Richard Hurley, **Senior Maritime Data Analyst** is responsible for the analysis and interpretation of data from the IHS Maritime global terrestrial and satellite AIS network, which monitors the movements of over 110,000 vessels daily. Richard joined IHS Maritime, then known as FISYS, in 1991 after serving in the Royal Navy as a Seaman Officer, and then subsequently taking a degree in Physics with Electronics. He specialises in the exploitation of data from the AIS network in combination with other IHS Maritime databases and has recently contributed analysis on a range of subjects including, The transport issues involved in exporting Canadian Oil Sands products from British Columbia, the Northern Sea Route through the Arctic, and Monitoring of Iranian Crude Oil Shipments. Richard is a Member of the Nautical Institute and a retired Lieutenant Commander in the Royal Naval Reserve.

Dispelling the AIS Security Myths!

I would first draw attention to the fact that the source of this story is a "Hacking Expert" talking at "a hacking and security conference", not a Maritime AIS expert talking at a Maritime Conference. As such we might not expect such a forum to come up with any topic which concludes there is no need for anti-hacking experts or cyber security firms. What the paper lacks is any apparent understanding of the rationale behind the introduction and use of AIS or any reasonably valid reason why the theoretical capabilities they have tested only in the laboratory have anything other than a nuisance value if transferred to the field.

First, the accusations.

That the AIS system is open and thereby potential able to hacking or interference.

True, but anybody with a basic knowledge of the parameters set out under SOLAS when designing the system knows it was always designed as an open system precisely to make it accessible to all in line with its primary goal of being a Navigation safety aid for vessel within sight of each other. To suggest it should have been designed with security checks is a post 9/11 reaction akin to suggesting that the 911/999 emergency telephone systems should be encrypted to prevent hoax messages. By its very nature any open radio communication system is open to spoofing, jamming or far more common simply misuse.

That the messages can be tampered with or faked to create false movements and or vessels

While true anybody can produce a false message as the format and protocols are openly available again by design. The question is why you would want to do this. The problems/considerations are:

To produce a convincing track you have to be able to generate a new message every 2-6 seconds and continue to broadcast this for as long as you want the illusion to continue. Not a situation a hacker wants to be in if they wish to avoid detection.

The only vessels required to transmit a valid AIS message are those mandated under SOLAS, all other vessels can far easier conceal their position by switching off or not fitting AIS equipment in the first place.

By transmitting a false position/identity you are effectively only removing the data flag from your ship not cloaking the vessel . The ship will still be visible to other ships / maritime authorities by all the usual means such as radar but the only difference is that they will now see you as an unknown vessel. A situation more likely to invite inspection rather than conceal.

Fake vessels will only exist on an AIS screen not physically, so again when compared to other sources of movements the effect will be to invite rather than deflect scrutiny.

Vessels seen as teleporting across the world or moving faster than normal are regularly identified by vessel tracking systems/maritime authorities for scrutiny.

That by tampering with AIS messages you can effectively control a vessel.

Not true. AIS is an information tool designed as an aid to safe Navigation only. As such unlike GPS which may be used to feed data automatically to the autopilot for steering and navigating the vessel, its function is solely to provide passive data to the Ships staff for evaluation.

That by tampering with the data you can swamp AIS traffic systems or AIS data collectors computers

Again this is not impossible however to do so would require you to be able to connect directly into the data collection network and to be able to maintain that connection for as long as you wished to disrupt the system.

What does AISLive have/do that mitigates the above risks.

1. We are well aware of the parameters and limitations of the basic AIS system as well as the quality of the data normally received and the most common types of data error experienced.
2. We already implement a number of error checking routines to identify data which may be suspect or incomplete (checks on incoming MMSI, Flag, Name, Imo number etc.) . In doing this we are able to draw on the data contained within our maritime databases for reference. A basic resource not available to many of our AIS only competitors.
3. We source our AIS data from reliable marine industry sources rather than amateur sites, thus ensuring we have partners with interest in maintaining reliable connections 24/7.
4. Wherever possible we try to obtain multiple AIS antenna sites in an area thus giving us several data sources for comparison, and to limit the effects of loss or damage to any single site. This redundancy also enables us to switch off or exclude any single supplier should we detect any anomalous data with minimal effect to the system.
5. We have a completely separate second source of AIS data from satellite AIS with which to compare our terrestrial data.

Are there any new short term worries as a result of this paper.

Obviously of concern is the effect on our customers' views of the reliability of the AIS system in general which we hope will be covered by the notes above.

Also of concern is that as a result of this publicity some amateur hackers will attempt to try this for themselves. While we do not believe that these attacks will be any other than a nuisance we will need to be alert for any signs of unusually high instances of poor data in the system. In this circumstance it is possible that the AIS data providers such as Marine traffic with a high proportion of amateur contributors to their networks may be at higher risk than ourselves.