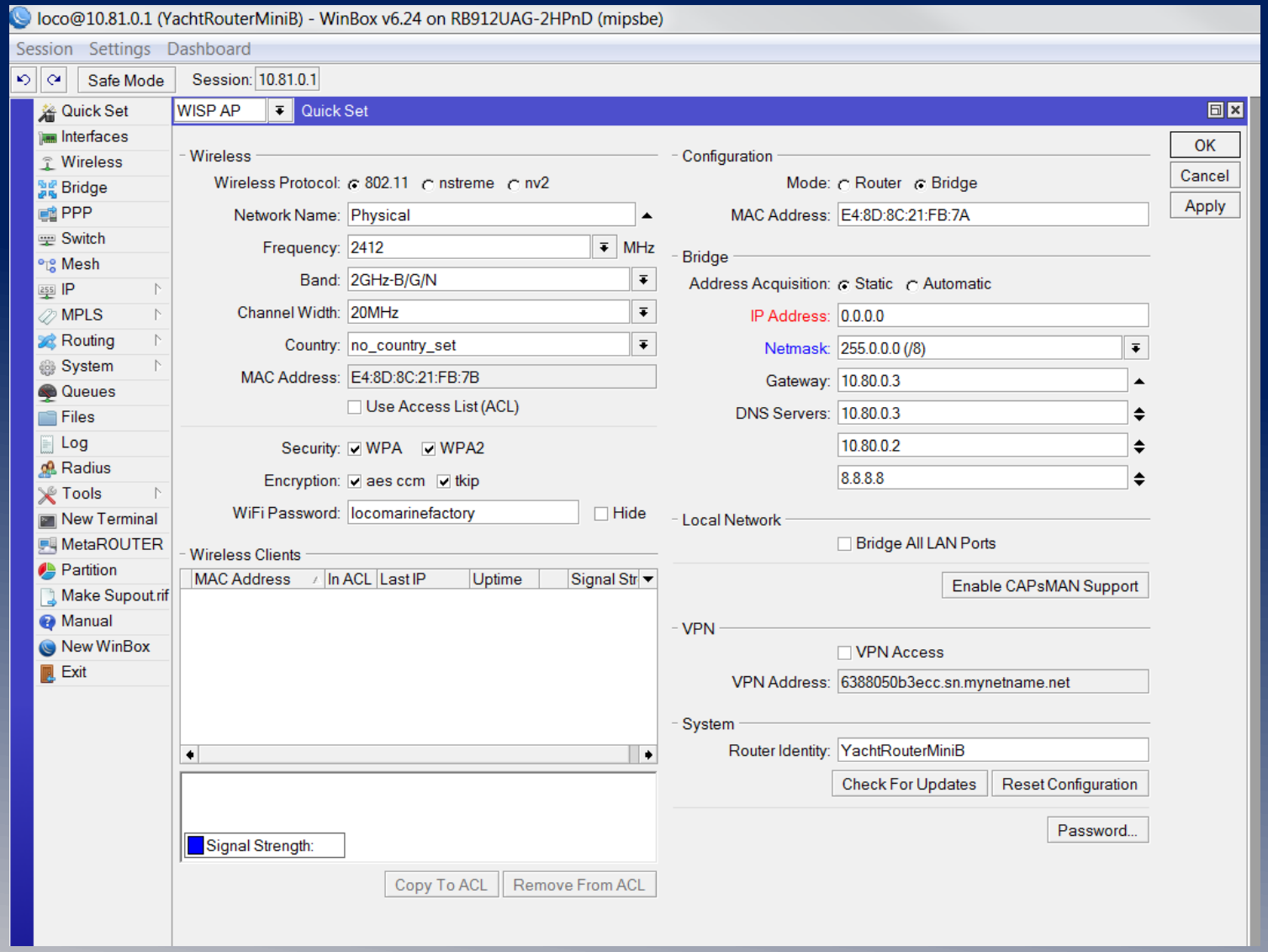
Router os= Mikrotik Router OS

8291/tcp open unknown

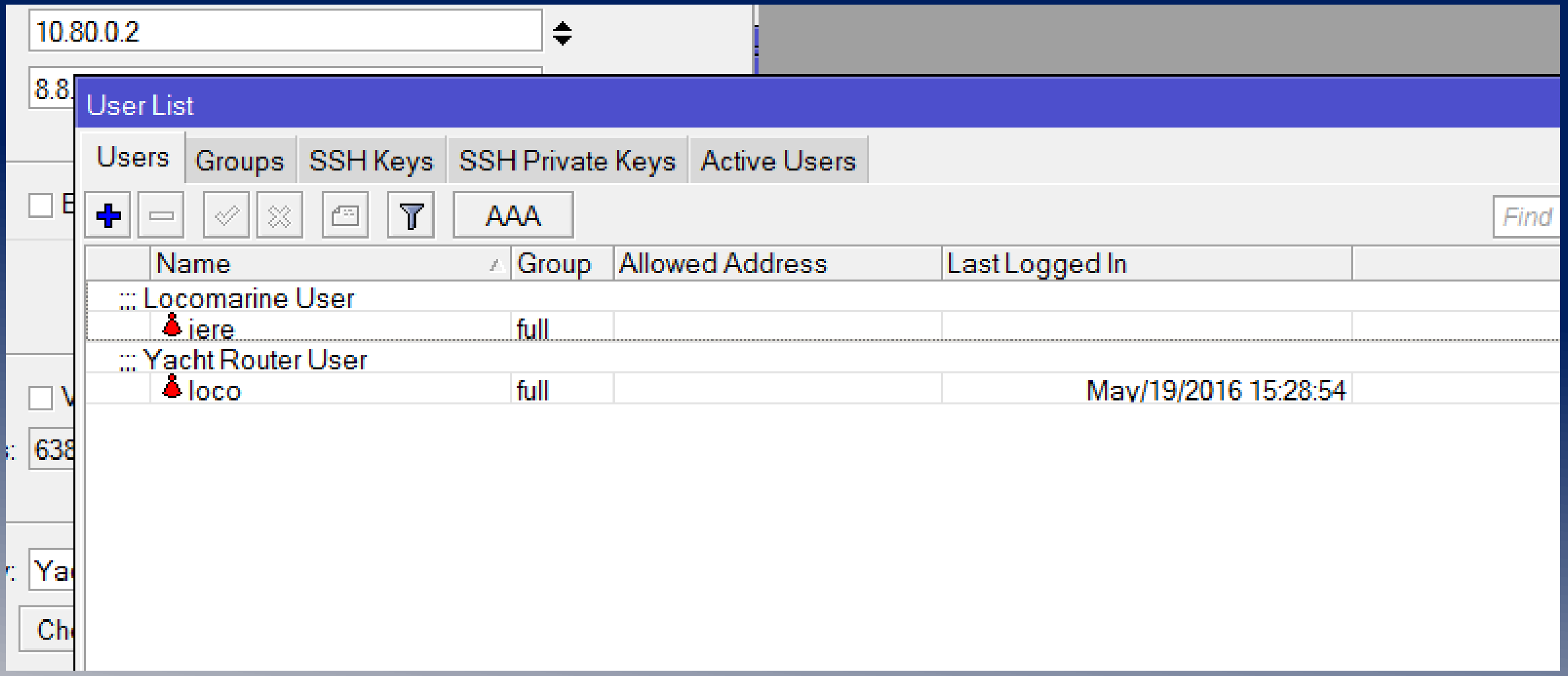
Port 8291/TCP belongs to Winbox Management

Ok, lets Try

Issue #4 – Remote support



Issue #4 – Remote support



Issue #4 – Remote support

https://securityandethic.wordpress.com/tag/api-port/

MKBRUTUS v1.0.0

Password bruteforcer for MikroTik devices or boxes running RouterOS
Site: https://github.com/mkbrutusproject/MKBRUTUS

How to find vulnerable Yachts

Locomarine | YACHT ROUTER

HOME NEWS PRODUCTS SERVICES SUPPORT CONTACT BUY

October 2015

Yacht Router on Yaghan

October 19th, 2015

Yacht Router on Yaghan Yaghan is a Hallberg-Rassy 62 sailed by Helene and Arne Mårtensson from Sweden. They sailed round the World via Antarctica 2006-2009 and wrote two exciting books about their voyage. Last winter Yaghan went through extensive preparations for a new adventure to Antarctica

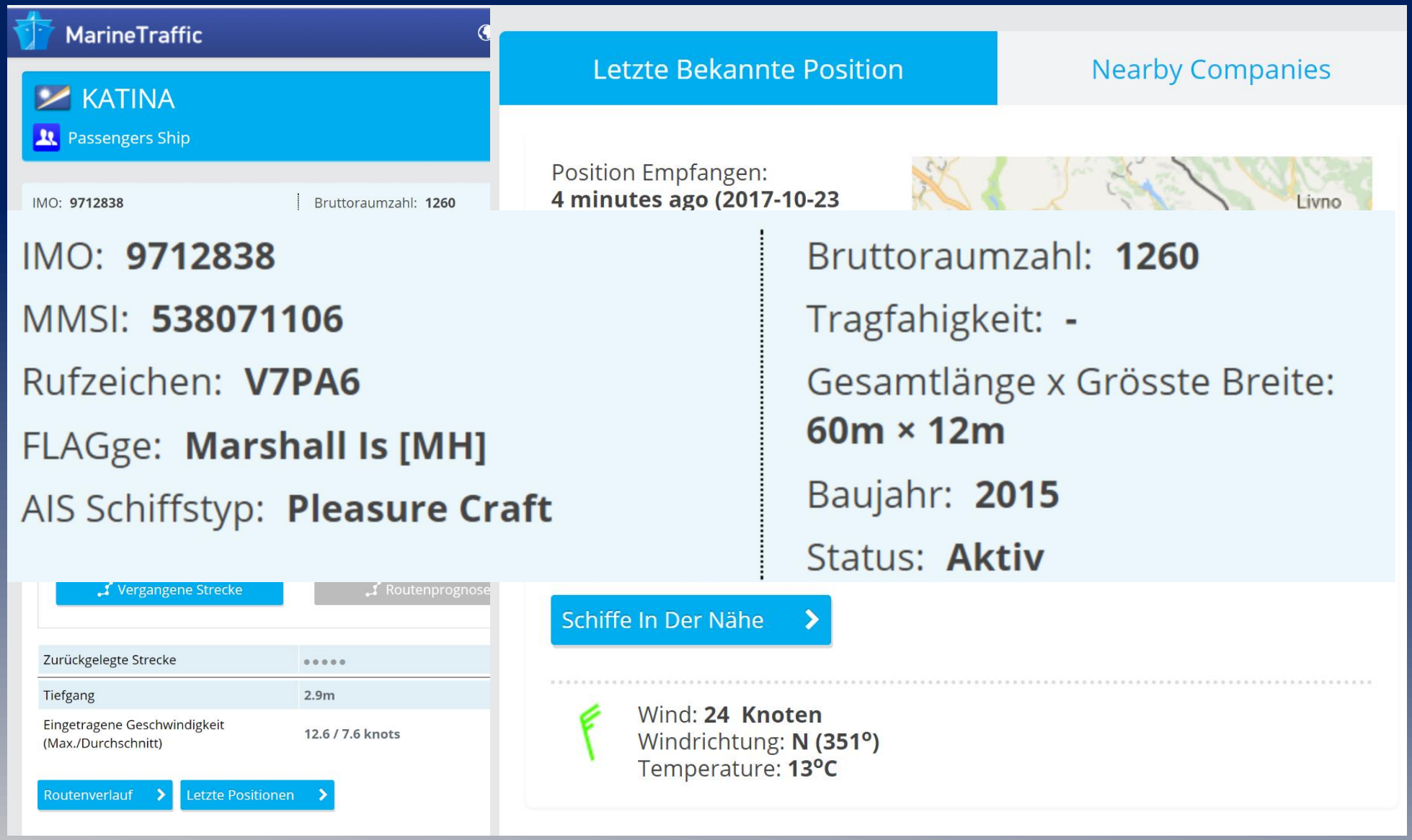
Yacht Router on-board Katina

October 24th, 2015

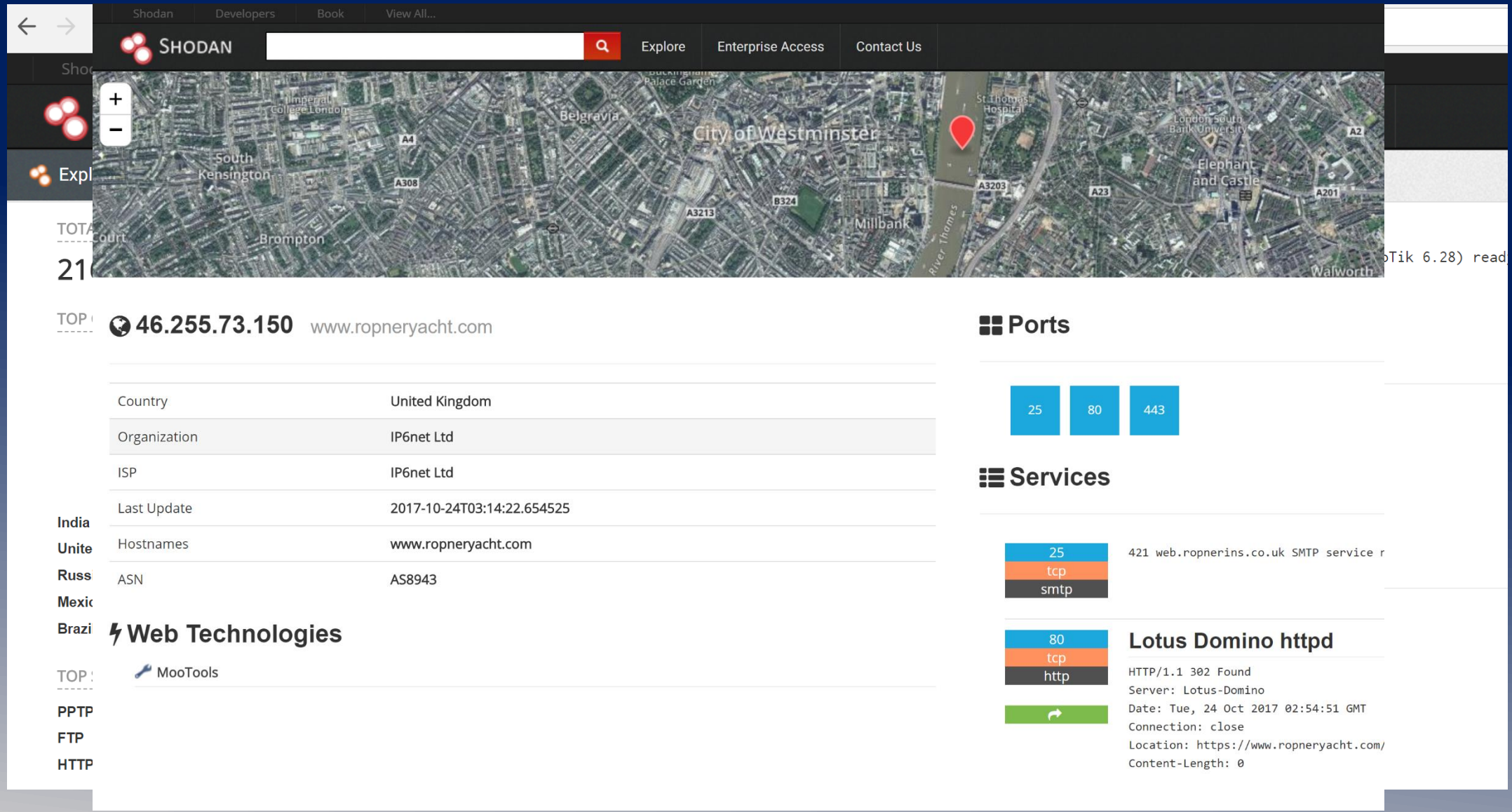
Yacht Router on-board Katina Katina is a new megayacht equipped with complete Yacht Router Pro system. It is 60 meters vessel able to accommodate 12 passengers in six VIP cabins on four decks. There will be 10 crew members, and the ship is intended for cruising [...]

Read More >

How to find vulnerable Yachts



How to find vulnerable Yachts



Vendor response

- Security issues reported in June 2017 to vendor
- 2 bugs intensely fixed
- New Apps and router firmware versions were developed
- In November finaly released
- Permission from vendor to present
- CVE ID requested

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-17673

Testing of the patched Software

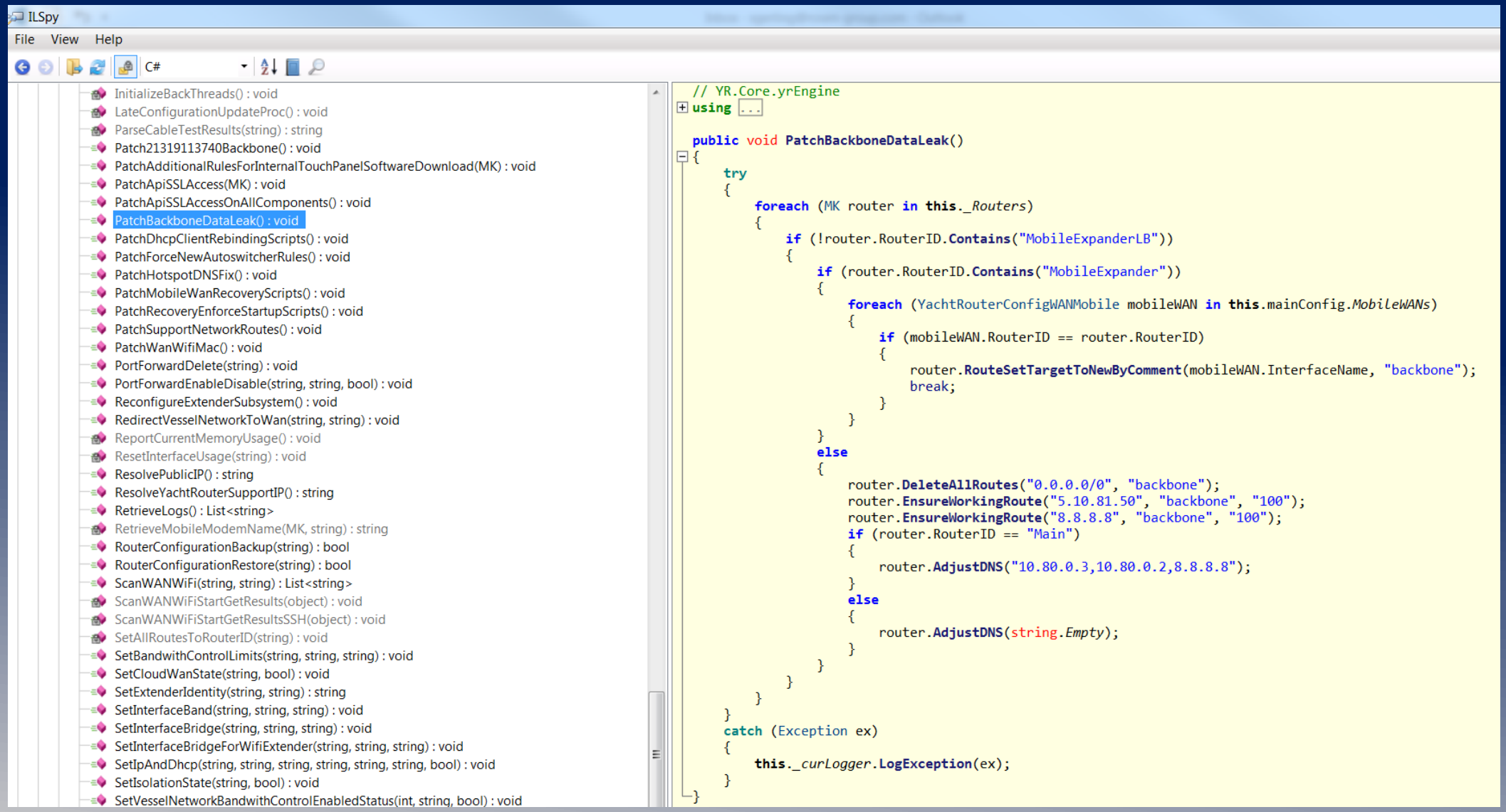
- Vendor send me a Test Router
- Tested the new Windows Software

Testing of the patched Software

```
// YR.Core.yrEngine
using ...

public class yrEngine
{
    public class MyUserInfo : UserInfo, UIKeyboardInteractive
    ...

    public static string RouterConfig_Username = "

    public static string RouterConfig_Password = "                    84D";

    public static List<string> RouterConfig_PasswordOlds = new List<string>
    {
        "SecureConnectingUser"
    };

    public static string RouterConfig_FtpPath = "ftp://10.80.0.1/YachtRouterGen3.xml";

    public static string RouterSupportInfo_FtpPath = "ftp://10.80.0.1/SupportInfo.png";

    public static string extenderIdentity = "YR_WIFI_EXTENDER";

    public static string rootExtenderDHCPServer = "dhcpBACKBONE";

    public static string bridgePrefix = "bridgeEoip_";
```

Secret

Testing of the patched Software



Summery of the Patches

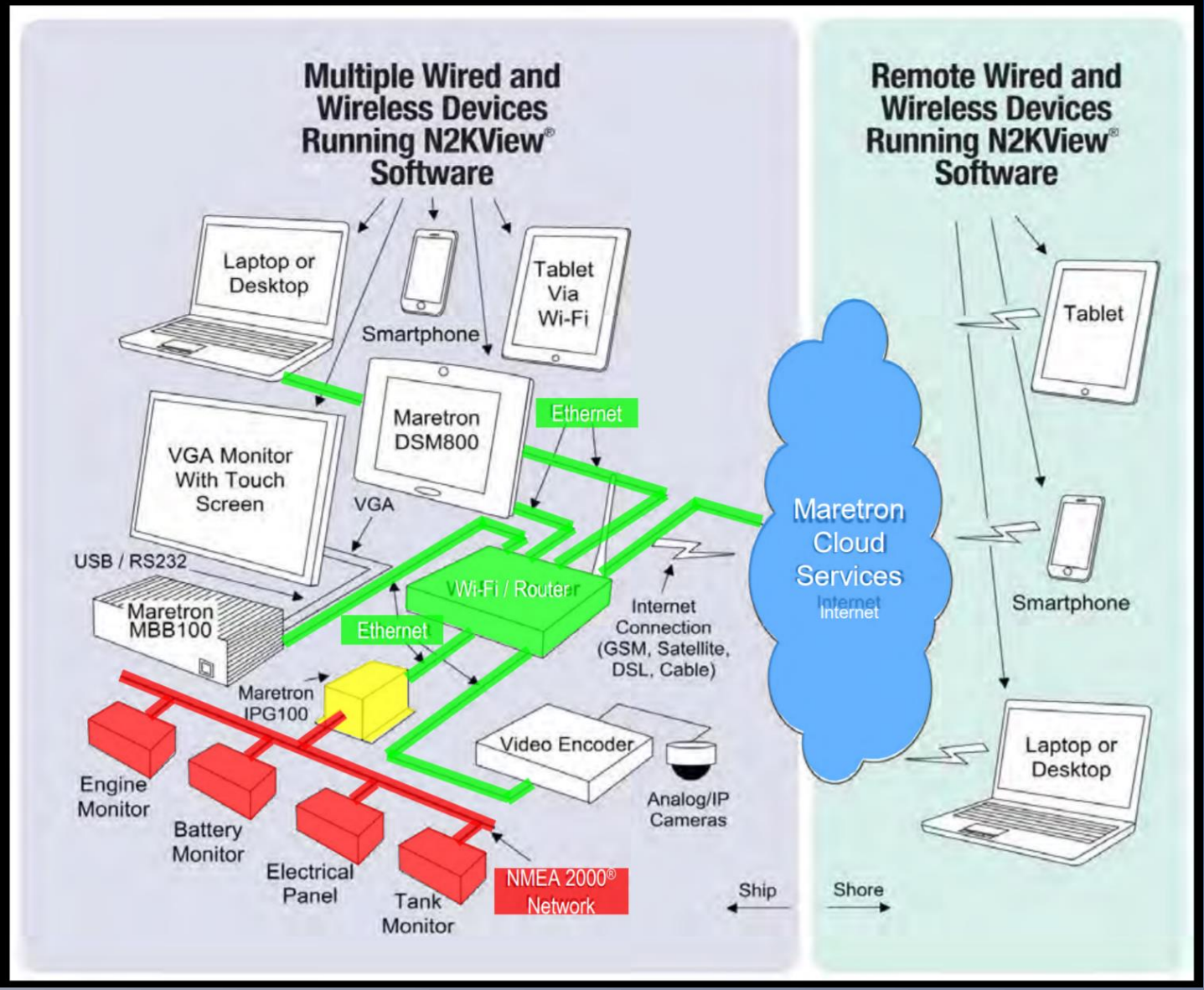
- Use of SSH instead of FTP
- Obfuscated Exe + DLL in Windows Version
- Android APK not obfuscated
- iOS Version not tested yest
- still Hardcoded credentials in yrEngine
- SSH and Winbox still reachable from Internet

What’s next?

- NMEA protocol needs more test
- Wireless Autopilot
- Other Internet Equipment tested by others
- Vessel hacking is just in the beginning
- Cloud services

future

- CAN Bus (NMEA 2000®)
- CAN Bus / Ethernet Gateway
- Ethernet (Internet Protocol)
- Internet



https://www.nmea.org/Assets/nmea%20ibex%20integrating%20smart%20phones%20%20marine%20electronics%20lr.pdf

Cloud services

- Engine control
- Monitoring
- From anywhere

https://www.nmea.org/Assets/nmea%20ibex%20integrating%20smart%20phones%20%20marine%20electronics%20lr.pdf

Researchs just started

- NMEA Gateways
- SAT Com (iOactive did some nice research)
- VTS
- Autopilot Remote control (my research started)
- Injecting NMEA messages to the Bus
- GPS spoofing protection (DLR “Galant” new Antenna array)

My conclusion: Maritime IT-Security research is in the beginning

Thank you for attention

May the force be with u

Twitter: @ObiWan666

Mail: SGerling@ROSEN-Group.com
office@CERTivation.com