A Trend Micro Research Paper

A Security Evaluation of AIS

Marco Balduzzi and Kyle Wilhoit
Trend Micro Forward-Looking Threat Research Team
Alessandro Pasta
Independent Researcher

CONTENTS

INTRODUCTION

Automatic Identification System (AIS) refers to a system introduced to enhance the safety of vessel traffic by automatically exchanging up-to-date information as well as tracking and monitoring ships. Since 2002, AIS has been a mandatory installation for international voyaging ships weighing (i.e., gross) at least 300 tons[1] and all passenger ships, regardless of size. Because it has been found useful to the maritime industry, even leisure crafts and fishing boats are now often equipped with AIS. With an estimated number of over 300,000 installations, according to a popular provider [1], AIS is currently an important and widely used technology and solution in smart transportation. It aids in traffic monitoring, collision avoidance, search-and-rescue (SAR) operations, accident investigation, and navigation. The number of AIS-equipped vessels may be higher because they are not required to register with online service providers.

AIS works by acquiring Global Positioning System (GPS) coordinates and exchanging current and up-to-date information (i.e., vessel traffic services [VTSs] located onshore) with ships and maritime authorities via radio transmission. AIS information includes but is not limited to ships' positions, names, and cargo, which aids in navigation. Port authorities frequently use AIS to warn ships about hazards, low tides, rocky outcroppings, and shoals that are commonly found at sea. In open sea, AIS-enabled distress beacons are used to signal and locate men who have fallen overboard. Providers operating online collect and exchange AIS data with one another for visualization, monitoring, and reporting purposes for free or commercially.

Given its primary importance and prevalence in maritime traffic safety, a comprehensive security evaluation of AIS was essential. We assessed the system from both a software and a hardware (i.e., radio frequency [RF]) perspective. Overall, we identified threats that affected AIS implementation and protocol specifications. These include disabling AIS communications (i.e., denial of service [DoS]); tampering with existing AIS data (i.e., modifying information ships broadcast); triggering SAR alerts to lure ships into navigating to hostile, attacker-controlled sea space; or spoofing collisions to possibly bring a ship off course. Interestingly, according to Bloomberg [2], AIS has been found to be polluted with counterfeit information (i.e., Iranian ships flagged as belonging to Zanzibar when the United States and Europe tightened sanctions related to nuclear programs).

In sum, the researchers:

- Conducted a security evaluation of AIS—a cyberphysical system (CPS) introduced to enhance vessel tracking and provide additional maritime traffic safety on top of conventional radar installations
- Designed and implemented a novel software-based AIS transmitter called "AISTX"
- Identified and verified several threats that affected existing AIS implementations and protocol specifications
- Notified and actively collaborated with affected providers, international standards organizations, and

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

community emergency response teams (CERTs) to improve the overall AIS situation

This research paper provides a general overview of the issues identified throughout the course of conducting research, including software-based threats. It also introduces and provides details on AISTX, the specially crafted AIS transmitter for RF evaluation, in detail. Finally, ethical implications, mitigation strategies, and collaboration with affected parties were also examined.

AIS

Since the 2002 International Maritime Organization (IMO) Safety on Life at Sea (SOLAS) convention [3], AIS has been required for international voyaging ships weighing (i.e., gross) 300 tons or more and all passenger vessels, regardless of size. Wide use and proven benefits to the maritime industry led to the introduction of second-generation AIS devices, termed "class-B transponders," in 2006. Compared with their predecessors (i.e., class-A transponders), class-B transponders were smaller, less expensive, and simpler to operate. Class-B transponders are typically used in smaller, leisure or fishing vessels weighing less than 300 tons. Since 2010, AIS-related regulations have been constantly adjusted to make the system easier to implement and deploy. At present, AIS is said to run on at least 300,000 vessels. In the near future, close to a million installations are expected.

AIS is currently a major technology and solution in traffic monitoring and vessel assistance. Shipowners and maritime authorities rely on AIS to supplement traditional radars for collision avoidance and location tracking, in addition to complementary systems for visual observation, audio exchange, and long-range identification and tracking (LRIT).

AIS boasts of several benefits. Any ship transmitting an AIS signal can be located by nearby ships. AIS also aids in navigation. It follows the Aids to Navigation (AtoN) standard, which was developed to broadcast the positions and names of objects other than vessels (e.g., navigational aids and marker positions) and dynamic data reflecting the markers' environments (e.g., currents and climatic conditions). These aids can be located onshore such as a lighthouse or on water such as buoys. Examples of AtoN installations are provided by online AIS providers such as MarineTraffic.com[2].

One of the most important uses of AIS is related to accident investigation. Since AIS provides GPS coordinates, course, ground speed, and additional information, it has proven more valuable in accident investigation compared with the widely used but less accurate radar technology today. Because of this, AIS is widely used in SAR transponders (SARTs). AIS-SARTs are self-contained, waterproof devices intended for emergencies. They primarily aid in detecting and locating vessels and people in distress (i.e., men who have fallen overboard).

2 http://www.marinetraffic.com/en/ais/index/lights/all

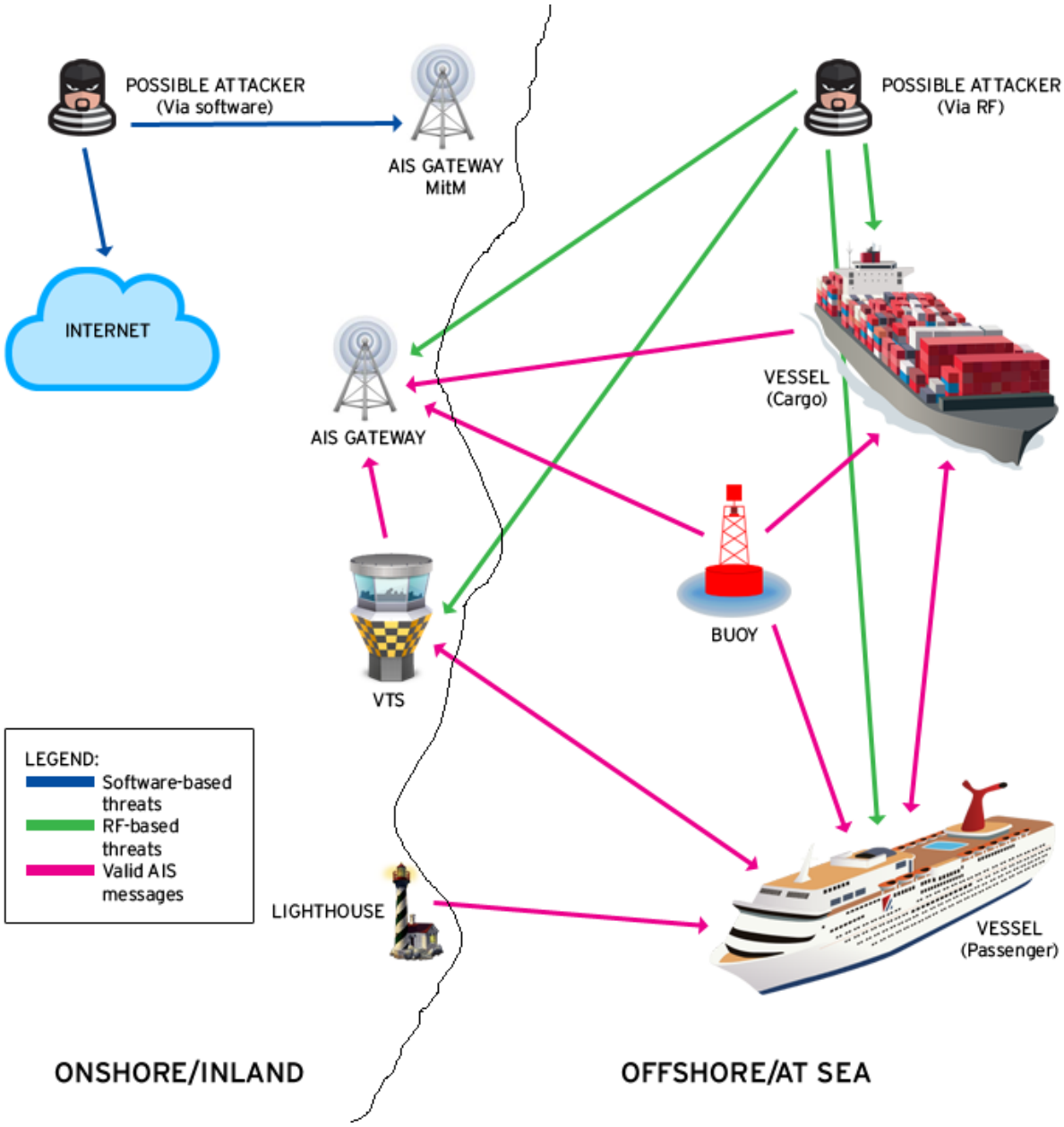

Figure 1: *Possible AIS attack scenarios*

AIS acquires GPS coordinates and exchanges regional information with nearby stations via VHF (i.e., two radio channels operating at 161.975MHz and 162.025MHz with AIS providers operating online) as shown in Figure 1. The providers primarily collect data through geographically deployed AIS gateways (i.e., along coastlines and via VTSs operated by port authorities). A VTS is a ship-traffic-monitoring system used by maritime authorities. It can be likened to an air traffic control system for aviation. Single individuals such as a ship's captain can also share AIS data with desired providers via a mobile app and a special forwarding application that duplicates and sends information as soon as it becomes available.

AIS information is broadcast, collected, and exchanged on a regular basis. The time intervals vary from a couple of seconds to minutes, depending on the type of

information and condition of a station. For example, a class-B-transponder-equipped ship navigating faster than 23 knots is supposed to broadcast its position every 5 seconds. Conversely, an AtoN such as a lighthouse or a buoy sends hazard notifications every 3 minutes.

By regulation, each communicating station such as a ship is required to register and obtain valid AIS identifiers—Maritime Mobile Service Identity (MMSI) number and call sign, which are issued by official maritime authorities such as the U.S. Coast Guard or the Italian Ministry of Economic Development. MMSI refers to a nine-digit number that uniquely identifies a station. Its first three digits known as "maritime identification digits (MID)" specify the country (e.g., 247 for Italy and 338 for the United States, according to ITU-R [4]. Call signs, meanwhile, are radio designations or AIS stations willing to communicate with marine, aviation, military, and spacecraft personnel and radio amateurs.

AIS information is rendered via chart plotters or providers (e.g., Vessel Finder) in near real-time. It visualizes the status of other vessels in the region, navigation aids, and other useful maritime information such as weather forecasts or critical situations. Providers allow worldwide access to AIS statistics; vessel, lighthouse, and buoy locations; and corresponding details via a simple, easy-to-navigate display or website. AIS information collected from providers can be used to identify ships spilling oil at sea [5] and predict financial gains that can be obtained via marine trading [6].

AIS-RELATED THREATS

This section provides an overview of the AIS-related threats that we have identified over the course of conducting research. As shown in Table 1, there are three macrocategories of threats—spoofing, hijacking, and availability disruption. We analyzed each threat in detail to determine if it is software or RF based or both. Figure 1 shows how attackers fit in the AIS infrastructure. Software- and RF-based AIS threats will be discussed in even more detail in later sections. Note that software-based threats will be discussed in a separate section.

TABLE 1
Summary of Identified AIS-Related Threats

Macrocategory	Threat	Software Based	RF Based
Spoofing	Ship spoofing	Yes	Yes
	AtoN spoofing	Yes	Yes
	SAR spoofing	Yes	Yes
	Closest point of approach (CPA) spoofing	No	Yes
	Distress beacon spoofing	No	Yes
	Faking weather forecasts	No	Yes
Hijacking	Hijacking	Yes	Yes
Availability disruption	Slot starvation	No	Yes
	Frequency hopping	No	Yes
	Timing attacks	No	Yes

RF-Based AIS Threats

CPA SPOOFING

Collision avoidance is one of the primary objectives of using AIS, especially in open sea where port authority monitoring does not occur. AIS allows precise vessel tracking and identification within RF coverage, allowing safer navigation when used with traditional preventative mechanisms such as visual observations, audio exchanges, and radars. AIS, in fact, allows automatic response when a collision is detected or expected. CPA works by computing the minimal distance between two ships, at least one of which is in motion. CPA can be configured to trigger an alert (e.g., visually on the captain's console or acoustically via a siren) when a possible collision is detected so the ship can change course.

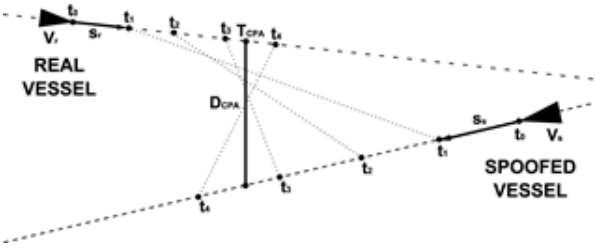

Figure 2: *CPA algorithm*

The CPA algorithm shown in Figure 2 allows ship captains to compute how much time and distance is left before they collide with another ship, assuming that the vessels are traveling at fixed speeds and courses. A CPA alarm is triggered if one of the two parameters is lower than the transponder's configured thresholds. T_{CPA} refers to the amount of time left before reaching the CPA point, D_{CPA} refers to the distance between the vessels before they reach the CPA point, $w(t_i)$ refers to the distance between the vessels at a certain time (t_i), and S_r and S_s are the vessels' vectors.

$$\begin{cases} T_{CPA} = \dfrac{-w(t_i)(S_r - S_s)}{|S_r - S_s|^2} \\ D_{CPA} = |w(t_i) + T_{CPA}(S_r - S_s)| \end{cases}$$

CPA spoofing involves faking a possible collision with a target ship. This will trigger a CPA alert, which could lead the target off course to hit a rock or run aground during low tide.

AIS-SART SPOOFING

Apart from collision avoidance, AIS also aids in SAR operations. SARTs are self-contained, waterproof devices that aid in detecting and locating vessels and people (e.g., men who have fallen overboard) in distress during emergencies. They use radio-beacon systems similar to mountaineering equipment to locate and rescue avalanche victims.

Figure 3: *Sample AIS-SARTs used in life vests (left) and lifeboats (right)*

AIS-SARTs such as those shown in Figure 3 are automatically activated when they come in contact with water and send distress radio beacons, followed by GPS coordinates, which help rescuers locate survivors. They were created to make up for the limitations of traditional radar-SARTs (e.g., emergency locator transmitters [ELTs]), which are more imprecise in locating survivors.

AIS-SART spoofing involves generating false distress beacons for men who have fallen overboard in specially chosen coordinates by attackers. AIS transponders are required to generate alerts when they receive distress messages. Attacker (e.g., pirates) can trigger SART alerts to lure victims into navigating to hostile and attacker-controlled sea spaces. Note that by law, vessels are required to join rescue operations when they receive SAR messages. Given the increasing number of piracy attempts (e.g., in the Gulf of Guinea and Somalia [7]), spoofing distress beacons can be an additional piracy tool.

FAKING WEATHER FORECASTS

AIS also communicates dynamic data to reflect changing environment conditions such as currents and the weather. It uses a special message format—binary—to convey this kind of information.

Faking weather forecasts involves announcing false updates such as a sunny day when a squall is actually expected.

AVAILABILITY DISRUPTION

Availability disruption attacks can be categorized into three kinds. Their practical implementations will be described in more detail later in this paper.

- **Slot starvation:** This involves impersonating maritime authorities to reserve the entire AIS transmission "address space" in order to prevent all stations within coverage from communicating with one another. These stations include ships, AtoNs, and AIS gateways, which are used in traffic monitoring. As a result, attackers can disable AISs on a large scale.

- **Frequency hopping:** Attackers impersonate maritime authorities to instruct one or more AIS transponders to change the frequencies on which they operate. Because receiving stations are mandated to follow maritime authorities' instructions, frequency-hopping attacks remain persistent. System rebooting does not help because receiving stations can only change frequencies if instructed.

  Frequency-hopping attacks can be contained to within certain geographical regions. Attackers can "program" target ships to switch frequencies when they reach certain regions of their choice, rendering AIS useless. Note that class-B transponders cannot be manually reset. Users do not even get notified of frequency changes.

- **Timing attacks:** Malicious users can instruct AIS transponders to delay transmission times by simply renewing commands, thus preventing further communications about vessels' positions. This allows vessels to "disappear" from AIS-enabled radars. Attackers can also overload (i.e., flood) marine traffic, including ship and VTSs, by requesting existing stations to send AIS information and updates very frequently.

Software- and RF-Based Threats

SHIP SPOOFING

Ship spoofing refers to the process of crafting a valid but nonexistent ship. It involves assigning static information such as vessel name, identifiers (i.e., MMSI and call sign), flag, ship type (e.g., cargo), manufacturer, and dimensions as well as dynamic information such as ship status (e.g., underway or anchored), position, speed, course, and destination to the fictitious ship. Apart from ships, aircraft involved in SAR operations can also be spoofed. In fact, SAR

aircraft are mandated to be equipped with AIS class-B transponders.

Ship spoofing provides attackers a wide range of malicious attack scenarios to play with. They can make vessels look like they are within the jurisdiction of an adversarial nation or carrying nuclear cargo while sailing the waters of a nuclear-free nation. Ship spoofing could cause issues for automated systems identifying data and making inferences based on collected AIS information. These systems could be detecting ships spilling oil in open sea or predicting marine trading. Attackers can fake information to blame another vessel, for example.

AtoN SPOOFING

AtoNs are commonly used to assist in vessel traffic management along channels or harbors or warn about hazards, low tides, rocky outcroppings, and shoals in open sea. AtoN spoofing refers to the process of crafting fake information to lure target ships into making wrong maneuvers. Attackers can place one or more fake buoys at a harbor entrance, for example, to tamper with traffic or trick ships into navigating in low waters. Given the number of different AtoNs, attackers can craft several attack scenarios as with ship spoofing.

AIS HIJACKING

AIS hijacking involves altering any information about existing AIS stations (e.g., cargo, speed, location, and country). Attackers can maliciously modify the information provided by AtoNs installed in ports by authorities for vessel assistance and monitoring.

In the software variant of hijacking, attackers can eavesdrop (i.e., man-in-the middle [MitM] attacks) on ongoing communications and arbitrarily replace AIS information. In the RF version, meanwhile, attackers can override original AIS messages with higher-powered fake signals. In both cases, recipients receive attacker-modified versions of victims' original AIS messages.

AIS hijacking allows malicious users to alter any information about real vessels. Attackers can, for example, "move" military ships to within the jurisdiction of adversarial nations, causing political tensions.

SOFTWARE EVALUATION

Three popular online AIS providers—MarineTraffic.com, AIS Hub, and Vessel Finder—were examined to determine how and if they could be affected by software-based threats.

AIVDM Protocol and Message Types

AIVDM refers to the application layer protocol AIS uses to exchange data sentences (i.e., from vessels' AIS transponders broadcasting their positions or VTSs monitoring ships at port).

TABLE 2
AIVDM Message Types

Type	Category	Description
1	Normal	Position report for class-A transponders
8	Control	Binary message
16	Control	Assignment mode command
18	Normal	Position report for class-B transponders
21	Control	AtoN report
22	Control	Channel management
23	Control	Assignment command
24	Normal	Static data report

AIVDM has 27 specific message types, each of which has a corresponding purpose and value that designates said purpose. Table 2 provides an overview of the main AIVDM message types [8]. Ships and VTSs use message type 1 to exchange up-to-date position reports. All AIS transponders support this message type, along with message type 24. Message type 24 describes ships' type (e.g., passenger; cargo; tanker; law

enforcement; military; SAR; or carrier of dangerous goods, harmful substances, and marine pollutants), cargo, dimensions, and name.

In addition to the above-mentioned message types, so-called "control messages," which are reserved for port authorities and cannot be transmitted by transponders, also exist. Control messages are used to control maritime traffic and are given higher priority with respect to normal AIS messages (e.g., position reports). VTSs that operate as controllers can ask ships at port to switch to different operating frequencies using message type 22. Another form of control message is binary (i.e., message type 8), which software use to exchange generic information. One common application of binary is when weather forecasts are broadcast[3].

AIVDM is a two-layer protocol. The outer layer is a variant of National Marine Electronics Association (NMEA) 0183—an ancient standard for data exchange in maritime navigation systems [9]. Listing 1 shows two examples of AIVDM sentences.

```
!AIVDM,1,1,,A,16SteH0P00Jt63hHaa6SagvJ087r,0*42
   MessageType:        1
   MMSI:               440348000
   NavigationStatus:   0
   Speed Over Ground:  0
   Longitude:          -70.7582
   Latitude:           43.08015
   Course Over Ground: 93.4
   TrueHeading:        511

!AIVDM,1,1,,A,H42O55i18tMET00000000000000,2*6D
!AIVDM,1,1,,A,H42O55lti4hhhilD3nink000?050,0*40
   MessageType:        24
   MMSI:               271041815
   Name:               PROGUY
   ShipAndCargo:       60
   VendorID:           1D00014
   CallSign:           TC6163
   Dimensions:         15x5
```

***Listing 1:** Sample AIVDM sentences for position (top) and static (bottom) reports*

3 IMO 236 and 289 met/hydro messages

The first sentence is for a position report for a class-A ship navigating in Antarctica while the second is for a static report of a Turkish passenger vessel called "PROGUY." One can tell that PROGUY is a Turkish vessel because its MDI is 271. Looking at the message format, the main comma-separated fields are fields 2 and 3 for fragmentation (i.e., not seen in the examples), field 5 is the radio channel code (i.e., channel A, 161.975MHz in default condition), and field 6 is the data payload [10].

For our experiments, we implemented an encoding tool written in Python called "AIVDM Encoder" to generate arbitrary AIVDM sentences and conduct both software- and RF-based evaluations of AIS.

Software-Based AIS Threats

While AIS installations on ships require hardware, they also need software to provide 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 information, which introduces several security issues.

AIS providers allow various ways of collecting AIS data such as sending preformatted emails as well as using mobile apps[4] and forwarding software such as AIS Dispatcher[5]. When AIS messages are generated, the forwarding software duplicates and sends them to the desired providers (e.g., over UDP/5321 for MarineTraffic.com). The interval at which messages are forwarded can be established to provide near real-

4 http://www.marinetraffic.com/ais/iphone.aspx

5 https://www.marinetraffic.com/files/AIS_Dispatcher_setup_guide.pdf

time statistics to AIS providers. The same software can be used to send AIS messages received from AIS gateways (i.e., local VHF receivers users have at home). Gateways are often located along coastlines and present in VTSs port authorities operate.

Analysis revealed security issues with regard to all three online providers. They do not vet sources, for one. They do not check if messages really originate from the vessels supposedly sending them. They have no means to authenticate the AIVDM sentence senders, which could allow attackers to carry out spoofing and MitM-style attacks.

We took a look at spoofing first. We crafted valid AIS information (e.g., a nonexistent ship or AtoN) from nowhere near a body of water or a real AIS station. To do this, we generated an innocuous sentence indicating a low tide in a nearby lake using AIVDM Encoder. We sent the information to the three providers using a generic networking client. Note that message type 21 is reserved for AtoN reports while type 13 is used for buoys. As specified in protocols, AtoN MMSI numbers should take a certain form, which we used.

```
$./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 2: *UDP spoofing sample sentence for MarineTraffic.com*

Next, we generated a preformatted email report for a moored vessel and sent it to the receiving address of the target provider.

```
To: report@marinetraffic.com

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

Listing 3: *Email spoofing sample sentence for MarineTraffic.com*

Finally, we implemented an automated script to spoof an AIS station that follows a path over a certain period of time (e.g., a fictional generic ship spelling "PWNED" in the Mediterranean Sea as shown in Figure 4). All of the experiments were successful. We were able to spoof and send valid AIS messages to the three providers.

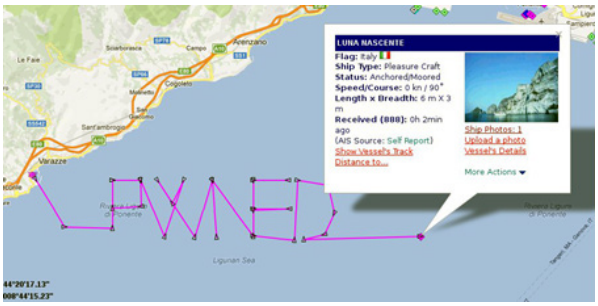

Figure 4: *Spoofed ship following a programmed path*

MitM attacks involve modifying or injecting erroneous data into AIS communications coming from stations that transmit valid AIVDM sentences. First, we physically intercepted valid AIVDM sentences transmitted over the air from a nearby station (i.e., our AIS transponder[6]) by deploying an AIS gateway we controlled. We configured it with AIS Dispatcher and a USB dongle AIS receiver[7]. We then used a proxy server to intercept, modify, and send AIS messages to the online providers, which accepted them.

In a second experiment, we selected a ship each online provider tracked[8] and modified its information via a software-based attack. We successfully caused the providers to show the ship in a different location from where it initially was.

6 Note that for ethical implications, we used our own AIS transponder for all experiments.
7 http://opencpn.org/ocpn/node/176
8 We sent the real position broadcast using our transponder.

AIS TRANSMITTER

This section focuses on RF-based threats. We designed and implemented a system to generate and transmit arbitrary AIS messages over the air. We used this system in our experiments, which will be discussed in more detail later.

Architecture

AISTX—our AIS transmitter—was designed and implemented as a software-defined radio (SDR). While traditional radios—both receivers and transmitters—are built-in hardware, SDRs have most of the circuitries needed for over-the-air transmission (e.g., modulation, mixing, and filtering) implemented in software. The introduction of SDRs made transmitting over the air easier and more accessible, reducing the need for specific hardware and measuring instrumentations. In fact, developing new radio applications is entirely done via software today. The advent of SDR has made maintenance much easier as well. In the past, any functional or frequency change required complete hardware design, development, and testing. Debugging has become quicker and simpler to do in software than hardware, which requires expensive and difficult-to-use electronic laboratory instruments and development kits.

An SDR consists of a software application that implements the signal elaboration chain and a hardware peripheral that converts binary data into RF signals for over-the-air transmission. The growth of PCs' computational capabilities and the decline of hardware acquisition costs have made SDR peripherals (e.g., universal software radio peripheral [USRP]) available at affordable prices.

AISTX was built on top of GNU Radio[9], an open source framework widely used to design and implement efficient SDRs. While it has been extensively used to conduct research on evaluating the ADS-B aviation protocol [11], Global System for Mobile Communication (GSM) security [12], and RF identification (RFID) use in TaipeiPass [13], we believe this is the first research that adopted GNU Radio to build an AIS transmitter.

With GNU Radio, an SDR is normally drafted as a flowchart of connected functional blocks that each performs a single operation such as filtering or modulating signals. The flowchart is then converted into an SDR application. In this process, GNU Radio provides the ability to modify an existing block or add a new one if additional functionalities are required (e.g., building an AIS frame).

9 http://gnuradio.org

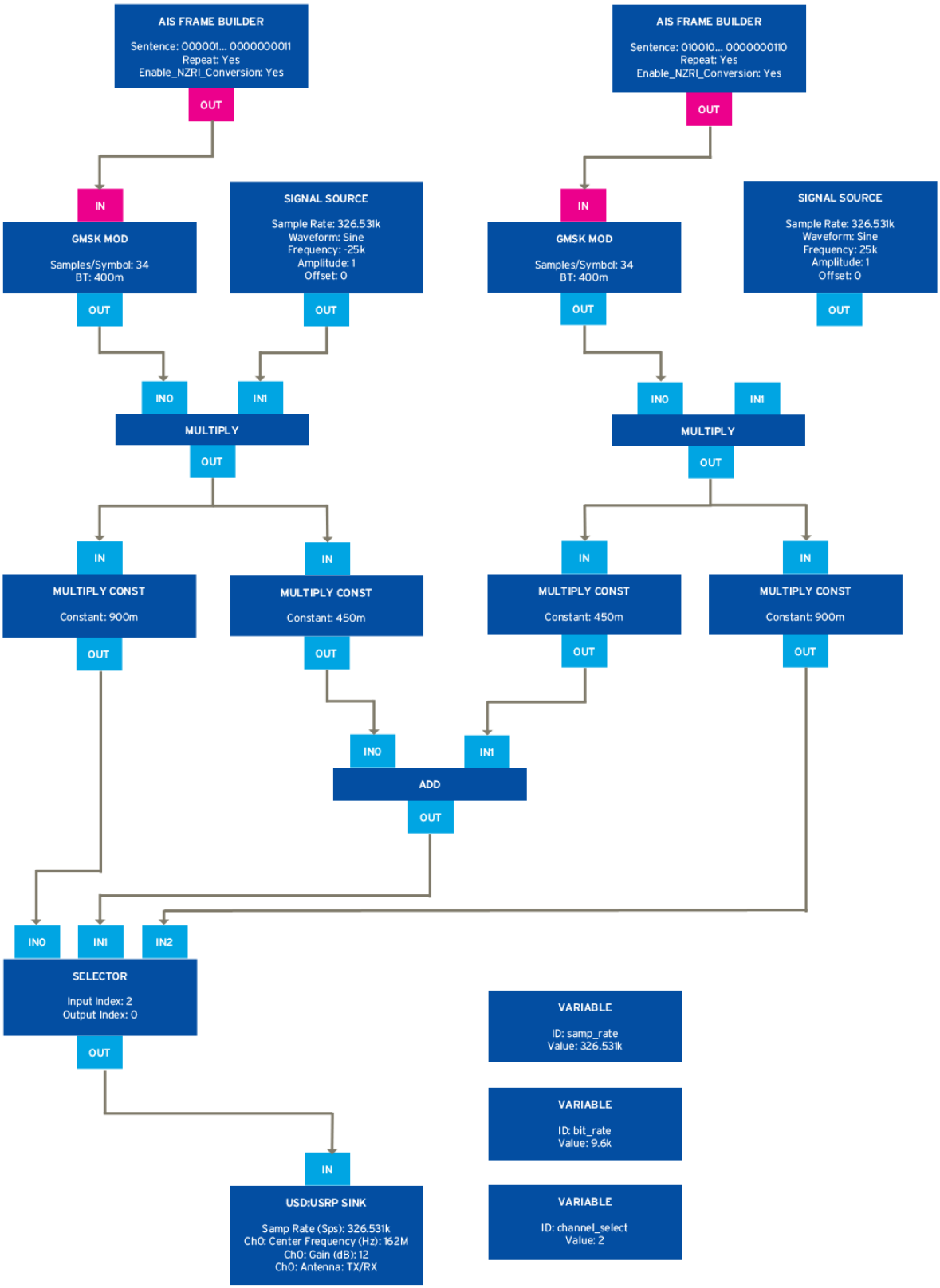

Figure 5: *AISTX architecture on GNU Radio*

Figure 5 shows that AISTX has two branches that implement two AIS channels. The upper branch implements channel A (i.e., 161.975MHz) and the lower, channel B (i.e., 162.025MHz). Transmissions are independent of each other (i.e., different messages can be simultaneously transmitted on both channels). This functionality is required to perform some of the attacks featured in this paper (e.g., hijacking existing communications between AIS stations).

AISTX generates AIS frames with a block called "AIS Frame Builder," which will be described in more detail later. Gaussian Minimum Shift Keying (GMSK) modulation of each frame is then performed over the two AIS channels. GMSK is a widely used form of digital modulation in mobile communication (e.g., in GSM and Digital Enhanced Cordless Telecommunications [DECT] transmission). The GMSK modulator is configured with parameters following AIS specifications [14]—a bandwidth-time product (BT) of 0.4, a bit rate (R) of 9,600bps, and the rounded-off samples/symbol ratio.

The modulated frames generated at baseband are then transposed to the default operating frequencies that AIS specifications dictate. First, we modulated the baseband signal around the frequencies of ±25KHz by multiplying it by 2 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 was reduced from ±1 to ±0.9. Finally, the resulting signal was shifted to the carrier frequency of 162MHz, resulting in two signals over the standard AIS frequencies—161.975MHz and 162.025MHz. The UHD:USRP Sink block acted as the driver for the SDR peripheral.

Building an AIS Frame

Although GNU Radio comes with a wide range of commonly used predefined blocks (e.g., filters, signal generators, and converters), for our purposes, we extended the suite with a custom block called "AIS Frame Builder," which served as an AIS frame generator.

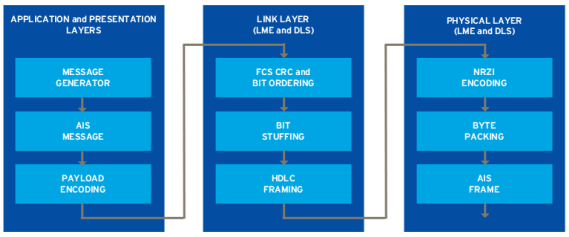

Figure 6: *AIS Frame Builder block components*

As shown in Figure 6, AIS Frame Builder implements the full AIS stack. It comprises three main components covering the application/presentation, link, and physical layers, following AIS protocol specifications. It takes as input an AIS message in AIVDM format. It encodes the message using a 6-bit ASCII alphabet. Only capital letters are supported (i.e., lowercase letters are replaced with uppercase ones). Numbers are written as decimals while negatives are expressed as two's complements. Padding with zeroes to multiples of 8 bits is then done for further processing. A short alphabet is used to reduce the average message length transmitted over the air.

In the link layer module, we computed a frame check sequence of the previous AIS-encoded message (i.e., the payload) using a 16-bit polynomial cyclic redundancy check. Receivers use this to validate the integrity of AIS messages. We also reordered the bits of the payload from big-endian to little-endian as specified. Bit stuffing—a technique that involves inserting a 0 if five consecutive ones 1s are found in the bit stream—is then done. Bit stuffing reduces errors in communication and ensures that the High-Level Data Link Control (HDLC) information is always in the same position.

This control information is added during HDLC framing and consists of a training sequence and a start/ending flag. The

training sequence comprises 24 bits of alternating 0s and 1s (i.e., 010101010...) and is used to synchronize receivers to data streams. The start/end flag consists of an 8-bit pattern (i.e., 01111110 [0 x 7E]) and is used to delimit the payload portion. Although this flag consists of 6 bits of consecutive 1s, it is not subjected to bit stuffing because it is meant to act as a delimiter. HDLC is used to synchronize senders and receivers and permits synchronous, code-transparent data transmission. This concludes the operation carried out in the link layer module.

Finally, the physical layer prepares the frame for GMSK modulation, which takes place after the AIS transmission chain described earlier. The data is encoded using nonreturn-to-zero inverted (NRZI) mapping, a method for mapping binary digits into a physical waveform that has 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 keeping the signal at a certain level whenever a logical 1 is transmitted. Note that AIS, similar to a USB, adopts a reverse transition convention with respect to the common use of NRZI.

The frame is then packed (i.e., transformed from a bit to a byte representation) to fit the modulation requirements of the following GMSK block.

RF EVALUATION

Our RF evaluation consists of two experiments. First, we conducted an in-lab experiment where we used three AIS receivers to verify if our transmitter works well and can be used to perform the attacks we identified. Later, we conducted a coverage assessment to verify if malicious actors can perform such attacks in an open-air environment such as onshore or in open sea against real vessels and authorities.

Our experiment setup consisted of a transmitter acting as an attacker and a receiver acting as a victim (e.g., a vessel or a VTS).

We used a standard Linux machine running AISTX together with a USRP device (i.e., a commonly used and well-supported SDR peripheral for transmitting signals over the air) as transmitter. Our USRP consisted of an Ettus USRP B100 Version 2[10] with a WBX-model daughterboard[11] as shown in Figure 7. This device was well-suited to our requirements because it supports VHF maritime frequencies.

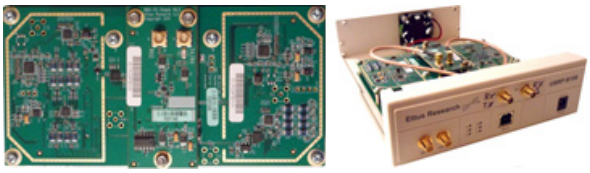

Figure 7: *USRP device used in the RF evaluation—WBX daughterboard (left) and Ettus USRP B100 Version 2 (right)*

From a receiver standpoint, we evaluated our ability to generate AIS signals over three distinct AIS receivers—Weatherdock EasyTRX2[12], a commercial and standard class-B transponder; AIS em-track R100[13], a hardware receiver; and a hybrid receiver (i.e., both hardware and software). The latest is based on a software-based AIS receiver and a standard YAESU VHF radio that was modified by adding an additional output port to interface the radio with a computer's audio port and bypass the final-stage audio filter. Note that we connected receivers and transmitters using physical cables to prevent any signal from being sent over the air[14]. The receivers' behaviors were analyzed in three ways—at the hardware, presentation, and application layers.

From a hardware standpoint, we equipped the AIS receivers with alarms to observe the behavior of a transponder installation when an attack occurs. At the presentation layer, we used the serial port provided by the AIS receivers to monitor the receipt of AIS messages. The serial port allowed us to 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-plotting software (i.e., OpenCPN[15]) to evaluate the receivers' behaviors at the application layer. OpenCPN implements a fully functional chart plotter for PCs and supports all AIS message types, including SART and CPA alerts. We used OpenCPN to visually render the results of the malicious messages received (i.e., impersonating onboard computers normally installed on vessels). Along with OpenCPN,

10 https://www.ettus.com/product
11 https://www.ettus.com/product/details/WBX
12 http://www.easyais.de/en/product_page.php?prodid=33
13 http://www.em-trak.com/PRODUCTS/Receiver/Receiver.aspx
14 A 90dB inline attenuator was installed to reduce the transmitter's power according to the receivers' specifications.
15 http://www.opencpn.org

we also used the official monitoring tool that came with EasyTRX2 for spoofing attacks[16] to understand how targets were affected by misleading transmissions.

To begin the evaluation, we provided AISTX valid AIVDM sentences for spoofing attacks. We created a fake Italian vessel (i.e., with MMSI prefix, 247) navigating east at a certain speed from a set of coordinates.

```
$ ./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 4: *RF-based ship spoofing static (top) and dynamic (bottom) reports*

Figure 8 shows that the receiver correctly interpreted the spoofed vessel as a valid one and reported it on the monitoring tool. The same attack methodology worked well when generating different ship types (e.g., law enforcement, military, SAR, dangerous-goods carrying, etc.) and AtoNs (e.g., buoys, SAR aircraft, etc.). This gave attackers the ability to inject malicious and bogus information into AIS traffic to target both vessels and authorities.

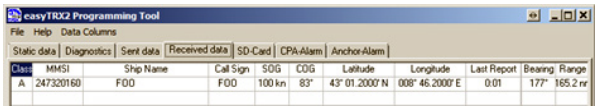

Figure 8: *EasyTRX2 monitoring tool correctly interpreting a spoofed vessel*

We then tried CPA spoofing. We faked a collision with our AIS transponder. We used the coordinates and course of a target transponder to fake a ship navigating to within the CPA threshold space we configured.

Figure 9 shows the result of the experiment. On the top-right window, attackers sent a spoofed vessel’s position report to the target. On the bottom-right window, a signal light was triggered because the spoofed ship is expected to collide with our vessel. The OpenCPN monitoring console (i.e., left window) confirmed the alert by informing us that a collision is expected to occur in 2 seconds (i.e., the spoofed ship was 6 meters away). Depending on how a vessel was configured, such an attack can cause a target vessel to go off course.

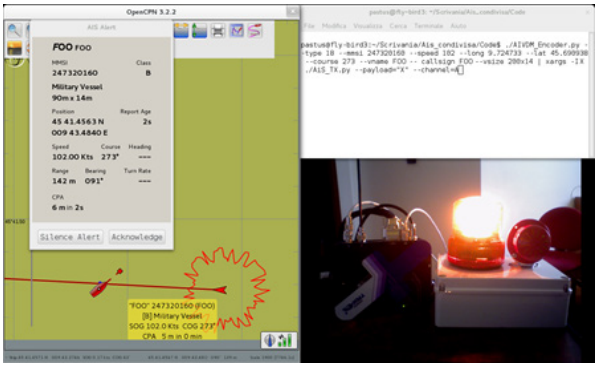

Figure 9: *CPA alert was triggered (i.e., shown via a signal light and OpenCPN)*

We confirmed that faking weather forecasts could be performed as well. We used a chart-plotting software that supports AIS binary messages, which are normally used by port authorities to issue weather forecasts (i.e., message type 8). This verified that weather-specific AIVDM sentences spoofed via RF were correctly interpreted by AIS receivers and reported by monitoring tools.

Attackers can generate SAR messages to trigger a SART alert to lure victims into navigating toward specifically chosen coordinates. AIS stations are mandated to trigger alerts when they receive distress beacons (i.e., informing captains that a rescue operation is needed for a man who fell overboard). Our experiments verified that we could appropriately spoof SAR messages and trigger SART alerts on our three AIS receivers (i.e., both visually and acoustically).

We emulated an AIS-SART transmitter for both AIS channels with an MMSI number in the specified form. We used the prefix

16 http://www.easyais.de/files/product_sofwtare/Softwarepacket_130927_0.zip

reserved for AIS-SARTs, as opposed to other MMSI prefixes that specify the countries that vessels are from.

```
$ ./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 5: *RF-based SART spoofing*

We created fictional ships, buoys, and other AIS stations to show that spoofing attacks are real and can affect the standard AIS transponders used worldwide.

Figure 10 shows how AIS hijacking occurs. For illustration purposes, we named the victim, "Bob"; the receiver installed onshore and manned by authorities, "Alice"; and the attacker located within Alice's RF coverage, "Mallory." Mallory, pretending to be Bob, generates a modified AIS message for Alice. To do this, Mallory overrides Bob's legitimate communication by transmitting messages with more power. Using a physical cable, we connected Bob's AIS transponder and Mallory's SDR transmitter to Alice's receiver ports. We simulated Bob's lower output power compared with Mallory's by installing a 120dB attenuator to the connection with Alice (i.e., 30dB attenuation more than Mallory's). By monitoring Alice's receiver, we proved that Mallory could override Bob's signal (i.e., to tamper with valid AIS information sent via RF).

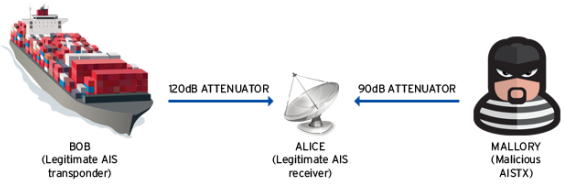

Figure 10: *RF-based AIS hijacking*

Next, we verified availability disruption attacks using a particular class of AIS messages reserved for port authorities and not supported by transponders—control messages (i.e., they can only be received). Port authorities use these to control maritime traffic so they are given higher priority compared with normal AIS traffic (e.g., position reports).

With regard to frequency hopping, we verified that by broadcasting certain messages we could immediately switch receivers to nonstandard channel frequencies (i.e., lowered their operating frequencies by 4.950MHz). This made the devices unavailable to receive (i.e., know the positions of nearby ships) and transmit (i.e., broadcast their positions) messages.

Note that our attack succeeded because we specified a geographical region apart from the vessel's current position. Alternately, attackers can "program" devices to disappear from AIS monitoring when they enter certain regions of interest such as the sea quadrant of Somalia[17].

```
$ ./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;VQcF0FA3EB200000 -chan=A
```

Listing 6: *Sample availability disruption attack sentence via frequency hopping*

In a timing attack, attackers inhibit the transmission capabilities of one or more AIS stations. Attackers can use VTS-reserved assignment command messages to instruct victims to delay transmissions by 15 minutes, allowing the former to perform denial-of-service (DoS) attacks.

Inversely, attackers can overload (i.e., flood) marine traffic by requesting existing stations to send 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 7: *Sample availability disruption sentence via timing attacks*

Finally, for the slot-starvation attack, we used

17 http://upload.wikimedia.org/wikipedia/commons/7/7e/Somalian_Piracy_Threat_Map_2010.png

message types 4 and 20 to simultaneously fake a base station installed at a VTS and allocate AIS transmissions to the entire "address space" (i.e., time division multiple access [TDMA] slots) in order to consume all of the slots and prevent all nearby stations to further operate (i.e., both to transmit and receive messages).

Coverage Experiment

The experiments featured in this paper showed that AIS transponders are vulnerable to attacks such as spoofing, hijacking, and DoS. We did make an assumption, however, in our in-lab evaluation. We physically connected AIS receivers to a transmitter so as not to send malicious AIS signals over the air. However, this methodology does not take into account real attack scenarios where attackers (e.g., pirates) need to operate within a certain range from their targets.

We performed a coverage experiment to simulate attackers' operational conditions (e.g., pirates situated in open sea, targeting a navigating ship). Our concerns are real and attackers can generate and convey arbitrary AIS messages to stations from a distance of approximately 16.5km.

Our coverage experiment involved installing our AIS transmitter at a fixed and defined position and a receiving station on a moving car[18]. Our evaluation consisted of generating a harmless test message with AISTX and verifying if and at what distance the receiver was able to correctly receive and decode it. Note that as we will extensively discuss later, we took the appropriate precautions to safely conduct the experiment.

We used an amplifier to raise the 50mW power output of the SDR peripheral to around the same capacity of commercial AIS transponders[19]. This was accomplished by modifying a traditional VHF transceiver—Kenwood TK-762G. Note that this is an affordable device (i.e., less than US$100 on eBay) but provides attackers easy access to hardware required to perform malicious deeds.

The radio's final component is based on a hybrid amplification module (i.e., M68702H) that fits the power output characteristics of the SDR peripheral we used. Hardware modification entailed disconnecting the preamplifier's output (i.e., the circuitry from a microphone to a 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. We used an omnidirectional antenna consisting of a 5-element collinear structure (i.e., a standard installation for ships and VTSs) for the receiver. We used a Moxon directional antenna to represent the attackers in order to sustain the amplified signal and improve their coverage and precision. The power gains provided by our antennas were 6dBi and 10dBi. Using home-made antennas showed that the threats we identified did not require a huge financial investment to carry out.

As previously mentioned, our coverage experiment involved transmitting a test message from a fixed station and using a movable receiver to verify the coverage. Using different configurations, we showed that attackers can access a victim station and convey AIS messages up to a distance of approximately 16.5km.

Figure 11 shows the sample locations with dots and the maximum estimated coverage with circles, which were determined via surveys. Note that some dots are located within circles because of the orography of

18 We used Weatherdock EasyTRX2 hardware transponder as receiver.

19 12.5W for class-A and 2W for class-B devices, as per specifications

the geographical area. Our testing site was located near mountains to the north, which attenuated transmitted signals, and flatlands to the south, which better simulated sea conditions.

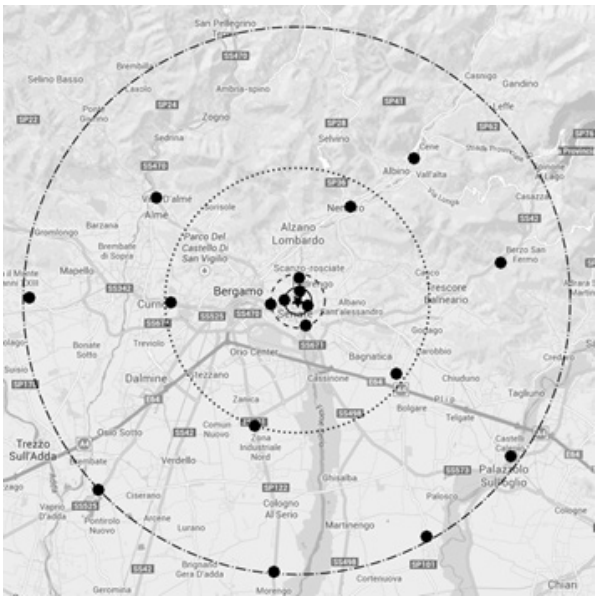

Figure 11: *Graphical representation of the coverage experiment's results*

As shown in Table 3, each line style refers to a particular attacker configuration. For example, by replacing the transmitter's default antenna (λ/4[20]) with the directional one we built, the coverage doubled (i.e., from 0.8km to 1.5km). Further improvements were observed when an amplifier was used. Note that our amplifier came with two selectable output power levels—5W (i.e., standard class-B transponders) and 15W (i.e., class-A transponders). With these conditions, we recorded coverage distances of 8km and 16.5km, respectively. Note, however, that the values were lower than our estimates because our testing site was located near mountains, which attenuated transmitted signals.

20 For AIS, a λ/4 antenna measures 46cm in length. Lambda corresponds to the wavelength (i.e., c/162MHz).

TABLE 3 Coverage Estimates				
TX Antenna	**RX Antenna**	**Amplifier**	**Output Power [W]**	**Coverage [km]**
Default (λ/4)	Omni		0.05	0.8
Directional	Omni		0.05	1.5
Directional	Omni	Y	5	8
Directional	Omni	Y	15	16.5

RESPONSIBLE DISCLOSURE AND MITIGATION STRATEGIES

Generating fake and tampering with AIS information may raise certain ethical concerns. But realistic experiments such as the ones conducted by Jakobsson, et al. [15, 16] are generally the only means to accurately evaluate real-world attacks.

Only harmless test messages, which did not interfere with existing systems, were used in the experiments. Our equipment (i.e., AISTX and receivers) were physically connected so as not to send RF signals over the air. The coverage experiment was conducted on land (i.e., at coordinates 45.69N, 9.72E) and we verified that no AIS receiving installations were present by using publicly available information on online providers' sites. The closest body of open water (i.e., the Mediterranean Sea) was 200km away and all nearby waters were not navigable.

In September 2013, we discussed the findings with the affected providers[21] and standards organizations[22]. At the time this paper was written, MarineTraffic.com and Vessel Finder provided us positive feedback and we actively collaborated with IMO and ITU-R. ITU-R even informed us that it would consider enhancing the security of AIS and announce enhancements made in the "World Radiocommunication Conference 2015." We also shared our concerns with selected CERTs and coastguards who expressed interest in discussing problems with us, standards organizations, and vendors.

In the interim, we propose 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 VTSs) in order to detect suspicious activities such as unexpected changes in vessel routes or static information. In addition, AIS data can be correlated with satellite information to find incongruities such as in vessel dimensions. Although anomaly detection can be valuable in data-collection systems, it does not seem to be a good solution for transponder installations on vessels, which remain vulnerable to RF-specific threats such as availability disruption and SART spoofing.

- **X.509 public key infrastructure (PKI):** A complementary form of mitigation consists in adopting a PKI schema in the AIS protocol used in RF communications. We suggest X.509 [17], a well-known PKI standard where digital certificates are issued by official national maritime authorities acting as certification authorities[23] and concurrently configured in transponders with other stations' identifiers (i.e., MMSI and call sign). X.509 authenticates messages that stations exchange (e.g., between ships and with port authorities). The certificates are handled in two ways—certificates that belong to noteworthy stations such as VTSs are preloaded

21 MarineTraffic.com, AIS Hub, and Vessel Finder
22 IMO, IALA, and ITU-R
23 The same organizations that issue MMSI and call sign identifiers for AIS stations (e.g., U.S. Coast Guard or Italian Ministry of Economic Development).

via onshore installations (e.g., when ships enter ports) while generic and those previously unknown to stations are exchanged with nearby stations (i.e., navigating vessels) on demand during the acquaintance phase of two vessels[24]. Vessels with satellite Internet access can also retrieve certificates from online services.

24 There is no need to exchange certificates over trusted channels because counterfeiting will invalidate them.

RELATED WORK

A large body of literature focuses on correlating and analyzing ship information collected from VTSs and online providers. Xianbiao, et al. [18] used online analytical processing (OLAP) to store, process, and correlate information for collision avoidance and investigation. The same authors also discussed [19] different techniques to efficiently organize AIS-collected data. Carthel, et al. [20] studied multisensor networks for data surveillance. They proposed to extend distributed multihypothesis tracking (DMHT), an algorithm originally designed for undersea surveillance networks, to AIS. Similarly, B.J. Tetreault [21] suggested ways to increase maritime domain awareness (MDA) by collecting and using AIS data. Other applications correlated oil slick shape and tracking data to identify ships that illegally spilled oil at sea [22] as well as predicting the financial gains given by commercial trading. With respect to navigational safety, most of the literature focus on collision-avoidance systems and prevention [23, 24].

Despite the large body of AIS research, to the best of our knowledge, we appear to be the first to conduct a security evaluation of AIS. We used SDRs to build a novel AIS transmitter (i.e., AISTX) and show that our concerns are valid. We used existing AIS receivers [25, 26, 27]. Both gr-ais and ais-tool are software-based receivers built on top of GNU Radio. We mainly used gr-ais in the hybrid receiver for RF evaluation. Compared with Guarnieri's work [28], which focused on data AIS leaked, we explored faults in AIS implementation and protocol specifications[25].

Similar to our research on smart transportation, Costin, et al. performed a security evaluation of Automatic Dependent Surveillance-Broadcast (ADS-B), an RF protocol used in aviation for data communication and monitoring. Using SDRs, they showed that ADS-B is vulnerable to eavesdropping, message jamming, and replaying injection. In similar work, Teso [29] showed how to use Aircraft Communications Addressing and Reporting System (ACARS) to upload malicious flight management system (FMS) plans to aircraft. Humphreys, et al. [30] also introduced a software-based GPS transmitter to fake GPS communication and demonstrate how to hijack valid GPS signals to bring a ship off course.

25 http://internetcensus2012.bitbucket.org/paper.html

CONCLUSION

AIS is a commonly used CPS in the marine industry for vessel traffic monitoring and assistance. Given its importance in collision detection, SAR operations, and piracy prevention, we conducted a unique security evaluation of AIS. Using a specially crafted software-based transmitter, we determined and showed that both AIS's implementation and protocol specifications, in fact, could be affected by several threats, offering malicious actors many attack possibilities. We notified affected providers and standards organizations and provided mitigation strategies. We are currently and actively collaborating with them to improve AIS's overall security.

Acknowledgments: The authors would like to thank Germano Valbusa (call sign: IW2DCK) for contributing to the development of the amplifier. Special thanks also goes out to Trend Micro, especially the Forward-Looking Threat Research (FTR) Team, who supported this research in various ways. Finally, we would like to thank the organizers of both Black Hat and Hack In The Box conferences for hosting our talk on AIS[26].

26 The video can be accessed at http://blog.trendmicro.com/trendlabs-security-intelligence/vulnerabilities-discovered-in-global-vessel-tracking-systems/.

REFERENCES

[1] Astra Paging Ltd. (2014). *Vessel Finder.* "Vessels Database." Last accessed November 18, 2014, http://www.vesselfinder.com/vessels.

[2] Michelle Wiese Bockmann. (October 19, 2012). *Bloomberg.* "Iran Oil Tankers Said by Zanzibar to Signal Wrong Flag." Last accessed November 18, 2014, http://www.bloomberg.com/news/2012-10-19/iranian-oil-tankers-said-by-zanzibar-to-be-signaling-wrong-flag.html.

[3] International Maritime Organization. (2014). *IMO.* "SOLAS Chapter V: Safety of Navigation." Last accessed November 18, 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/343175/solas_v_on_safety_of_navigation.pdf.

[4] ITU. (2014). *ITU.* "Table of Maritime Identification Digits." Last accessed November 18, 2014, http://www.itu.int/online/mms/glad/cga_mids.sh.

[5] Cecilia Ambjörn. (2008). In U.S./EU-Baltic International Symposium. "Seatrack Web, the HELCOM Tool for Oil Spill Prediction and Identification of Illegal Polluters." Last accessed November 18, 2014, https://portal.helcom.fi/Archive/archive2/RESPONSE%2014-2011_Presentation-7%20STW.pdf.

[6] Bloomberg Finance L.P. (2014). *Bloomberg.* "Commodities." Last accessed November 18, 2014, http://www.bloomberg.com/professional/markets/commodities/.

[7] International Maritime Organization. (2014). *IMO.* "Piracy and Armed Robbery Against Ships." Last accessed November 20, 2014, http://www.imo.org/OurWork/Security/PiracyArmedRobbery/Pages/Default.aspx.

[8] U.S. Coast Guard Navigation Center. (August 5, 2014). *Navigation Center.* "AIS Meaages." Last accessed November 20, 2014, http://www.navcen.uscg.gov/?pageName=AISMessages.

[9] National Maritime Electronics Association. (2008–2012). *NMEA.* "NMEA 0183 Standard." Last accessed November 20, 2014, http://www.nmea.org/content/nmea_standards/nmea_0183_v_410.asp.

[10] Eric S. Raymond. (August 29, 2014). *AIVDM/AIVDO Protocol Decoding.* Last accessed November 20, 2014, http://catb.org/gpsd/AIVDM.html.

[11] Andrei Costin and Aurélien Francillon. In Black Hat 2012. "Ghost in the Air(Traffic): On Insecurity of ADS-B Protocol and Practical Attacks on ADS-B Devices." Last accessed November 20, 2014, https://media.blackhat.com/bh-us-12/Briefings/Costin/BH_US_12_Costin_Ghosts_In_Air_WP.pdf.

[12] Fabian van den Broek. (2011). "Eavesdropping on GSM: State of Affairs." Last accessed November 21, 2014, http://www.cs.ru.nl/~fabianbr/WISSec2010_GSM_Eavesdropping.pdf.

[13] Chun-Chieh Chen, Inn-Tung Chen, Chen-Mou Cheng, Ming-Yang Chih, and Jie-Ren Shih. (May 2009). In Mobile Data Management: Systems, Services, and Middleware, 2009. "A Practical Experience with RFID Security." Last accessed November 21, 2014, http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5088976&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5088976.

[14] ITU. (2008). *ITU.* "M.1371 : Technical Characteristics for an Automatic Identification System Using Time-Division Multiple Access in the VHF Maritime Mobile Band." Last accessed November 21, 2014, http://www.itu.int/rec/R-REC-M.1371/en.

[15] M. Jakobsson, P. Finn, and N. Johnson. (2008). *Security & Privacy, IEEE (Volume: 6, Issue: 2).* "Why and How to Perform Fraud Experiments." Last accessed November 21, 2014, http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=4489852.

[16] Markus Jakobsson and Jacob Ratkiewicz. (2006). In WWW 2006. "Designing Ethical Phishing Experiments: A Study of (ROT13) rOnl Query Features." Last accessed November 21, 2014, http://www2006.org/programme/item.php?id=3533.

[17] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. (2008). *IETF.* "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile." Last accessed November 24, 2014, https://datatracker.ietf.org/doc/rfc5280/.

[18] Xianbiao Ji, Zheping Shao, Jiacai Pan, and Cunbao Tang. (2009). *ASCE Library.* "A New AIS-Based Way to Conduct OLAP of Maritime Traffic Flow." Last accessed November 24, 2014, http://ascelibrary.org/doi/abs/10.1061/41039%28345%29613.

[19] Z. Shao, C. Tang, J. Pan, and X. Ji. (2011). *ASCE Library.* "The Application of Database Techniques in the Integrated Vessel Information Service System." Last accessed November 24, 2014, http://ascelibrary.org/doi/abs/10.1061/41184%28419%29442.

[20] Craig Carthel, Stefano Coraluppi, and Patrick Grignan. (2007). In Information Fusion 2007. "Multisensor Tracking and Fusion for Maritime Surveillance." Last accessed November 24, 2014, http://www.isif.org/fusion/proceedings/fusion07CD/Fusion07/pdfs/Fusion2007_1224.pdf.

[21] B.J. Tetreault. (2005). *Research Gate.* "Use of the Automatic Identification System (AIS) for Maritime Domain Awareness (MDA)." Last accessed November 24, 2014, http://www.researchgate.net/publication/224634730_Use_of_the_Automatic_Identification_System_%28AIS%29_for_maritime_domain_awareness_%28MDA%29.

[22] C. Ambjorn. (2008). *Research Gate.* "Seatrack Web Forecasts and Backtracking of Oil Spills—An Efficient Tool to Find Illegal Spills Using AIS." Last accessed November 24, 2014, http://www.researchgate.net/publication/4371427_Seatrack_Web_forecasts_and_backtracking_of_oil_spills_-_an_efficient_tool_to_find_illegal_spills_using_AIS.

[23] Li Li-na, Yang Shen-hua, Cao Bao-gen, and Li Zi-fu. (2006). *CAOD.* "A Summary of Studies on the Automation of Ship

Collision Avoidance Intelligence." Last accessed November 24, 2014, http://caod.oriprobe.com/articles/10391122/A_Summary_of_Studies_on_the_Automation_of_Ship_Collision_Avoidance_Int.htm.

[24] Li Li-na. (2002–2003). *CNKI.* "Determination of the Factors About Safe Distance of Approach and Etc. on the Research of Ship Automatic Avoidance Collision." Last accessed November 24, 2014, http://en.cnki.com.cn/Article_en/CJFDTOTAL-DLHS200203006.htm.

[25] Kgabo Frans Mathapo. (2007). *SUNScholar Research Repository.* "A Software-Defined Radio Implementation of Maritime AIS." Last accessed November 24, 2014, https://scholar.sun.ac.za/handle/10019.1/2215.

[26] *Sourceforge.net.* (2014). "GNU AIS—Automatic Identification System for Linux." Last accessed November 24, 2014, http://gnuais.sourceforge.net/.

[27] *FunWithElectronics.com.* (2014). "Automatic Identification System (AIS) Using GNU Radio." Last accessed November 24, 2014, http://www.funwithelectronics.com/?id=9.

[28] Claudio Guarnieri. (April 29, 2013). *Security Street.* "Spying on the Seven Seas with AIS." Last accessed November 24, 2014, https://community.rapid7.com/community/infosec/blog/2013/04/29/spying-on-the-seven-seas-with-ais.

[29] Hugo Teso. (2013). In Hack In The Box 2013. "Aircraft Hacking: Practical Aero Series." Last accessed November 24, 2014, http://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf.

[30] Daniel P. Shepard, Todd E. Humphreys, and Aaron A. Fansler. (2012). *International Journal of Critical Infrastructure Protection, 5(3–4):146–153.* "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks." Last accessed November 24, 2014, https://radionavlab.ae.utexas.edu/images/stories/files/papers/spoofSMUCIP2012.pdf.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO™

Securing Your Journey to the Cloud

225 E. John Carpenter Freeway, Suite 1500
Irving, Texas 75062 U.S.A.

Phone: +1.817.569,8900