Hey Captain, Where’s Your Ship? Attacking Vessel Tracking Systems for Fun and Profit

Marco Balduzzi, Kyle Wihoit, Alessandro Pasta
(@embyte / IZ2PMO, @lowcalspam, IZ2RPA)
Ingredients
Automatic Identification System

- Tracking system for ships
  - Centralized management for port authorities (VTS)
  - Ship-to-ship communication in open-sea
- Used for plot, course, position, and speed
- Some Applications:
  - Vessel Traffic Services
  - Collision Avoidance
  - Maritime Security
  - Aids to Navigation (AtoN)
  - Search and rescue, Accident investigation
  - Binary messages, e.g. weather forecasting
Automatic Identification System

• Introduce to supplement the existing safety systems, e.g. traditional radars
• IMO agreement 2002, widely used since 2006
  – Required on any international ship with gross tonnage of 300 or more tons.
  – Also required on ALL passenger ships regardless of size
• Estimated 400,000 installations. Expected over a million within 2014.
Online AIS Services

- Collects and visualizes ships information
- Upstream done via:
  - Email
  - TCP/UDP Socket
  - Commercial Software
  - Smartphone Apps
  - Radio-Frequency Gateways (deployed regionally)
AIS Application Layer

- AIVDM Sentences
- NMEA Sentences, as GPS

![AIVDM, 1, 1, , B, 177KQJ5000G?tO`K>RA1wUbN0TKH, 0*5C
TAG, FRAG_, FRAG_ID, N/A, CHANNEL, PAYLOAD, PAD, CRC]
Message 1/18: Position Report

Maritime Mobile Service Identity (MMSI) number: Shared among multiple messages

- Longitude, latitude, navigation status, speed-over-ground (SOG), course-over-ground (COG)
- Sent every 3 to 30 seconds, depending on ship speed
- 168 bits
Message 24: Static Report

- Types 24A [160 bits] and 24B [168 bits]
- Name, callsign, dimension
- Type of ship and cargo type, e.g.
  - 35: Engaged in military operations
  - 51: Search and rescue
  - 55: Law enforcement
  - 5X: Carrying dangerous goods (e.g. Nuclear)
Few-Others

- Type 8: Binary Broadcast Message
  - Weather Forecasting
- Type 22: Channel-Management
  - Reserved for Port Authorities
- Type 14: Safety-Related Broadcast Message
  - SOS, Man-In-Water
Generate Valid AIVDM Sentences

$ ./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 = 9.72357833333333
- --lat=LAT
  18. Latitude, default = 45.6910166666667
- --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
AIVDM_Encoder Example

- Example of generation of AIVDM Sentence for
- Ship involved in Military Operations
- Named HiTB13

```
$ ./AIVDM_Encoder.py --type=24 --part=B --callsign=HiTB13 --vtype=35 --vsize=20x10
0110000000111010111101110011001100100100100110000000000000000000000000000000000000
000000010000001010000001010001110011000000000000010100000010100001010000101000000
$ ./AIVDM_Encoder.py --type=24 --part=B --callsign=HiTB13 --vtype=35 --vsize=20x10 | xargs -I X ./unpacker X 1 B
!AIVDM,1,1,,B,H3cc>HTS000000089D2ik01@:550,0*2D
$ ./AIVDM_Encoder.py --type=24 --part=B --callsign=HiTB13 --vtype=35 --vsize=20x10 | xargs -I X ./unpacker X 1 A
!AIVDM,1,1,,A,H3co>HTS000000089D2ik01@:550,0*2E
$ 
```
Identified Threats

- Grouped in two macro families:
  - Implementation-specific VS protocol-specific
Spoofing Attack

- Ships, AtoN, Aircrafts
Autopwning

- Script to make a ship follow a path over time
- Programmed with Google Earth's KML/KMZ information
Ship Hijacking via AIS Gateway

Upstream Provider
(http://www.marinetraffice.com)

High Seas!!!
Eleanor Gordon

- Eleanor Gordon...Real ship...

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)

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
Replay Attack

Upstream Provider
(http://www.marinetracking.com)

High Seas!!!

AIS Receiver

Antennae

Internet

Endpoint

Interval Time Change
AIS Communication over the Air

- No authentication, no integrity check
- Protocol designed in a “hardware-epoch”
- Hacking: Difficult and cost expensive

- Fake AIS Signals?
- Let's do it via software!
SDR: Software Defined Radio

- Paradigm switch from Hardware to Software
- Reduced costs, Reduced complexity, Increased flexibility
- Many application, e.g. Radio/TV receiver, 20 USD
- Accessible by many, bad guys included!

UP TO 1600 kHz. Spectrum Display and Record
GnuRadio and USRP Synergy

Universal Software Radio Peripheral
AIS Transmitter

- GnuRadio flowchart for transmitting AIS message on the air
- 4 main components / blocks
- IDE → Python script
AIS Frame Builder

- Implements the AIS Stack (C code)
- Builds the Frame to be modulated

Application and Presentation Layers
- Message Generator
  - AIS Message
  - Payload Encoder

Link Layer (LME and DLS)
- FCS CRC & Bit orderer
- HDLC Encoder
- Framer

Physical Layer
- NRZI Encoder
- Byte Packer
- AIS Frame
Equipment

Universal Software Radio Peripheral

AIS Transceiver
Outdoor experiments

Standard VHF Transceiver (Radio)

MOXXON Directional Antenna
Attack 1: Man-in-water Spoofing

- Fake a "man-in-the-water" distress beacon at any location
- Similar to Avalanche Safety Beacons
- <live demo>
Attack 2: Frequency Hopping

- Disable AIS transponders
  - Up to 5 weeks
- Switch to non-default frequency
- Stored in flash memory
- Specify a desired targeted region
  - Geographically remote region applies as well
- E.g. Pirates can render a ship invisible in Somalia
Attack 3: CPA Alerting

- Fake a CPA alert (Closest Point of Approach) and trigger a collision warning alert.
Attack 4: Weather Forecasting
Real-World Experiment

- Generate a valid over-the-air AIS message
- Target: AIS proxy
- Demo
Responsible Disclosure

- Our experiments are conducted **without** interfering with existing systems
  - Messages with safety-implications tested **only** in remote lab environment
- We reached out the appropriate providers and authorities within time
- Online providers:
  - MarineTraffic, AisHub, VesselFinder, ShipFinder
- Standard bodies:
  - ITU-R: 11 September 2013
  - IALA, IMO, US Coast Guards: No answer yet
Countermeasures

- **Authentication**
  - Ensure the transmitter is the owner
- **Integrity Monitoring**
  - Tamper checking of AIS message
- **Time Check**
  - Avoid replay attack
- **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!
Questions?

• Thanks! FTR, Germano (IW2DCK), ITU-R