(ETHICAL) PIRATES OF THE NORTH SEA

JOHN-ANDRÉ BJØRKHAUG

HACKING #15

ABOUT ME

- John-André Bjørkhaug
- Principal Ethical Hacker @ NTT Ltd.
- Wireless systems and telco engineer
- Penetration tester for 11 years +
- GWAPT, GCFA. CPT, CEPT, CREA, CEH , x-CCNP Sec

WHAT WE DO

- Applications
- Infrastructure
- Physical security
- Humans (social engineering)
- OT/ICS/SCADA/PCDA

- Alarms
- IoT
- Smart houses
- Embedded system
- SHIPS!

RED TEAM

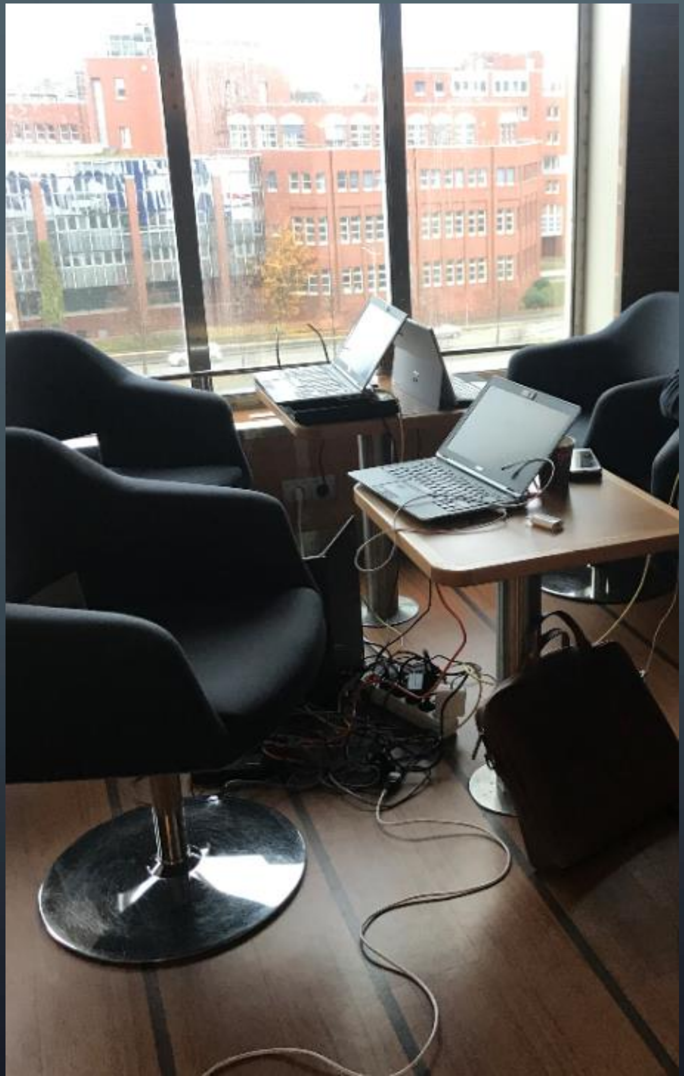
ABOUT SHIP HACKING

- How:
  - Learning by doing.
- Where:
  - Norway, Sweden, Germany, UK, Ireland, Netherlands, Belgium, Somewhere outside Africa
- When:
  - 2017 =>

REMOTE

- The boring one…
- Oil tanker!
- NUC w/Kali dropbox
- VPN via 4G modem (aka iPhone)
- Worked surprisingly good
- The usual …
  - Domain admin in 7 minutes..
  - Password = Username on all users incl Domain Admin
- ESX with all servers and network segments incl. cargo and ballast systems…

ONBOARD TESTING



SCOPE

- Cruiseships
- Part 1: Go onboard undercover as regular guests
  - Network sockets & WiFi
    - Get Domain Admin
  - Physical security
  - !!! Access to critical areas and systems !!!
- Part 2: Together with crew
  - Crew areas
  - Bridge systems
  - Engine room
  - Etc.
- Part 3: Dining at the Captains table

FINDINGS [1]

- A large number of live networks sockets
  - Mostly office networks
    - As usual, domain admin in short time
      - Responder
      - Weak creds !!!
      - Missing patches
    - No segmentation ship-to-ship and ship-to-shore
      - One ship to rule them all

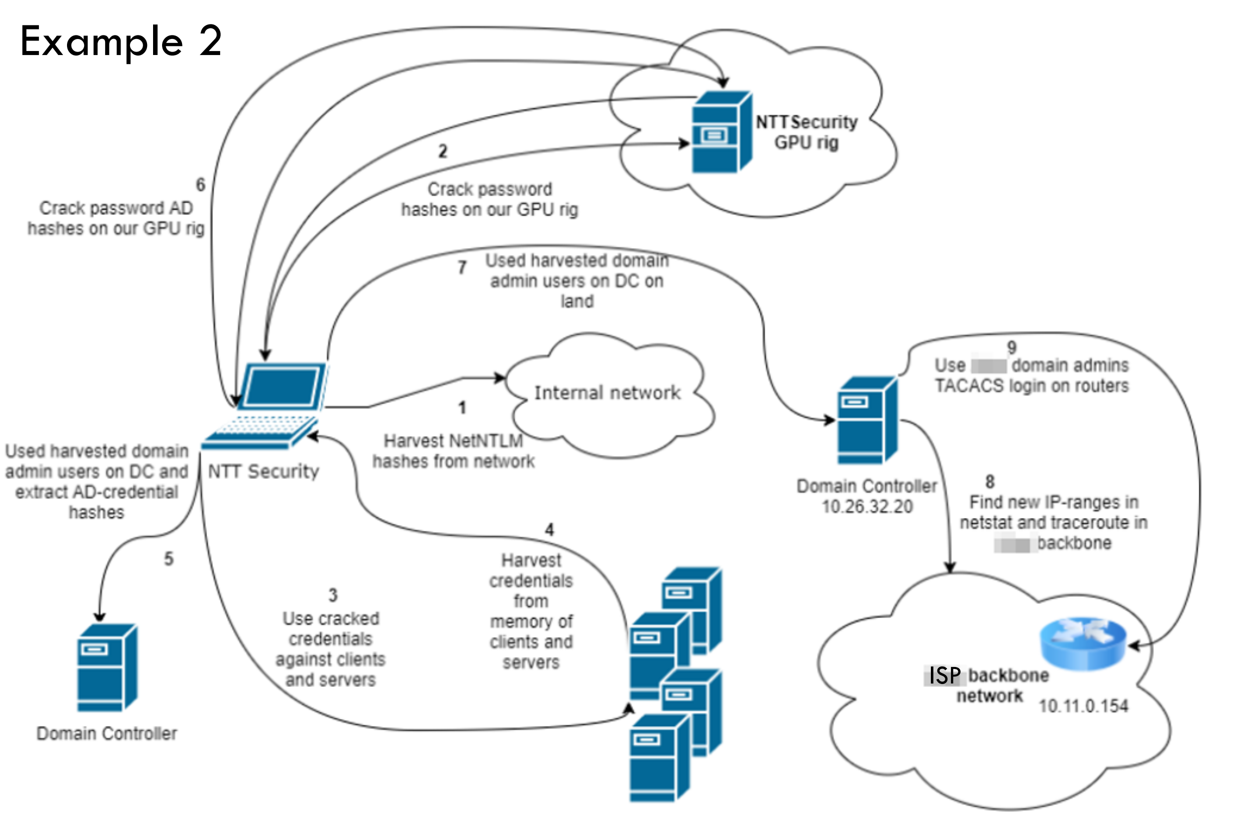
FINDINGS [2]

- Guest WiFi
  - No segmentation between clients
    - Corp equipment connected to guest WiFi …
      - Responder => Hashes
  - Shared FW/router with corp and critical networks
    - Default password ….
    - Shutdown = Black ship!

FINDINGS [3]

- Service providers!
- Example 1:
  - Satcom and WiFi provider
  - AP network = SP 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 2



NTTSecurity GPU rig

6 Crack password AD hashes on our GPU rig

2 Crack password hashes on our GPU rig

7 Used harvested domain admin users on DC on land

Internal network

1 Harvest NetNTLM hashes from network

NTT Security

Used harvested domain admin users on DC and extract AD-credential hashes

5

Domain Controller

3 Use cracked credentials against clients and servers

4 Harvest credentials from memory of clients and servers

Domain Controller 10.26.32.20

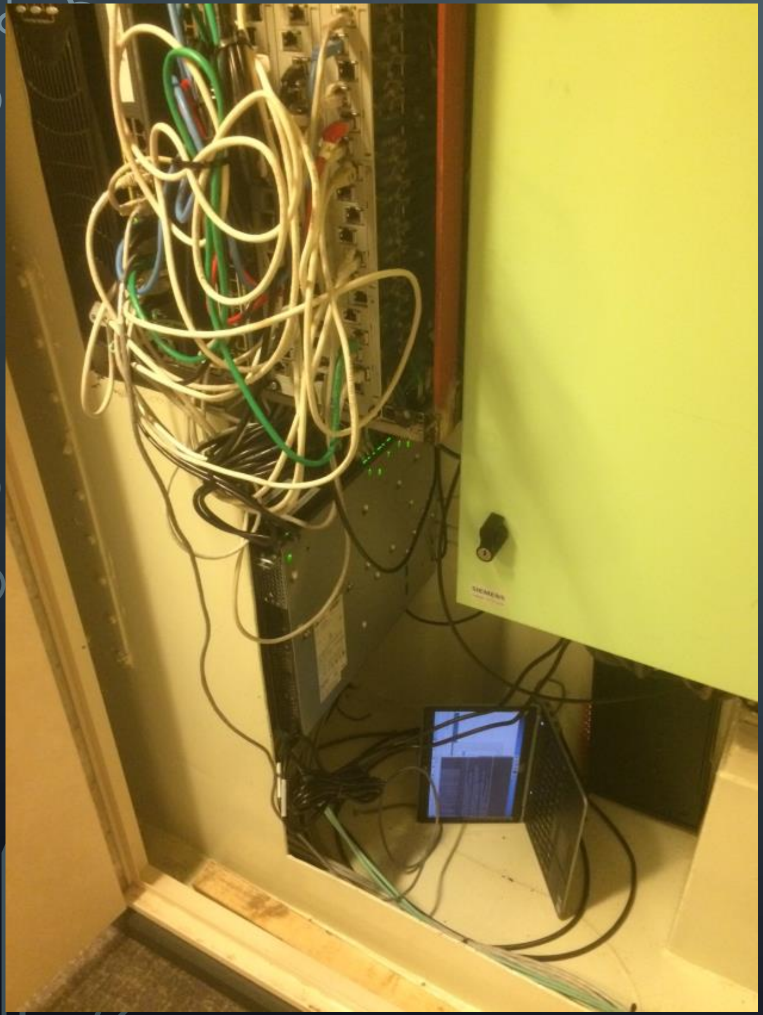
9 Use [redacted] domain admins TACACS login on routers

8 Find new IP-ranges in netstat and traceroute in [redacted] backbone

ISP backbone network

10.11.0.154

PHYSICAL SECURITY



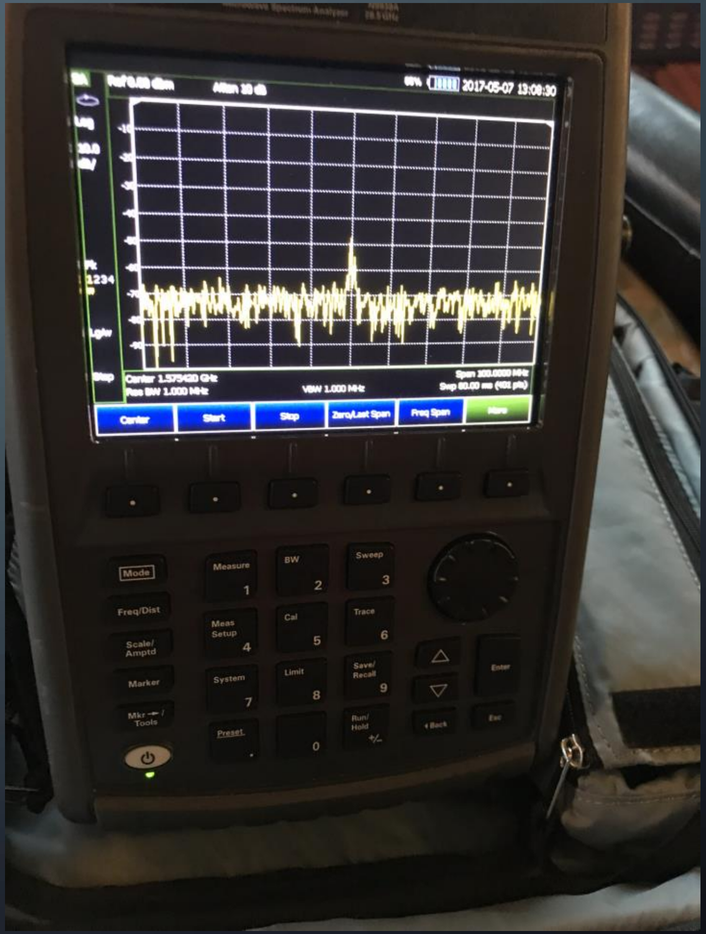
PHYSICAL SECURITY

PHYSICAL SECURITY

TAKING DOWN NAVIGATION

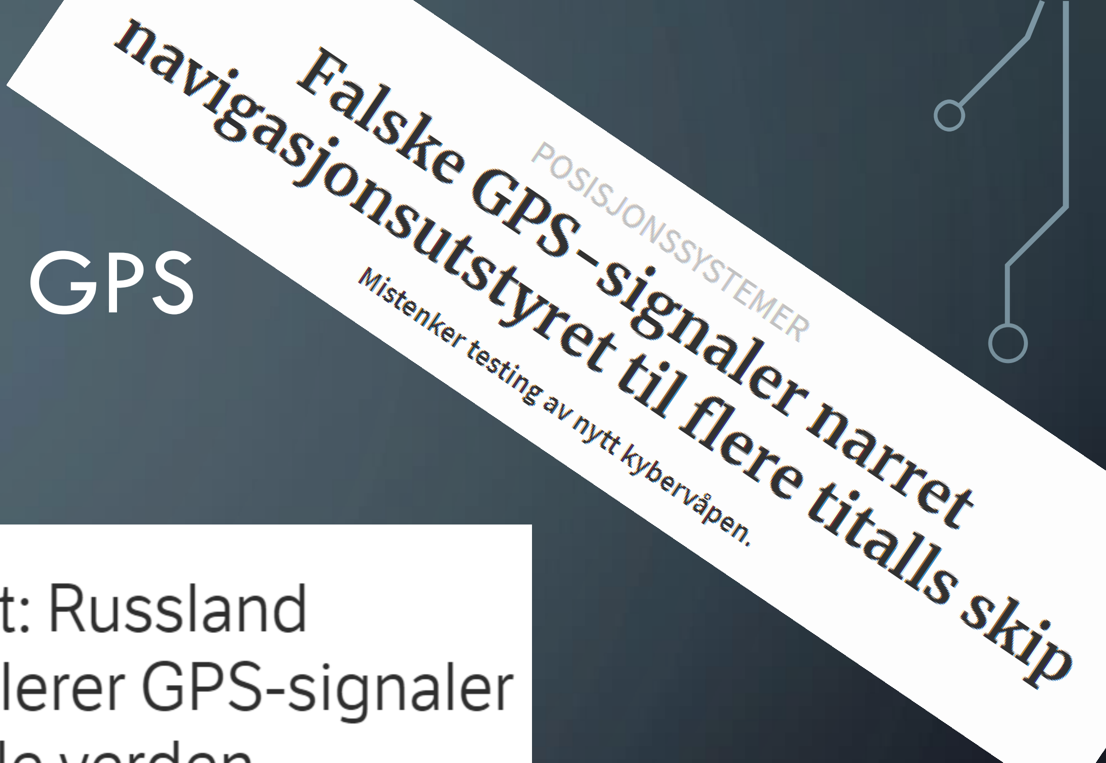
- Jamming and spoofing navigation
  - Software Defined Radio (HackRF & BladeRF)
  - Collaboration with the Goverment
  - In Dry dock!!!

TAKING DOWN NAVIGATION: GPS



TAKING DOWN NAVIGATION: GPS

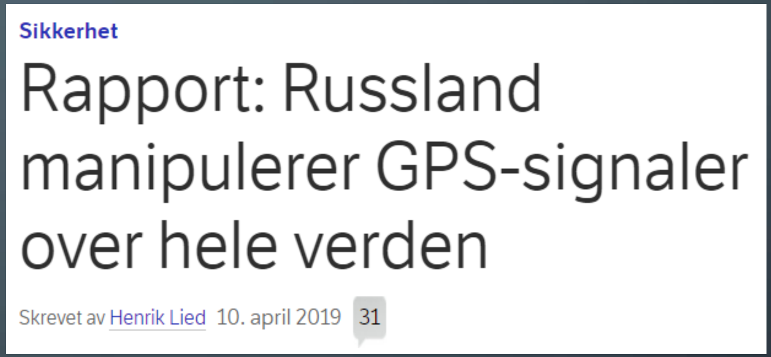
- Jamming
  - Bridge
- Spoofing
  - Not fake news …



POSISJONSSYSTEMER

Falske GPS-signaler narret navigasjonsutstyret til flere titalls skip

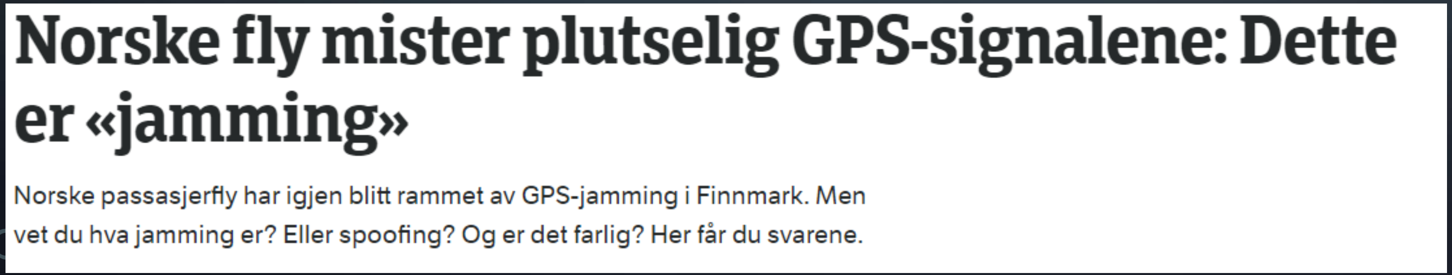
Mistenker testing av nytt kybervåpen.



Sikkerhet

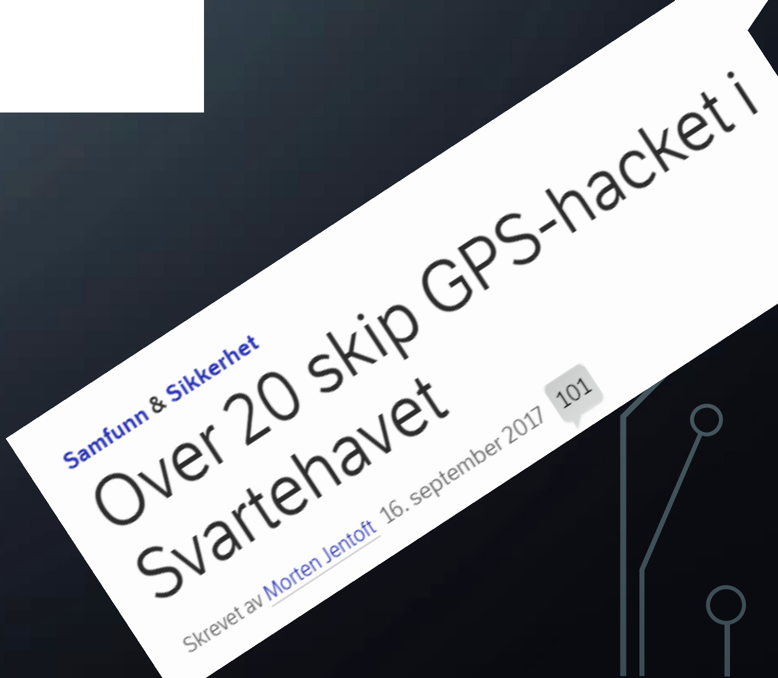
Rapport: Russland manipulerer GPS-signaler over hele verden

Skrevet av Henrik Lied 10. april 2019 31



Norske fly mister plutselig GPS-signalene: Dette er «jamming»

Norske passasjerfly har igjen blitt rammet av GPS-jamming i Finnmark. Men vet du hva jamming er? Eller spoofing? Og er det farlig? Her får du svarene.



Samfunn & Sikkerhet

Over 20 skip GPS-hacket i Svartehavet

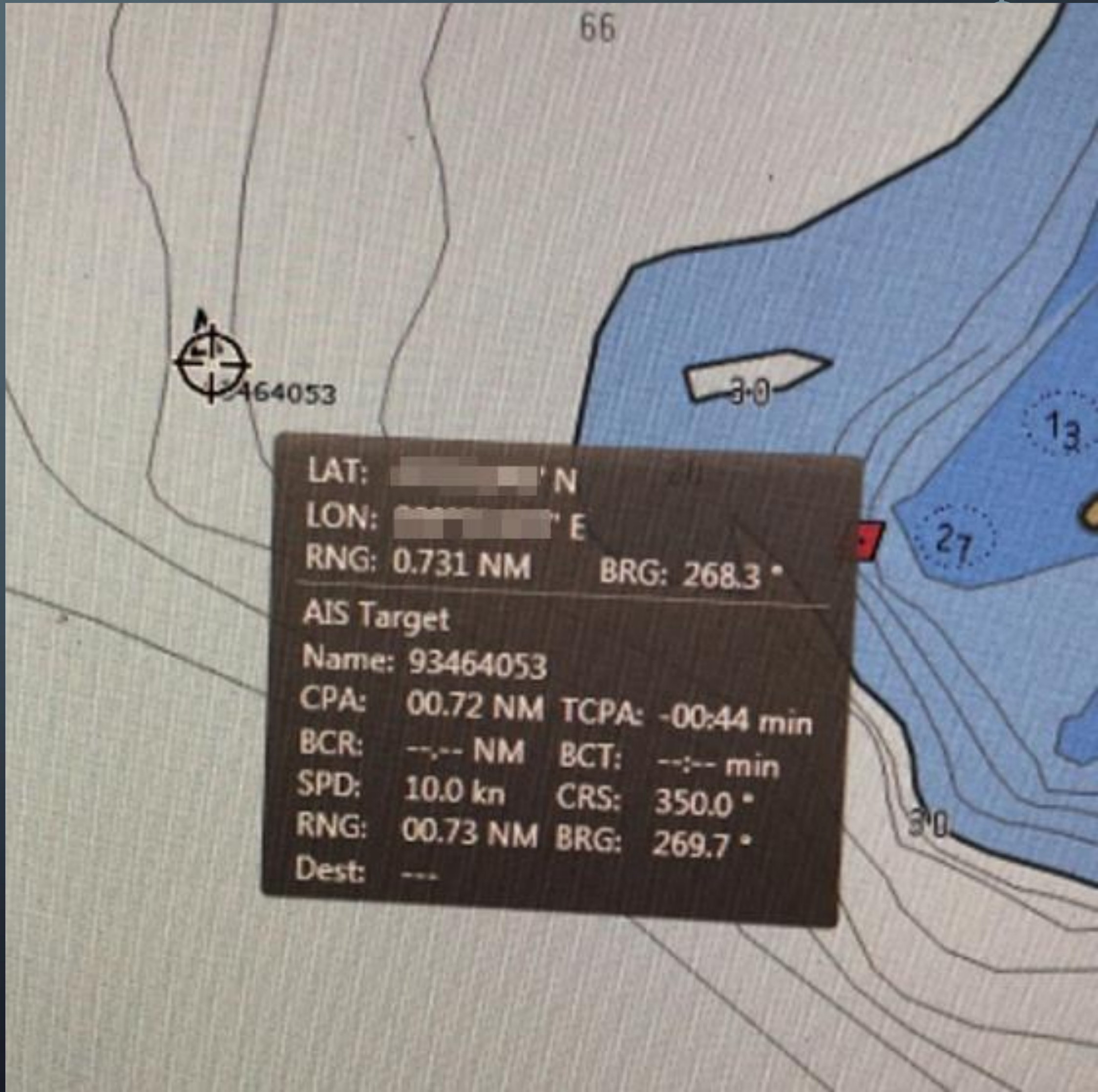
Skrevet av Morten Jentoft 16. september 2017 101

TAKING DOWN NAVIGATION: AIS

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

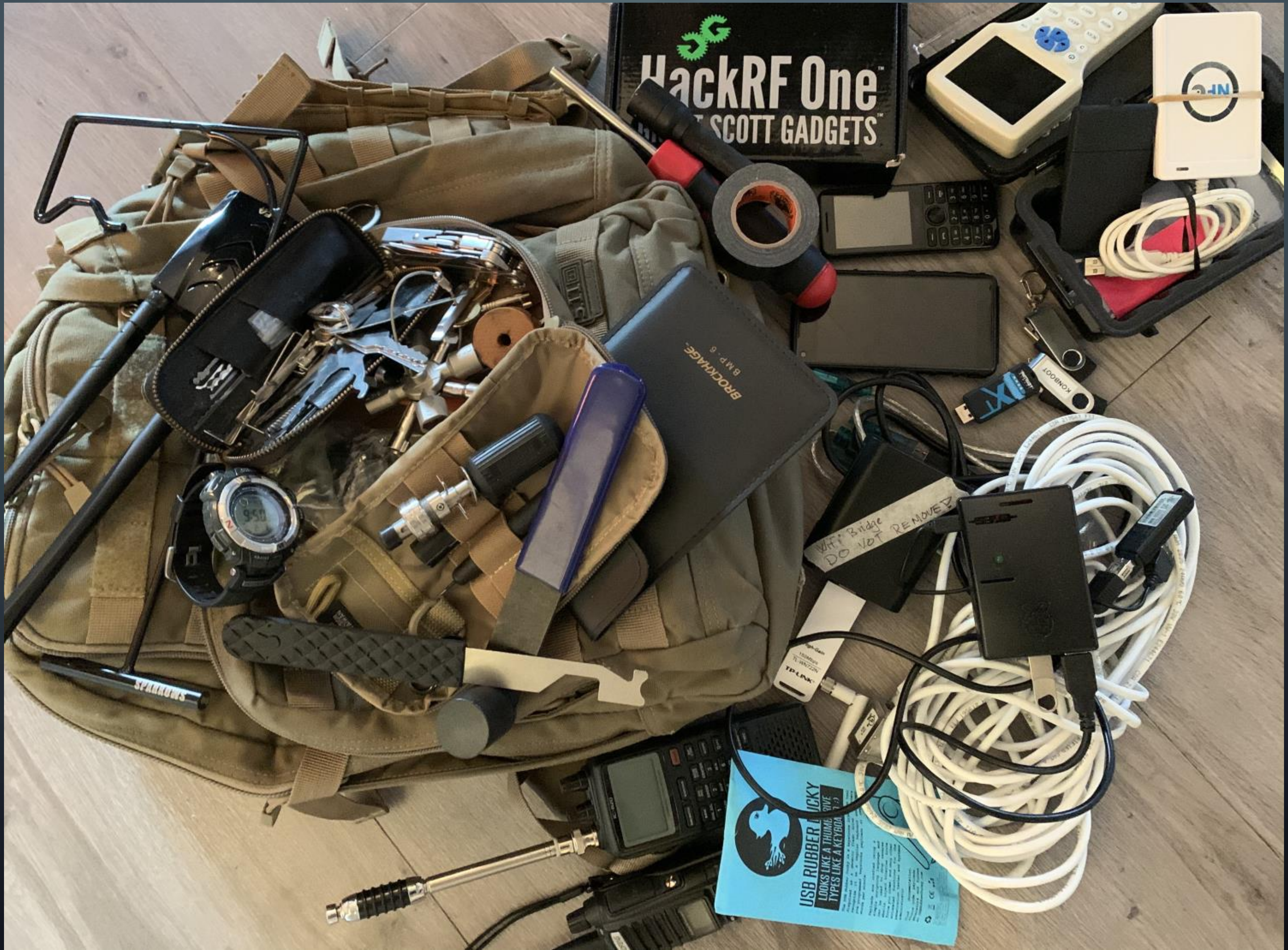
TAKING DOWN NAVIGATION: AIS

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



```
LAT: [redacted]' N
LON: [redacted]" E
RNG: 0.731 NM       BRG: 268.3 °
AIS Target
Name: 93464053
CPA:  00.72 NM  TCPA: -00:44 min
BCR:  --.-- NM  BCT:  --:-- min
SPD:  10.0 kn   CRS:  350.0 °
RNG:  00.73 NM  BRG:  269.7 °
Dest: ---
```

OFFICE TESTING

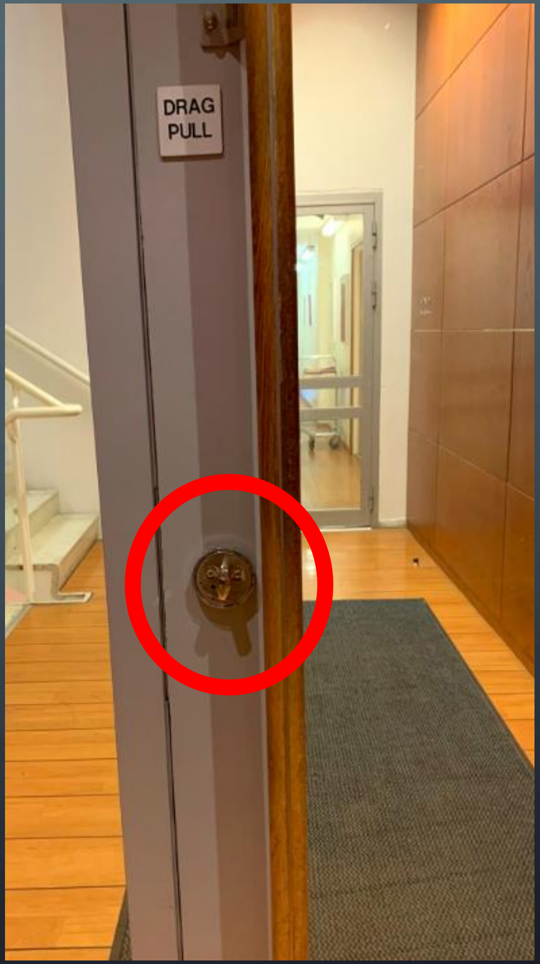


GETTING IN TO BOARD ROOM [1]

- Large international shipping company
- Goal
  - Get in to board room
- Plan
  - Spoof access cards
  - FAILED

GETTING IN TO BOARD ROOM [2]

- How we did it.
  - Walk by reception
  - Open door
  - Knock on door
  - Ask for board room …



RUN

GETTING HIRED

- Hack AD
- Chit chat with receptionist
- Send e-mail
- More chit chat
- Get access card …
- Walk in and bring guest aka co-hacker

[redacted]

[redacted]

THANK YOU!

- John-André Bjørkhaug
- john.bjorkhaug@gmail.com
- john-andre.bjorkhaug@global.ntt
- +47 93 46 40 53
- @jabjorkhaug