



Ship Hacking 101

A Primer For The Modern Pirate



October 7, 2018
Brian Olson, Brian Satira
Project Gunsway

A scene from the movie Pirates of the Caribbean: At World's End. Will Turner (played by Orlando Bloom) is on the left, wearing his signature straw hat and vest, looking towards the camera with a serious expression. Ragetti (played by Kevin Richardson) is on the right, holding a large, ornate silver hook and shouting. They are in a dark, metallic environment, possibly the interior of a ship or a foundry.

Where Everyday Is ITLAPD

Aye! Avast!

Overview

- Introductions
- Basic Seamanship
- Pirate's Primer
- Original Research
- Conclusions and Questions

BLUF:

Maritime infosec immature and pirates are taking notice but the infosec community can help.



“They're not here to fish.”
--Captain Richard Phillips

Obligatory WHOAMI



Brian Satira

- Volunteer
 - I Am The Cavalry
 - Project Gunsway
- Reverse Engineer
 - Malware
 - ICS, IoT, Embedded
- Past work for Navy
 - Risk Analysis
 - DFIR
- Some diesel experience
 - Motorpool, pmcs
 - Annapolis School of Seamanship
- Nova Hackers, Nova TOOOL, Nova Labs



@r3doubt
<https://blog.r3doubt.io>

Brian Olson

- Volunteer
 - Project Gunsway
- Engineer
 - R&D
 - Threat Emulation
 - Architect
 - ICS, IoT
- Past work for Marines
 - Risk Analysis
 - DFIR
- Amateur Meteorologist
- Amateur Sailor/Tactician
 - Ship systems and Networks

@akordingtobrian
brian.olson@corescout.com

Volunteer Organizations

I Am The Cavalry

- Intersection of computer security, public safety, and human life
- Areas of research and advocacy
 - Medical
 - Automotive
 - Public Infrastructure
 - Maritime
 - Smart Home



Project Gunsway

- Grassroots organization
- “Home” is Nova Labs / DC area
- Share The Cavalry’s goals
 - Some of us are The Cavalry members
- Day jobs in IT but maritime connections
- Focused on maritime domain
 - Current project is propulsion controls
- Follow The Cavalry’s disclosure standards



Basic Seamanship (For Pirates)

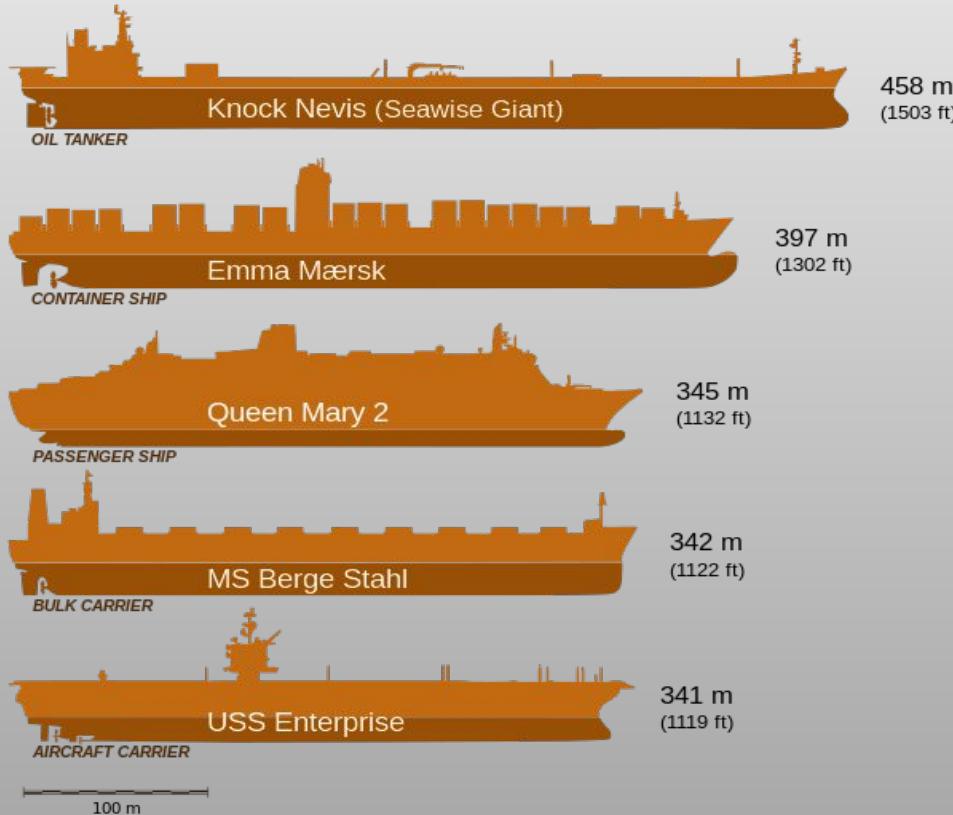


What's At Stake

- Economy
 - \$19 Trillion goods
 - Roughly size of US GDP
- 10.3 Billion tons of cargo
 - 52% containerized cargo (CONEX)
 - 90,000+ ships, 360+ Million containers
- Environment
 - Exxon Valdez (P. W. Sound), \$6.3 Billion, 38,000 tons
- Human life
 - Forget PII, how many people die?
- Regulations, practices are ~~a joke~~ not yet “mature”
 - IMO Guidelines, 2017
 - MSC-FAL.1-Circ.3, Resolution
 - MSC.428(98)
 - Goal for shippers-- plan by 2021
 - Coast Guard NVIC 05-17
 - Cut and paste of NIST guidelines, CISSP practice test questions



Ultra Large Container Vessel (ULCV)

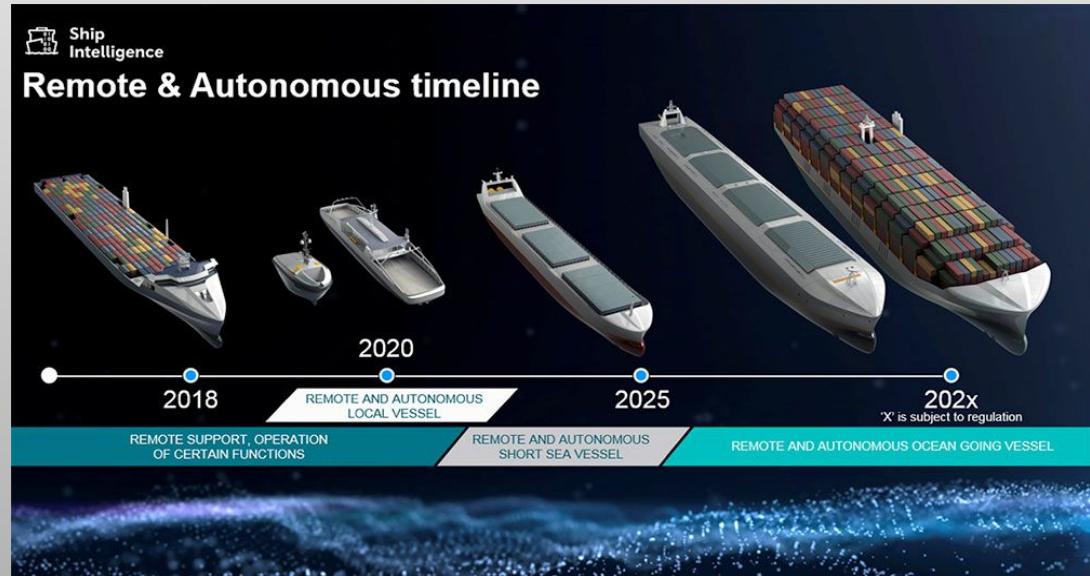


Emma Maersk

- IMO: 9321483
- Type: Container Vessel
- Owner: A.P. Moller-Maersk Group
- Shipyard: Odens Steel Shipyard Ltd
- Delivered: 2006
- Tonnage: 11,000 TEU
 - Twenty-Foot Equivalent Unit
- Length: 398m (1,306ft)
- Breadth: 56m (184ft)
- Speed: 25.2kts (30mph)

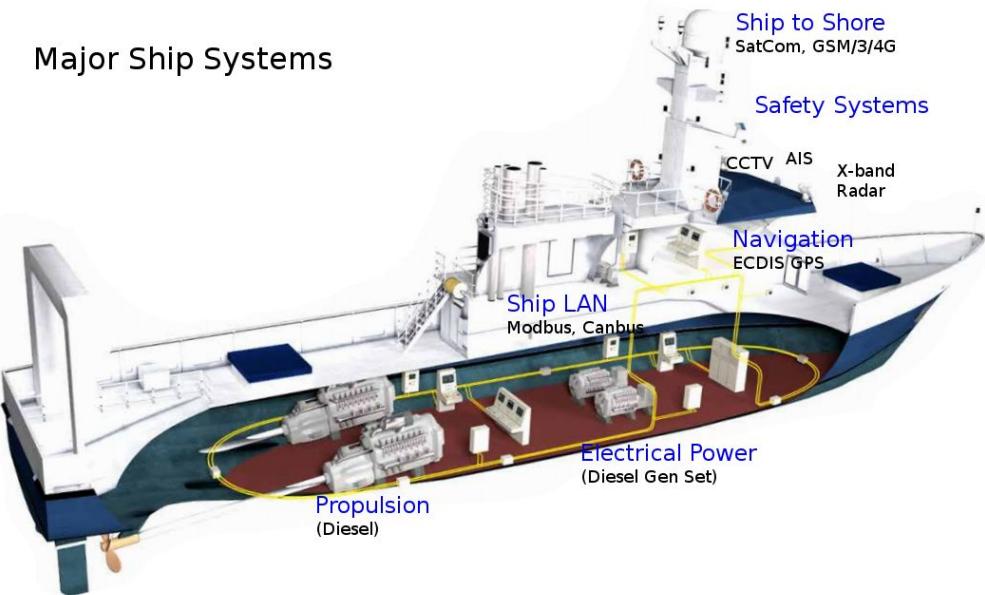
Ship Automation--ICS to Autonomous Vessels

- E-Class ULCV Stats
 - \$145 million per ship
 - 6.22 MT per hour at \$500 per ton
 - \$50,000 per day to operate
 - Crew already 15 or less
 - Crew and Fuel Biggest Expense
 - Status autonomous vessels
 - RR starts first in 2020
 - Shoreside “bridge”
 - Current limit is regulation
 - SOLAS



Major Ship Systems

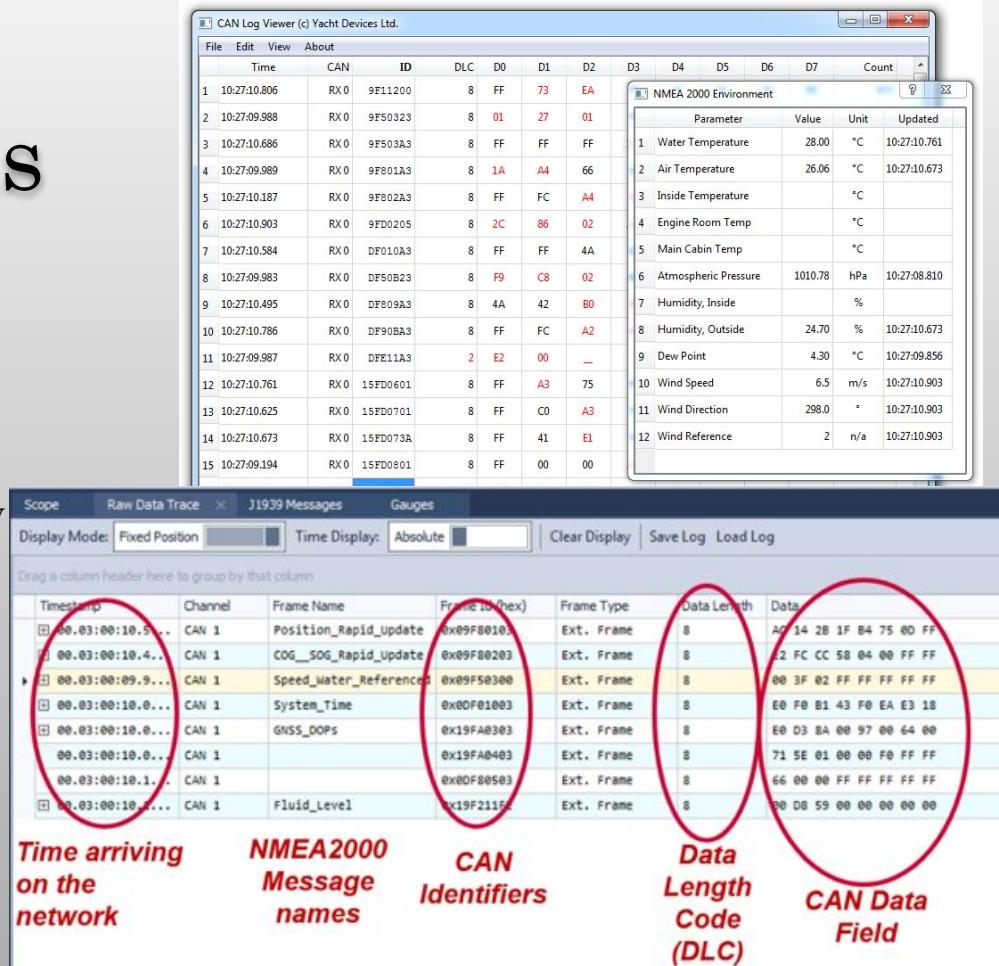
Major Ship Systems



- Cargo management
 - Smart Cargo
 - EDIFACT
- Communications
 - Ship to shore
 - GSM, 3G, 4G
 - Satellite
 - Ship LAN
- Safety
 - VTS (Vessel Tracking System)
 - AIS
 - CCTV
 - X-Band radar
 - GMDSS
 - NAVTEX, DSC, EPIRB, SART
- Propulsion and Power
 - Direct or diesel-electric
 - Gen sets
- Navigation
 - ECDIS (Electronic Chart Display)
 - GPS

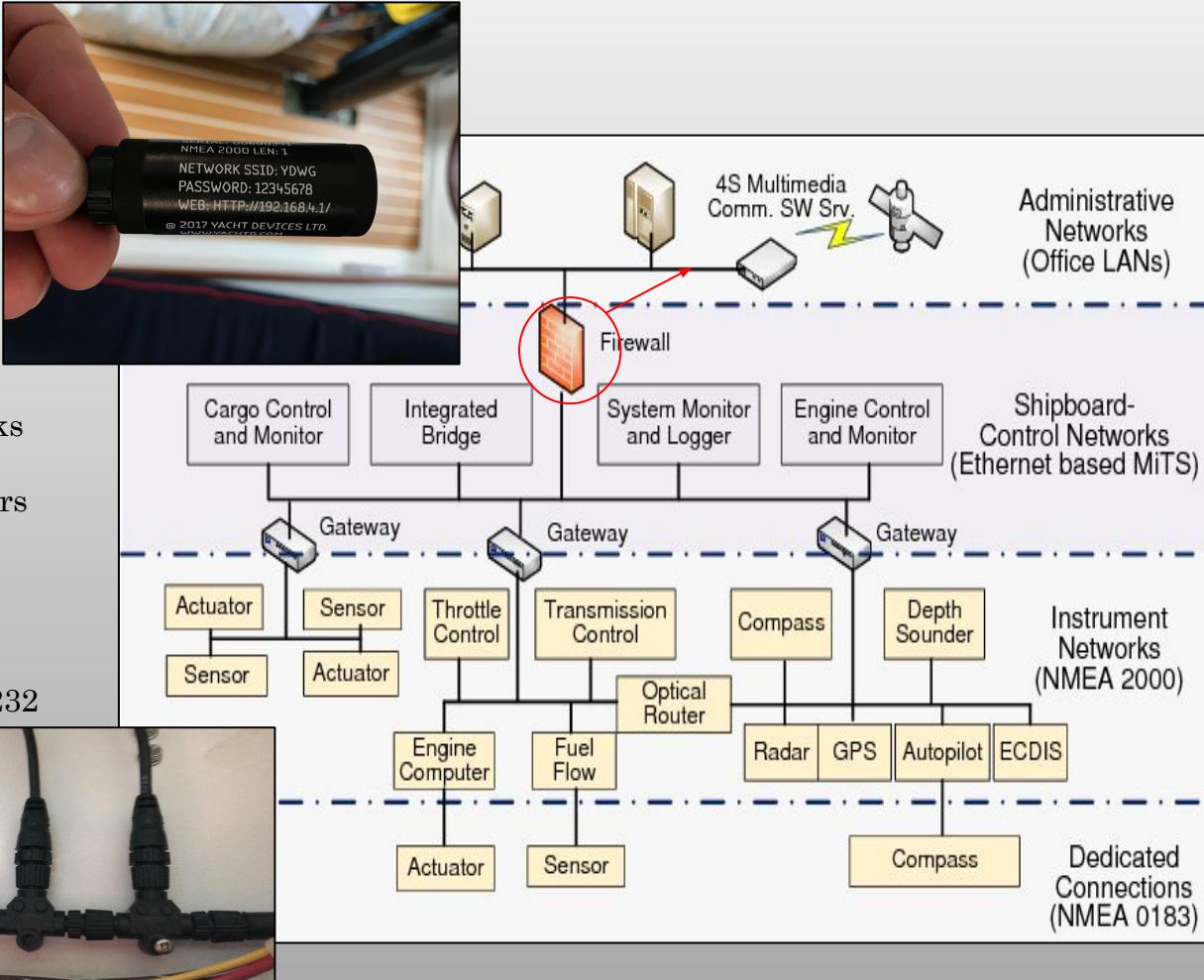
Maritime Protocols

- NMEA 0183
 - Released 1983
 - only one talker supported
 - 4800 baud speed
- NMEA 2000 (N2K)
 - controller area network (CAN) technology
 - power and signal on single cable
 - Bandwidth <1Mbit/s
- Modbus TCP/IP
 - application messaging structure
 - allows for multiple master-slave for monitoring
 - Supports up to 247 devices/slaves
- Synchronous Serial Interface (SSI)
 - based on RS-422 standards
 - standard for industrial application between controller and sensor



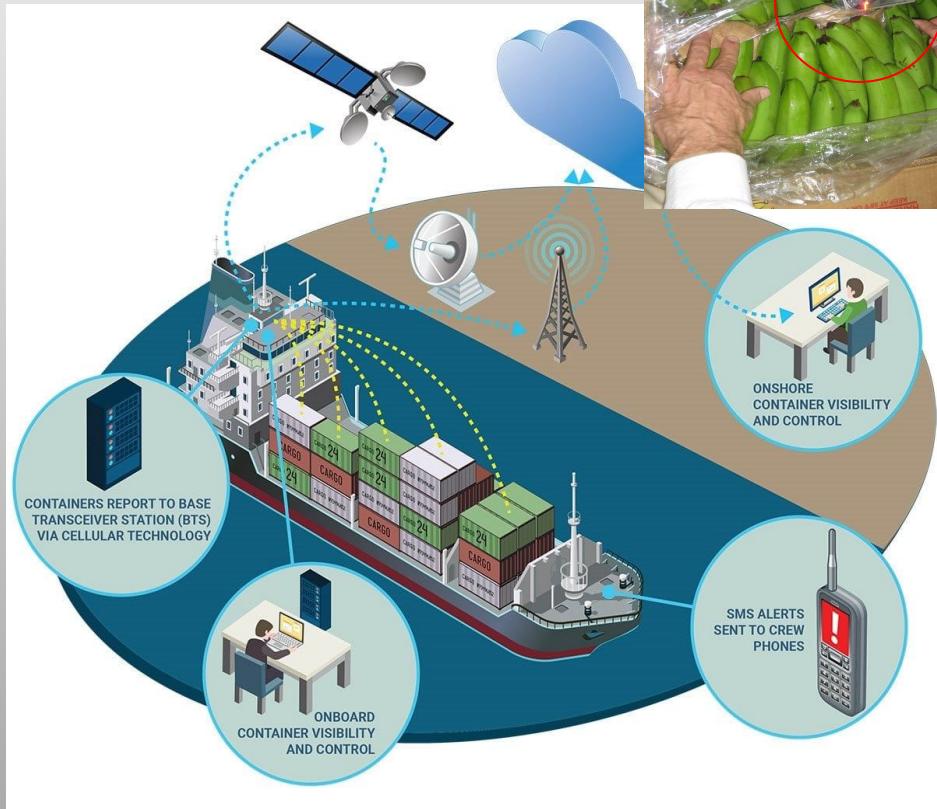
Ship As ICS

- Human Machine Interface (HMI)
 - Windows and linux embedded
 - Networked to shore-side networks
 - Third-parties
 - TCP/IP, Modbus, serial-converters
- Field Devices
 - RTUs
 - N2K CAN, CAN open
- Sensors
 - TCP/IP CAN, SSI, Modbus, RS-232 serial



Smart Cargo

- Wide variety of IoT tech, not standard
- Assorted RFID
 - NFC popular
- Gateways
 - GSM, 3G, 4G data
- Shoreside management software, DB
 - Web GUI, email alerts
- Bosch Banana Monitoring example
 - Wireless ethylene sensors
 - Freight Supervision Unit (FSU)
 - Per container monitoring node
 - Actuates fresh air intake
 - Telematics Unit
 - 3G gateway, real-time
 - Costa Rica to Antwerp Belgium



EDIFACT

- Electronic Data Interchange (EDI)
 - Started with teletype machines in 1960s
 - Conducting business transactions w/ standard message formats
 - multi-country/multi-industry
- Elec-tronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT)
- Ship-Planning Message Development Group (SMDG)



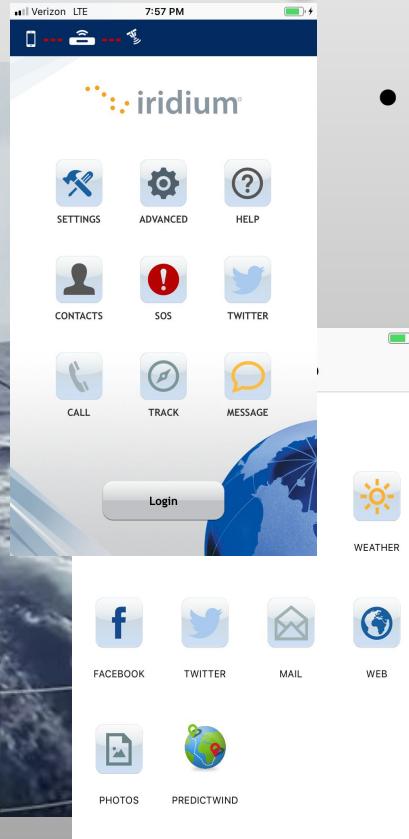
The screenshot shows the homepage of the C-point EDI Web Portal. At the top, there's a header with the C-point logo and a search bar. Below the header is a banner with the text "Smart electronic solutions for transparent logistic flows". Underneath the banner are two search fields: "Choose a target group" and "Choose a service category", followed by a "Search" button. A large red section below the banner contains the text "What is C-point?" and a detailed description of the platform. To the right of this text is a small map of a port area. At the bottom of the red section, the text "Antwerp Port EDI Web Portal" is displayed in green.

- Specific EDIFACT message for shipping
 - load planning
 - special handling instructions
 - perishable or hazardous cargo
- Four current mechanisms for exchange
 - AS1-Email (SMTP/S/MIME)
 - AS2 HTTP and S/MIME
 - AS3 FTP
 - AS4 ebXML

Communications Ship to Shore

Inmarsat fleet broadband: 432kbps

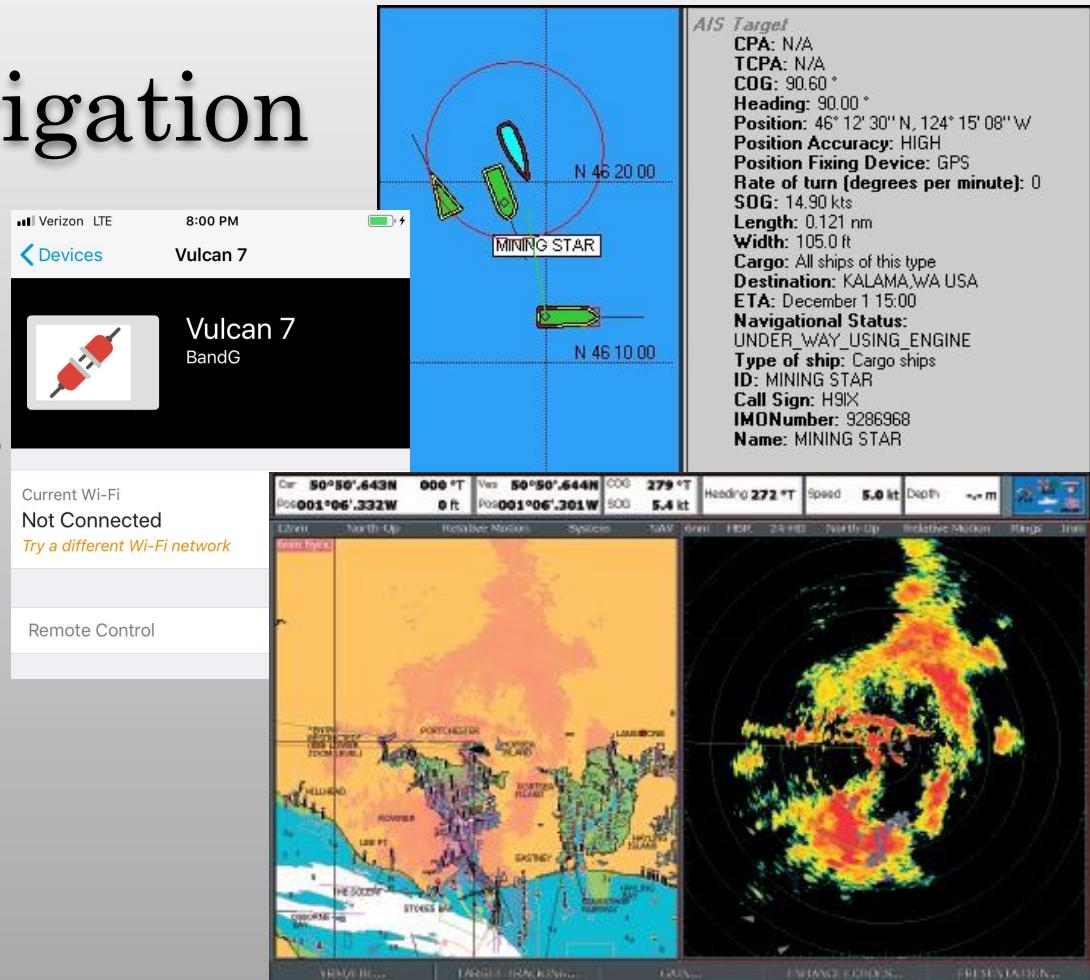
Inmarsat globalXpress: 50Mbps



- HQ Communication with the fleet with ‘always on’ connection
 - Position, conditions
 - Instant access via Video, Audio, Text
 - Internet access
 - Emails
 - Calls
 - Weather
 - Telemedicine
- Remote operation and support of hardware
- Relay Emergency information
 - Emergency Position Indicating Radio Beacons (EPIRBs)
 - Personal Location Beacons (PLBs)
 - Search and Rescue Transponders (SARTs)
 - VHF and Aviation freq emergency radio

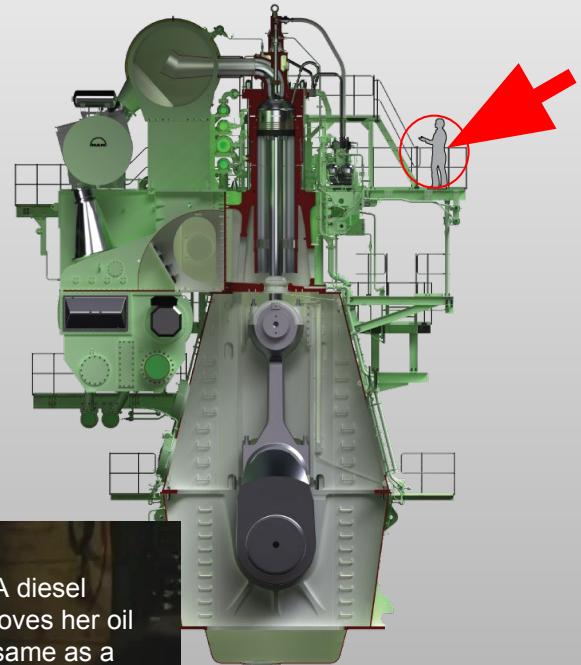
Safety And Navigation

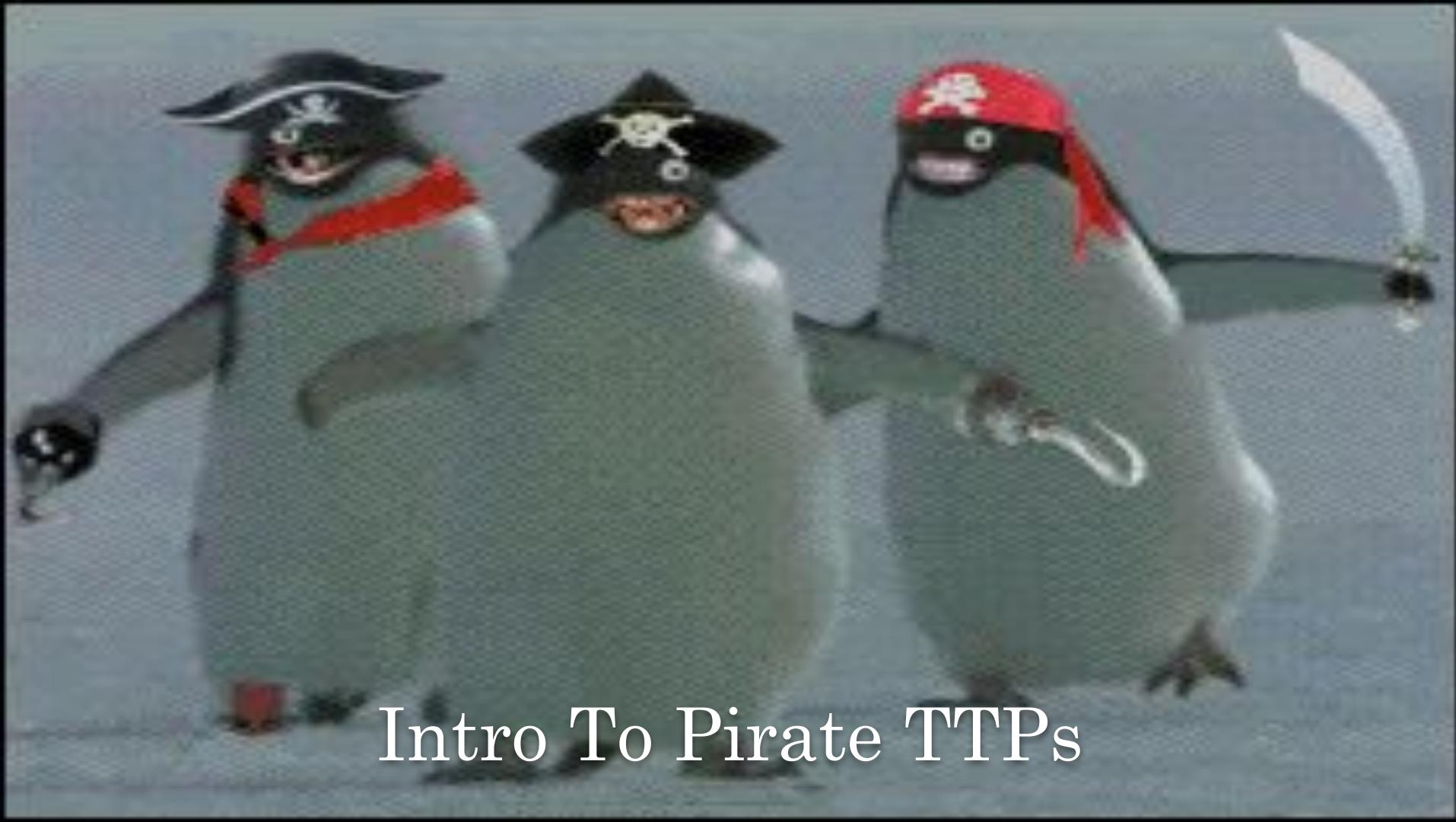
- Global Maritime Distress & Safety (GMDSS)
 - NAVTEX, DSC, EPIRB, SART
 - Vessel Traffic System (VTS)
 - Automated Identification System (AIS)
 - Sat and RF
 - CCTV
 - X-Band radar
 - GNSS
 - GPS (US)
 - GLONASS(Russia)
 - Galileo(EU)
 - Beidou (China)
 - Electronic Chart Display Info System (ECDIS)
 - Updates
 - USB, DVD, network



ICS on Propulsion System

- B&W 12S90ME-C Mark 9.2 (2x2)
 - two-stroke diesel
 - 12 cylinders
 - 98,000 hp at 84 rpm
 - controlled by MAN Engine Control System
- Wartsila-Sulzer RTA96-C Flex
 - two-stroke diesel
 - 14 cylinders
 - 108,920 hp at 102 rpm
 - controlled by Wartsila Engine Control System
- Common Rail Diesel
 - Computerized, no camshaft

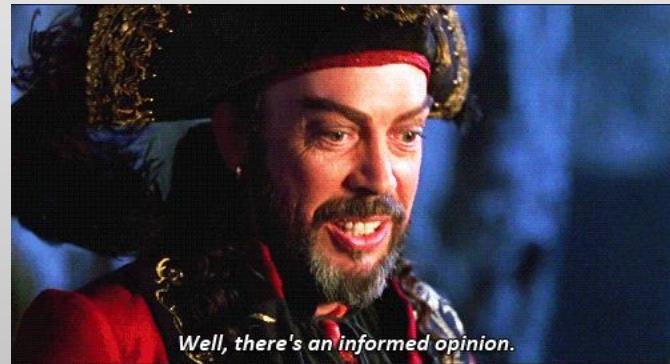




Intro To Pirate TTPs

The Five W's Every Pirate Should Ask

- Who
 - Built the ship
 - Owns, operates and insures the ship
 - Maintains and supplies the ship
 - Handles the cargo
 - Crews the ship
- What
 - Is the ship carrying – is it cargo we'd want
 - Systems are onboard
- When
 - Is the ship scheduled to be at locations



- Where
 - Is the ship now
 - Is the ship headed
 - Any counter-piracy patrols in area
- Why take the risk
 - Is the cargo valuable enough
 - Is there another way to get the loot

Why Risk It ? - The New Era

- Gulf of Aden and Indian Ocean ('08-'12)
 - Ransom payments \$53 million month
 - Insurance premiums \$20k per voyage
 - Private security \$5000-\$10000 per day, per ship
 - Counter-piracy \$450million per year



- Post 2012 standard piracy became less lucrative and more deadly
 - 191 attacks (2017)
 - Lowest in 18 years
- Successful operations today
 - Fast, targeted, intelligence-driven
 - Steal cargo, not ransom
 - Geographically diverse
 - Attack off Peru 0(2015), 11(2017)
 - Leveraging cyber attacks

Pirate OSINT (When And Where)

- Ship tracker websites and Apps
 - Leverage AIS data
 - Identify schedule and destinations
 - Identify shipowner, flag, and shipping line operator
 - Real time location
 - Call signs
- Using this info
 - Identify what domains, websites, or networks to compromise
 - Gain access to EDIFACT
 - Determine possible time and location to intercept
 - Determine risk of being pursued
 - Gain info to aid further reconnaissance

The screenshot shows the SHIPSPOTTING.com website interface. At the top, there's a navigation bar with links for HOME, PHOTOS, VIDEOS, SHIPS, AIS, FORUM, NEWS, SUPPORT, CONTACT, SHIPTRAX, and XML DATA. A search bar is also present.

The main content area is for the ship **ARROW - IMO: 9119414**. It features a large night photograph of the ship at sea. To the right of the photo is a box containing "General Information" about the vessel:

- Current name: ARROW
- IMO: 9119414
- Callsign: 2GFGS
- MMSI: 235096892
- Vessel type: RO-RO CARGO
- Built year: 1998
- Current flag: ISLE OF MAN (UK)
- Home port: DOUGLAS (ISLE OF MAN)

Below this, it says "Photos: 54 photos by 33 photographers" and "Total hits: 26,709".

Further down, there's a section titled "AIS DATA" which provides real-time information:

| AIS Type | Cargo ship |
|-----------------|------------------------|
| Flag | United Kingdom |
| Destination | LERWICK |
| ETA | Sep 24, 07:00 |
| IMO / MMSI | 9119414 / 235096892 |
| Callsign | 2GFGS |
| Length / Beam | 123 / 20 m |
| Current draught | 4.9 m |
| Course / Speed | 299.8° / 0.0 kn |
| Coordinates | 60.1627 N/1.15707 W |
| Last report | Sep 24, 2018 15:28 UTC |

Hey, Friend! (Who)

- Myship.com
 - Browse thousands by ship or crew
 - Easy to create an account
 - Website not secure
- Identify crew from a ship or port
- Obtain information about them
 - Create credible phishing emails
 - Wordlists for usernames, passwords, and security questions
 - Identify possible insiders to assist
 - Social engineering to gain technical info
 - Armed security
- Maltego and SET here we go...

MyShip.com — Mat... x
Not secure | myship.com Like 10K

Find your ship, mates and job!

MyShip.com

Social and career website

Email or Profile no. Password Login

Remember me [Forgot Password / Profile No.?](#)

Join us today »

Nationalities ▶ All 116006 seafarers

Mates 116 006
Seafarers, cadets of all nationalities and ranks

Ships 115 141
Cargo, offshore, cruise, platforms, inland ships

Crewing Agencies 2 348
Your profile is your application

Invitations to work 4 750
Registration for agencies, crew management companies, shipowners [here»](#)


OFFSHORE OLYMPIA
Filipino, Greg 2/Officer


SEYCHELLES PROGRESS
Polish, Marcin 2/Engineer


ARDMORE CENTURION
Italian, Rossella Master Mariner


BOXY LADY
Indonesian, Triahma Chief Officer


NORWEGIAN SUN
American, Dennis Data System Manager


DELPHIN VOYAGER
Romanian, Iovi Purser


NOBLE GLOBETROTTER II
German, Grunenber Chief Officer


MAERSK PENANG
American, Scott R. 2/Officer - DPO


Dutch, Wilson 3/Officer

It's All about the Booty (What)



- Compromising EDIFACT, Smart Cargo
 - Which ship has what containers
 - Which container has what cargo
 - Ensure the containers are located on accessible upper deck
 - Have delivered port
 - Steal pin to sign for it
- Smart Cargo
 - Identify containers quickly
 - On board or at port

Cargo Timeline

- Iranian IRISL (2011)
 - Cargo containers “disappear”
- Australian Customs and Border Protection Service (2012)
 - Criminals monitor customs inspection information
- Antwerp Port (2013)
 - Systems manipulated to smuggle contraband
 - MitM then spoof EDIFACT messages
- World Fuel Services (2014)
 - Bunker fuel ordered, stolen at sea, and charged to USG accounts
 - Spoofed EDIFACT messages
- Verizon report (2016)
 - Pirates identify which cargo to steal
 - Insecure file upload, executable directory, webshell
- Cargotec Navis WebAccess (2016)
 - CVE-2016-5817 SQL Injection POCs



The How

- Network Access
 - Satcoms
 - Crew PED
 - Corporate networks shoreside
- Physical Access
 - Avoid detection
 - VTS, CCTV, X-band, AIS
 - Visual horizon problem
 - How to board
 - GPS, ECDIS, Propulsion
 - Bare steerage versus dead steerage
- CONOPs summary
 - CONOP 1 via personal electronic device PED hack
 - CONOP 2 via a third-party vendor network for a shipping company



Network Access

- Find out satellite gear vendor
 - Shodan
- KVH Commbox example
 - HTTP header not (s)
 - Known vulnerabilities
 - Map location
- Since 2017
 - A lot fewer results
- Other options?
 - Owner or operator network
 - Third party vendor network
 - Crew PED and accounts

The screenshot shows the Shodan search results for the IP address 168.227.251.44. At the top, there's a map of Rio de Janeiro, Brazil, with a red marker indicating the location. Below the map, the IP address is listed as 168.227.251.44. The page includes sections for "Ports" (showing port 80), "Services" (listing 80, tcp, and http), and "Vulnerabilities" (listing CVE-2014-0117). To the right, a screenshot of a web browser showing the KVH Commbox Applications Suite login page is visible.

Secure | https://www.shodan.io/host/168.227.251.44

SHODAN

Explore Downloads Reports Developer Pricing Enterprise Access Contact Us My Account Upgrade

168.227.251.44 168-227-251-44.7lan.net View Raw Data

Country: Brazil
Organization: Intesys Informatica LTDA
ISP: Intesys Informatica LTDA
Last Update: 2018-09-10T07:54:33.422773
Hostnames: 168-227-251-44.7lan.net
ASN: AS264898

Ports

Services

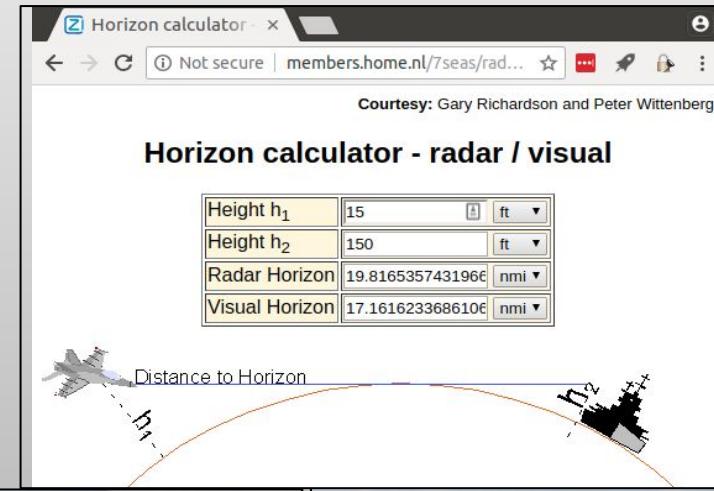
Vulnerabilities

Apache httpd Version: 2.4.6

CVE-2014-0117 The mod_proxy module in the Apache HTTP

Physical Access-The Approach

- Approaching the objective
 - Visual horizon and radar horizon
- Compromise VTS
 - For radar serial converter best bet
 - e.g. Moxa Nport Serial converter
 - CVE-2016-9361 (Cisco Talos)
 - auxiliary/admin/scada/moxa_credential_recovery
 - CCTV
 - AIS
 - Balduzzi / Trend Micro (2014)
 - Fake warning messages too!
 - Pen Test Partners (2016)



Physical Access-Boarding

- Vessel Boarding Search and Seizure (VBSS)
 - Non-compliant vessel (NCV) very difficult
 - Need to control course and speed
 - Need to lock-out crew access
 - Retreat to safe rooms w/ redundant systems
 - Navigation, propulsion, Fire suppression
- Controlling course
 - GPS
 - University of Texas yacht “hijack” (2013)
 - ECDIS and Nav computer
 - NCC group (2015), PTP (2016)
 - Can also inject via Navtex or AIS compromise
- Controlling Speed
 - Propulsion proof of concepts?
 - Want bare steerageway not dead steerage



CONOPS Summary Diagram I

OSINT:



Access:



Cargo:



Stealth:



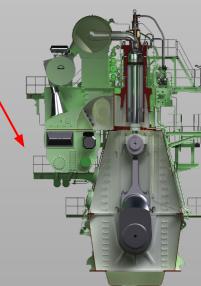
Course:



Success



Speed:



CONOPS Summary Diagram II

OSINT:



Access:



Cargo:



Stealth:



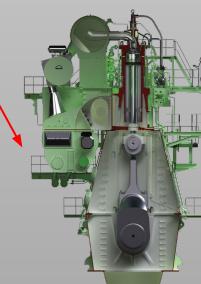
Course:



Success



Speed:





Our Research: Project Gunsway

Auto-Maskin Marine Pro Control Systems



- Marine Pro product line
 - Vessel management software
 - Provides integration and HMI for whole ship
 - Field devices
 - Gateway/Converters
 - Emergency shutdown units
 - RTUs
- Equipment used
 - RP 210E Remote Panel
 - DCU 210 E Engine Control Unit
 - Marine Pro Observer App (Android)

Why We Chose Auto-Maskin

- Cost, availability
 - We were able to order w/out a ship
 - Didn't ask questions
 - Other Marine Pro equipment
 - Just nicer touch screens
- Purpose built for maritime use
 - Not general purpose ICS
 - Established vendor for propulsion
- Widely used in maritime, offshore oil & gas
- Major supplier to marine diesel OEMs
 - Yanmar, Caterpillar, Cummins, Scania
 - Equipment is “rebranded”



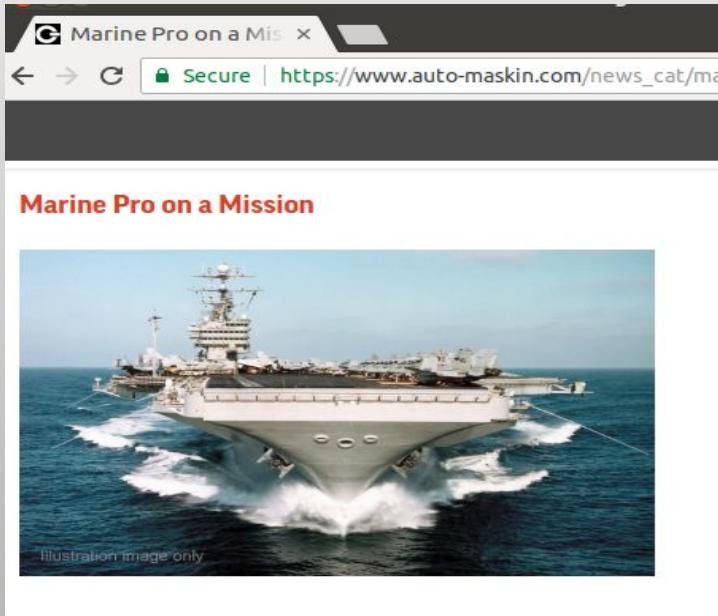
NOAA Research Vessels



Example:

- NOAA vessel(s)
 - Equipped with Cummins diesel engines
 - Rebranded Auto-Maskin units
 - Likely affected
- Coordinated with NOAA officials
 - Currently assessing and mitigating
- Notified maritime sector via MPS-ISAO
- Supply chain complexity
 - Can make it hard to identify risk

On a Mission...for the Lulz



| New Carriers 2017-2018 | | |
|---------------------------------------|----------|------------|
| Name | Country | Aircraft |
| HMS Queen Elizabeth & Prince of Wales | UK | Fixed Wing |
| PLAN 001A and 002 | China | Fixed Wing |
| INS Vikramaditya & Vikrant | India | Fixed WIng |
| Trieste | Italy | Rotor |
| ROKS Marado | S. Korea | Rotor |

“With a hint to one of the world leaders, NAME REDACTED (Auto-Maskin Manager) finishes off with; ‘we don’t have the biggest button – but it works, every time.’”

Skadoosh



© 2015 DWA LLC. All Rights Reserved

Our Lab Setup and Methodology



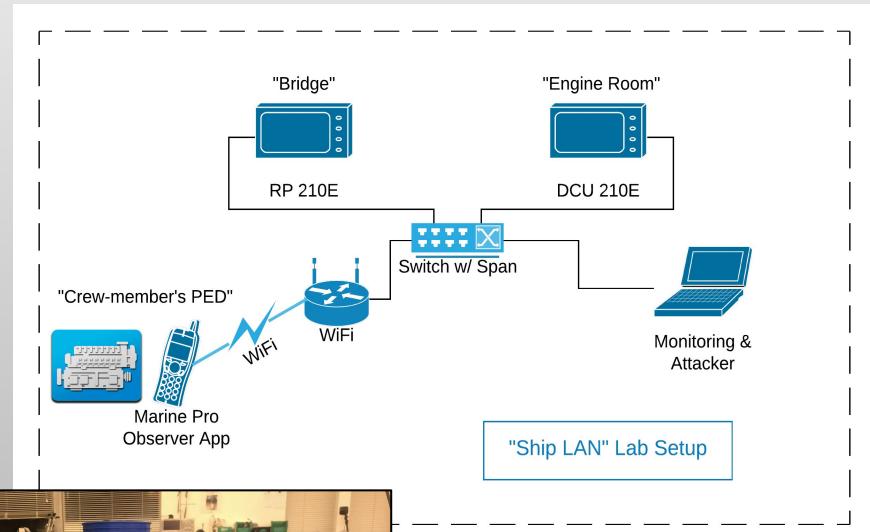
+



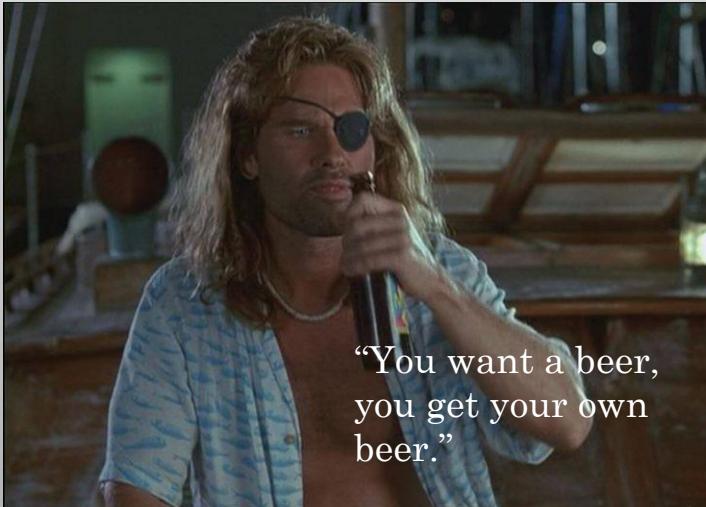
Our Lab Setup

Tools on Laptop:

- Wireshark v2.6
- Nmap v7.70
- Arp-Scan v1.9 with libpcap version 1.8.1
- Skipfish 2.10b
- Binary Ninja disassembler v1.1.1038
- Dex2Jar decompiler (reader-1.15, translator-0.0.9.15, ir-1.12)
- Hydra v8.6
- Netcatv1.10-41.1



Methodology



“You want a beer,
you get your own
beer.”

- Basic, Basic, Basic
- Focused on effects
 - Not enumeration
- Open source research
 - RTFM
- Network scans
- Static Code Analysis
- Brute-Force
- Web scans, then manual
- Packet fuzzing (Modbus data)
- Develop, test POC

Initial Findings

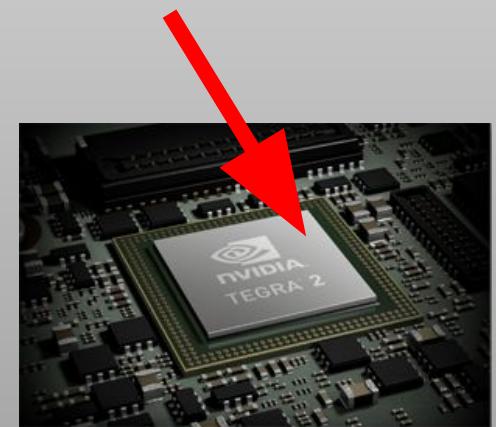
| Vulnerability | Description | Affected Products |
|---------------|----------------------------|--------------------|
| CVE-2018-5399 | Hardcoded credentials | RP 210E, DCU 210E* |
| CVE-2018-5400 | Origin Validation Error | RP 210E, DCU 210E* |
| CVE-2018-5401 | Cleartext Modbus | RP 210E, DCU 210E* |
| CVE-2018-5402 | Cleartext HTTP credentials | RP 210E, DCU 210E* |



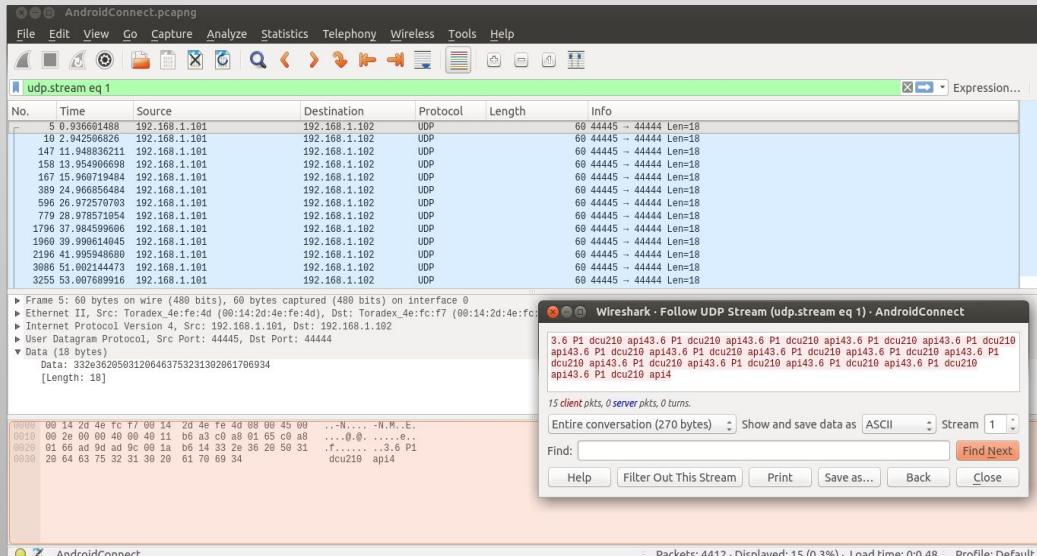
*Affects firmware
v3.7 and earlier

What's Inside?

- Toradex Colibri T20
 - System on a module
- NVIDIA TEGRA 2
 - ARMv7 Processor rev 0 (v7l)
- Angstrom v2017.11 embedded Linux
- Busy Box tools
- DropBear SSH 2012.55
- Trolltech aka Qt
 - Touchscreen framework
- Binaries for Auto-Maskin
 - Firmware v3.7
 - firmware 3.8, 09/18



Details--Android & Modbus



- Observed Activity
 - DCU to RP connection
 - Android to DCU connection
 - Engine Over-Speed Test
 - Various DCU command from RP
- Custom hand-shake
 - “protocol”48:65:6c:6c:6f:20:57:6f:72:6c:64, “Hello World”
 - UDP Ports 44444-44446 to broadcast
 - Response from device to UDP port
 - Model and firmware version
 - Modbus Communications
 - TCP port (502)

Details--Android & Modbus

- No authentication
- No encryption
- Replay attacks and spoofed messages work, even from Android MariTrojan



Recommended Fix:

- Implement Modbus TCP Security Protocol (v21, 2018)
 - port 802 TCP
 - Encryption and authentication

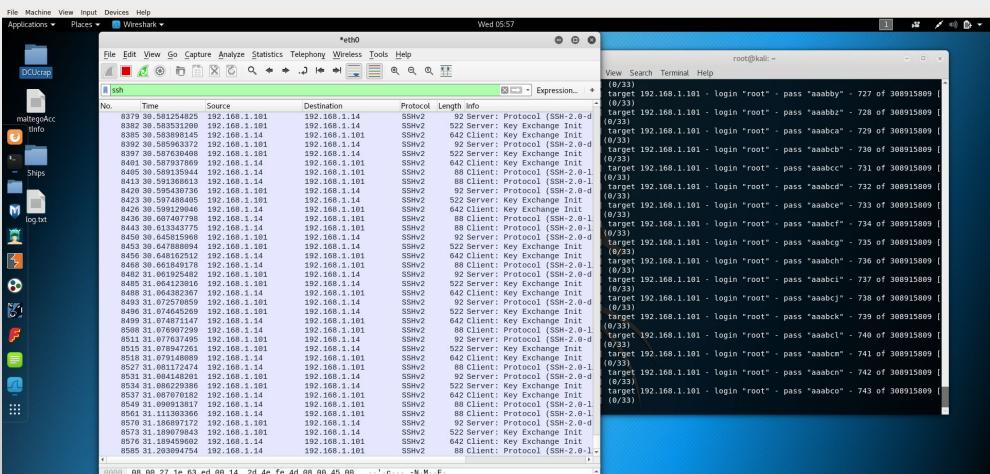
The image consists of three main parts. On the left, a mobile device screen shows a fake Android interface with icons for Calculator, Calendar, Camera, Chrome, Clock, Contacts, Drive, Duo, Files, Gmail, Google, Maps, MariTrojan (which is highlighted in red), Messages, Phone, Photos, Play Movies, Play Music, Play Store, and Settings. On the right, a web browser window displays a login form for 'auto MASKIN' with fields for 'IP Address' and 'Port'. Below the browser is a product listing for the 'DCU 210E Engine Controller' on a website. The listing includes a product image, a brief description, and links for 'Product Description', 'Specifications', 'Documentation', and 'Accessories'. It also lists 'DCU 410E Engine Controller' and 'DCU 210E Engine Controller'.

Details--SSH

- Undocumented Dropbear 2012.55 SSH
 - Hard-coded password for root
 - Six char, all lowercase
 - "amroot"
 - Password only authentication
 - Host-key w/ fingerprint
 - RSA:43:b5:7c:43:4b:62:bf:49:58:9b:57:13:04:34:98:7c
 - So you can Punk.sh or Shodan.io

Recommended Fix:

- Remove or properly document the server



```
File Edit View Search Terminal Help
root@kali:~# sudo ssh root@192.168.1.101
root@192.168.1.101's password:
root@marine-pro:~# whoami
root
root@marine-pro:~# ls
root@marine-pro:~# uname -a
Linux marine-pro 3.1.10-hmq537-3-p1b #1 SMP PREEMPT Tue Apr 28 08:50:05 CEST 2011
5 armv7l GNU/Linux
root@marine-pro:~#
```



Details--Web Server

- Started with Skipfish, manual attempts
 - No verified SQL injection or XSS, yet
 - Accidentally “DOS” DCU
 - Triggered change in voltage setting causing alarms/shutdown
- HTTP unencrypted authentication
- Pre-authentication file upload
 - User “wallpaper” files
- Authenticated upload
 - Config files and firmware update
- Weak authentication
 - Four digit numerical pin (1234 default)
 - Prompts with correct username
 - Failed login provides five digit pin
 - Email them and they give you pin
 - Found the math in system binary

The screenshot shows a Kali Linux desktop environment. In the top right, a Firefox window displays a scan result from Skipfish, showing a connection to 192.168.1.101. Below it, another Firefox window shows a login page for 'DCU - Engine #1' with the URL http://192.168.1.101. The page includes fields for 'User Name' (set to 'root') and 'Password' (set to '****'). A 'Cancel' and 'OK' button are visible. In the bottom left, a terminal window runs the command 'cat check_for_upgrade.sh'. The script checks for an upgrade file, extracts its integrity, and performs an upgrade. It also removes upgrade artifacts. On the right, a GDB debugger is open, showing assembly code for the 'encrypt_pin_code' function and a stack dump.

```
root@marine-pro:/opt/bin# cat check_for_upgrade.sh
#!/bin/bash

# Check for upgrade file
if [ -e /opt/init/upgrade/firmware.tar.gz ]; then
    # Check integrity of archive here...
    gunzip -t /opt/init/upgrade/firmware.tar.gz

# Check result code of archive integrity
if [ $? -eq 0 ]; then
    # Good archive. Extract start upgrade script
    cd / && tar zxvf /opt/init/upgrade/firmware.tar.gz
    opt/init/upgrade/start_upgrade.sh > /dev/null 2>&1
    # Do the actual upgrade
    cd /opt && init/upgrade/start_upgrade.sh
fi

# Remove upgrade stuff
rm -rf /opt/init/upgrade/*
```

```
# system_server -- Binary Ninja
File Edit View Tools Help
File Edt View Tools Help
system_server (ELF Graph) <:
rp_init_queue
strtok
rpc_get_request_param_
rp_lookup_errcode
rp_init_timer
puts
_log_debug
rpc_register_function_
rp_create_queue
rpc_get_request_strin_
rp_get_integer
fork
udev_monitor_new_from_
lseek
rpc_create_server_ex
rpc_print_parameters
rp_execute_process
reset_millis_count
strcmp
rpc_add_character_out_
pipe
rpc_create_asynch_req_
strcmp
exit
log_error
__errno_location
sprintf
rp_get_string
fputs
main

 encrypt_pin_code:
    movw    r3, #0x270f
    push   {r4, r5, r6, r7, lr}
    cmp    r0, r3
    sub    sp, #0x44 {var_58}
    mov    r4, r0
    bhi   #0xd136

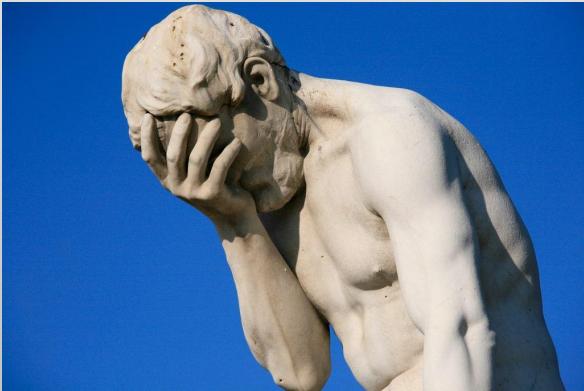
c] {data_d148} {0x1223c, "invalid pin (%d)"}
rsb    r2, r0, #0x18600
ldr    r1, [pc, #0xc0] {data_d148}
adds   r2, #0x9f
mov    r0, sp {var_58}
blx   #sprintf
ldrb  r5, [sp] {var_58}
movw  r6, #0x2710
ldrb  r7, [sp, #2] {var_56}
mov    r0, #0x308
```

Looking Forward

- Examine related Products
 - WiFi router accessory
 - Marine View HMI software
 - Rebranded devices
 - Gateway / Serial Converter
- Finish POC work
 - Webserver firmware upload
 - Engine overspeed POC
- More bug-hunting
 - Debugging using Toradex dev board
 - Further static code analysis
- Other propulsion controllers
 - Wirtsila, B&W, and Kongsberg



Conclusions



Don't worry, it's on an
“isolated network”

- Auto-Maskin research
 - Supply-chain of diesel OEMs
 - Caterpillar, Cummins, Scandia, Yanmar
 - Could affect unaware “consumer” end-users
 - Reminiscent of recent IoT botnets
 - Bricker bot
 - Difference is public safety
- Maritime ICS Security
 - Can't rely solely on “Isolated network”
 - Simple vulnerabilities, serious consequences
 - Low-hanging fruit
 - Have to start somewhere
 - Already have the answers

You Are The Cavalry

I Am The Cavalry

To find out more and get involved:

<https://www.iamthecavalry.org/>

@iamthecavalry

Project Gunsway

For more information:

<https://blog.gunsway.org/>

Email: info@gunsway.org

@projectgunsway



- Be a hero like Sloth
- Join Gunsway, ARRGH!

We'd Like To Thank

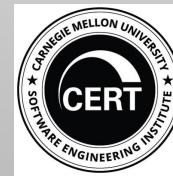
Follow these awesome people on Twitter

- Stephan Gerling @obiwan666
- Nate Guagenti @neu5ron
- Adam Swan @acalarch
- John Palmisano @palmisjt
- Beau Woods @beauwoods
- The Cavalry @iamthecavalry
- Dan Klinedinst @dklinedinst
- Alex Caceres @_hyp3ri0n

Special thanks to @HackingDave and DerbyCon Staff

Thanks to these great organizations

- Maritime and Port Security ISAO (MPS-ISAO)
- Nova Labs
- CERT/CC
- VAE, Inc
- Norway CERT, ICS-CERT, US-CERT (Thanks Majed!)



Questions?



References

<https://www.reuters.com/article/us-iran-sanctions-shipping/irans-top-cargo-shipping-line-says-sanctions-damage-mounting-idUSBRE89L10X20121022>

<https://www.brookings.edu/wp-content/uploads/2016/06/03-cyber-port-security-kramek.pdf>

<https://www.bbc.com/news/world-europe-24539417>

https://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xq.pdf

<https://www.kaspersky.com/blog/maritime-cyber-security/8796/>

<https://www.k2intelligence.com/en/insights/thought-leadership/increased-cyber-attacks-on-shipping-and-logistics-highlight-the-need-for-preventative-strategy>

<https://www.pentestpartners.com/security-blog/maersk-wasnt-hacked/>

<http://www.reuters.com/article/2012/10/22/us-iran-sanctions-shipping-idUSBRE89L10X20121022>

<https://www.pentestpartners.com/security-blog/cosco-incident-phishing-frenzy-and-exploding-goods/>

<https://blog.bosch-si.com/industry40/container-4-0-smart-transport-high-seas/>

<https://www.intel.com/content/www/us/en/logistics-and-supply-chain/connected-logistics-platform/overview.html>

<https://www.pentestpartners.com/security-blog/sinking-container-ships-by-hacking-load-plan-software/>

<https://www.unece.org/cefact/edifact/welcome.html>

<http://www.smdg.org/documents/ship-planning/>

<http://www.smdg.org/assets/assets/005-UN-EDIFACT-Container-Messages.pdf>

<https://tools.ietf.org/html/rfc3335>

<http://www.ietf.org/rfc/rfc4823.txt>

<https://ediacademy.com/blog/cusper-edifact/>

<https://www.c-point.be/nl/>

<https://securityaffairs.co/wordpress/50564/security/navis-webaccess-sqlinj.html>

<https://www.businessinsider.com/worlds-newest-aircraft-carriers-2018-3#hms-queen-elizabeth-4>

https://www.auto-maskin.com/news_cat/marine-pro-on-a-mission

<https://oceanexplorer.noaa.gov/technology/vessels/ronbrown/ronbrown.html>

<https://www.omaio.noaa.gov/learn/marine-operations/ships/ronald-h-brown/about-noaa-ship-ronald-h-brown>

<http://www.angstrom-distribution.org/>

<https://shipandbunker.com/news/world/340232-court-backs-world-fuel-services-following-17-million-bunker-theft>

<https://www.nxtport.eu/>

