ENAV15 Input paper

Agenda item 10

Task Number

Author(s) / Submitter(s) N Ward

Guidance on AIS Vulnerability

# Summary

**1.1 Purpose**

This paper proposes guidance for IALA Members on dealing with vulnerability of AIS to accidental and deliberate disruption.

**1.2 Background**

The Automatic Identification System (AIS) is an internationally standardised, VHF Broadcast system providing identity, position and status of ships. AIS was originally provided for safety reasons, not for security purposes, so it was never designed to be resistant to malicious interference.

Research results were published last year showing that AIS information can be spoofed, that is false information can be presented, including the names and other details of vessels, their position and status. These results have been presented again this year, with the additional possibility of spoofing DGNSS corrections provided by AIS.

**2 ACTION REQUESTED**

The Committee is invited to consider the information provided in the Annex, with a view to possible development into a Guideline.

**ANNEX**

**Introduction**

Research results were published last year showing that AIS information can be spoofed, that is false information can be presented, including the names and other details of vessels, their position and status:

<http://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabiliesties-discovered-in-global-vessel-tracking-systems/>

Further discussion, including an IMO response, can be found on: <http://www.technologyreview.com/news/520421/ship-tracking-hack-makes-tankers-vanish-from-view/>

These results have been given further publicity at a recent conference in the Netherlands:

http://haxpo.nl/hitb2014ams-marco-balduzzi/

with the additional possibility of spoofing DGNSS corrections from AIS, suggesting that this could lead ships off course and into danger.

AIS is an open system and its vulnerability to disruption has long been known. However, this publicity may result in IALA Members facing questions, therefore guidance may be helpful.

**About AIS**

The Automatic Identification System (AIS) is an internationally standardised, VHF Broadcast system providing identity, position and status of ships. Carriage of Class A AIS units is required for SOLAS Convention vessels. Class B equipment is now carried voluntarily on many non-SOLAS vessels, including leisure and fishing craft and service vessels. AIS is also used to provide Aids to Navigation (AtoN) on fixed and floating platforms. The position of vessels and floating AtoN used by AIS is generally provided by GPS, although other electronic position fixing systems (EPFS) could be used.

**Nature of Vulnerabilities**

It should be noted that AIS was originally provided for safety reasons, not for security purposes, so it was never designed to be resistant to malicious interference.

Previous studies have identified the following potential causes of failure:

* Incorrect data input to AIS unit
* Disruption to GNSS (GPS)
* Failure of AIS unit
* Degradation of VHF propagation
* Loss of VHF reception
* Control system malfunction

The first two of these causes can be brought about by deliberate broadcast of false information, including manipulation of GPS, so-called spoofing, for example a false position or identity can be broadcast. The recent suggestion that false DGNSS corrections could be broadcast introduces another approach. In common with other navigation and communications systems, AIS should not be relied upon as the sole source of information.

**Precautions**

Administrations providing services via AIS, such as AIS AtoN or DGNSS corrections, or using AIS data for analysis purposes should be aware of these vulnerabilities and should consider taking the following precautions:

* All AIS information should be verified by some other means, for example radar or VHF DF
* Any apparently false or anomalous signals should be investigated by cross-checking with other AIS receiving stations and displays
* The integrity of broadcast information, especially AIS AtoN and DGNSS corrections, should be monitored to ensure that identity, position, status and other message contents are correct
* The integrity of GPS (or other EPFS) should be monitored, for example by Differential GPS
* The validity of any DGNSS corrections provided via Message 17 should be continuously checked against corrections provided by authorised reference stations with integrity monitoring, such as those used with MF beacons
* Equipment used to broadcast AIS signals, such as base stations, should be located in secure premises and unauthorised access should not be possible
* AIS monitoring provided via the internet should only be relied upon if control and access are provided by secure systems.
* Local Navigation Warnings should be issued if false AIS signals are being broadcast
* The source of any false AIS signals should be identified and preventive action taken

**Conclusions**

* AIS does not have inherent integrity or authentication
* It is possible to broadcast false information via AIS
* AIS should not be used as a sole source of information
* Other means should be used to verify AIS information
* Integrity of AIS information should be monitored
* Preventive action should be taken against false broadcasts