Protected AIS

Gary C. Kessler, Ph.D., CISSP
DEFCON
08 August 2020
Contents

• Overview
• Technology Review
  - AIS
  - Hash functions and checksums
  - Public Key Cryptography
• Problem Statement
• Proposed Solution
• Features
Overview

• The Automatic Identification System (AIS) is used by vessels at sea to maintain situational awareness.

• AIS suffers from several security vulnerabilities that make it prone to spoofing, so that a Bad Guy can send bogus messages.

• The proposed solution employs public key cryptography (PKC) methods to provide Protected AIS in order to address the vulnerabilities and maintain backward-compatibility with existing protocols.
## Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASCII</td>
<td>American Standard Code for Information Interchange</td>
</tr>
<tr>
<td>AIS</td>
<td>Automatic Identification System</td>
</tr>
<tr>
<td>ATON</td>
<td>Aid to navigation</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate authority</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations (U.S.)</td>
</tr>
<tr>
<td>ECDIS</td>
<td>Electronic Chart Display and Information System</td>
</tr>
<tr>
<td>ETA</td>
<td>Estimated time of arrival</td>
</tr>
<tr>
<td>ITU-R</td>
<td>International Telecommunication Union, Radiocommunication sector</td>
</tr>
<tr>
<td>MMSI</td>
<td>Mobile Marine Service Identifier</td>
</tr>
<tr>
<td>NMEA</td>
<td>National Marine Electronics Association</td>
</tr>
<tr>
<td>PKC</td>
<td>Public key cryptography</td>
</tr>
<tr>
<td>PKI</td>
<td>Public key infrastructure</td>
</tr>
<tr>
<td>PUB</td>
<td>Public key</td>
</tr>
<tr>
<td>PVT</td>
<td>Private key</td>
</tr>
<tr>
<td>RF</td>
<td>Radio frequency</td>
</tr>
<tr>
<td>RSA</td>
<td>Rivest, Shamir, and Adleman</td>
</tr>
<tr>
<td>SOLAS</td>
<td>International Convention for the Safety of Life at Sea</td>
</tr>
<tr>
<td>VTMS</td>
<td>Vessel traffic management system</td>
</tr>
<tr>
<td>XOR</td>
<td>Exclusive OR</td>
</tr>
</tbody>
</table>

© Gary C. Kessler, 2019-2020
Technology Review
Automatic Identification System

• AIS is a tracking system used by ships and VTMS
  - Provides a vessel with situational awareness about surrounding traffic

• AIS provides a ship's name, unique identifier, position, course, speed, destination, ETA, vessel type/activity, and more

• Data can be displayed on a screen, ECDIS, or mobile app
Vessels Required to use AIS

• Defined in 2002 SOLAS, Chapter V, Regulation 19 and 33 CFR 164.46

• In general, AIS is required on:
  - All vessels ≥1600 gross tons
  - Commercial power vessels ≥65 ft (20 m)
  - Commercial towing vessels ≥26 ft (8 m) or >600 horsepower
  - Power vessels certified to carry >150 passengers

• Warship exemption
FindShip mobile app

WHITE ROSE OF DRACHS

MMSI: 235862000
IMO: 1008140
Length: 65 m
Depth: 7.4 m
Width: 12 m
Build year: 2004/06
DWT: 269
Gross ton: 1643
Callsign: MEEW5
Flag: GBR
Type: Pleasure Craft

Lat: 43°43.415 N
Lon: 7°24.954 E
Course: 270.0°
Truehead: 264°
Speed: 0.0 kts
Draught: 4.6 m
Status: Moored
Dest: CAP DAIL
ETA: 09-03 16:00
Time: 2017-10-22 08:13:42

© Gary C. Kessler, 2019-2020
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MMSI</td>
<td>2260999000</td>
</tr>
<tr>
<td>IMO</td>
<td>9595137</td>
</tr>
<tr>
<td>Callsign</td>
<td>FICZ</td>
</tr>
<tr>
<td>Type</td>
<td>Tanker</td>
</tr>
<tr>
<td>Length</td>
<td>184 m</td>
</tr>
<tr>
<td>Width</td>
<td>27 m</td>
</tr>
<tr>
<td>Depth</td>
<td>16.7 m</td>
</tr>
<tr>
<td>Build</td>
<td>*****</td>
</tr>
<tr>
<td>DWT</td>
<td>*****</td>
</tr>
<tr>
<td>Last Time</td>
<td>2017-11-03 15:25</td>
</tr>
<tr>
<td>Status</td>
<td>Under way using engine</td>
</tr>
<tr>
<td>Latitude</td>
<td>44-5.580N</td>
</tr>
<tr>
<td>Longitude</td>
<td>29-26.238E</td>
</tr>
<tr>
<td>Course</td>
<td>278.7°</td>
</tr>
<tr>
<td>Truehead</td>
<td>278°</td>
</tr>
<tr>
<td>Speed</td>
<td>12.1 kts</td>
</tr>
<tr>
<td>Draught</td>
<td>8 m</td>
</tr>
<tr>
<td>ETA</td>
<td>11-04 00:30</td>
</tr>
<tr>
<td>Dest</td>
<td>MIDIA AND</td>
</tr>
</tbody>
</table>

http://www.findship.co/
AIS Communication Protocol

- AIS defined in ITU-R Recs. M.585-7 and M.1371-5
  - Radio employs self-organized time division multiple access (SOTDMA)
  - NMEA serial communications protocol
  - AIVDM packets contain data received from other vessels
  - AIVDO packets contain your vessel's information
Types of Cryptography and Applications

• Hash function
  - No key; one-way encryption
  - *Used for message integrity*

• Secret key cryptography
  - Single key used for both encryption and decryption
  - *Used for privacy/confidentiality*

• Public key cryptography
  - Uses two keys that are a mathematically-related pair; one key used to encrypt and the other to decrypt
  - Knowledge of one key does not provide knowledge of the second key
  - *Used for authentication, non-repudiation, and key exchange*
Hash Functions and Checksums

• Hash functions and checksums provide bit integrity
  - Mathematical formula that provides a digital fingerprint of a message, file, frame, packet, or other binary string
  - Length of the output is dependent upon the algorithm and independent of message or file size
    o E.g., a 16-bit checksum will always generate a 16 bit value regardless of the length of the input
  - The content and length of the binary string is impossible to retrieve from the checksum/hash value
PKC Applications

• In PKC, one key is kept as a closely held secret (the *private key*) and the other key is posted on the Internet and/or key servers (the *public key*)

• If Alice encrypts a message with Bob's public key, only Bob -- using his private key -- can decrypt
  - This provides secure communication from Alice to Bob

• If Alice encrypts a message with her own private key, anyone can decrypt using her public key
  - This authenticates Alice as the sender of the message
Alice sends a message encrypted with her own PVT key; Bob decrypts using her PUB key. 
*This signed messages authenticates Alice as the sender.*

Alice sends a message encrypted with Bob's PUB key; Bob decrypts using his own PVT key. 
*This private message is for Bob only.*

---

- Alice's PVT key
- Alice's Private Keychain
- Alice's PUB key
- Bob's PUB key
- Carol's PUB key
- Dave's PUB key
- Bob's PVT key
- Bob's Private Keychain

*Shared Public Keychain*
Problem Statement
AIS Security Weaknesses

• AIS security vulnerabilities include:
  - Lack of geographic validity checks
  - Lack of timing checks
  - Lack of sender authentication
  - Lack of message bit integrity checks

• If compromised, AIS communications can be hijacked to create fake vessels or virtual ATONs, trigger false SOS or collision alerts, and more

• REF: Balduzzi, Pasta, & Wilhoit (2014); Balduzzi, Wilhoit, & Pasta (2014); Kessler, Craiger, & Haass (2018); Kessler (2020)
AIS Attack Vectors
(from Balduzzi, Wilhoit, & Pasta, 2014)
Standards

• The most common standard for AIS equipment is the National Marine Electronics Association (NMEA) 0183 specification
  - NMEA 2000 and OneNet (2020) are newer standards but largely limited for use onboard a vessel
  - Significant embedded base of NMEA 0183 equipment
  - NMEA 0183 largely used over the air
0183 AIS Sentence Structure

- Prefix
- Talker ID
- Sequence information
- Channel number

- Encapsulated payload

- No. of padding bits
- Sentence checksum
  Covers Content field

Message might be fragmented across several sentences
0183 AIS Message Fields

Commas (,) are field separators and the asterisk (*) indicates checksum field

REF: https://gpsd.gitlab.io/gpsd/AIVDM.html
Enter message type (1-5, 8, 10, 11, 14, 18-24) or 'X' to halt:
AIVDM Example #1

Moriarty:protected gck$ ./pAIS_ping.pl --type=1 --mmsi=369121053 --lat=29.1 --long=-80 --nmea=A

***** AIS_ping (Version: 6.0.5p, Build date: 10/12/2019) *****
Use the following command(s) next:
perl AIS_NMEA.pl --
payload=000001000101110000000001010111001110111111000000111111111011010010001110010100000000
000100001010011010110010000011100001000011111111111111000000000000000000000000000 --channel=A

Moriarty:protected gck$ ./AIS_NMEA.pl --
payload=0000010001011100000000010101110001110111111000000111111111011010010001110010100000000
00010000101010111000001110000100001111111111111111111111111100000000000000000000 --channel=A

***** AIS NMEA (Version: 5.3.1, Build date: 10/20/2019) *****
AIS sentence type: !AIVDM Channel: A Payload length: 168 bits Pad: 0 bit(s)
1 fragment(s)
Input:
00001000101110000000001010111001111111111111111111111111111111111111111111111100000000000000000000000000000000000000000000
Armored ASCII: 15P1G7OP?wJAjP0@ac8>4?wp0000

AIS Message:
!AIVDM,1,1,,A,15P1G7OP?wJAjP0@ac8>4?wp0000,0*2D

Done!
Moriarty:protected gck$

GCK's program to create AIS messages
AIS sentence(s) input from file test_01pres.txt.

AIS sentence: !AIVDM,1,1,,A,15P1G7OP?wJAjP0@ac8>4?wp0000,0*2D
Talker ID: !AI - Mobile AIS station
AIS Encapsulation Formatter: VDM - AIS VHF Data-Link Message
Checksum verified
1 sentence(s) processed

Binary string:
00001000101100000000101011100111111111111111011010010011100101000000000000100010100110101100111000000001011111111111111111111111111111111001000000000000000000000000000000000000

Message Type = 1 (Position Report Class A)
Repeat indicator = 0
Maritime Mobile Service Identity (MMSI) = 369121053
  ** This MMSI represents a ship.
  ** The Maritime Identification Digits (MID) are 369 -- United States of America
Navigation Status = 15 (Not defined [default])
Rate of Turn (ROTAIS) = -128 (no turn information available [default])
Speed over ground (SOG) = 102.3 (Information not available)
Position accuracy = 0 (Low, >10 m [default])
Longitude = 080.000000°W (080°00.00'W)
Latitude = 29.100000°N (29°06.00'N)
  ** Use this URL for a Google map of this position:
  ** http://www.google.com/maps/place/29.100000,-80.000000
Course over ground (COG) = 360.0 (Information not available)
True heading = 511 (Information not available)
Timestamp = 60 (Time stamp is not available [default])
Maneuver indicator = 0 (Not available [default])
Spare = 0 (Unused; should be 0)
Receiver Autonomous Integrity Monitoring flag = 0 (RAIM not in use [default])
--- SOTDMA Communication State ---
Synchronization state = 0 (UTC direct)
Slot timeout = 0 slots remaining until slot change
Slot offset = 0

GCK's program to parse AIS messages

© Gary C. Kessler, 2019-2020
This **AIS online decoder** can decode AIVDM & AIVDO NMEA messages with codes #1-26. Paste your AIS message in the field below and click "Decode".

AIS message: (for example: AIVDM,1,1,A,15MgK45P3@G7f0E^Jbr0OwT0@MS,0^4E)

!AIVDM,1,1,A,15P1G7OP?wJApP0@ac8>47wp0000,0*2D|

https://www.aggsoft.com/ais-decoder.htm
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Type</td>
<td>AIVDM</td>
<td></td>
</tr>
<tr>
<td>CHANNEL</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Message Type</td>
<td>1</td>
<td>Scheduled Position Report</td>
</tr>
<tr>
<td>Repeat Indicator</td>
<td>Default</td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td>369121053</td>
<td></td>
</tr>
<tr>
<td>Navigation Status</td>
<td>15</td>
<td>Not defined (default)</td>
</tr>
<tr>
<td>Rate of Turn (ROT)</td>
<td>-729</td>
<td></td>
</tr>
<tr>
<td>Speed Over Ground (SOG)</td>
<td>102.3</td>
<td>Speed is not available</td>
</tr>
<tr>
<td>Position Accuracy</td>
<td>An unaugmented GNSS fix with accuracy &gt; 10 m</td>
<td></td>
</tr>
<tr>
<td>Longitude</td>
<td>-79.9999983333333</td>
<td>West</td>
</tr>
<tr>
<td>Latitude</td>
<td>29.1</td>
<td>North</td>
</tr>
<tr>
<td>Course Over Ground (COG)</td>
<td>360</td>
<td>Not available</td>
</tr>
<tr>
<td>True Heading (HDG)</td>
<td>511</td>
<td>Not available (default)</td>
</tr>
<tr>
<td>Time Stamp</td>
<td>60</td>
<td>Time stamp is not available (default)</td>
</tr>
<tr>
<td>Reserved for regional</td>
<td>Not available (default)</td>
<td></td>
</tr>
<tr>
<td>RAIM flag</td>
<td>RAIM not in use (default)</td>
<td></td>
</tr>
<tr>
<td>Communication State</td>
<td>Sync state: UTC Direct; Slot Timeout: This was the last transmission in this slot; Slot offset: 0</td>
<td></td>
</tr>
<tr>
<td>Communication Sync State</td>
<td>Sync state: UTC Direct</td>
<td></td>
</tr>
<tr>
<td>Communication Slot Timeout</td>
<td>Slot Timeout: This was the last transmission in this slot</td>
<td></td>
</tr>
<tr>
<td>Communication Sub Message</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Communication Utc Hour</td>
<td>No value</td>
<td></td>
</tr>
<tr>
<td>Communication Utc Minute</td>
<td>No value</td>
<td></td>
</tr>
<tr>
<td>Communication Time Stamp</td>
<td>No value</td>
<td></td>
</tr>
<tr>
<td>Communication Slot Number</td>
<td>No value</td>
<td></td>
</tr>
<tr>
<td>Communication Received Stations</td>
<td>No value</td>
<td></td>
</tr>
<tr>
<td>Communication Slot Offset</td>
<td>No value</td>
<td></td>
</tr>
</tbody>
</table>

Showing 1 to 26 of 26 entries
AIS Message Types

- Types 1, 2 and 3: Position Report Class A (168 bits)
- Type 4: Base Station Report (168 bits)
- Type 5: Static and Voyage Related Data (424 bits)
- Type 6: Binary Addressed Message (Variable length, max. 1,008 bits)
- Type 7: Binary Acknowledge (72-168 bits in 32-bit increments)
- Type 8: Binary Broadcast Message (Variable length, max. 1,008 bits)
- Type 9: Standard SAR Aircraft Position Report (168 bits)
- Type 10: UTC/Date Inquiry (72 bits)
- Type 11: UTC/Date Response (168 bits)
- Type 12: Addressed Safety-Related Message (Variable length, max. 1,008 bits)
- Type 13: Safety-Related Acknowledgment (72-168 bits in 32-bit increments)
- Type 14: Safety-Related Broadcast Message (Variable length, max. 1,008 bits)
- Type 15: Interrogation (88-160 bits)
- Type 16: Assignment Mode Command (96 or 144 bits)
- Type 17: DGNSS Broadcast Binary Message (80-816 bits)
- Type 18: Standard Class B CS Position Report (168 bits)
- Type 19: Extended Class B CS Position Report (312 bits)
- Type 20 Data Link Management Message (72-160 bits)
- Type 21: Aid-to-Navigation Report (272-360 bits)
- Type 22: Channel Management (168 bits)
- Type 23: Group Assignment Command (160 bits)
- Type 24: Static Data Report (160 or 168 bits)
- Type 25: Single Slot Binary Message (Max. of 168 bits)
- Type 26: Multiple Slot Binary Message (60-1064 bits)
- Type 27: Long Range AIS Broadcast message (96 bits)
Proposed Solution
Design Criteria

- Message integrity
- Timing integrity
- Validity and authentication
- Backward compatibility
Proposed Solution

• A sender operating in protected mode will:
  1. Create a 16-character string composed of a timestamp and checksum for entire payload of a message
  2. Encrypt the string with the sender's private key
  3. Append the signed protection string to the message, formatting as a normal NMEA sentence

• A receiver operating in protected mode will:
  1. Read the signed protection string, decrypt it with the sender's public key, and recover the timestamp and checksum
  2. Compute a checksum and compare to the received checksum
  3. Compare the received timestamp with the current time
PKC Application

• Each AIS device is assigned a unique Mobile Marine Service Identifier (MMSI)
  - The MMSI is different from the International Maritime Organization (IMO) identifier, which is assigned to a vessel

• Each MMSI has an assigned private-public key pair
  - The private key should be closely held by the AIS device
  - The public keys should be available on a public Web server
AIS device prepares outgoing message (NMEA 0183)
If used, pAIS protect string encrypted with device’s private key

Device transmits pAIS message as it would standard AIS message.

AIS device receives incoming message (NMEA 0183)
If present, pAIS protect string decrypted with sender’s public key

Device receives pAIS message as it would standard AIS message. If pAIS is not supported, only the standard message is parsed; extra bits are ignored.
Protected AIS Sentence Structure

- Prefix
- Talker ID
- Sequence information
- Channel number
- Encapsulated payload
- Message
- Protect String
- Timestamp
- Message checksum
- String encrypted with sender's MMSI as the key
- No. of padding bits
- Sentence checksum
  Covers Content field

Message + Protect String might be fragmented across several sentences.
Protect String Characteristics

• Timestamp
  - yyyymmddHHMMSS

• Checksum
  - 8-bit XOR

• pAIS uses 256-bit RSA keys
  - Shortest key that will encrypt 16B; creates a 258-bit encrypted string (26-154% overhead)
  - 128-bit key only encrypt a 5B string; a 512-bit key created a 540-bit protected string
The OpenSSL RSA Crypto Library

- Crypt::OpenSSL::RSA
- Functions
  - generate_key
    - get_public_key_string
    - get_private_key_string
  - encrypt [with public key]
  - decrypt [with private key]
  - private_encrypt [with private key]
  - public_decrypt [with public key]
  - sign

Generate a key pair and then extract the public and private keys.

Encrypt using the private key and decrypt using the public key will authenticate the sender.
AIVDM Example #2

In protected mode, additional information is appended to the end of a standard AIS message.

The payload will be appended with the encrypted Protect String comprising a timestamp '20200727213423' and NMEA checksum '3B' --> '202007272134233B' encrypted using the private key associated with MMSI 369121053.

Use the following command(s) next:

Moriarty:protected gck$ ./AIS_ping.pl --type=1 --mmsi=369121053 --lat=29.1 --long=-80 --protect --nmea=A

***** AIS_ping (Version: 6.0.5p, Build date: 10/12/2019) *****

***** AIS NMEA (Version: 5.3.1, Build date: 10/20/2019) *****

AIS Message:
!AIVDM,2,1,7,A,15P1G7OP?wJAjP0@ac8>4?wp0000RIAvijPOuies3Dta>qh`t9?EloV<DFOhNOqLmfGo8n@,
!AIVDM,2,2,7,A,NOqLmfGo8n@,0*5D,
!AIVDM,2,2,7,A,NOqLmfGo8n@,0*18

Done!
Moriarty:protected gck$
Moriarty:protected gck$ ./AIS_parser.pl -sf test_01pres_protect.txt

***** AIS Parser (Version: 3.4.0p, Build date: 10/22/2019) *****

AIS sentence(s) input from file test_01pres_protect.txt.

AIS sentence: !AIVDM,2,1,7,A,15P1G7OP?wJAp0@ac8>4?wp0000RlAvjPOuies3Dta>qh`t9?EloV<DPOh,0*5D
  Talker ID: !AI - Mobile AIS station
  AIS Encapsulation Formatter: VDM - AIS VHF Data-Link Message
  Checksum verified
AIS sentence: !AIVDM,2,2,7,A,NOqLmfGo8n@,0*18
  Talker ID: !AI - Mobile AIS station
  AIS Encapsulation Formatter: VDM - AIS VHF Data-Link Message
  Checksum verified
2 sentence(s) processed
Message Type = 1 (Position Report Class A)
Repeat indicator = 0
Maritime Mobile Service Identity (MMSI) = 369121053
  ** This MMSI represents a ship. **
  ** The Maritime Identification Digits (MID) are 369 -- United States of America **
Navigation Status = 15 (Not defined [default])
Rate of Turn (ROTAIS) = -128 (no turn information available [default])
Speed over ground (SOG) = 102.3 (Information not available)
Position accuracy = 0 (Low, >10 m [default])
Longitude = 080.000000°W (080°00.00'W)
Latitude = 29.100000°N (29°06.00'N)
  ** Use this URL for a Google map of this position: **
  ** http://www.google.com/maps/place/29.100000,-80.000000 **
Course over ground (COG) = 360.0 (Information not available)
True heading = 511 (Information not available)
Timestamp = 60 (Time stamp is not available [default])
Maneuver indicator = 0 (Not available [default])
Spare = 0 (Unused; should be 0)
Receiver Autonomous Integrity Monitoring flag = 0 (RAIM not in use [default])
--- SOTDMA Communication State ---
Synchronization state = 0 (UTC direct)
Slot timeout = 0 slots remaining until slot change
Slot offset = 0
--- Protected AIS Information ---
### Sender’s MMSI (369121053) is authenticated.
Timestamp = 07/27/2020 21:34:23 UTC
  Received time = 08/07/2020 13:59:11 UTC (Difference >30 seconds)
Check sum = 0x3B (Verified)
Public Web site accepts the two sentences...

AIS ONLINE DECODER. AIVDM & AIVDO NMEA MESSAGES

This **AIS online decoder** can decode AIVDM & AIVDO NMEA messages with codes #1-26. Paste your AIS message in the field below and click "Decode".

AIS message: (for example: AIVDM,1,1,A,15P1G7OF?wJAjP0@ac8>4?wp0000RDIAViJPOui3Dta>qh`97EloV<DFOh,0*5D
!AIVDM,2,2,7,A,NOqLmfGo8n8,0*18|
...and interprets only the "standard" NMEA sentence, ignoring the extra bits.
Features
How the Solution Addresses the Problems

• Problem #1: Message integrity
  - Solution: Use a simple checksum

• Problem #2: Timing integrity
  - Solution: Use a simple timestamp

• Problem #3: Validity and authentication
  - Solution: Use sender's private key to sign a message composed of the checksum and timestamp

• Problem #4: Backward compatibility
  - Solution: AIS receivers ignore excess bits in messages that are larger than expected

• Problem #5: Geographic integrity
  - (Not addressed)
Key Distribution

• Protected AIS requires public-private key pairs, but is not dependent upon the key distribution method

• pAIS messages can be accepted in parallel to obtaining the key
  - Could use existing public key infrastructure (PKI) methods, including use of certificates
  - 1 billion hosts in the distributed, hierarchical DNS database while there are <<1 billion assigned MMSIs
  - Pretty Good Privacy (PGP) "web of trust" method not scalable to the scope of the maritime industry
Other Solutions

• Many papers describing solutions to AIS security including use of public key methods without a central CA
  - Hall et al. (2015) describe a change to the AIS protocol using security standards described in the IEEE 1609 family of standards for Wireless Access in Vehicular Environments (WAVE)
  - Goudossis & Katsikas (2018) describe Secure AIS, using public key cryptography, secret key cryptography, and a maritime PKI
  - Goudossis & Katsikas (2020) continue describing using MMSIs as key into Maritime Identity-Based Cryptography (MIBC) system
Open Issues

• This method does not protect against a bad actor who legitimately has a "protected" AIS device with a registered public-private key pair
  - Nothing stops a device owner from sending purposefully false information albeit they can only do it once using the single MMSI assigned to their device before others catch on…

• Backward compatibility means that devices will still accept unprotected AIS messages which means… nothing to stop a Bad Actor
More Open Issues

• Devices theoretically could use a different color to indicate:
  - AIS messages that are authenticated
  - AIS messages using protect mode but not yet authenticated (i.e., waiting for the public key)
  - Unauthenticated AIS messages
Future Research

- Bit-wise XOR is a weak checksum
  - CRC-8 is better; would maintain size of Protect String
- Current timestamp is 14 characters (112 bits)
  - Unix epoch time is 10 char. or a 32-bit number
  - Neither changes size of Protect String (and binary is not human readable)
- Current public key sharing is via Web of Trust
  - Need a more dynamic and distributed method
- Difficult to implement with message types that are of variable-length
References


Contact Information

Gary C. Kessler, Ph.D., CCE, CISSP
USCG 50GT Master/Assistance Towing

mobile:  +1 802-238-8913
e-mail:  gck@garykessler.net
Skype:  gary.c.kessler

https://www.garykessler.net