HACKING YACHTS REMOTELY

IOT HACKING AT SEA

HITB2018DXB · Stephan Gerling · ©ROSEN-Group.com · 27-Nov-2018

CERTivation


FANDANGO
MOVIECLIPS

Overview

- Introduction
- Maritime 1x1
- Router and SatCom vulnerabilities
- Autonomous Ships
- Q&A

Why hacking yachts?

Yachts mostly privately owned or chartered

CEO’s running their business from Yachts while traveling
Celebrities like showstars, actors & others

What, if I could control the Internet access of a yacht?
What, if I have remote access to the smart devices?

Stephan Gerling @ObiWan666

I am older than the internet
Certified as “GCFA, CISSP, MCSE, CCNA, etc.”
Electronic Specialist,
several years German Aviation Army navigation system electronic specialist
More than 31 years a volunteer firefighter in my town
Security Evangelist @ROSEN-Group in Oil & Gas Industrie
and CERTivation, latest ROSEN Group Spin Off
I void warranties

Volunteering
- Geraffel (group of „hacker nerds at ist best“)
- IamTheCavalry


BBC
Sign in
News
Sport
NEWS
Home
Video
World
UK
Business
Tech
Science
Magazine
THE DISRUPTORS
How will we shop in the future?
Technology
How hackers are targeting the industry
Sicher
https://www.theguardian.com/
Advertisement
Ford Umwelt-Initiative
Bis zu 8.000,- E
Umweltbonus sich
home › world
europe
US
americas
asia
Water transport
Cybercrime on the high s
threat facing billionaire su
owners
Buyers at London superyacht conference shown the e
take control of vessels – and even procure private phot


Jim Rickards
@JamesGRickards
Follow
Second tragic collision of U.S. warship with merchant vessel raises suspicion of nav system hacking on merchantmen. Are we already at war?
6:38 PM - 20 Aug 2017
241 Retweets
400 Likes


ant Ship Hacked? McCain
Run For Navy Cyber
per
erangriffe.
Süddeutsche Zeitung
SZ.de
Magazin
Sport
München
Bayern
Kultur
Gesellschaft
Wissen
Digital
Karriere
Reise
Auto
Hacker und Schiffe
enn die Yacht wie von Geisterhand
en Kurs ändert

Accidents

Feb.2017	Containervessel 10h without access to Navigationsystem
Sep.2017	Norwegian: GPS Jamming from eastern direction

US Navy involved in 4 collisions in eastern pacific in 2017

• 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

Norwegian Frigate collided with a crude Oil vessel and aground & tilting

This happened Nov.2018 during major NATO military exercice

SOLA TS

Photo Details

Place of Photo	Porvoo 60.300°, 25.554°
Date Taken	2018-06-10 10:36
Uploaded	2018-06-10 18:03
Original Size	2048 x 1105 pixels
Camera & Settings	**Model :** Canon EOS 6D **Exposure :** 1/1500, 11.0 **ISO :** 500, f.length:329mm

Suggest Photo Removal

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.) maybe GPS
Yacht	>= 10m (33 Fuß) GPS, maybe Autopilot
Super Yacht	bigger than 24m (79 ft.) GPS, GSM/Wifi Internet, smart TV, VoIP
mega yacht	any yacht over 50 meters (164 ft.) GPS, GSM/WiFi Internet, smart TV, Autopilot, SatCom, smart Home, VoIP, ICS (propulsion) etc.

Superyacht

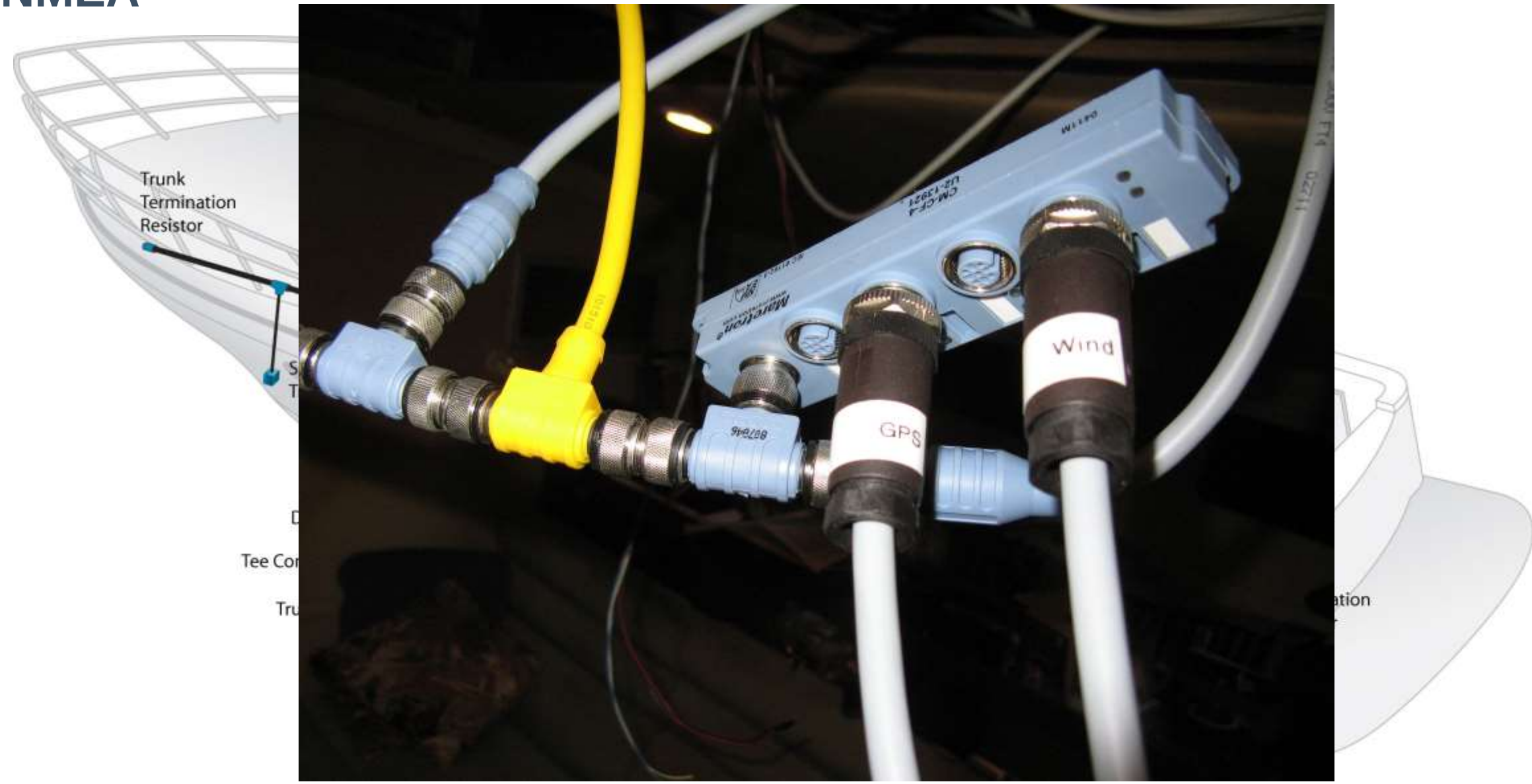
Indigo Star
Length 38,8m
Beam 7,7m

Swimming IoT

Modern vessels become 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

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

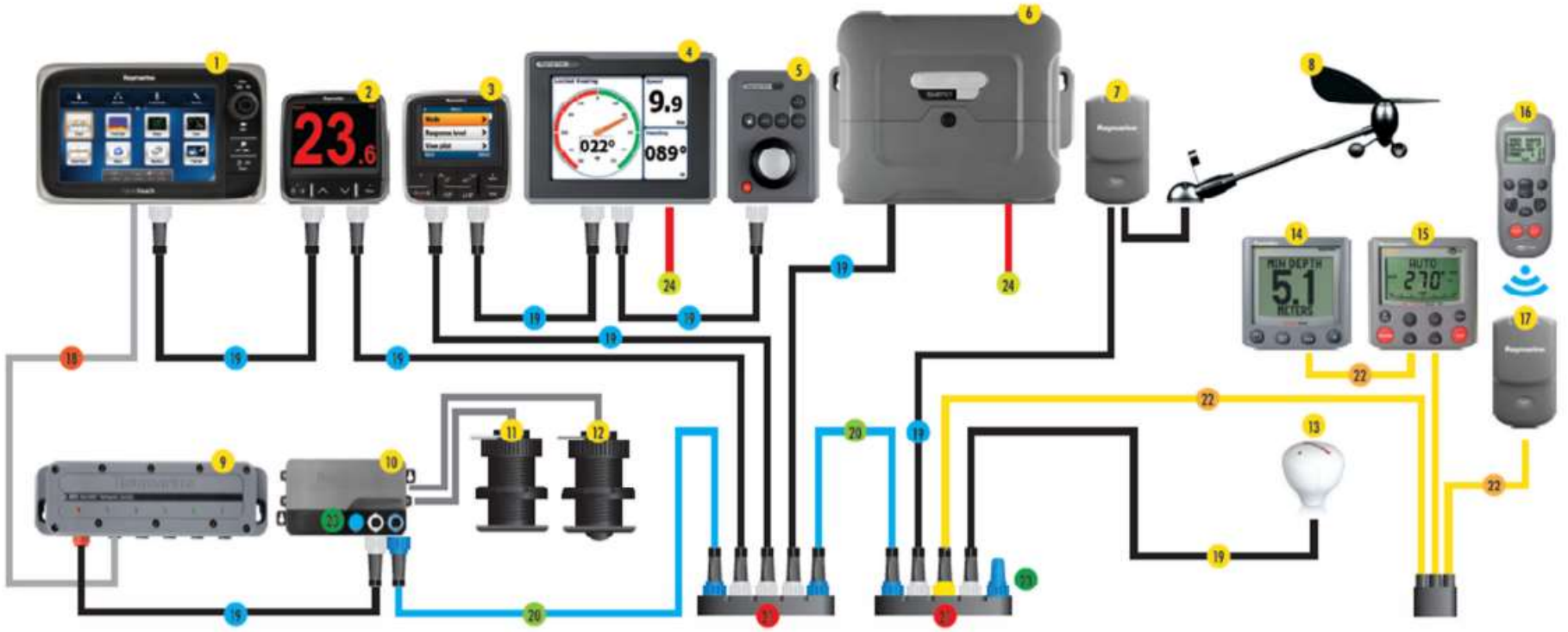
NMEA 2000

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

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

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.

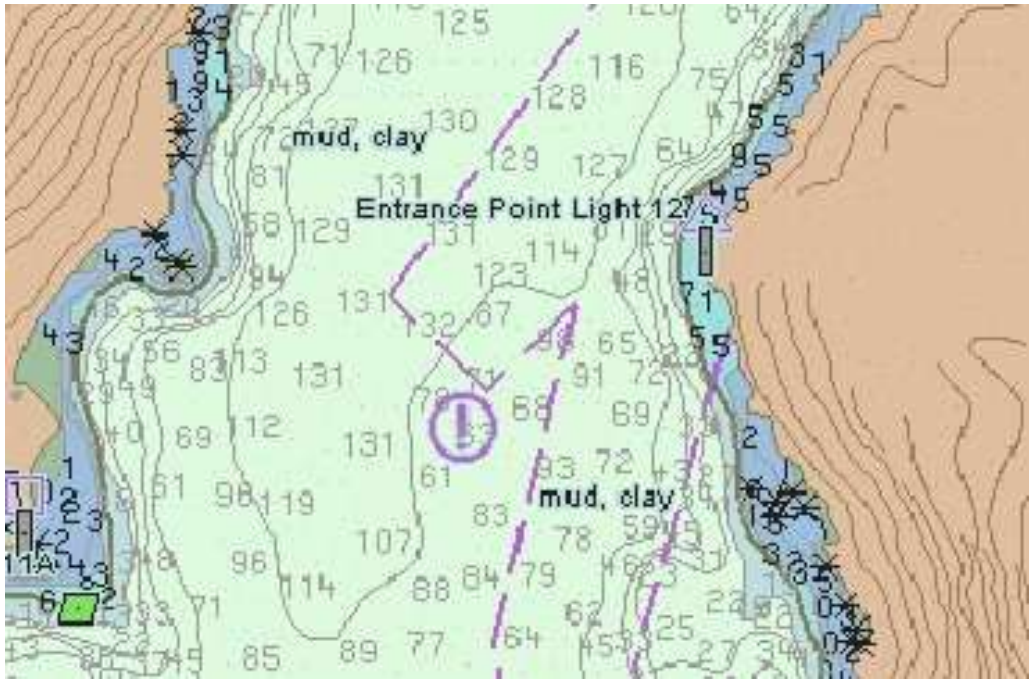
AIS uses the GPS information from the internal NMEA network!

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

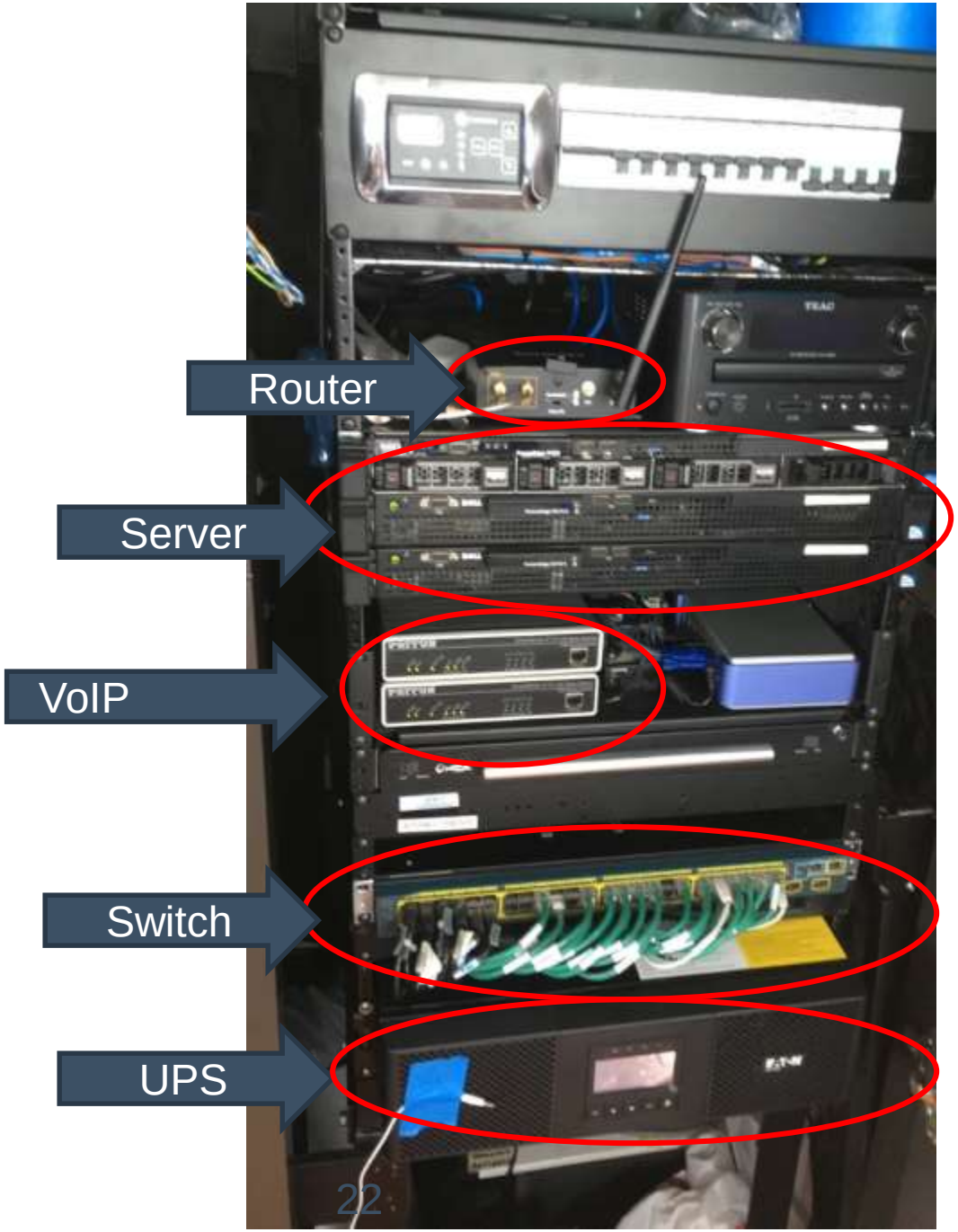
1 Internet Router (GSM, WiFi, SAT)

1 rack mounted Switch (48ports)

1 UPS

4 WiFi Access Point

(Crew, Guest/Owner)



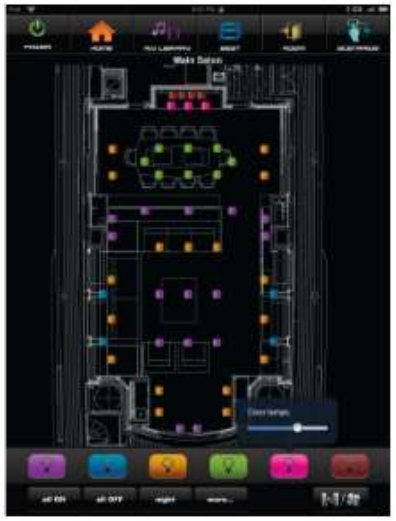
Smart Ships

Audio & Video Streaming

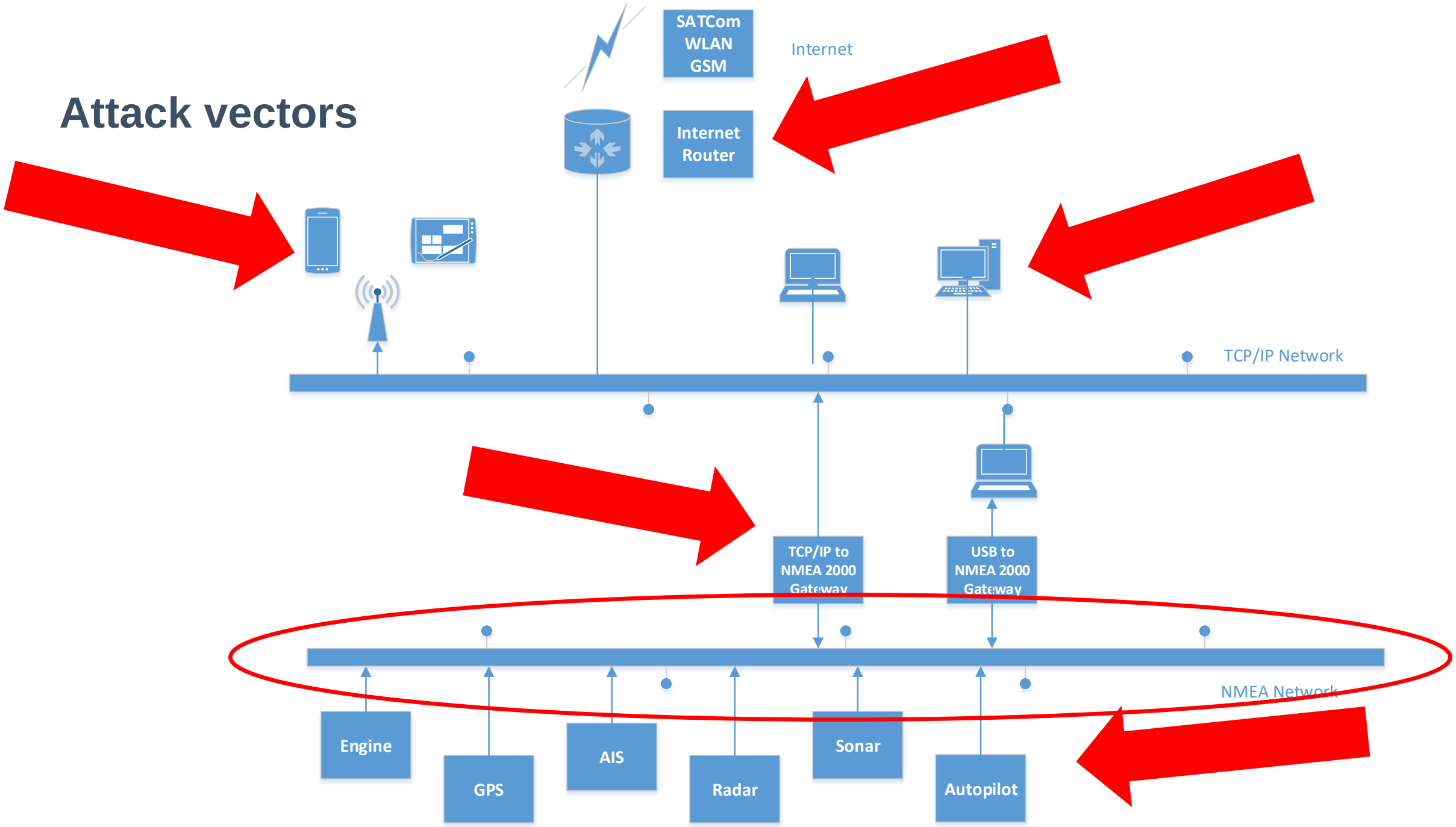
iPhone/iPad remote control of

- Lights
- Electric curtains
- Engine monitor
- ruder

Etc.



Attack vectors



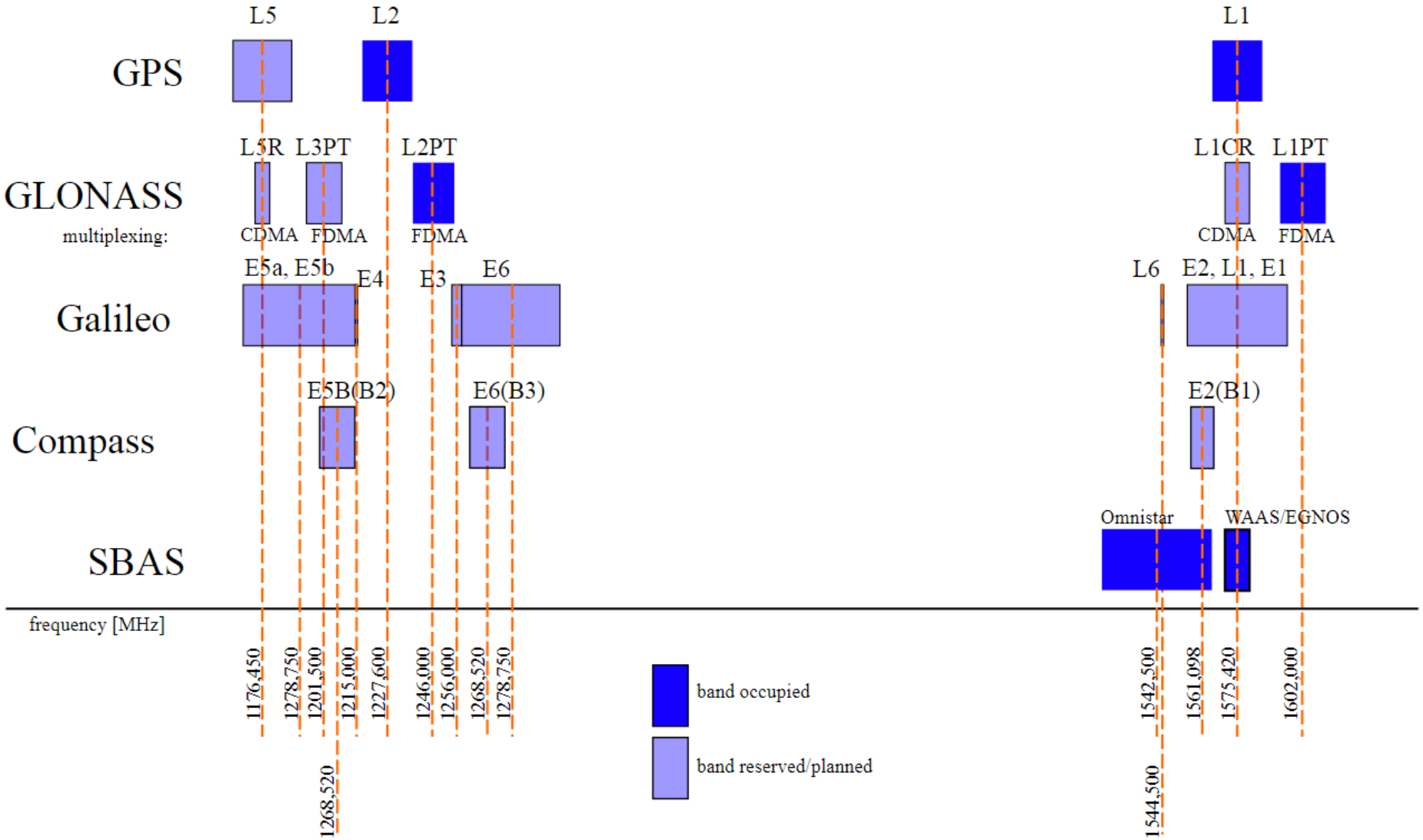
GNSS or GPS attacks

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 on the Bus

GPS – receiver sends the position onto the NMEA Bus

Services that rely onto this:

- ECDIS
- AIS
- Autopilot
- VTS

GPS

2 Scenarios are possible

- jamming
- spoofing

complexibility:

Jamming = quite simple

Spoofing

- requires special hardware
- spoof message over NMEA Gateway (TCP or USB)

GPS attacks

How to spoof GPS?

Specialized Hardware available for it.

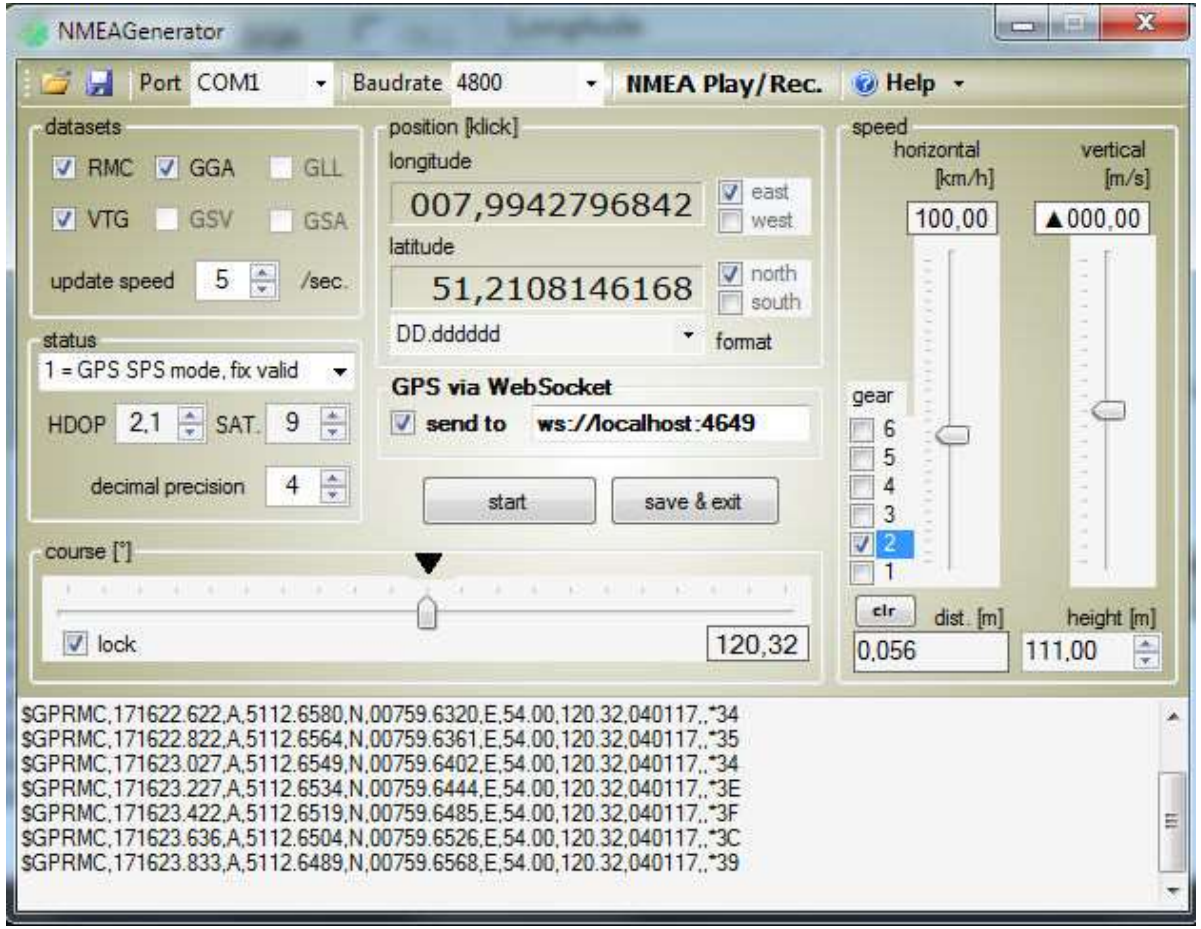
For example Labsat GNSS Simulator
https://www.labsat.co.uk/index.php/de/produkte/labsat-3-de

Or use a BladeRF with GNSS Antenna and BladeGPS
https://github.com/osqzss/bladeGPS

But sometimes it’s easier to fake the NMEA data of the GPS Sensor

Current Project

If physical access to NMEA network once is given



http://www.atlsoft.de/gps-simulator/

GPS - Jamming

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

- US Navy teaching again offline Navigation with Sixtant

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

AIS RF part

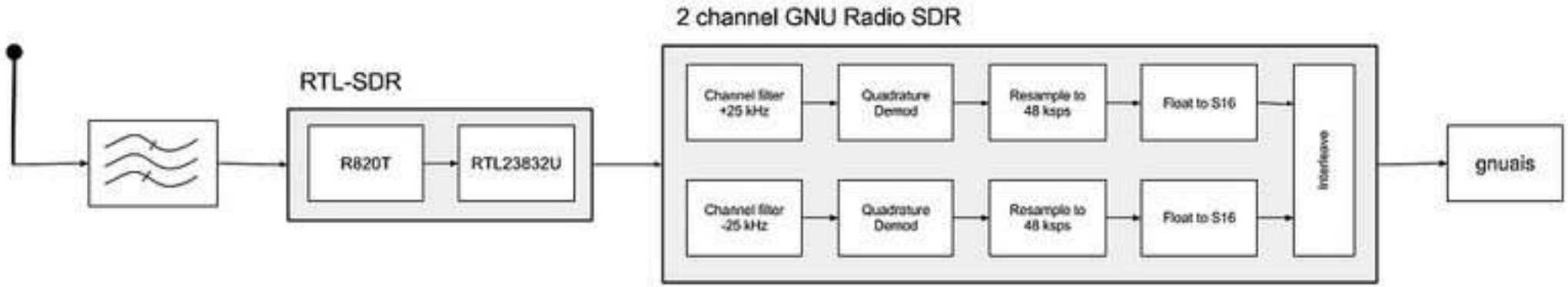
AIS uses the globally allocated Marine Band channels 87 & 88.

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/

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)

The control software (PC/Android/iOS)

The control software

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

The control software

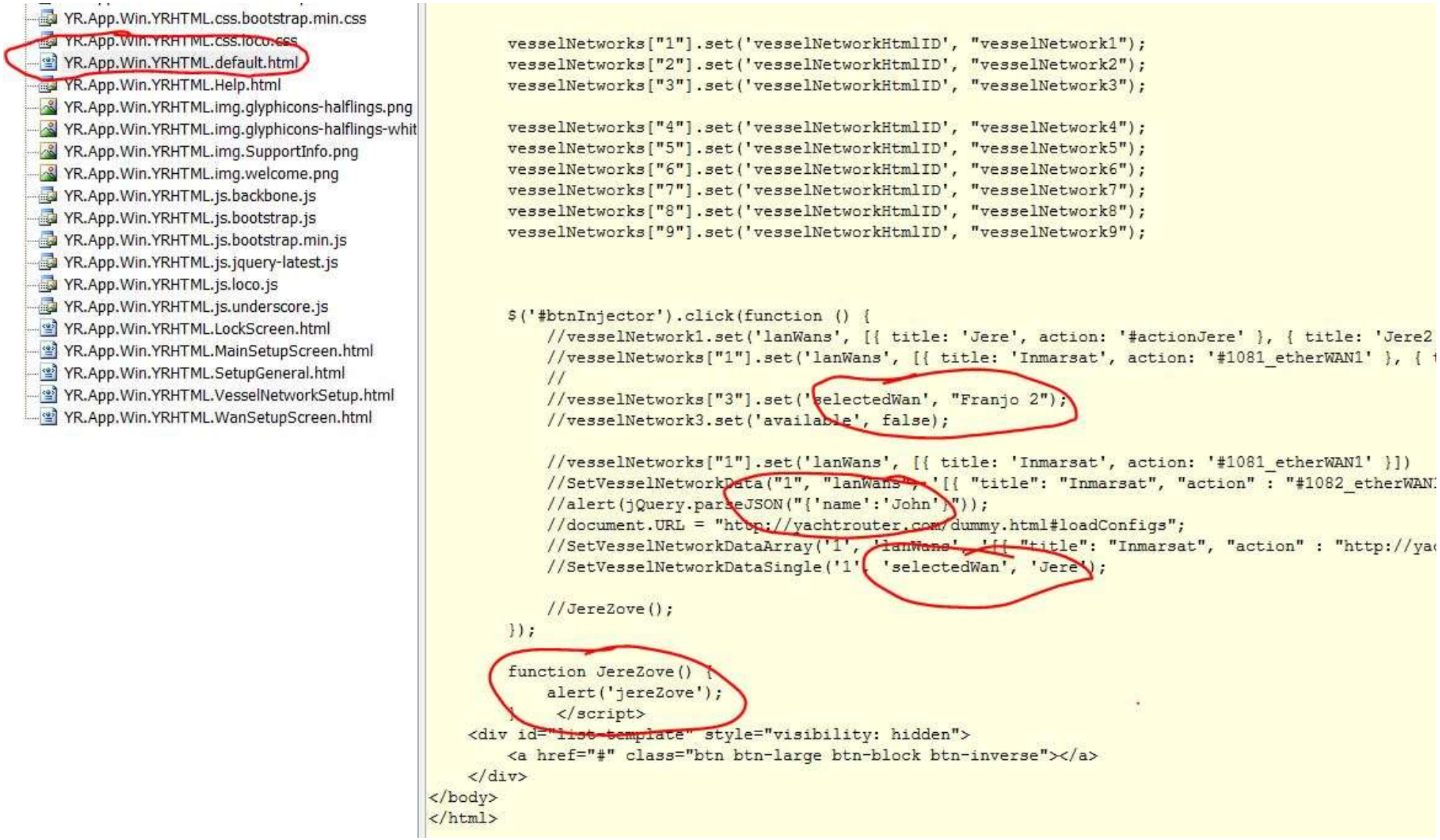
- FTP is clear text
- Hardcoded credentials used !!!
- …xml file contains WLAN SSID and Password (clear text)

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 SecureConnectingUser
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
```

Don’t use disassembler – u will get confused code contains juicy informations



code contains juicy informations

```
static yrEngine()
{
  yrEngine.RouterConfig_Username = "loco";
  yrEngine.RouterConfig_Password = "SecureConnectingUser";
  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.";
```

Do we need a firewall?

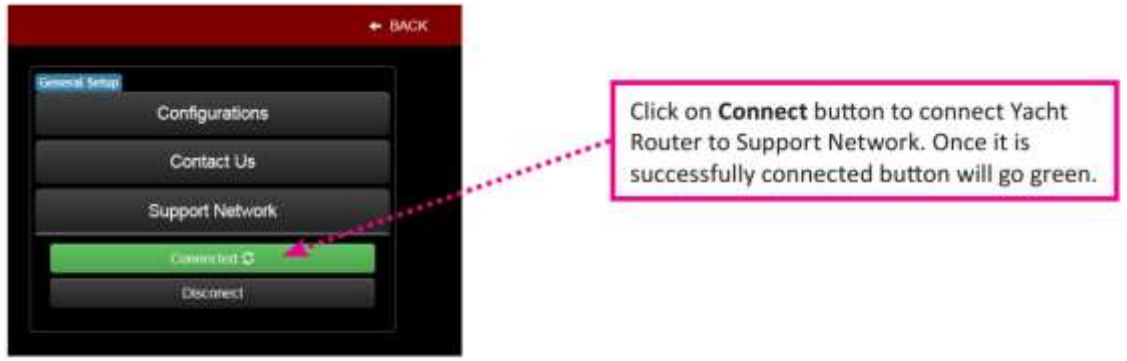
NMAP scan on the puplic IP

- 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

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)



Remote support

Yacht Router model & serial number ?

How do they know the IP address?

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

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" fla

% Information related to '5.10.88.128 - 5.10.88.135'

% Abuse contact for '5.10.88.128 - 5.10.88.135' is 'abuse@softlay

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
```

Remote support

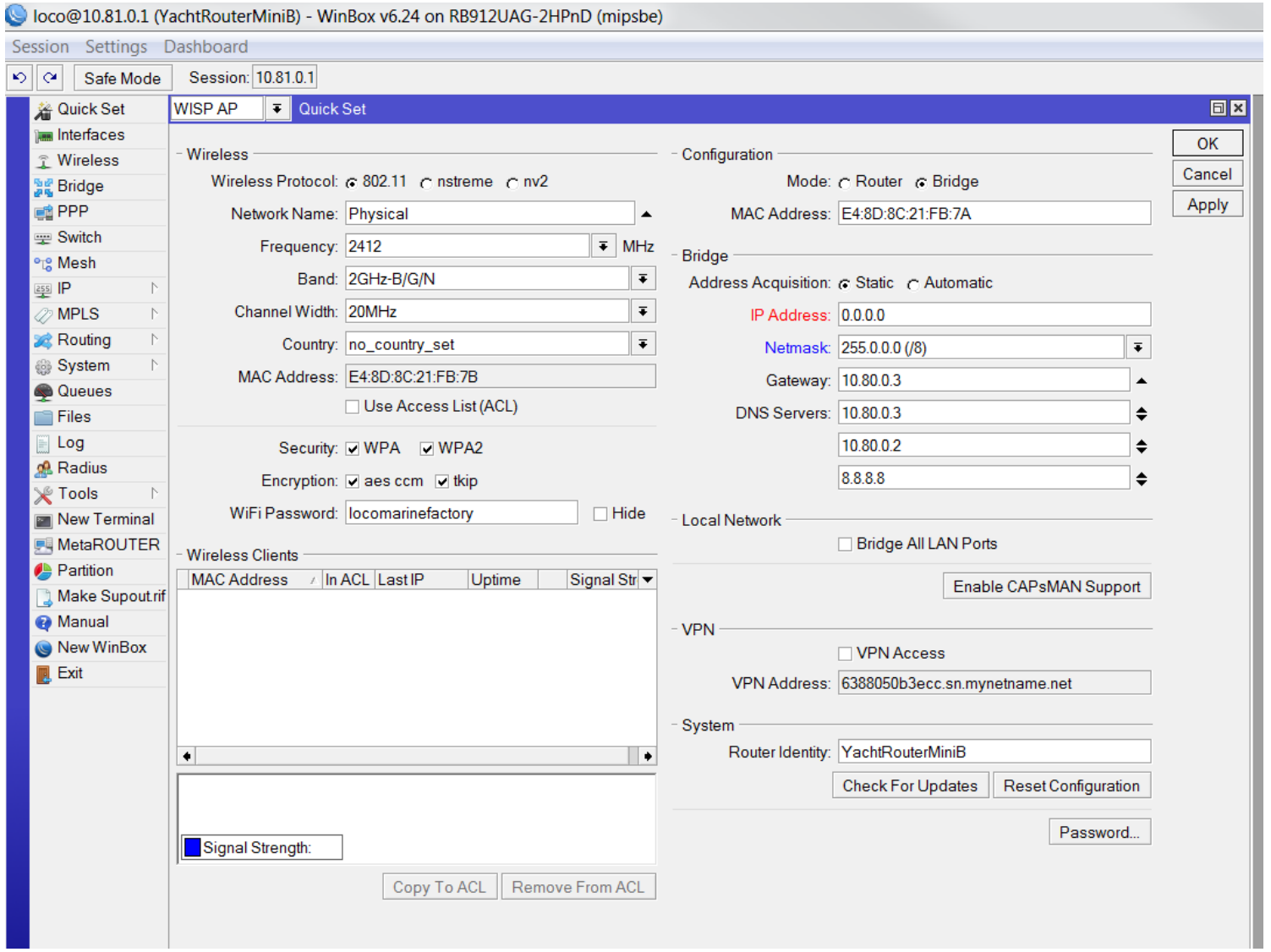
Remember the Portscan ?

Router os= Mikrotik Router OS
8291/tcp open unknown

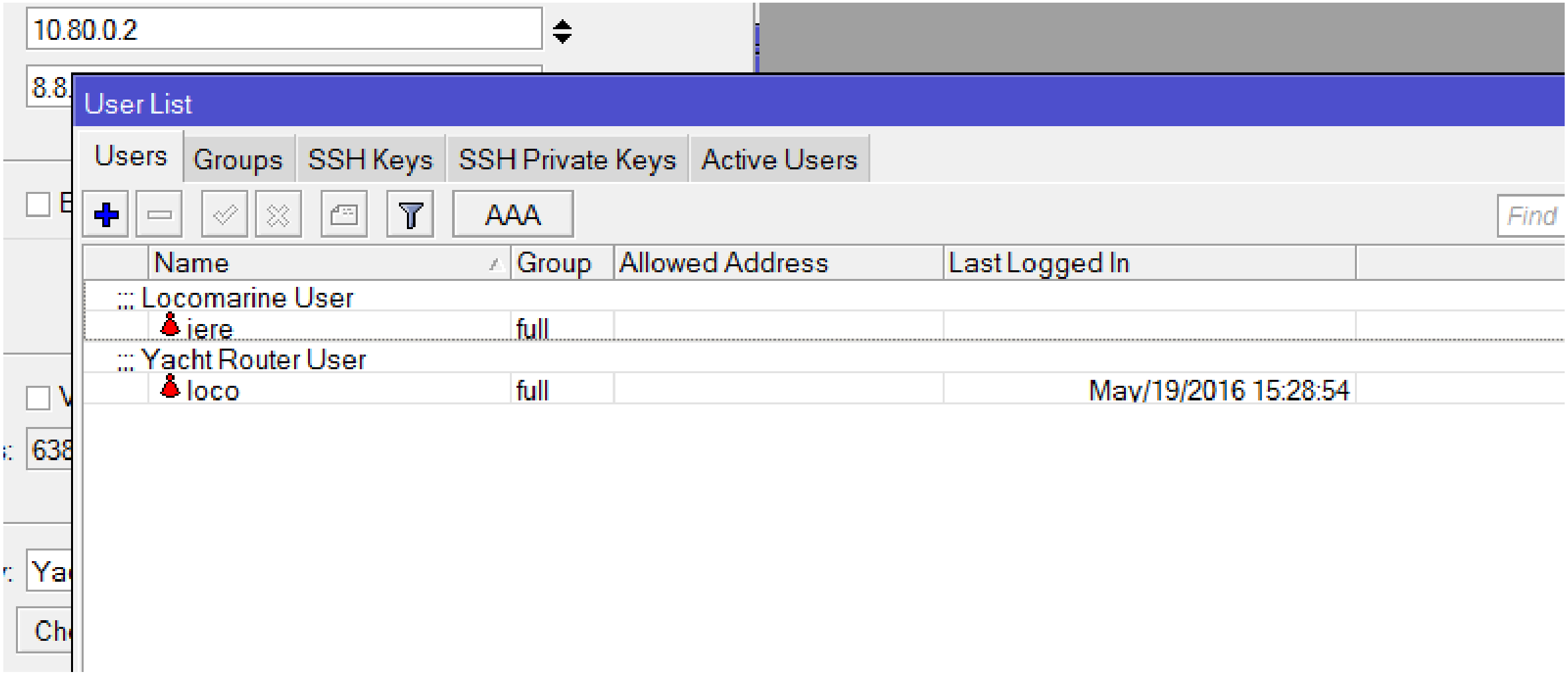
Port 8291/TCP belongs to Winbox Management

Ok, lets Try with the passwords from the source

Issue #4 – WinBox Management



Issue #4 – Winbox Management



Issue #4 – Winbox Management Cracking

MKBRUTUS v1.0.0

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

Or use CVE-2018-14847 (works on Mikrotik 6.42 or below)
https://github.com/BigNerd95/WinboxExploit

$ python3 WinboxExploit.py 192.168.0.1

- User: the user
- Pass: StrengGeheim

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-2017-17673 requested

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

Testing of the patched Software

- Vendor asked me to test the patched software
- They send me a Test Router
- .Net application is now obfuscated
- SSH instead of FTP

But…. Security by obscurity – seriously ?

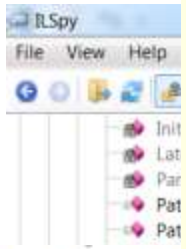
Testing of the patched Software

```
ICSharpCode.Decompiler.DecompilerException: Error decompiling System.String YR.Core.yrEngine/MyUserInfo::getPassword()
 ---> System.NullReferenceException: Object reference not set to an instance of an object.
   at ICSharpCode.Decompiler.CecilExtensions.GetPopDelta(Instruction instruction, MethodDefinition methodDef)
   at ICSharpCode.Decompiler.ILAst.ILAstBuilder.StackAnalysis(MethodDefinition methodDef)
   at ICSharpCode.Decompiler.ILAst.ILAstBuilder.Build(MethodDefinition methodDef, Boolean optimize, DecompilerContext context)
   at ICSharpCode.Decompiler.Ast.AstMethodBodyBuilder.CreateMethodBody(IEnumerable`1 parameters)
   at ICSharpCode.Decompiler.Ast.AstMethodBodyBuilder.CreateMethodBody(MethodDefinition methodDef, DecompilerContext context, IEnumera
   --- End of inner exception stack trace ---
   at ICSharpCode.Decompiler.Ast.AstMethodBodyBuilder.CreateMethodBody(MethodDefinition methodDef, DecompilerContext context, IEnumera
   at ICSharpCode.Decompiler.Ast.AstBuilder.CreateMethod(MethodDefinition methodDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.AddTypeMembers(TypeDeclaration astType, TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.CreateType(TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.AddTypeMembers(TypeDeclaration astType, TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.CreateType(TypeDefinition typeDef)
   at ICSharpCode.Decompiler.Ast.AstBuilder.AddType(TypeDefinition typeDef)
   at ICSharpCode.ILSpy.CSharpLanguage.DecompileType(TypeDefinition type, ITextOutput output, DecompilationOptions options)
   at ICSharpCode.ILSpy.TextView.DecompilerTextView.DecompileNodes(DecompilationContext context, ITextOutput textOutput)
   at ICSharpCode.ILSpy.TextView.DecompilerTextView.<>c__DisplayClass31_0.<DecompileAsync>b__0()
```

Don‘t forget the APP‘s

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

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

    pub
    pub  RouterConfig_Username = "loco";
    pub
    {    RouterConfig_Password = "ySyteMJwWuyAyMu84D";
    };

    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_";
```

Testing of



PatchApiSSL
PatchBackbo
PatchDhcpC

```
public void PatchBackboneDataLeak()
{
    try
    {
        foreach (MK router in this._Routers)
        {
            if (!router.RouterID.Contains("MobileExpanderLB"))
            {
                if (router.RouterID.Contains("MobileExpander"))
                {
                    foreach (YachtRouterConfigWANMobile mobileWAN in this.mainConfig.MobileWANs)
                    {
                        if (mobileWAN.RouterID == router.RouterID)
                        {
                            router.RouteSetTargetToNewByComment(mobileWAN.InterfaceName, "backbone");
                            break;
                        }
                    }
                }
                else
                {
                    router.DeleteAllRoutes("0.0.0.0/0", "backbone");
                    router.EnsureWorkingRoute("5.10.81.50", "backbone", "100");
                    router.EnsureWorkingRoute("8.8.8.8", "backbone", "100");
                    if (router.RouterID == "Main")
                    {
                        router.AdjustDNS("10.80.0.3,10.80.0.2,8.8.8.8");
                    }
                    else
                    {
                        router.AdjustDNS(string.Empty);
                    }
                }
            }
        }
    }
    catch (Exception ex)
    {
        this._curLogger.LogException(ex);
    }
}
```

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

Satcom

Satcom

- Offshore internet acces via Satcom
- Patching ?
- Many old Versions still online
- A sample

Satcom

Shodan.io search hint’s for possible vulnerable devices

- “Sailor 900”
- “Inmarsat Solutions”
- “Telenor Satellite”
- “Commbox”
- org:"Intelsat GlobalConnex Solutions (GXS)“
- org:"Telenor UK Ltd"

Satcom

Did u know? Shodan.io has a Live Shiptracker

URL: Shiptracker.shodan.io

Tracks via VSAT connected Antennas and exposes Web Services

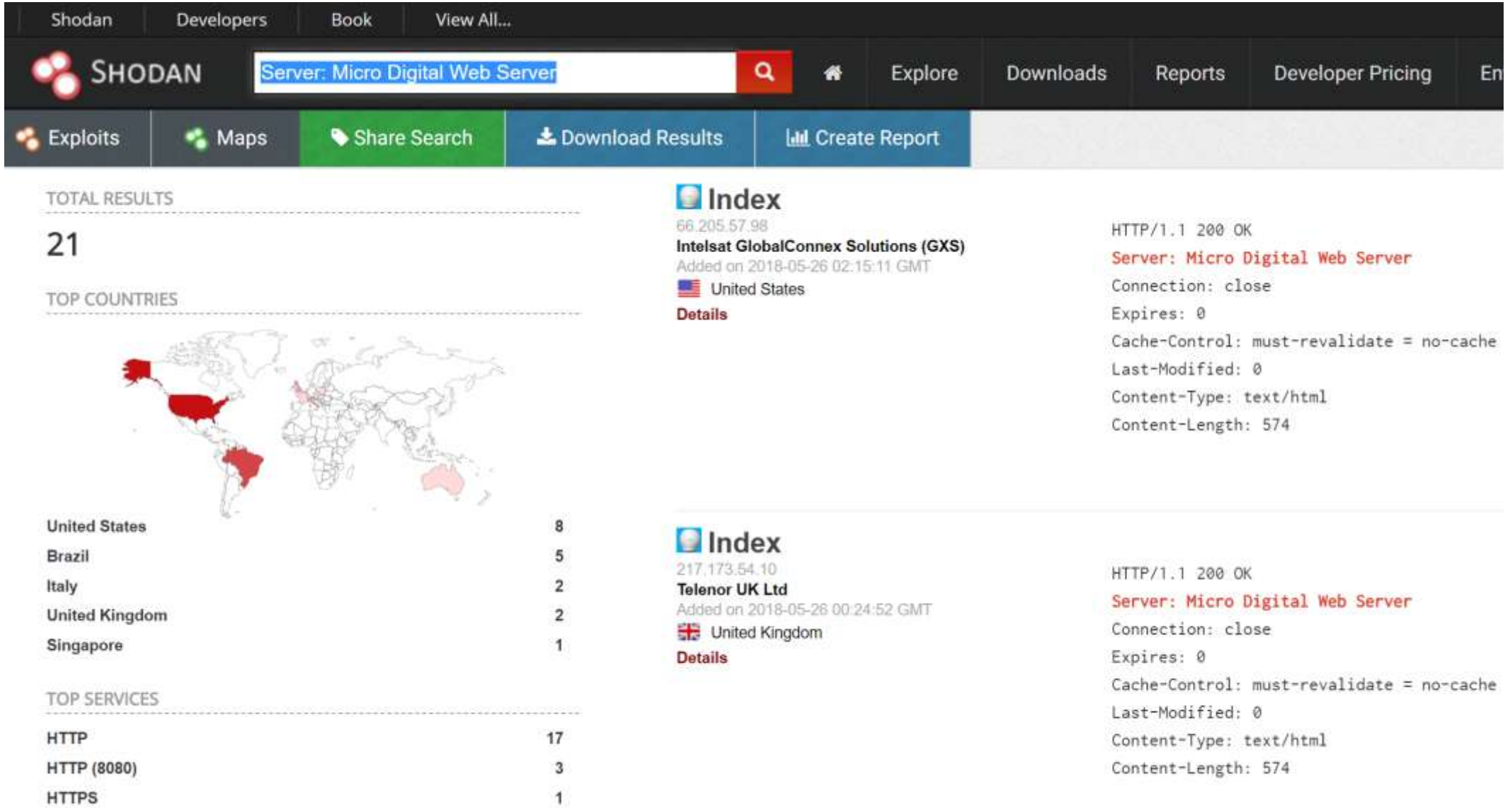
Satcom

Was shodan surfing for other Satcom Boxes !
“stabilized Digital Antenna System” result paid my attention

- Results in Cobham MXP Webserver
- Shodan Query for “Server: Micro Digital Webserver” gives better result


```
HTTP/1.1 200 OK
Server: Micro Digital Web Server
Connection: close
Expires: 0
Cache-Control: must-revalidate = no-cache
Last-Modified: 0
Content-Type: text/html
Content-Length: 574
```

Search “Server: Micro Digital Webserver”

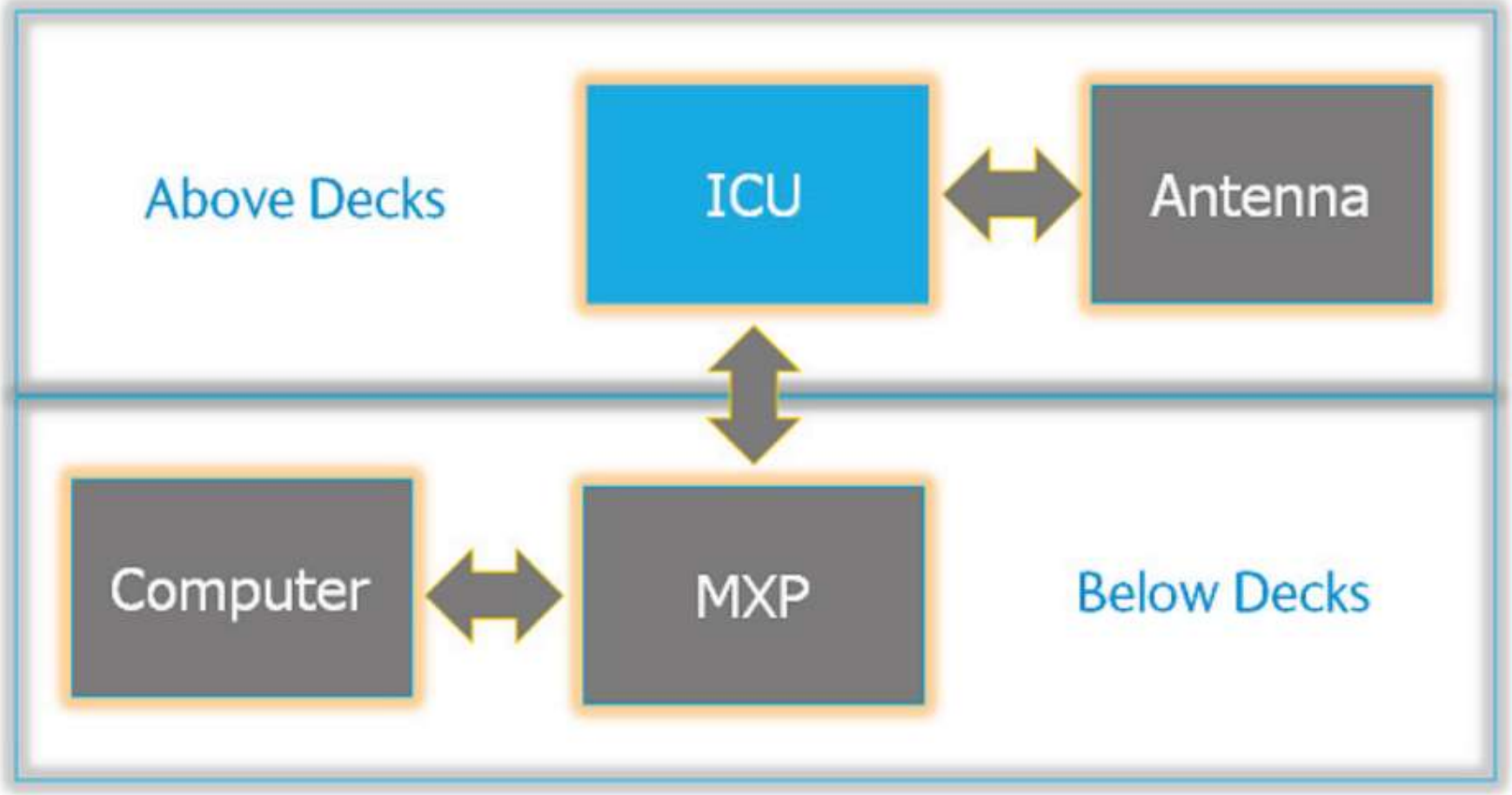


Cobham Seatel Satcom

- Was looking for Satcom devices via Shodan
- Found some online
- Analyzed Webinterface with Fiddler/burpsuite
- Found some juicy javascripts

SatCom


Sea Tel
COBHAM


Above Decks
ICU
Antenna
Computer
MXP
Below Decks

Cobham Seatel Satcom

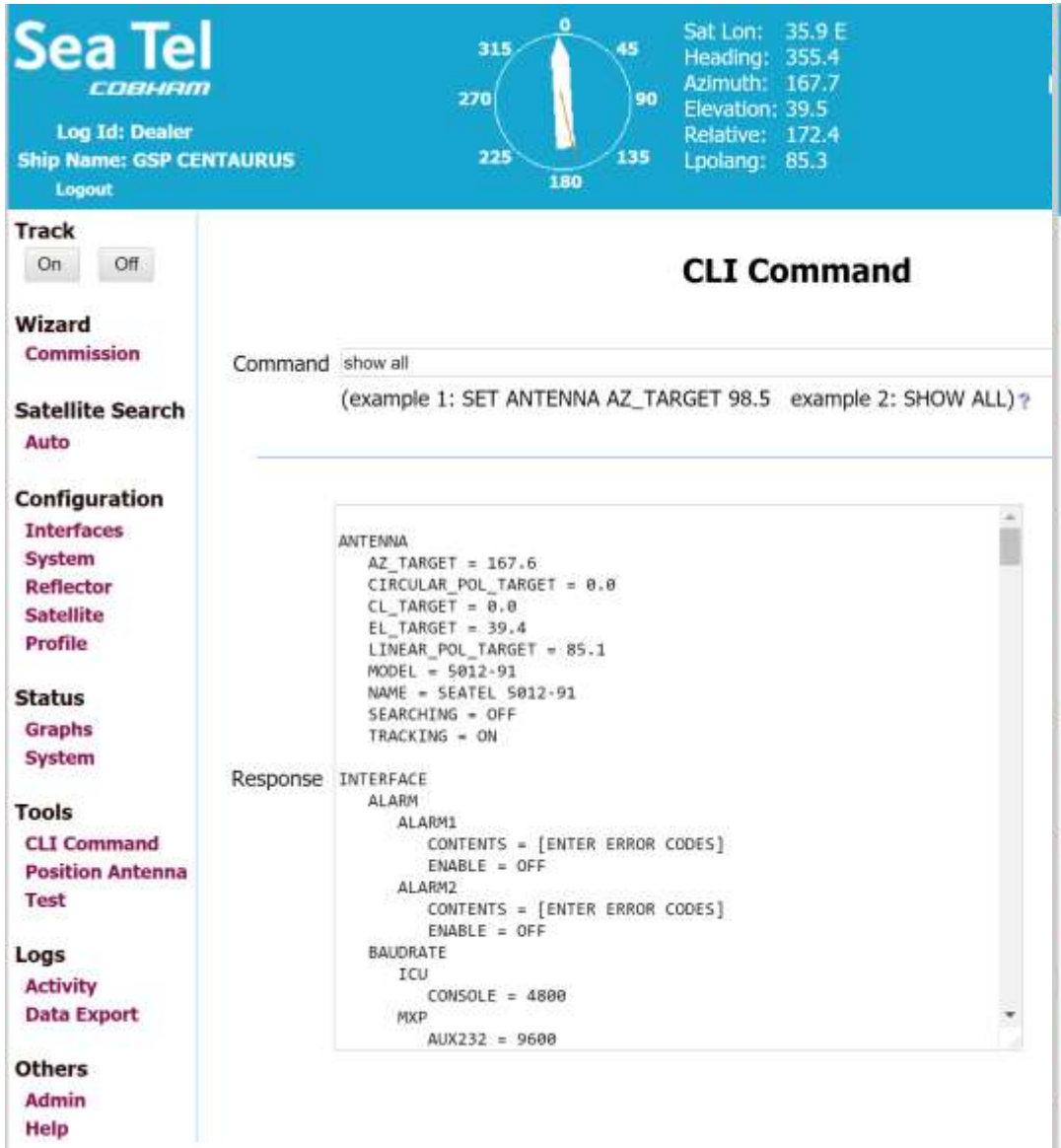
Demo

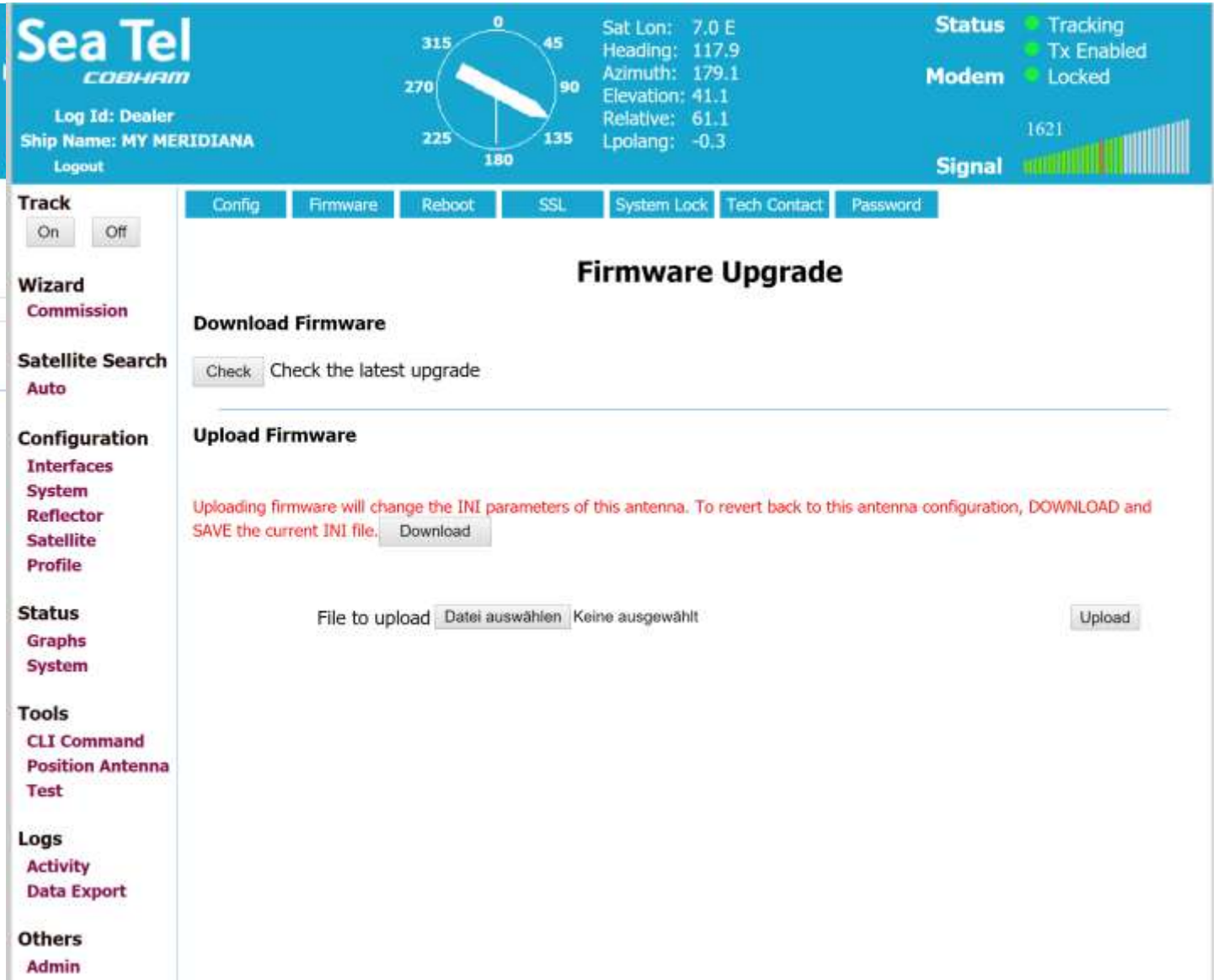
Cobham Seatel Satcom

/js/userLogin.js contains some hints

if(t=="**Dealer**"){if(r=="true"){e="**MenuDealerGx.html**"}else{e="**MenuDealer.html**"}}else
if(t=="**SysAdmin**"){if(r=="true"){e="**MenuSysGx.html**"}else{e="**MenuSys.html**"}}else
if(t=="**User**"){if(r=="true"){e="**MenuEuNCGx.html**"}else{e="**MenuEuNC.html**"}}

Cobham Seatel Satcom





Cobham Seatel Satcom RTFM

RTFM ! In the manual: default username and password

- Dealer
- seatel3

- SysAdmin
- seatel2

- User
- seatel1

Cobham Seatel Satcom

CVE Lookup if someone found already:

F..K – someone was already faster

But….

Cobham Seatel Satcom

CVE-2018-5267 reported Auth bypass only in Version 121 Build 222701

I can confirm following other versions too:

- Version number: 186 (Build:225xxx)
- Version number: 179 (Build:224945)
- Version number: 171 (Build:224753)
- Version number: 148 (Build:223591)
- Version number: 147 (Build:223551)

Vulnerability fixed in version >200

Cobham Seatel Satcom

To have fun with the seatel device, following Menues are available without authentication:

ConfigPortGx.html	configuration der IO Ports
CommDiag.html	cli command interface
PositionAntGx.html	change Antenna configuration
FileAdmin.html	
CfgFileDnUpload.html	down/upload config
FirmwareUpload.html	firmware update
CfgSysCommon.html	rename ship name in menue
SysStatus.html	
RebootUnit.html	reboot

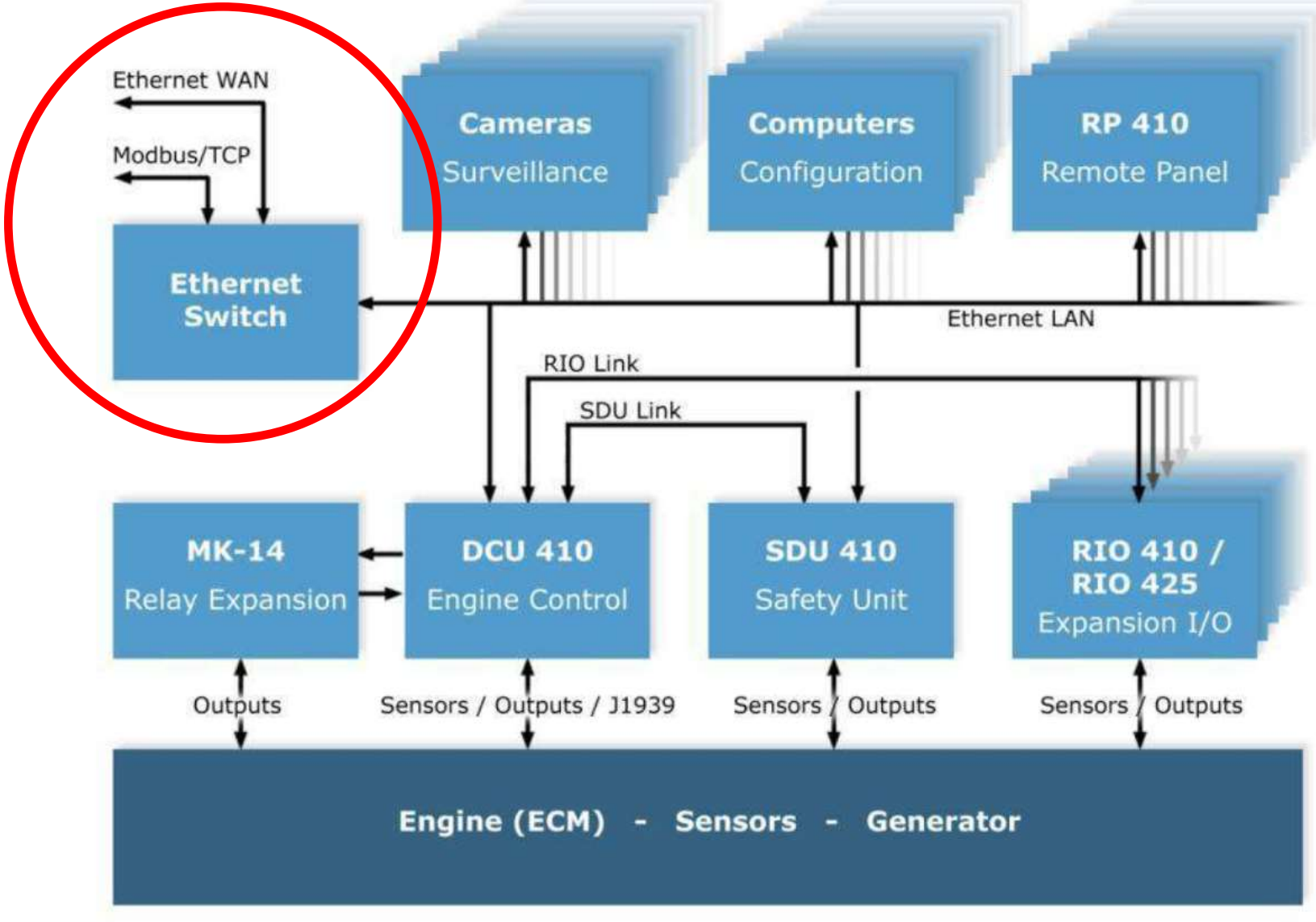
Cobham Seatel Satcom

Whats the Risk now?

- Increase Cost
- Denial of Service

Engine Control units

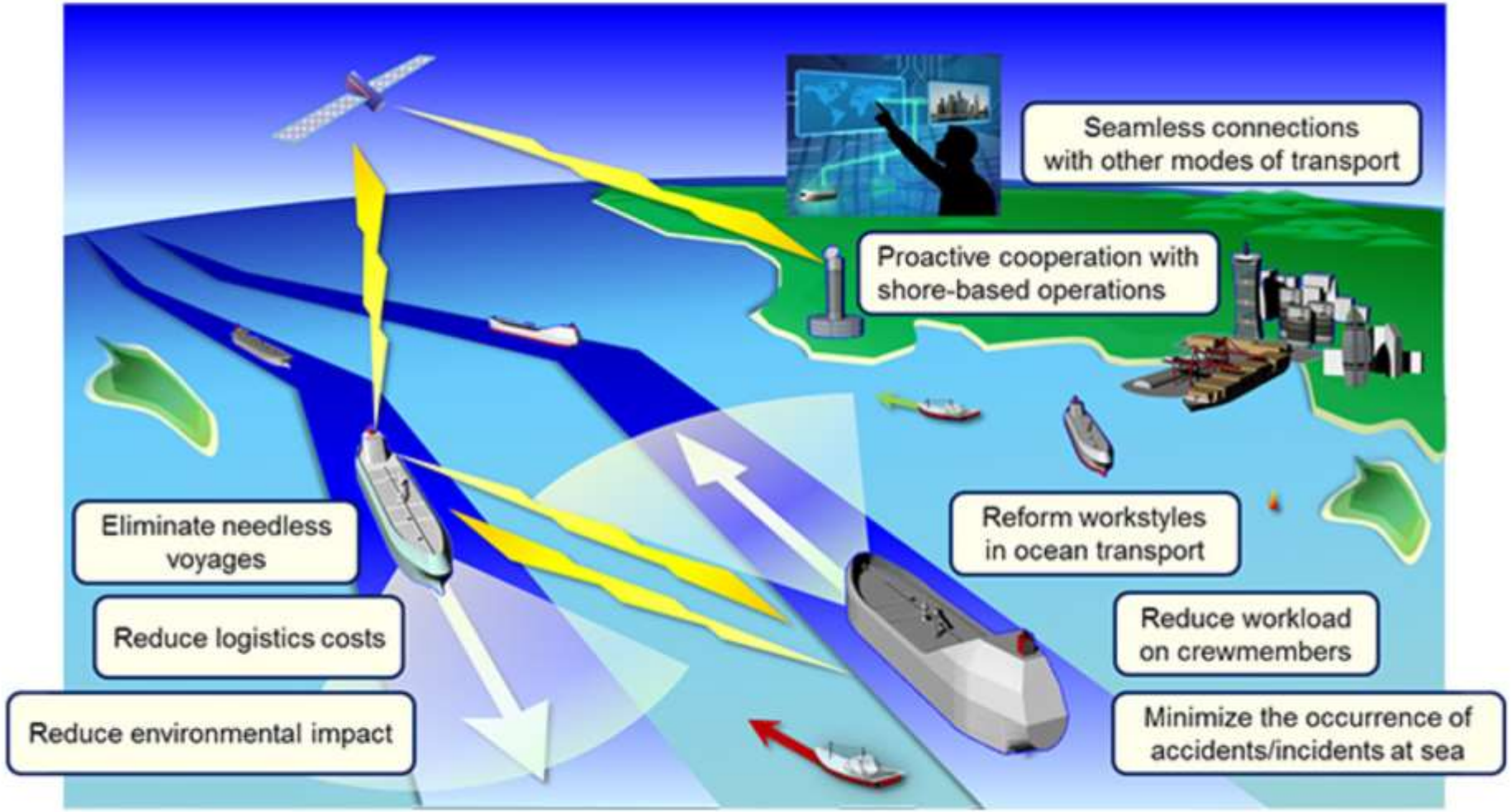
ECU
Remote Panel
Safety Unit
Etc.



Auto Maskin 400_Series_Installation_and_Configuration__Manual_2_11.pdf

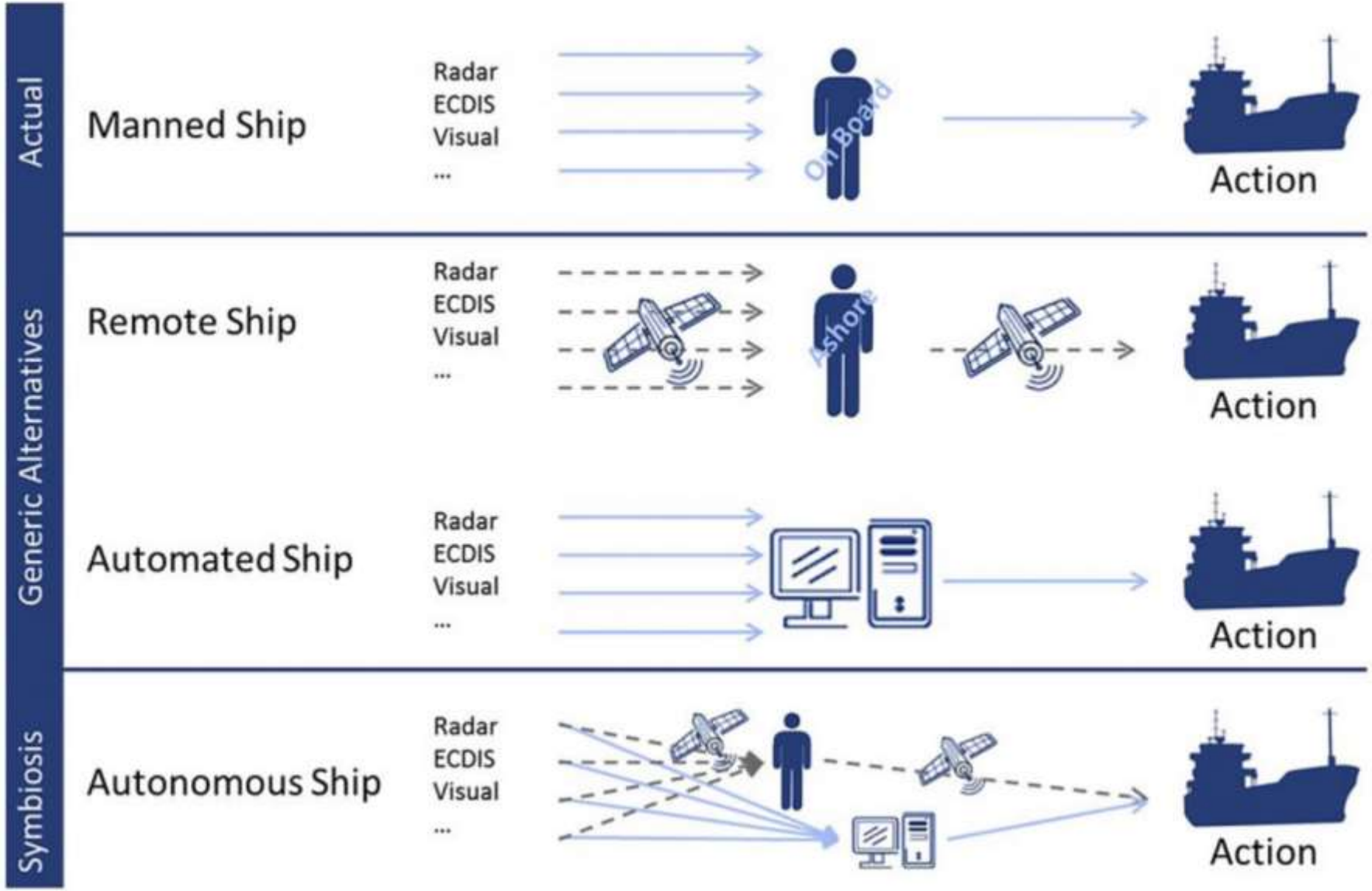
Mostly Connected to
the Ethernet like a
MTU wired remote control for engines and bow-thruster

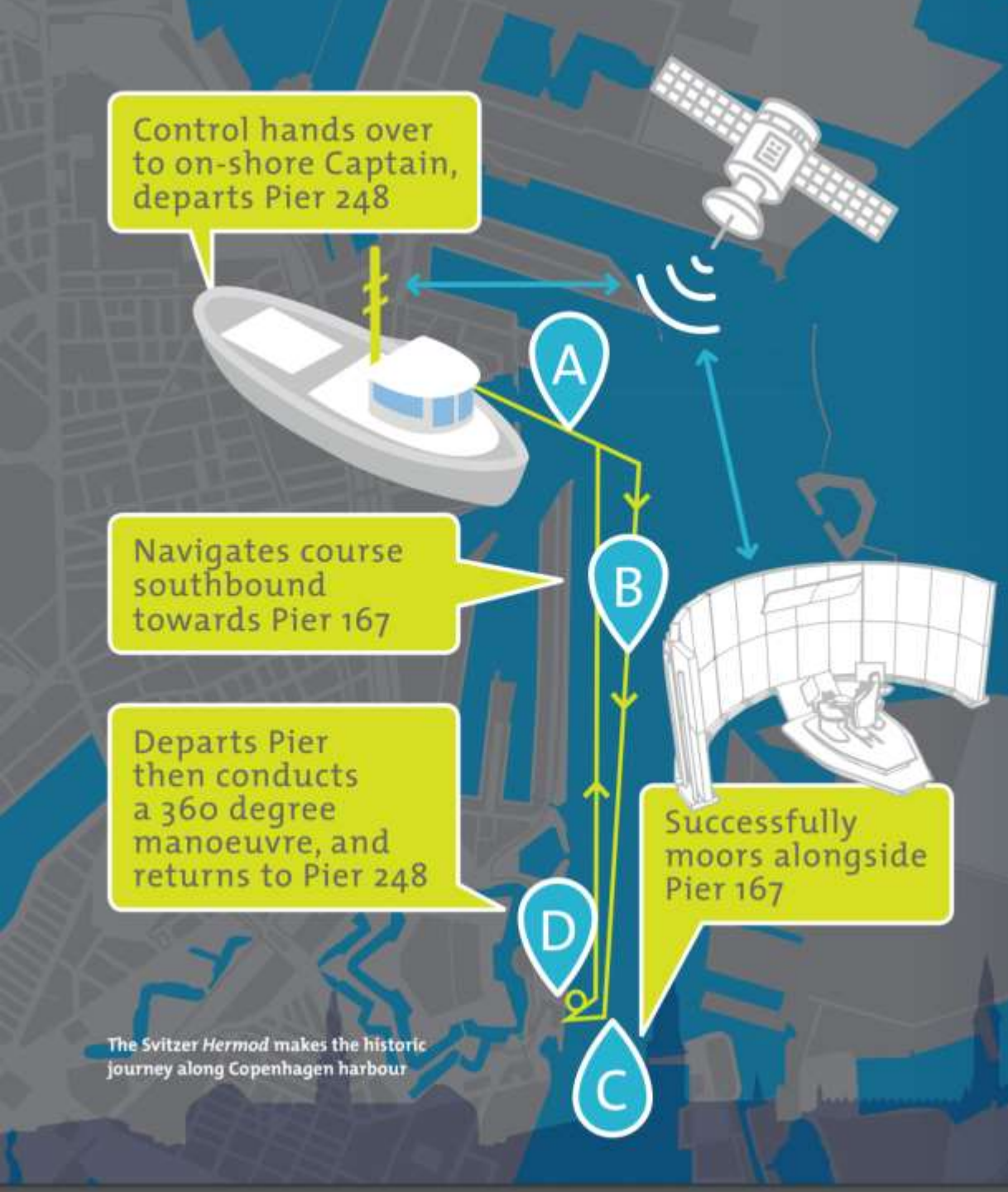
The future: Autonomous ships



An illustration of the benefits of autonomous ships – from Mitsui O.S.K. Lines, Ltd.

The future: Autonomous ships





The Svitzer *Hermod* makes the historic journey along Copenhagen harbour

The world's first remote control commercial vessel

Key facts

Rolls-Royce and Svitzer demonstrate the world's first remote controlled commercial vessel • Test took place in Copenhagen harbour • The 28 metre Svitzer *Hermod* was controlled by a Captain from shore • It successfully demonstrated vessel navigation, situational awareness, remote control and communications systems • Rolls-Royce Remote Operations Centre features state-of-the-art control • Combination of Radar, Lidar and camera technology ensures Captain's awareness of surroundings

The tech

On board sensors to give Captain full awareness of surroundings

Sensors covering Radar, Lidar, camera and audio

State-of-the-art Remote Operations Centre on shore

Rolls-Rolls Dynamic Positioning systems control position of the vessel via satellite

The test

400+ individual validations met

42 individual safety requirements met

Passed 61 mandatory cyber security tests

Completed 16 hours of remote control operation and overseen by Lloyd's Register

The vessel

28 metre tug Svitzer *Hermod*

Built in 2016

2 x MTU 16V4000 M63 diesel engines

Rolls-Royce

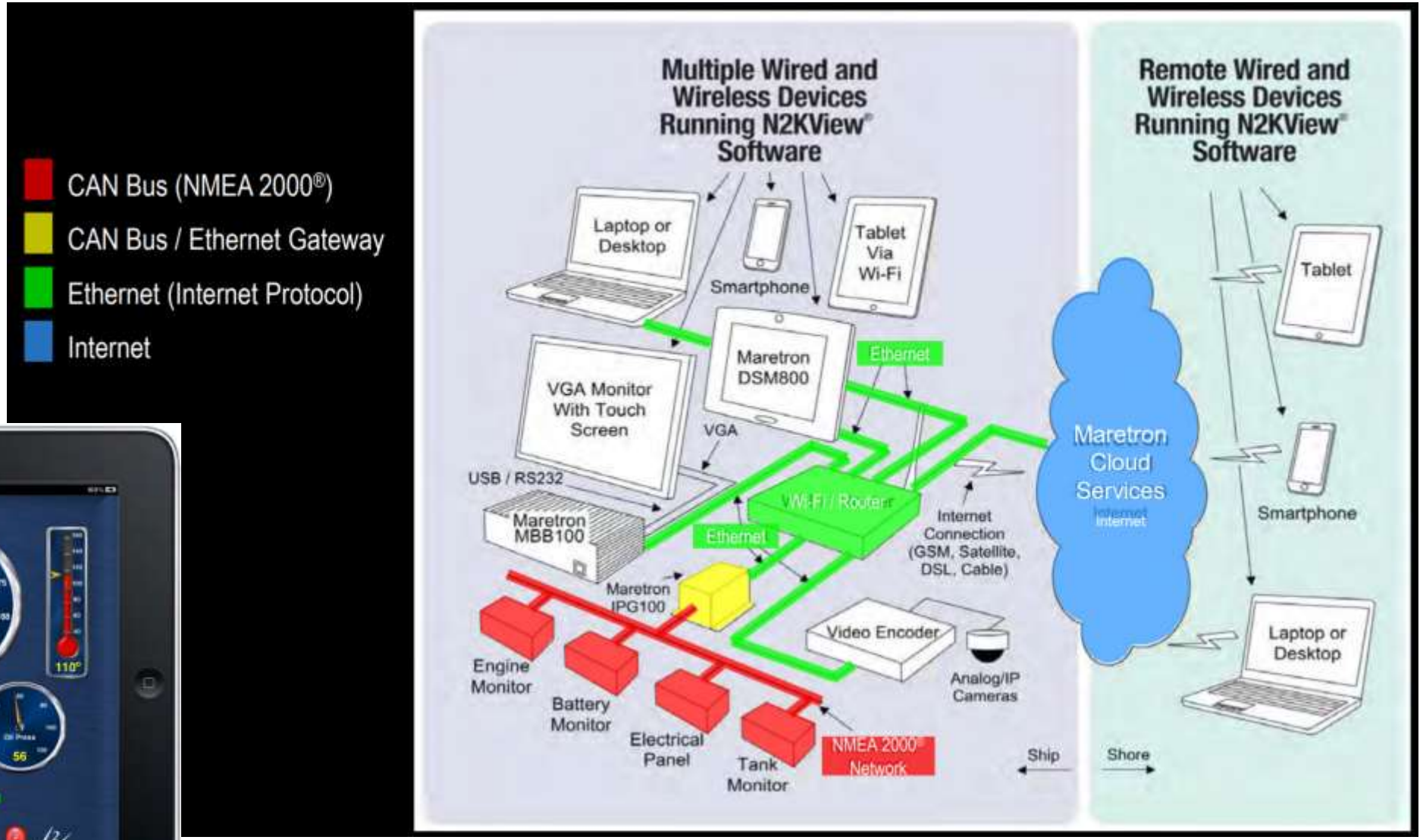
What’s next?

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

- Release of CVE-2018-16114 and PoC code when fixed

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

Future is cloud



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

conclusion

- NMEA Gateways needs more research
- SATCom Boxes mostly unpatched (or only once a year)
- VTS is unexplored
- Autopilot Remote control (currently working on)
- Injecting NMEA messages to the Bus (currently working on)
- GPS spoofing protection (DLR “Galant” new Antenna array)

Special thank to

- you, for attending my talk
- HITB2018DXB for this great event again
- “I am The cavalry”
- Brian Satira @r3doubt and Brian Olson @akordingtobrian
  great talk @derbycon “Ship Hacking: a Primer for Today’s Pirate”
  http://www.irongeek.com/i.php?page=videos/derbycon8/track-4-12-ship-hacking-a-primer-for-todays-pirate-brian-satira-brian-olson
- Ken Munro from Pentest Partners
- My employeer ROSEN for supporting me
- My Security friends (family) around the world

May the force be with u

Twitter: @ObiWan666

SGerling@ROSEN-Group.com

THANK YOU FOR JOINING THIS PRESENTATION.

www.certivation.com

CERTivation