

Pirates of the North Sea

John-André Bjørkhaug

Maritime Hacking Village @ DEFCON #33

whoami

- John-André Bjørkhaug
- Norwegian
- Principal Penetration Tester @ Netsecurity
- Electronics engineer (TelCo & Wireless systems)
- Penetration tester for 17 years
- Picked my first lock when I was 10 years old



(Also seen in pictures in this presentation:

Egil Aspevik, long time friend and colleague)

Netsecurity

About

- Zero experience with maritime industry when we started.
  - Inland geeks, afraid of water…
  - Where the h*** is Bow and aft ??
- Large number of shipping companies in many countries. 2017 - 2025
  - Norway, Sweden, Finland, Estonia, Spain, Germany, UK, Ireland, Holland, Poland, Croatia, Congo, USA ++
- Cruise, freight, LNG, Ferries etc.
- Remote, onboard, dry dock

Why Hacking/Pentest Ships

- Increasing focus on attacking the shipping industry
- Requirements from industry -> IMO*
- Before
  - Low bandwidth / delay - InmarSat, VSAT etc.
- Now:
  - **Everything** is connected with high speed - 4G/5G + Starlink!

```
Pinging example.com [93.184.216.34] with 32 bytes of data:

Reply from 93.184.216.34: bytes=32 time=560ms TTL=54
Request timed out.
Reply from 93.184.216.34: bytes=32 time=732ms TTL=54
Reply from 93.184.216.34: bytes=32 time=648ms TTL=54

Ping statistics for 93.184.216.34:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 560ms, Maximum = 732ms, Average = 646ms
```

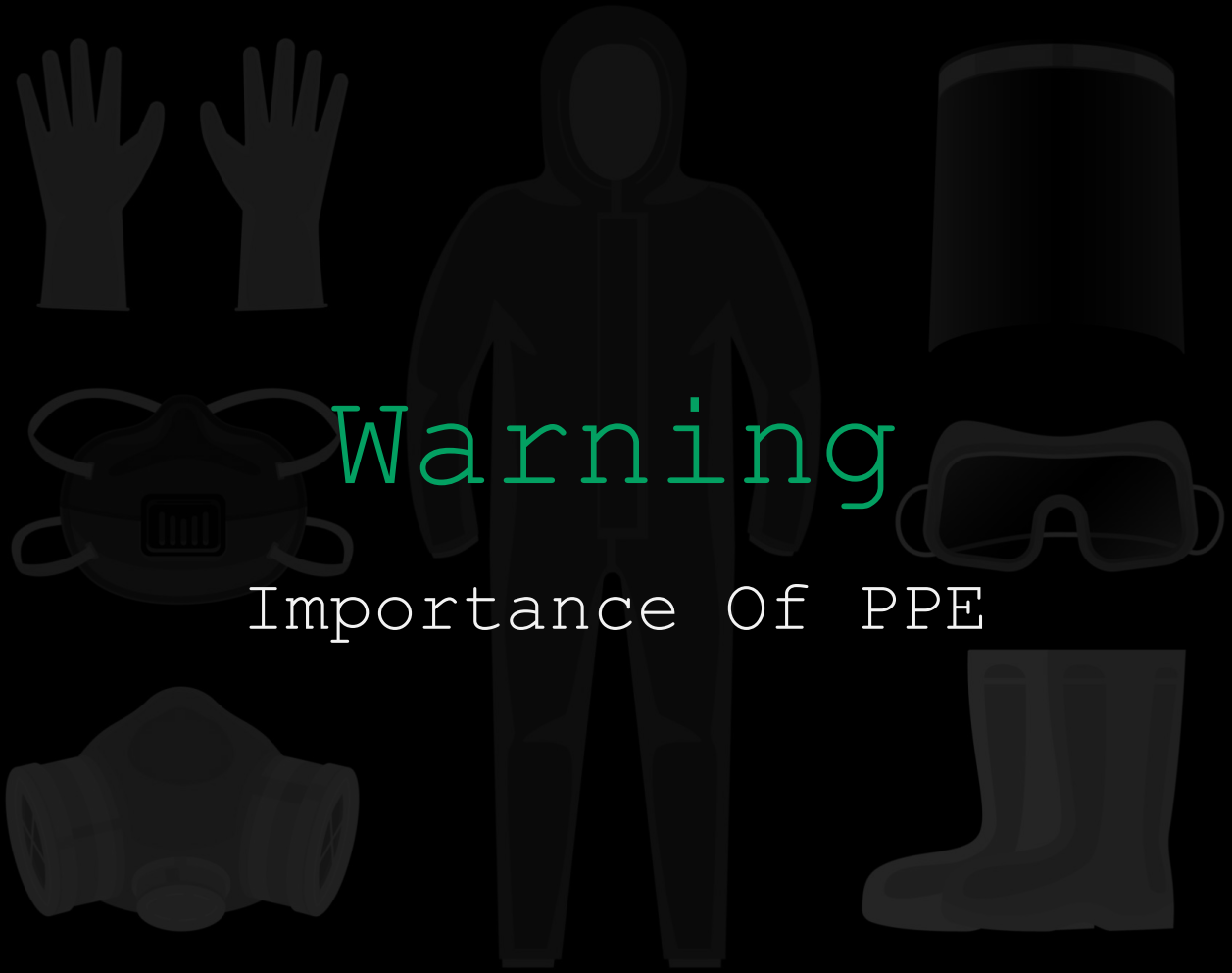
* International Maritime Organization

Why Shipping Industry Should Take Cyber Security More Seriously



- HUGE values
  - LNG tanker: 300-400M USD
  - Cruise ship: 400M-1.5B USD!
- OT systems can be old on new ship
  - Win XP in OT on ship from 2024
- Lifes on stake !!!
- Vast number of integrated systems equals gigantic attack vector for an adversary

Copyright © Microsoft Corporation



Warning

Importance Of PPE

Always Wear The Correct PPE

- Personal Protective Equipment (PPE)
- Safety gloves
- Hard hat / helmet
- High-visibility clothing
- Safety shoes (steel/composite toe)
- Additional gear as required (harness)
- On vessels with explosive cargo: only use Ex-certified (ATEX/IECEx) equipment





Onboard Cruise Ships: Scope

- Part 1: Go onboard undercover as regular guests or workers
  - Network sockets & WiFi
  - Physical security
  - Social Engineering
  - Main objective: Get access to critical areas and systems
- Part 2: Together with crew
  - Crew areas
  - Bridge systems
  - Engine room
  - Etc.
  - Kind of like an audit

Onboard Cruise Ships: Typical Findings

- Large number of live networks sockets
  - Mostly office networks
- Access Point network
  - Guest-, Office- or Management- network or all (trunk) :)
- Domain admin in short time
  - responder, password reuse, cleartext passwords in docx files, weak passwords, ADCS ++
- Missing patches
- No segmentation ship-to-ship and ship-to-shore
- Unauthorized WiFi networks
- Dual/Triple/Quadruple-homed network cards


Covert Hacking On Cruise Ships…


Metasploit






1500 €


EXIT


Rabbids
lywood




HIKOKI
18V

Warstory 1

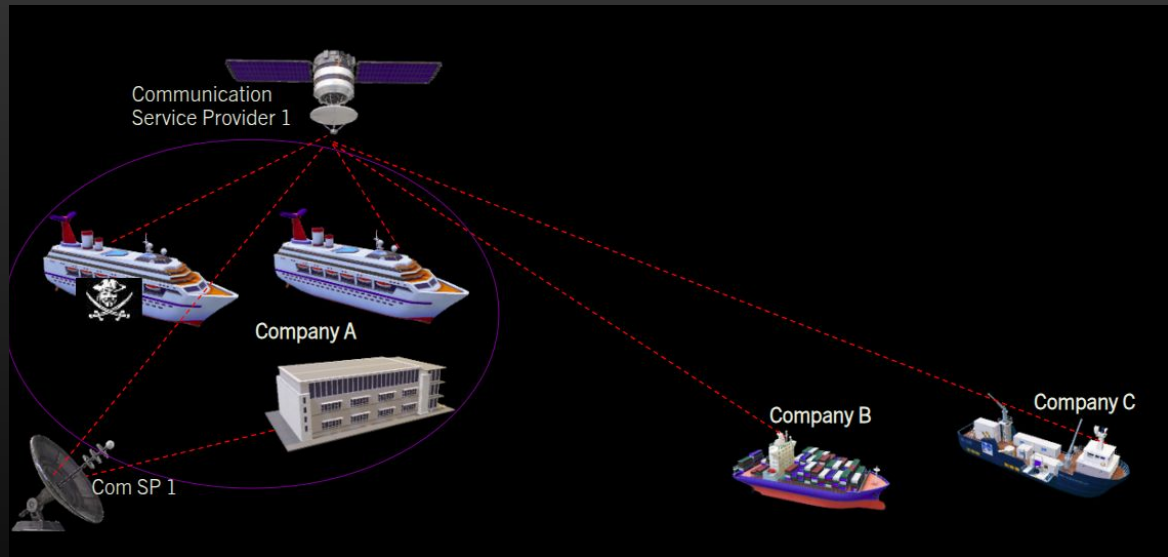





FSB
FSB
FSB

Example from Cruise Ship: Satcom And WiFi Provider

- AP network = Service Provider management network!
- No segmentation between customers all over the world
- Default password on network equipment all over
- Ship in “our” company => oil rig in a totally different company!



Example From Remote Internal Testing (LNG)

- Assumed breach of office computer
- Office test, DA in short time
- ESXi with password from Electricians desktop
- ESXi have server which controls ballast tanks
- We stopped…



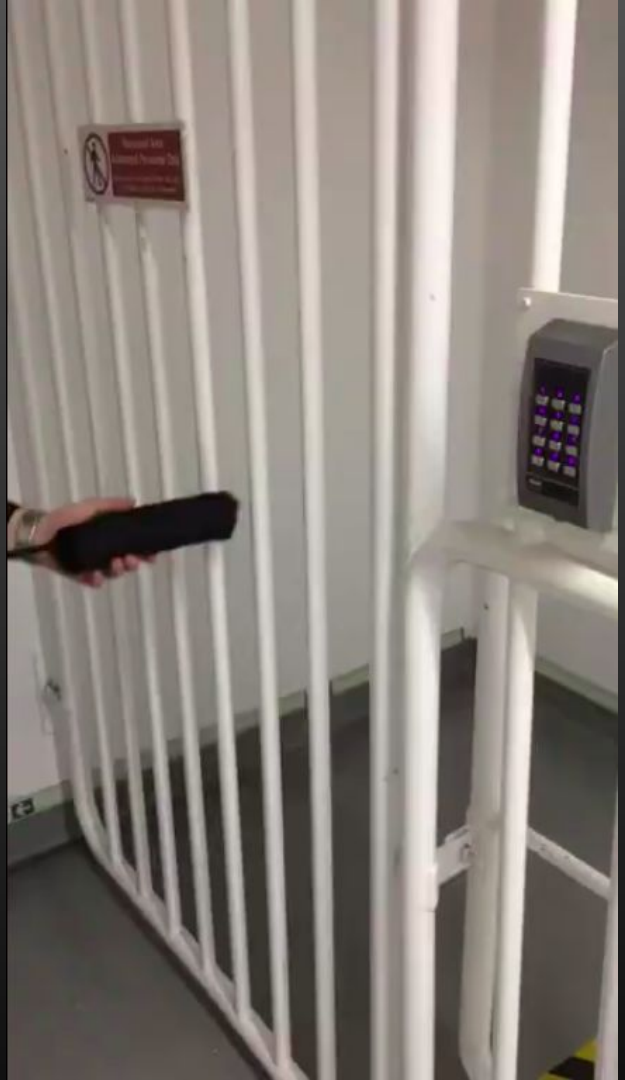

Physical!






estricted Area,
ised Personnel Only
sed Presence Within This Area
itutes a Breach of Security













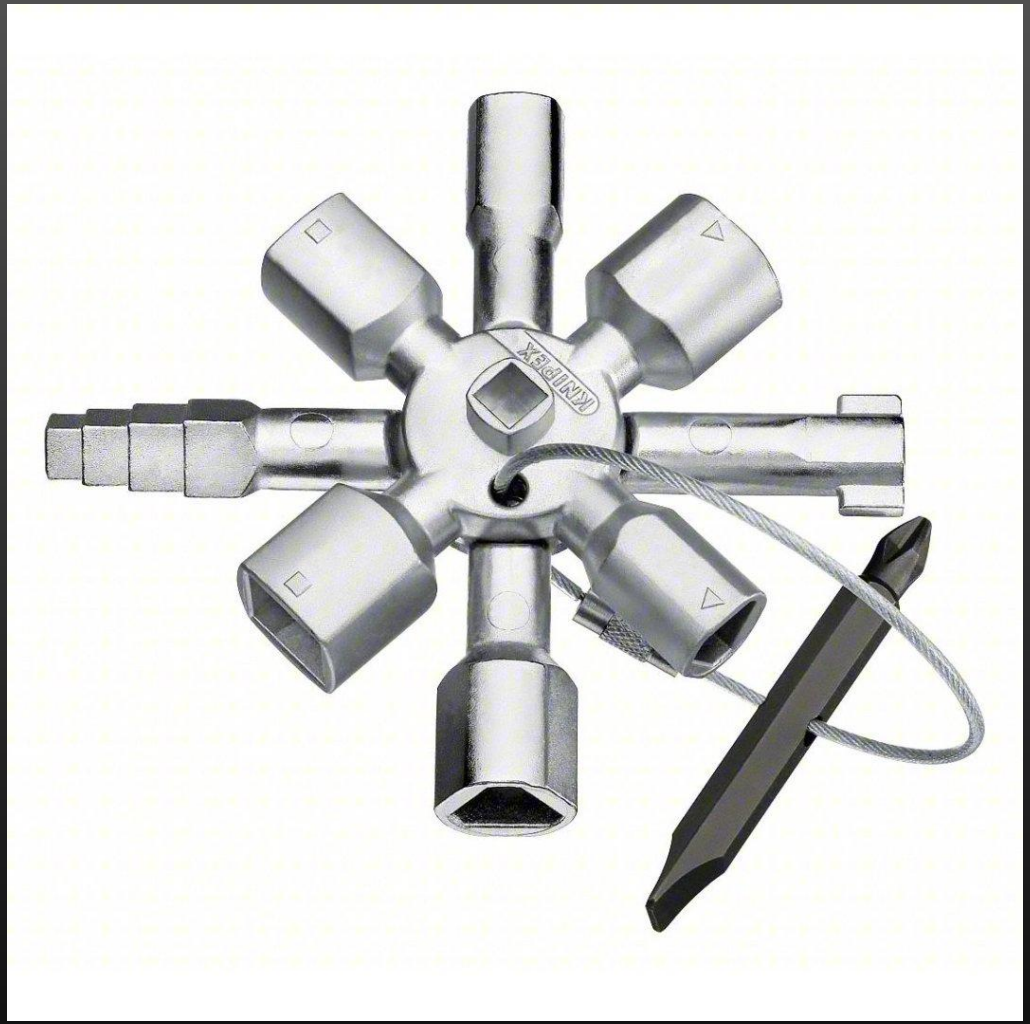











KNIPEX


In dry dock

Scope

- Network segmentation
  - Especially towards OT/Navigation etc.
  - Is air gapped systems really air gapped…
- Rogue WiFi networks
- (Spoofing/Jamming of communication/navigation)

Air Gapped Is Not Really Air Gapped

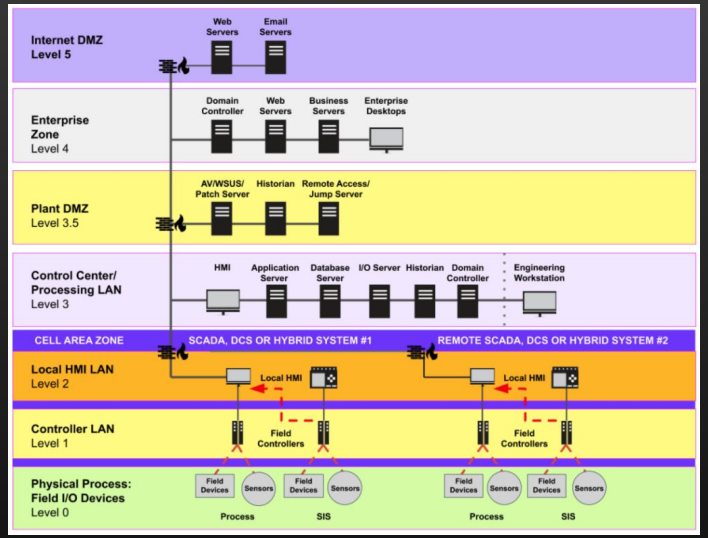
Example:

Office, OT, Navigation. Everything share same router…



Examples On Missing Network Segmentation

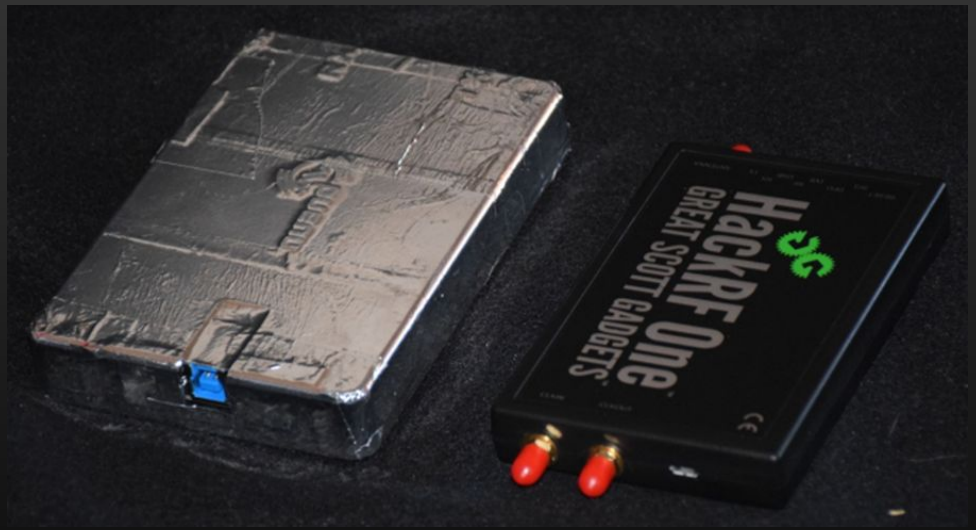
- Office <-> Navigation
- Office <-> Management network
  - Network equipment
  - Communication equipment
  - iDRAC/iLO/ ++
- VDR connected to crew WiFi…




Radio Wavez

Taking Down Navigation

- Jamming and spoofing navigation
  - Software Defined Radio (HackRF & BladeRF)
  - Collaboration with the Government/Military
  - In Dry dock!!!

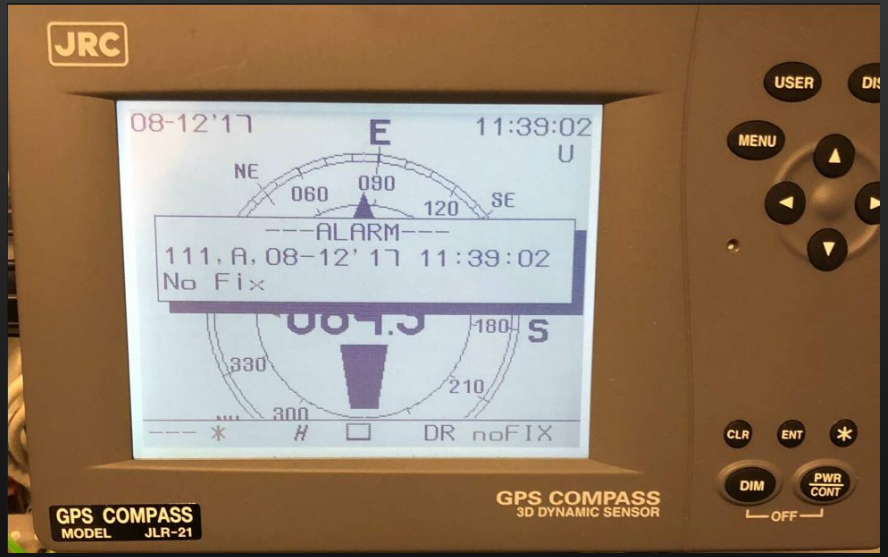


GPS Jamming



GPS Jamming

All screens on bridge went black when GPS was lost…





AIS Spoofing

- AIS (Automatic Identification System)
  - No authentication
  - No integrity check
  - Open medium
- https://github.com/trendmicro/ais



AIS Spoofing

- Jamming -> Invisible ships
- Spoofing -> Ghostship
- Emergency messages => M.O.B = Sirenes



Top 5 Findings In Testing On Board Ships

1. Network segmentation issues
   - It is so convenient to reach everything from everywhere
2. Default or weak passwords
   - As most OT systems..
3. Non-hardened and outdated Operating Systems
   - “It is working, do not touch!!”
4. Non-hardened Network equipment
   - Apparently hard to set up correct, missing competence…
5. Weak configuration in communication solutions
   - Old and proprietary protocols

The identification and remediation of these vulnerabilities will seriously reduce the risk for APT/malicious activity on board ships.

…and A Few More

Physical security

- Unlocked doors
- Weak locking mechanisms
- Stupid designs

Service Providers

- Missing segmentation between customers
- Do YOU trust you service providers?



John-André Bjørkhaug

john@netsecurity.no

john.bjorkhaug@gmail.com

linkedin.com/in/bjorkhaug

Questions?

Netsecurity