A Security Evaluation of AIS Automated Identification System

Marco Balduzzi
Trend Micro Research

Alessandro Pasta
Independent Researcher

Kyle Wilhoit
Trend Micro Research

ABSTRACT

AIS, Automatic Identification System, is an application of cyber-physical systems (CPS) to smart transportation at sea. Being primarily used for collision avoidance and traffic monitoring by ship captains and maritime authorities, AIS is a mandatory installation for over 300,000 vessels worldwide since 2002. Other promoted benefits are accident investigation, aids to navigation and search and rescue (SAR) operations. In this paper, we present a unique security evaluation of AIS, by introducing threats affecting both the implementation in online providers and the protocol specification. Using a novel software-based AIS transmitter that we designed, we show that our findings affect all transponders deployed globally on vessels and other maritime stations like lighthouses, buoys, AIS gateways, vessel traffic services and aircraft involved in SAR operations. Our concerns have been acknowledged by online providers and international standards organizations, and we are currently and actively working together to improve the overall security.

1. INTRODUCTION

AIS is an Automatic Identification System introduced to enhance the safety of vessels traffic by automatically exchanging up-to-date information, as well as tracking and monitoring of ships. Since 2002, AIS is a mandatory installation for international voyaging ships having a gross tonnage of at least 300[1], and all passenger ships regardless of their size. Found to be beneficial to the maritime industry, nowadays pleasure crafts and fishing boats are often equipped with an automatic identification system. With an estimated number of over 300,000 installations according to a popular online AIS provider[2], AIS is currently an important and widely used technology and solution in smart transportation. Some known benefits are traffic monitoring, collision avoidance, search and rescue operations, accidents investigations and aids to navigation. Clearly, the number of AIS-equipped vessels might be higher because vessels are not required to register with online providers.

AIS works by acquiring GPS coordinates and exchanging via radio transmissions current and up-to-date information between ships and maritime authorities – i.e. vessel traffic services located onshore. AIS information includes, but is not limited to, ships' position, name and cargo and aids to navigation, frequently used by port authorities to assist a ship's navigation or warn about hazards, low tides, rocky outcroppings and shoals commonly found at sea. In open sea, AIS-enabled distress beacons are used to signal and locate a man overboard. AIS data is collected and exchanged between AIS providers operating over the Internet, which offer AIS data visualization, monitoring and reporting in free or commercial forms.

Given its primary importance and prevalence in maritime traffic safety, we conducted a comprehensive security evaluation of AIS, by tackling it from both a software and a hardware (i.e., radio-frequency) perspective. Overall, we identified threats affecting AIS globally, either at its implementation level or in the protocol specification. They allow, for example, disabling AIS communications (i.e., DoS), tampering with existing AIS data (i.e., to modify the information broadcast by a ship), triggering search and rescue alerts in order to lure a victim ship into navigating to a hostile and attacker-controlled sea space, or spoofing a collision in order to possibly bring a ship off course. Interestingly, according to Bloomberg [3], AIS was found, in the past, to be polluted with counterfeit information, i.e. with Iranian ships having switched their flagged countries to Zanzibar as US and Europe tighten sanctions over their nuclear programs.

In summary, our contributions are the following:

- We conducted a security evaluation of AIS – A cyber-physical system introduced to enhance vessels tracking and provide extra safety to maritime traffic, on top of conventional radar installations;
- We designed and implemented a novel software-based AIS transmitter, that we called *AISTX*;
- We identified and verified several threats affecting both the current implementation and the protocol specification of AIS;
- We did responsible disclosure and collaborated actively with the affected providers, international standards organizations and CERTs to improve the overall situation.

The remainder of the paper is structured as follows. Sec-

[1] Unitless index related to a ship's overall internal volume.

[2] http://www.vesselfinder.com/vessels

ACSAC '14 December 08 - 12 2014, New Orleans, LA, USA
Copyright 2014 ACM 978-1-4503-3005-3/14/12 ...$15.00.
http://dx.doi.org/10.1145/2664243.2664257

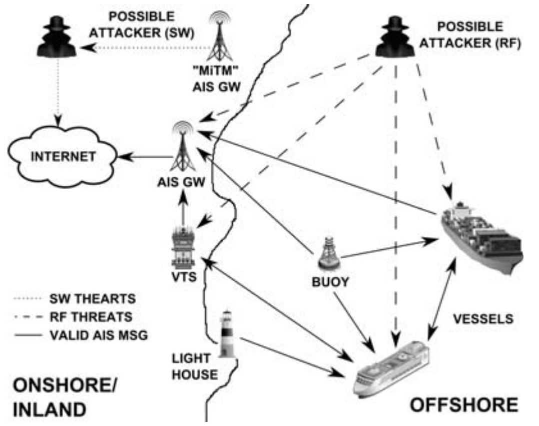


Figure 1: The Automatic Identification System (AIS).

tion 2 introduces AIS and explains how it works. Section 3 gives a general overview of the issues that we identified. Section 4 describes the software-based threats. In Section 5 we introduce and detail *AISTX*, the AIS transmitter that we designed and implemented to conduct the radio-frequency evaluation described in Section 6. Section 7 discusses ethical implications, mitigation strategies and collaboration with the affected parties. Finally, Sections 8 and 9 look over related work and briefly conclude.

2. AUTOMATIC IDENTIFICATION SYSTEM

Since 2002 IMO's SOLAS convention[3] the Automatic Identification System (*AIS*) is required for international voyaging ships having a gross tonnage of 300 or more, and all passenger vessels regardless of their size. Found to be heavily used and widely beneficial to the maritime industry, a second generation of AIS devices, termed *class-B* transponders, were introduced in 2006. When compared with their predecessors, i.e. *class-A*, class-B are typically smaller, lower cost, and simpler to operate. These are typically used in smaller vessels, pleasure vessels, or any fishing vessel less than 300 tons. Since 2010, AIS-related regulations have been constantly adjusted, making it easier to implement and deploy AIS installations. As of 2014, AIS is estimated to be running on at least 300,000 vessels, and in the near future, there is expected to be near a million installations. Nowadays, AIS is a major technology and solution in traffic monitoring and vessels assistance. Shipowners and maritime authorities rely on AIS to supplement traditional radars for collision avoidance and location tracking, in addition to complementary systems like visual observations, audio exchanges and LRIT (long-range identification and tracking).

AIS has many promoted benefits. Any ship transmitting an AIS signal can be received by nearby ships and help make the captains aware of the other shipsâĂŹ location. In addition, AIS provides navigational aids. The aids-to-navigation (AtoN) standard was developed with the ability to broadcast the positions and names of objects other than vessels, such as navigational aid and marker positions and dynamic data reflecting the markerâĂŹs environment (e.g., currents and climatic conditions). These aids can be located on shore, such as in a lighthouse, or on water platforms, such as buoys. Examples of AtoN installations are provided by online AIS providers, such as Marine Traffic[4]. Finally, an example of the importance of the utilization of AIS revolves around accident investigation. Since AIS provides GPS coordinates, course, ground speed, and additional information, it proves more valuable in accident investigation versus the less accurate radar technology used widely today. For the same reason, AIS is largely used in search-and-rescue transponders. AIS-SARTs are self-contained, waterproof devices intended for emergencies, mainly to help the detection and location of vessels and people in distress, i.e. a man overboard.

AIS, as we depict in Figure 1, works by acquiring GPS coordinates and exchanging regional information with nearby stations via VHF, i.e. two radio channels operating at 161.975 and 162.025 MHz, and with AIS providers operating over the Internet. These providers collect data primarily through AIS gateways deployed geographically, i.e. along coast lines and in vessel traffic services (VTS) operated by port authorities. A VTS is a ship traffic monitoring system established by maritime authorities, similar to air traffic control systems for aviation. In addition, single individuals, such as a ship's captain, can upstream AIS data by using a mobile app and a special forwarding software, which duplicates and sends the data to the desired providers as soon as the data is made available. AIS information is broadcasted, collected and exchanged on a regular basis – varying from a couple of seconds to minutes, depending on the type of information and condition of the station. For example, a class-B equipped ship navigating faster than 23 knots is supposed to broadcast its position every 5 seconds. Conversely, an aid to navigation, for example a lighthouse or a buoy notifying an hazard, is sent every 3 minutes.

By regulation, each communicating station, such as a ship, is required to register and obtain valid AIS identifiers, namely MMSI and call-sign, which are issued by official maritime authorities like the US Coast Guard or the Italian Ministry of Economic Development. The maritime mobile service identity (MMSI) consists of a nine-digits number uniquely identifying a station. The first three digits of the MMSI, the maritime identification digits (MID), specifies the country – e.g. 247 for Italy and 338 for United States of America according to ITU-R[5]. The call-signs are a designation for radios, or AIS stations willing to communicate, and are widely used in marine, aviation, military, spacecraft, and by radio amateurs. Finally, AIS information is rendered via chartplotters or providers, e.g. Vessel Finder[6], which, in near real-time, visualize the status of other vessels in the region, navigation aids and other useful maritime information, such as weather forecasts or critical situations. These systems allow worldwide access to AIS statistics, vessels, lighthouses, buoys locations, and corresponding details on a simple, easy to navigate display or website. In addition, AIS information collected from providers is useful in identifying, for example, ships spilling oil in open sea [1] and predicting the financial gain given by marine trading [17].

[3] International Maritime Organization, http://www.imo.org/ourwork/facilitation/documents/solasvonsafetyofnavigation.pdf

[4] http://www.marinetraffic.com/ais/it/datasheet.aspx?datasource=LIGHTHOUSE

[5] http://www.itu.int/online/mms/glad/cga_mids.sh

[6] http://www.vesselfinder.com/

Category	Threat	SW	RF
Spoofing	Ships	✓	✓
	AtoNs	✓	✓
	SARs	✓	✓
	Collisions (CPA)		✓
	Distress Beacons		✓
	Weather Forecasting		✓
Hijacking	Hijacking	✓	✓
Availability Disruption	Slot Starvation		✓
	Frequency Hopping		✓
	Timing Attack		✓

Table 1: Summary of the Identified Threats

3. THREATS OVERVIEW

In this Section, we give a general overview of the threats that we identified in our research. As reported in Table 1, we grouped them in three macro categories, namely spoofing, hijacking, and availability disruption. For each threat, we detail whether it can be performed via software (SW), radio-frequency (RF), or both. Note that Figure 1 includes the information on where attackers fit in the AIS infrastructure. We describe in more detail the software and RF-based attacks later in the paper, respectively in Sections 4 and 6.

Ship Spoofing [SW/RF].

This first threat consists of crafting (i.e., spoofing) a valid non-existent ship. This process involves assigning to the fictitious ship static information, such as the vessel's name, identifiers (i.e., MMSI and call sign), flag, type of ship, cargo type, manufacturer and dimension, and dynamic information like the ship's status (e.g., under way or anchored), position, speed, course and destination. On top of ships, aircraft involved in search and rescue (SAR) operations can be spoofed as well. In fact, SAR aircraft are equipped with AIS class-B transponders as per regulation.

As the reader can imagine, this threat gives an attacker a wide surface of malicious scenarios, such as spoofing a vessel into the jurisdiction of an adversarial nation or making a nuke-carrying cargo sailing the waters of a nuclear-free nation. In addition, vessels spoofing represent an issue for automated systems doing data identification and inference on collected AIS information, for example to detect ships spilling oil in open sea or to predict marine trading. An attacker can counterfeit this information to blame someone else's vessel, for example.

AtoN Spoofing [SW/RF].

Navigational aids, also known as aids-to-navigation (AtoNs), are commonly used to assist vessel traffic, for example along a channel or a harbor, or to warn about hazards, low tides, rocky outcroppings and shoals commonly found in open sea. Spoofing AtoNs consists of crafting fake information to lure a targeted ship into conducting wrong maneuvers. Some examples consist of placing one or more buoys at the entrance of a harbor to tamper with existing traffic, or installing a fake buoy that maliciously instructs a ship into navigating in low water. Given the number of different aids-to-navigations, there are multiple attack scenarios such as for the spoofing of ships.

Collision Spoofing (CPA) [RF].

Collision avoidance is a primary application of AIS, which has been effectively introduced as a system to reduce the risk of collisions among vessels, especially in open sea where no port authority monitoring is in place. The AIS system, in fact, allows for automatic response upon detection and expectation of a collision. This feature is called CPA (closest point of approach) and works by computing the minimal distance between two ships in which at least one is in motion. Using CPA, a ship can be configured to trigger an alert, both visually on the captain's console or acoustically via a siren, and change course in order to avoid a collision. The threat consists of spoofing a ship navigating on a collision course with a targeted vessel. This triggers a collision alert in the CPA system on the victim ship, and could lead the vessel off course into a rock or running it aground during low tide.

AIS-SART Spoofing [RF].

Apart from collision avoidance, AIS is largely used for search and rescue operations. Search and rescue transponders (SARTs) are self-contained, waterproof devices intended for emergency, mainly to help the detection and location of vessels and people in distress, i.e. a man overboard. An AIS-SART activates automatically when in contact with water, and sends a distress radio beacon followed by the GPS position to help aid in locating the survivor. The threat we identified consists of generating a false distress beacon for a man overboard at coordinates chosen by the attacker. By protocol specification, AIS transponders are required to generate an alert when such a message is received. In this scenario, the attacker (i.e., a pirate) triggers a SART alert to lure its victim into navigating to a hostile and attacker-controlled sea space. Note that by law a vessel is required to join a rescue operation upon receiving a search and rescue message.

Weather Forecasting [RF].

One application of AIS is the communication of dynamic data reflecting the changing environment like currents and climate conditions. A special type of messages, namely binary, is used to convey such information. This threat consists of announcing false weather forecasts, for example a sunny day when a squall is expected.

AIS Hijacking [SW/RF].

AIS hijacking consists of altering any information about existing AIS stations, e.g. about the cargo, speed, location and flag of country of a real vessel. As another example, the attacker can maliciously modify the information provided by aids-to-navigation installed at port by authorities for vessels assistance and monitoring. In the software variant of the attack, the attacker eavesdrops (i.e., MiTM) on the communication and replaces AIS information arbitrarily; in the radio-frequency version, the attacker overrides the original AIS message with a higher powered fake signal. In both cases, the recipient receives an attacker-modified version of the victim's original AIS message.

Availability Disruption Threats [RF].

We identified three attacks that go under the same category, namely availability disruption. Since these attacks can be performed only in radio-frequency, we describe their practical implementation later in detail in Section 6. Here, we summarize them:

- *Slot Starvation*: This attack consists of impersonating the maritime authority to reserve the entire AIS transmission "address space", in order to prevent all stations within coverage in communicating; this includes ships and aids-to-navigation, as well as AIS gateways used in traffic monitoring. As a result, the attacker can disable AIS systems on a large scale;
- *Frequency Hopping*: In a frequency hopping attack, the attacker impersonates the maritime authority to instruct one or more AIS transponders to change their frequencies of operation. By protocol specification, the receiving station is required to maintain the information, which makes the attack persistent even if the system is rebooted. In addition, this operation can be bound to a geographical region, i.e. an attacker can "program" a targeted ship into switching the frequency upon reaching a region chosen by the attacker; this makes AIS useless. Note that for class-B devices, the AIS standard prevents a manual reset of the transponder, and *not* notify the user of the frequency change;
- *Timing Attack*: In this attack, the malicious user instructs the AIS transponder(s) to delay its transmission time – the attacker, by simply renewing the command, can prevent the transponder(s) from further communicating its position. This makes a vessel disappear from the AIS-enabled radars, for example. Inversely, the attacker can overload (i.e., floods) the marine traffic, including ships and vessel traffic services, by requesting the existing stations into sending AIS information and updates at a very-high rate.

4. SOFTWARE EVALUATION

In this Section, we discuss the software-based threats that we identified. We evaluated three popular online AIS providers, namely Marine Traffic[7], AisHUB[8] and Vessel Finder[9], and showed that they are affected by the same threats.

When referencing AIS, we have to address AIVDM, the application layer protocol used by AIS to exchange data sentences, i.e. from vessels' AIS transponder broadcasting their position, or from vessel traffic services (VTS) monitoring the ships at port. AIVDM specifies 27 message types; each one having a corresponding purpose and value that designates its purpose. The full list is given in [10]. For example, message type 1 is used in communications between ships and ship-to-VTS to exchange updated position reports, and message 24 describes the type of ship, its cargo, dimensions and name. For our experiments, we implemented an encoding tool written in Python, named *AIVDM Encoder*, that we used to generate arbitrary AIVDM sentences and conduct both the software and the radio-frequency evaluation of AIS[10].

While AIS installations on ships involve hardware, software is used to upstream AIS data to online providers. While these services are very useful for tracking and navigation, there are security issues with their implementations. Because of the loosely implemented nature of AIS receivers, online providers are often required to accept any data they receive, since they represent a consortium of users and enthusiasts sharing data. This however, introduces several security issues.

AIS providers allow multiple ways of collecting AIS data like pre-formatted emails, mobile apps[11] and forwarding software such as `AIS Dispatcher`[12]. When an AIS message is generated, the forwarding software duplicates and sends the message to the desired providers – e.g., over `UDP/5321` for Marine Traffic. The interval of forwarding these messages can be established, thus forwarding near real-time statistics to AIS providers. The same software can be used to upstream AIS messages received from an AIS gateway, i.e. a local VHF receiver one may have in their home. Gateways are often located along coast lines and present in vessel traffic services operated by port authorities.

Throughout our analysis, we identified security issues with all of the aforementioned online providers. These providers, for example, lack source vetting. They do not check to ensure the message originating for a vessel comes from the same region as the vessel purportedly sending the message. Likewise, there is no authentication present to ensure the vessel sending the AIVDM sentence is the proper sender. As shown in Table 1, the identified problems allow an attacker to carry out both spoofing and MiTM-style attacks against the affected providers as we discuss in the following.

Spoofing consists of crafting valid AIS information remotely, e.g. a non-existent ship or aid to navigation, from nowhere near a body of water or a real AIS station. To verify this threat we first used our *AIVDM Encoder* to generate an innocuous AIVDM sentence indicating low tide in a closed lake nearby. We upload it to the providers by using a generic networking client like `netcat`. Note that message 21 is reserved for AtoNs reports and type 13 is used for buoys. In addition, AtoNs have a MMSI in the form of `99MIDXXXX` as per specification. An example is given in the following Listing:

```
$ ./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
```

Listing 1: UDP spoofing example for Marine Traffic.

Second, we generated a pre-formatted email report for a moored vessel, i.e. of Listing 2, and sent it to the receiving address of the targeted provider:

```
To: report@marinetraffic.com

MMSI=247320161
LAT=44.3522
LON=8.5665
SPEED=0
COURSE=243
TIMESTAMP=2013−11−11 13:11
```

Listing 2: Email spoofing example Marine Traffic.

[7] http://www.marinetraffic.com/

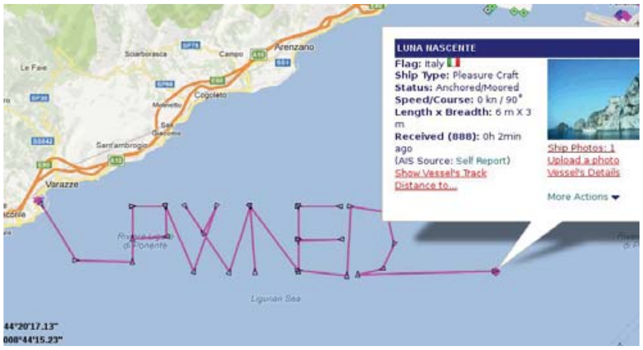
[8] http://www.aishub.net

[9] http://www.vesselfinder.com/

[10] The tool will be made publicly available on the Security Intelligence Blog of Trend Micro [24] and on the personal page of one of the authors [2].

[11] http://www.marinetraffic.com/ais/iphone.aspx

[12] http://www.marinetraffic.com/ais/downloads/aisdispatcher.zip



LUNA NASCENTE
Flag: Italy
Ship Type: Pleasure Craft
Status: Anchored/Moored
Speed/Course: 0 kn / 90°
Length x Breadth: 6 m X 3 m
Received (888): 0h 2min ago
(AIS Source: Self Report)
Show Vessel's Track
Distance to...
Ship Photos: 1
Upload a photo
Vessel's Details
More Actions

Figure 2: Example of spoofed ship following a pr grammed path.

Finally, we implemented an automated script that u Google Earth's KMZ files to make a spoofed AIS station follow a path over time, e.g. a fictional generic ship spelli the word `PWNED` in the Mediterranean Sea, as depicted Figure 2. Overall, all of the experiments were successf and allowed us to spoof and upstream valid AIS messag to the evaluated providers.

Man-in-the-middle involves the modification or injecti of erroneous data in the AIS communication of a stati transmitting valid AIVDM sentences. We first physically tercepted valid AIVDM sentences transmitted via air fron nearby station (i.e. our AIS transponder[13]), by deploying AIS gateway we controlled. We configured it with `AIS Dispatcher` and an USB dongle AIS receiver[14]. We then used a proxy server to intercept, modify and upstream the AIS messages to the online providers, which accepted any tampered message unhindered. In a second experiment, we picked an existing ship being rendered on online providers[15] and we spoofed via software – as described previously – modified information for the vessel. We were able to make the providers rendering the ship in a different location from where initially located.

5. AIS TRANSMITTER

In the previous Section, we described the software-based threats that we identified, i.e. how to upstream arbitrary AIVDM sentences to AIS providers and how to tamper with existing AIS information sent by real ships to the providers. In the following, we focus on radio-frequency-based threats. We describe the system that we designed and implemented for generating and transmitting arbitrary AIS messages over the air. Later in Section 6, we present the experiments that we conducted to show that our concerns are real and affect all AIS transponders installed on vessels worldwide.

5.1 Architecture

Our AIS transmitter that we called *AISTX*, is designed and implemented as a software defined radio (SDR)[16].

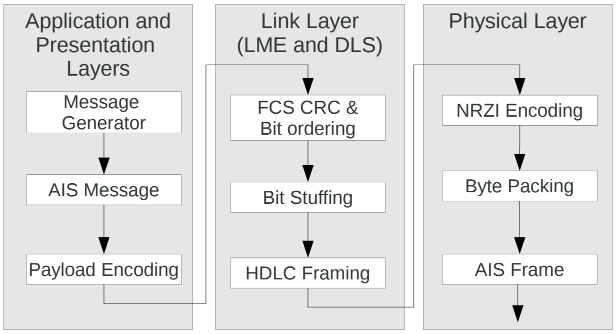


Figure 4: Detail of the *AIS Frame Builder* block.

A SDR consists of a software application, which implements the signal elaboration chain, and a hardware peripheral, which converts binary data to radio-frequency signals for over-the-air transmission. The growth of personal computers' computational capabilities and the drop of hardware acquisition costs have made SDR peripherals available at affordable costs. One example is the universal software radio peripheral (USRP), being one of the most used SDR peripherals. Our *AISTX* is built on top of GnuRadio[17], an open source framework widely used to design and implement efficient software defined radios. While it has been extensively used to conduct research in security, for example in evaluation of the ADS-B aviation protocol [7], GSM security [26] and RFID used in Taipei Metro's EasyCard [5], we believe we are the first to adopt it for building an AIS transmitter.

Figure 3 shows the general architecture of *AISTX*. We generate the AIS frames with a block called *AIS Frame Builder*, thoroughly described later in Section 5.2. We then realize a GMSK modulation of each frame, and over the two AIS channels. GMSK (Gaussian Minimum Shifting Keying) is a form of digital modulation widely used in mobile communication, e.g. in GSM and DECT transmission. The GMSK modulator is configured with parameters as per AIS specification [11]: A bandwidth-time product (BT) of 0.4, a bit rate (R) of 9,600 bps, and a samples/symbol as rounded ratio of sampling and bit rate.

The modulated frames, generated at baseband, are then transposed to the default operating frequencies that the AIS specification dictates. We first modulate the baseband signal around the frequencies of ± 25 KHz, by multiplying it by two sinusoids of said frequency. To prevent signal clipping and linearity distortion in the digital-to-analog converter (DAC) of the SDR peripheral, the amplitude range of the signal is reduced from ± 1 to ± 0.9. Finally, we shift the resulting signal over the carrier frequency of 162 MHz, resulting in two signals over the AIS standard frequencies of 161.975 MHz and 162.025 MHz. The *UHD: USRP Sink* block acts as a driver for the SDR peripheral.

5.2 Building an AIS Frame

Although GnuRadio comes with a wide range of commonly-used pre-defined blocks – e.g. filters, signal generators and converters – for the purposes of our work, we extended the

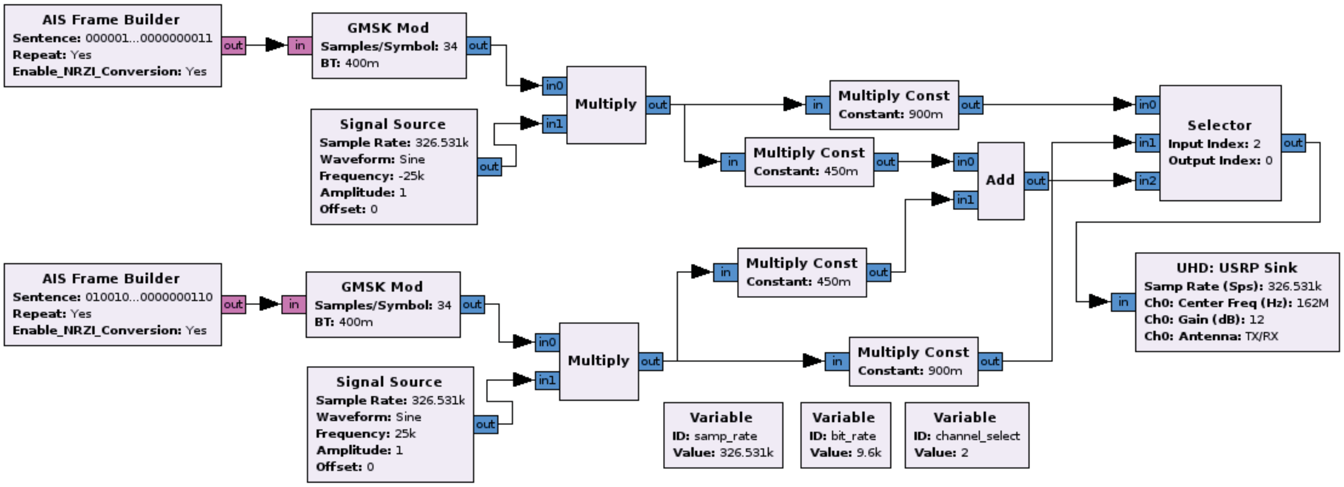
[13] Note that for ethical implications (ref. Section 7), we used our own AIS transponder for this and the following experiment.

[14] http://www.radargadgets.com

[15] We upstreamed the real position broadcast from our transponder.

[16] The transmitter and the *AIS Frame Builder* block we describe later will be made publicly available on the Security Intelligence Blog of Trend Micro [24] and on the personal page of one of the authors [2].

[17] http://gnuradio.org


AIS Frame Builder
Sentence: 000001...0000000011
Repeat: Yes
Enable_NRZI_Conversion: Yes

GMSK Mod
Samples/Symbol: 34
BT: 400m

Signal Source
Sample Rate: 326.531k
Waveform: Sine
Frequency: -25k
Amplitude: 1
Offset: 0

Multiply

Multiply Const
Constant: 900m

Multiply Const
Constant: 450m

Add

Selector
Input Index: 2
Output Index: 0

AIS Frame Builder
Sentence: 010010...0000000110
Repeat: Yes
Enable_NRZI_Conversion: Yes

GMSK Mod
Samples/Symbol: 34
BT: 400m

Signal Source
Sample Rate: 326.531k
Waveform: Sine
Frequency: 25k
Amplitude: 1
Offset: 0

Multiply

Multiply Const
Constant: 450m

Multiply Const
Constant: 900m

UHD: USRP Sink
Samp Rate (Sps): 326.531k
Ch0: Center Freq (Hz): 162M
Ch0: Gain (dB): 12
Ch0: Antenna: TX/RX

Variable
ID: samp_rate
Value: 326.531k

Variable
ID: bit_rate
Value: 9.6k

Variable
ID: channel_select
Value: 2

Figure 3: *AISTX* architecture on GnuRadio.

suite with a custom block, named *AIS Frame Builder*, which serves as generator of AIS frames. As Figure 4 shows, our block implements the full AIS stack, and it is composed of three main components covering respectively the application/presentation layers, the link layer and the physical layer, as defined in the protocol specification for AIS. Our block works as following. It takes as input a AIS message, formatted using the AIVDM format. At first, it encodes the message using a 6-bit ASCII alphabet. Only capital letters are supported, i.e. lower-cases are substituted with upper-cases. Numbers are in decimal notation and negatives are expressed using a 2's complement. A padding with zeros (0's) to a multiple of 8 bits is done for further processing. The reason behind the use of such a short alphabet is to reduce the average message length transmitted over the air.

In the link layer module, we compute a frame check sequence of the previous AIS-encoded messaged (i.e., the payload), by using a 16-bit polynomial cyclic redundancy check. This is used by the receiver to validate the integrity of our AIS message. We also reorder the bits of the payload from big-endian to little-endian as per specification. Next, application of bit stuffing occurs – a technique consisting of inserting a zero (0) if five consecutive ones (1's) are found in the bit stream. Bit stuffing reduces the chance of errors in communication and makes sure that HDLC control information is always in the same position.

This control information is added during HDLC framing and consists of a training sequence and of a start/ending flag. The training sequence are twenty-four bits of alternating 0's and 1's (010101010...) and is used to synchronize the receiver to the data stream; the start/end flag consists of a 8-bit pattern 01111110 (0x7E) and is used to delimit the payload portion. Although this flag consists of 6 bits of consecutive ones (1's), it is not subjected to bit stuffing because the flag is meant to act as a delimiter. HDLC is used to synchronize the sender and receiver, and permits synchronous, code-transparent data transmission. This concludes the operations carried out in the link layer module.

Finally, the physical layer prepares the frame for the GMSK modulation, which takes place following in the AIS transmission chain, as we described in Section 5.1 and in Figure 3. The data is encoded using the NRZI mapping, which stands for non-return-to-zero inverted mapping. NRZI is a method for mapping binary digits to a physical waveform and it is characterized by two levels (high and low). The mapping works by having a signal transition on the clock boundary whenever a logical 0 has to be represented, and by keeping the signal at level whenever a logical 1 is transmitted. Note that AIS, similarly to USB, adopts a reverse transition convention with respect to the common use of NRZI.

To conclude, the frame is then packed, i.e. transformed from a bit to a byte representation in order to fit the modulation requirements of the following GMSK block.

6. RADIO-FREQUENCY EVALUATION

Our radio-frequency evaluation consists of two experiments. In the first, we conducted an in-lab experiment in which we used three AIS receivers to verify that our transmitter works well in practice and can be used to run the attacks we identified. Later, we conducted a coverage assessment, in which we verified that a malicious actor can perform such attacks in an open air environment like onshore or open sea, targeting real vessels and authorities.

Our experimental setup consisted of a transmitter acting as an attacker and of a receiver acting as victim (e.g., a vessel or a vessel traffic service). For the transmitter, we used a standard Linux machine running our *AISTX* transmitter together with a USRP device, i.e. a commonly used and well-supported SDR peripheral for transmitting signals over the air. Our USRP consisted of an Ettus USRP B100 completed with a WBX-model daughter-board[18]. This device was well suited for our requirements because it supports VHF maritime frequencies. From the receiver standpoint, we evaluated our ability to generate AIS signals over three distinct AIS receivers: A commercial and standard class-B transponder called Weatherdock EasyTRX2[19], a hardware receiver called AIS em-track R100[20], and a hybrid receiver (hardware and software). The latest is based on a software-

[18] https://www.ettus.com/product/details/UB100-KIT

[19] http://www.easyais.de/en/product_page.php?prodid=33

[20] http://www.em-trak.com/PRODUCTS/Receiver/Receiver.aspx

based AIS receiver[21] and a standard YAESU VHF radio, which we modified by adding an additional output port in order to interface the radio with a computer's audio port and bypass the final-stage audio filter. Note that we connected receivers and transmitter by physical cable to prevent any signal from propagating over the air[22].

As said, we used our *AISTX* transmitter to generate the appropriate AIS messages and perform the attacks, and the receivers to validate the threats. We analyzed the receivers' behavior in three ways: At the hardware layer, at the presentation layer and at the application layer. From a hardware standpoint, we equipped the AIS receivers with alarming lights, in order to observe the behavior of a transponder installation when an alarm is triggered. At the presentation layer, we used the serial port provided by the AIS receivers to monitor the AIS messages received. In fact, via the serial port, we could see all AIS-demodulated messages, including those that are not handled by the software at the application layer (e.g., message type 22, which is used to control the operating frequency of the transponder). Finally, we used a standard chart-plotter software, i.e. OpenCPN[23], to evaluate the receivers' behavior at the application layer. OpenCPN implements a fully-functional chart plotter for personal computers and supports all AIS message types, including SART and CPA alerting. We used OpenCPN to visually render the results of the received malicious messages, i.e. impersonating the on-board computer normally installed on vessels. Together with OpenCPN, for the spoofing attacks we also used the official monitoring tool offered by one of the transponders, i.e. EasyTRX2. This enabled us to understand how and in which way the target was impacted by our misleading transmissions.

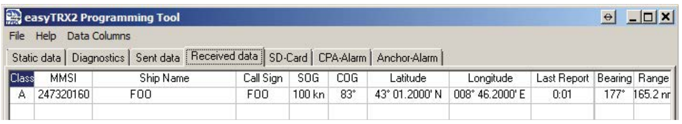
We started our evaluation by using the *AIVDM Encoder* introduced in Section 4 to provide *AISTX* with valid AIVDM sentences for the *spoofing-related attacks*. The Listing 3 gives an example for the generation of an AIS radio message on channel A (161.975 MHz) for a spoofed vessel called FOO, having Italian nationality, i.e. the MMSI prefix is 247, and navigating at 100 knots East out of the coast of Sardinia, at the coordinates 43.01N,8.46E.

```
$ ./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
```

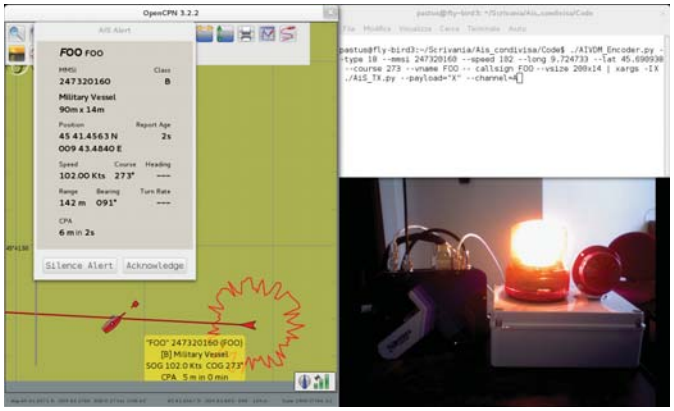
Listing 3: Ship spoofing in radio-frequency (static and dynamic reports).

Figure 5 shows that the receiver correctly interpreted the spoofed message as a valid vessel and reported it on the monitoring tool. The same methodology of attack is confirmed to work well for generating different types of ships (e.g., law enforcement, military, search and rescue, carrying dangerous goods, etc...), aids-to-navigation like buoys and SAR aircraft, giving the ability to inject malicious and bogus information in AIS traffic, targeting both vessels and authorities.



Class	MMSI	Ship Name	Call Sign	SOG	COG	Latitude	Longitude	Last Report	Bearing	Range
A	247320160	FOO	FOO	100 kn	83°	43° 01.2000' N	008° 46.2000' E	0:01	177°	165.2 nr

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



```
pastus@fly-bird3:~/Scrivania/Ais_condivisa/Code$ ./AIVDM_Encoder.py -
-type 18 --mmsi 247320160 --speed 102 --long 9.724733 --lat 45.690938
 --course 273 --vname FOO -- callsign FOO --vsize 200x14 | xargs -IX
./AiS_TX.py --payload="X" --channel=A
```

FOO FOO
MMSI 247320160 Class B
Military Vessel
90m x 14m
Position 45 41.4563 N 009 43.4840 E Report Age 2s
Speed 102.00 Kts Course 273° Heading ---
Range 142 m Bearing 091° Turn Rate ---
CPA 6 m in 2s

"FOO" 247320160 (FOO)
[B] Military Vessel
SOG 102.0 Kts COG 273°
CPA 5 m in 0 min

Figure 6: Collision alert being triggered via signaling light and software (OpenCPN).

We then focused on *collision spoofing* (ref. Section 3). For this attack to work, we spoofed a vessel colliding with our AIS transponder. We used the coordinates and course of the targeted transponder to fake a ship navigating within the CPA threshold-alarm configured in the equipment. Figure 6 shows the result. On the top-right window, the attacker sent the spoofed vessel's position report to the target, shown in the other two windows. On the bottom-right, we see the signaling light being triggered because a ship is expected to collide. The monitoring console of OpenCPN (on the left) confirmed the alert by informing that the collision is expected in 2 seconds and 6 meters away. Depending on the final configuration, this threat could lead the targeted vessel off course.

In a similar way, we confirmed that malicious *weather forecasting* is achievable. We used AIS+[24], a chart-plotting software supporting AIS binary messages normally employed to broadcast weather forecasts by port authorities (i.e., type 8). This verified that weather-specific AIVDM sentences spoofed via RF, such as `!AIVDO,1,1,5,A,8>jR06@0Gwli:QQUP3en?wvlFR06Eu0wgwl?wnSwe7wvlOwwsAwwnSGmwvh0,0*51`, were correctly interpreted by the AIS receivers and reported by the tool.

A malicious user can generate search and rescue messages to trigger a *SART alert*, for example to lure the victim into navigating to the coordinates chosen by the attacker. In fact, by protocol specification and legislation, AIS stations are required to trigger an alert when a distress beacon is received, i.e. informing the captain that a rescue operation is needed for a man overboard. In our experiments, we exper-

[21] https://www.cgran.org/wiki/AIS

[22] A 90 dB in-line attenuator was installed to reduce the transmitter's power according to the receivers' specification

[23] http://www.opencpn.org

[24] http://www.aisplus.vtt.fi/

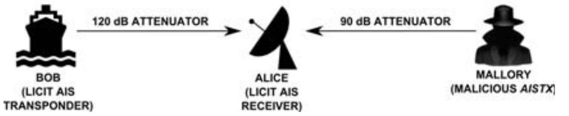


Figure 7: AIS Hijacking in radio-frequency.

imentally verified that we could appropriately spoof such messages and trigger the alert of our three AIS receivers, both visually and acoustically. The strategy was to emulate an AIS-SART transmitter by generating over both AIS channels a class-A position report (i.e. a message type 1) having MMSI in the form of `970YYXXXX`: The prefix (970) is reserved for AIS-SARTs, opposed to other MMSI prefixes that specify the country. The Ys are assigned by CIRM[25] and refer to the SART manufacturer, while the Xs are sequential digits assigned by the manufacturer identifying the SART. The command reported in Listing 4 was used.

```
$ ./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.

We have impersonated fictional ships, buoys and other AIS stations, showing that spoofing threats are real and affect standard AIS transponders used worldwide in maritime traffic.

Next, we describe *AIS hijacking* (ref. Fig 7). Bob, the victim, communicates its AIS information to Alice, an AIS receiver installed onshore from authorities or another ship navigating nearby. The attacker, Mallory, is situated within the radio-frequency coverage of Bob and Alice's AIS stations. She generates a modified AIS message for Alice, pretending to be Bob, and overrides the legitimate communication of Bob by transmitting with higher power. Using a physical cable, we connected Bob's AIS transponder and Mallory's SDR-transmitter to Alice's receiver's ports. We simulated Bob's lower output power (when compared with Mallory), by installing a 120 dB attenuator on its connection with Alice (i.e., 30 dB attenuation more than Mallory). By monitoring Alice's receiver, we proved that Mallory is able to override Bob's signal, i.e. to tamper with valid AIS information sent via radio-frequency.

Following, we verified the *availability disruption* threats by using a particular class of AIS messages, called control messages, which are reserved to port authorities and *not* supported in transmission by transponders, i.e. only in reception. Control messages are used by port authorities to control the maritime traffic and have higher priority with respect to normal AIS traffic, e.g. position reports.

For the *frequency hopping* attack, we verified that by broadcasting the message shown in Listing 5 we immediately switched the receivers to non-standard channel frequencies (i.e., we lowered their operating frequencies of 4.950 MHz). This made the devices unavailable to receive, i.e. to know the position of nearby ships, and to transmit, i.e. to broadcast their positions. Note that this operation was applied immediately because we specified a geographical region including their current position. As an alternative form of attack, an attacker can "program" the devices to disappear from AIS monitoring upon entering a region of interest for the attacker, for example the sea quadrant of Somalia[26].

```
$ ./AIVDM_Encoder.py -type=22
                        -channel_a=2080 -channel_b=2081
                         -ne_lat=45.8 -ne_lon=9.9
                         -sw_lat=45.5 -sw_lon=9.5
F3co>HR22240;VQcF0FA3EB20000
$ ./AiS_TX.py -payload=F3co>HR22240;VQcF0FA3EB20000
              -chan=A
```

Listing 5: Example of availability disruption by frequency hopping.

In a similar attack, that we call *timing* attack, the attacker inhibits the transmission capabilities of one or more AIS stations. For example, in the targeted attack of Listing 6, she uses VTS-reserved `assignment command` messages to instruct a victim to delay the transmission for 15 minutes; by iterating through the command, she accomplishes a denial-of-service attack. Inversely, the attacker can overload (i.e., floods) the marine traffic by requesting the existing stations into sending AIS updates at a very-high rate.

```
$ 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 6: Example of availability disruption by timing attack.

Finally, for the *slot starvation* attack, we used the message types 4 and 20 to simultaneously fake a base station installed at VTS and allocate the AIS transmission "address space" entirely (i.e., the TDMA slots), in order to consume all slots and prevent all nearby stations to further operate (both in transmission and reception).

6.1 Coverage Experiment

In the following, we performed a coverage experiment to simulate the operational conditions of an attacker, e.g. a pirate targeting a ship in navigation, and we showed that our concerns are real. Our coverage experiment consisted of installing our AIS transmitter at a fixed and defined position and a receiving station on a moving car[27]. Our evaluation consisted of generating a harmless testing message with *AISTX* and verifying if, and at which distance, the receiver was able to correctly receive and decode the testing message. Note that as we extensively discuss in Section 7, we took appropriate precautions to conduct the experiment in a safe manner.

We used an amplifier to raise the 50 mW power output of the SDR peripheral to values being in the same order of commercial AIS transponders[28]. This was accomplished through a hardware modification of a traditional VHF transceiver – KENWOOD TK-762G. Note that this device is affordable (i.e., less than 100$ on eBay) and gives attackers an easy

[25] The International Association for Marine Electronics Companies

[26] http://upload.wikimedia.org/wikipedia/commons/7/7e/Somalian_Piracy_Threat_Map_2010.png

[27] As a receiver, we used the Weatherdock EasyTRX2 hardware transponder

[28] 12.5 W for class-A and 2 W for class-B devices as per specification [11]

access to the hardware needed to conduct malicious activities. The hardware modification entailed disconnecting the pre-amplifier's output, i.e. the circuitry from microphone to hybrid module's input, and soldering an external coaxial cable to connect the SDR.

We then built two AIS antennas to simulate a more accurate attack scenario. For the receiver, we used an omnidirectional antenna consisting of a 5 element collinear structure, i.e. a standard installation for ships and VTS. For the attacker, we used a Moxon directional antenna in order to sustain the amplified signal and improve the attacker's coverage and precision. The power gain of our antennas was respectively 6 and 10 dBi.

As we already mentioned, our coverage experiment consisted of transmitting a testing message from a fixed station and of using a movable receiver to verify the coverage experimentally. By using different configurations, as we report in Table 2, we showed that an attacker is able to reach a victim station and convey AIS messages from a distance of approximately 16.5 kilometers, at the least.

For example, by substituting the transmitter's default antenna ($\lambda/4$[29]) with the directional one that we built, the coverage doubled, i.e. from 0.8 to 1.5 kilometers. Further improvements are confirmed when the amplifier is used. Note that our amplifier comes with two selectable output power levels of 5 W and 15 W. These values are in the same order of standard AIS transponders, i.e. class-B and class-A respectively. In these condition, we scored a coverage of 8 and 16.5 kilometers. Note that this value is a lower estimation because our testing site was located near mountains that attenuated the signal we transmitted.

7. RESPONSIBLE DISCLOSURE AND MITIGATION STRATEGIES

Clearly, generating and tampering with AIS information may raise ethical concerns. As researchers, we are fully aware of that and we believe that realistic experiments, like the ones conducted by Jakobsson et al. in [12, 13], are the only way to reliably evaluate attacks in a real-world.

During our experiments, we only used harmless and testing messages and we did *not* interfere with existing systems. We also physically connected our equipment, i.e. *AISTX* and receivers, in order to *not* propagate RF signals over the air. The coverage experiment was conducted on land (at the coordinates 45.69N,9.72E) and we verified that no AIS receiving installations were present by using information made public by online providers; the closest open water (Mediterranean Sea) was 200 kilometers away and all nearby waters were *not* navigable.

As part of responsible disclosure, we reached out upfront on September 2013 the affected providers[30] and involved standards organizations[31]. At the time of writing, we received positive feedback from Marine Traffic and Vessel Finder, and we are actively collaborating with IMO and ITU-R – The latest informed us that they will consider enhancements to AIS, in terms of security, at the World Radiocommunication Conference in 2015. We also shared our concerns with selected CERTs and coastguards, which are interested in discussing the problems with us, standards organizations and vendors.

In addition, we propose and share the following possible mitigation strategies.

Anomaly Detection This strategy consists of applying anomaly detection techniques to AIS data collected, e.g. by online providers and vessel traffic services, in order to detect suspicious activities like unexpected changes in vessels' route or static information. In addition, AIS data can be correlated with satellite information to find incongruities, for example the dimensions of a vessel. Although anomaly detection may be valuable in data collection systems, it seems not a solution for transponders installations on vessels, which remain vulnerable to RF-specific threats like availability disruption and SART spoofing.

X.509 PKI A complementary form of mitigation consists in adopting a public-key infrastructure schema in the AIS protocol used in the RF communications. We suggest X.509 [9], a well-known PKI standard, in which the digital certificates are issued by official national maritime authorities acting as certification authorities[32] and configured in a transponder concurrently with the other station's identifiers, i.e. MMSI and call-sign. X.509 provides authentication on messages exchanged among stations, e.g. between ships and with port authorities. The certificates are handled in two forms: certificates belonging to noteworthy stations like VTSs are preloaded via onshore installations, e.g. when a ship enters a port; generic certificates and certificates previously unknown to a station are exchanged with nearby stations (i.e., vessels in navigation) on demand, during the acquaintance phase of two vessels[33]. Vessels with satellite Internet access can additionally retrieve the certificates from online services.

8. RELATED WORK

A large body of literature focuses on correlating and analyzing ships information collected from vessel traffic services and online providers. Xianbiao et al. in [14] use online analytical processing (OLAP) to store, process and correlate information for collision avoidance and investigation. The same authors discuss in [19] different techniques to organize AIS-collected data in an efficient manner. Carthel et al. in [4] research on multi-sensor networks for data surveillance. They suggest to extend DMHT tracking, an algorithm originally designed for undersea surveillance networks, to AIS. Similarly, authors in [23] suggest ways to increase the maritime domain awareness (MDA) by collecting and using AIS data. Other applications consist of correlating oil slick shape and tracking data to identify ships illegally spilling oil in the sea [1] and of predicting the financial gain given by commercial trading [17]. With respect to navigational safety, most of the literature focuses on collision-avoidance systems and prevention, for example as reported in [15] and [16].

Despite the large body of AIS research, and to the best of our knowledge, we are the first to conduct a security evaluation of the automatic identification system. We use software-defined-radio to build a novel AIS *transmitter*, namely *AISTX*, and to show that our concerns are real. With respect to existing AIS receivers, we report [8], [18], [21], and [25]. Both

[29] For AIS, a $\lambda/4$ antenna measures 46 cm of length. Lambda corresponds to the wavelength (i.e., $c/162$ MHz.)

[30] Marine Traffic, AisHUB and Vessel Finder

[31] IMO, IALA and ITU-R

[32] The same organizations issuing MMSI and call-sign identifiers for AIS stations, e.g. the US Coast Guard or the Italian Ministry of Economic Development

[33] There is no need to exchange the certificates over trusted channels because counterfeiting will invalidate them

TX Antenna	RX Antenna	Amplifier	Output Power [W]	Coverage [Km]
Default ($\lambda/4$)	Omni		0.05	0.8
Directional	Omni		0.05	1.5
Directional	Omni	✓	5	8
Directional	Omni	✓	15	16.5

Table 2: Measured coverage.

gr-ais [8] and ais-tool [25] are software-based receivers built on top of GnuRadio. In particular, we used gr-ais in the hybrid receiver introduced in our radio-frequency evaluation. When compared with Guarnieri [6], our work looks at faults in the AIS's implementation and protocol specification, while his work focuses on data leaked from AIS data collected in Internet Census 2012[34].

Similarly to our research in smart transportation, Costin et al. [7] perform a security evaluation of ADS-B[35], a radio-frequency protocol used in aviation for data communication and monitoring. Using software-defined-radio, they show that ADS-B is vulnerable to eavesdropping, message jamming and replaying of injection. In a similar work, Teso [22] shows how to use ACARS[36] to upload malicious flight management system (FMS) plans to aircraft. More recently, Humphreys et al. in [20] introduce a software-based GPS transmitter to fool GPS communication and demonstrate how to hijack valid GPS signals to bring a ship off course.

9. CONCLUSIONS

AIS is a cyber-physical system commonly used in the marine industry for vessels traffic monitoring and assistance. Given its importance in collision detection, search and rescue operations and piracy prevention, we conducted a unique security evaluation of AIS. Using a software-based transmitter that we introduced, we discovered and experimentally proved that both the AIS's implementation and the protocol specification are affected by several threats, offering malicious actors many attack possibilities. We did responsible disclosure and notified upfront with mitigation strategies the affected providers and involved international organizations, with which we are currently and actively collaborating in order to improve the overall security. We hope that our research will help in this direction.

Acknowledgements The authors would like to thank Germano Valbusa – call sign IW2DCK – for contributing to the development of the amplifier (ref. Section 6.1). A special thanks goes to the Forward-Looking Research team and Trend Micro who supported the research in different forms. Finally, we thank the organizers of both Black Hat and Hack In The Box conferences for hosting our talk on AIS[37].

10. REFERENCES

[1] C. Ambjorn. Seatrack web forecasts and backtracking of oil spills. efficient tool to find illegal spills using ais.

[2] M. Balduzzi. Personal Page. http://iseclab.org/people/embyte/.

[3] Bloomberg. Iran Oil Tankers Said by Zanzibar to Signal Wrong Flag. http://www.bloomberg.com/news/2012-10-19/iranian-oil-tankers-said-by-zanzibar-to-be-signaling-wrong-flag.html.

[4] C. Carthel, S. Coraluppi, and P. Grignan. Multisensor tracking and fusion for maritime surveillance.

[5] C.-C. Chen, I.-T. Chen, C.-M. Cheng, M.-Y. Chih, and J.-R. Shih. A practical experience with rfid security.

[6] Claudio, Guarnieri. Spying on the Seven Seas with AIS.

[7] A. Costin and A. Francillon. Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices. In *BLACKHAT 2012*.

[8] N. Foster. GnuRadio AIS Receiver. https://www.cgran.org/wiki/AIS.

[9] R. Housley, W. Ford, W. Polk, and D. Solo. Rfc 5280: Internet X. 509 Public Key Infrastructure Certificate and CRL profile, 2008.

[10] R. S. I.-R. International Telecommunication Union. AIS AIVDM Message Types. http://www.navcen.uscg.gov/?pageName=AISMessages.

[11] ITU-R. Technical characteristics for an automatic identification system using time-division multiple access in the VHF maritime mobile band. http://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.1371-4-201004-I!!PDF-E.pdf.

[12] M. Jakobsson, P. Finn, and N. Johnson. Why and how to perform fraud experiments. *Security Privacy, IEEE.*

[13] M. Jakobsson and J. Ratkiewicz. Designing ethical phishing experiments: a study of (rot13) ronl query features. In *Proceedings of WWW 2006.*

[14] X. Ji, Z. Shao, J. Pan, and C. Tang. *A New AIS-Based Way to Conduct OLAP of Maritime Traffic Flow.*

[15] L.-n. LI, S.-h. YANG, B.-g. CAO, and Z.-f. LI. A summary of studies on the automation of ship collision avoidance intelligence. *Journal of Jimei University.*

[16] L. Li-na. Determination of the factors about safe distance of approach and etc on the research of ship automatic avoidance collision.

[17] B. L.P. Bloomberg Commodities. http://www.bloomberg.com/professional/markets/commodities/.

[18] K. F. Mathapo. A software-defined radio implementation of maritime AIS. https://scholar.sun.ac.za/handle/10019.1/2215.

[19] Z. Shao, C. Tang, J. Pan, and X. Ji. The application of database techniques in the integrated vessel information service system.

[20] D. P. Shepard, T. E. Humphreys, and A. A. Fansler. Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks.

[21] O.-S. Software. Gnu AIS. http://gnuais.sourceforge.net/.

[22] H. Teso. Aircraft Hacking - Practical Aero Series.

[23] B. Tetreault. Use of the automatic identification system (ais) for maritime domain awareness.

[24] TrendMicro. Security Intelligence Blog. http://blog.trendmicro.com/trendlabs-security-intelligence/category/internet-of-everything/.

[25] R. Undheim. Ais-Tools. http://www.funwithelectronics.com/?id=9.

[26] F. van den Broek. Eavesdropping on gsm: state-of-affairs. 2011.

[34] http://internetcensus2012.bitbucket.org/paper.html

[35] Automatic Dependent Surveillance-Broadcast

[36] Aircraft Communications Addressing and Reporting System

[37] The slides are available on the personal page of one of the authors [2].