

NAUFRAGEURS 4.0

plateforme de leurrage et de simulation hybride d'activités maritimes

David Le Goff¹ and David Brosset^{2,3}

¹ `david.le-goff@protonmail.com`

² Institut de recherche de l'école navale (IRENAV), Arts et métiers Sciences et Technologies

`david.brosset@ecole-navale.fr`

³ Chaire de cyberdéfense des systèmes

navalshttps://www.overleaf.com/project/5f6dd9d5e7297c0001badd6a

Résumé Le monde maritime n'a évidemment pas échappé pas à la numérisation. Les capacités des navires et la sécurité en mer ont bénéficié de l'ensemble des systèmes numériques qui sont apparus à bord des navires. Mais ces bénéfices sont également associés à une forte dépendance à des systèmes qui peuvent être vulnérables d'un point de vue cybersécurité. Dans cet article est présentée une approche de leurrage de navires dont le but est de démontrer les fragilités des systèmes utilisés pour développer de nouveaux systèmes ou des solutions permettant de détecter des actes de malveillance.

Keywords: AIS · GSM · WIFI · Empreinte numérique · signature · SDR · ICS · SCADA · Maritime

1 Introduction

Les systèmes à base de géolocalisation sont connus pour être faillibles. Il s'agit de la porte d'entrée la plus facile pour réaliser une cyberattaque sur objet mobile comme un drone, une voiture autonome ou un navire. Cette facilité vient du but original des systèmes de géopositionnement ainsi que de la numérisation que nous connaissons maintenant qui était difficile à imaginer il y a des dizaines d'années.

Le signal que nous recevons des satellites en orbite est extrêmement faible, de l'ordre de quelques nanowatts, et il est donc facile d'émettre un signal plus fort qui effacera le signal légitime. Le système d'identification automatique (AIS) à bord des bateaux permet de connaître l'environnement à proximité du navire équipé et également d'émettre sa position et un ensemble d'information pour les autres. Ce partage d'information permet d'améliorer de façon significative la sécurité des personnes et des biens. Malheureusement, ce système utilisant la VHF n'est pas chiffré, ce qui serait incompatible avec son objectif de sécurité pour tous, et est donc vulnérable. Les informations provenant de ce système ne

peuvent être considérées comme fiables si elles ne sont pas corrélées avec d'autres sources comme le radar par exemple.

Un navire en mer n'est plus complètement isolé du fait du partage d'informations numériques constant. Au contraire, de nombreuses connexions sont présentes. Les informations diffusées par le bateau proviennent entre autres de la connexion satellite à bord et aussi des informations AIS transmises qui se retrouvent sur le réseau Internet. Ainsi, un navire est relié à Internet à la fois directement par sa connexion Internet satellite ou GSM et par les informations qu'il émet par d'autres sources. L'augmentation de la surface d'échange d'information numérique est toujours synonyme d'augmentation du nombre de vulnérabilités et donc d'opportunités pour un attaquant cyber.

Dans ce papier, nous expliquons comment utiliser à la fois les informations émises à proximité du bateau comme l'AIS et le GSM et aussi les informations des navires qui arrivent directement sur Internet dans un but de leurrage. Ce leurrage consiste à créer des différences entre la situation réelle du bateau et la situation affichée sur les consoles de la passerelle. La section 2 fait un rapide état de l'art des travaux sur les vulnérabilités et le leurrage des objets mobiles. La section 3 détaille la méthodologie générale de l'approche en définissant la signature d'un navire et les différentes étapes utilisées pour le leurrage. Des pistes de solutions sont exposées dans la section 4 avant de conclure et proposer des perspectives dans la dernière section.

2 État de l'art

Selon certaines légendes, des naufrageurs faisaient échouer les bateaux à proximité des côtes bretonnes en allumant des feux près de passages dangereux. Leur but était d'amener les navires à penser qu'ils étaient à un endroit sécurisé du fait du faux balisage et ainsi les faire couler. La cargaison était alors récupérée sur la plage pour en tirer profit par les pilleurs d'épaves.

Ce type d'attaque serait-il possible de nos jours avec l'ensemble des équipements à bord des navires ? Système de positionnement par satellite (GNSS), radar, carte électronique et système d'identification des navires permettent une navigation en toute sécurité. Mais ces systèmes numériques peuvent être utilisés à des fins malveillantes, car ils peuvent être trompés et usurpés.

Les systèmes de positionnement par satellites, GNSS (Global Navigation Satellite System), sont au coeur des cyberattaques des objets mobiles. Que ce soient des drones aériens, des voitures autonomes ou bien l'autopilote d'un bateau [2], produire un signal de positionnement qui va masquer le signal légitime est une attaque qui a un fort taux de réussite. En effet, le signal GPS qui est le système le plus utilisé n'est ni chiffré ni authentifié pour l'utilisation civile. Le principe est de créer une fausse constellation de satellites et d'envoyer vers la cible des informations de position ou de temps fausses. Le signal émis à proximité ayant plus de puissance que le signal légitime provenant des satellites géostationnaires, il sera accepté par les appareils de navigation.

Le système AIS (Automated Identification System) permet l'identification des navires à proximité et aussi l'envoi de messages spécifiques pour l'amélioration de la sécurité en mer. Il fait partie des systèmes obligatoirement à bord depuis 2004 à bord des navires d'un certain tonnage, des navires de passagers et des porte-conteneurs ou des navires avec une réglementation particulière.

En 2014, Balduzzi a été un des premiers à montrer que l'utilisation de l'AIS pouvait être détournée [1]. Transmis par VHF et ni chiffré ni authentifié, le signal radio transportant les messages AIS peut donc être reproduit et accepté par les équipements de navigation. Il est possible de parler à la place d'un navire et d'envoyer des informations erronées sur sa position par exemple. Les différentes vulnérabilités et attaques possibles sur ce système ont été largement étudiées [4,5].

3 Méthodologie

Dans cette section nous expliquons comment une plateforme logicielle et radio logicielle pourrait leurrer une partie des systèmes de navigation d'un navire. Cette approche est basée sur l'empreinte numérique d'un bateau. Les équipements à bord d'un navire émettent de nombreux signaux qui peuvent permettre d'établir une signature du bateau. Cette empreinte se compose de trois signatures (Figure 1) :

1. une signature acoustique
2. une signature numérique
3. une signature Radio

Dans notre approche nous ne considérons pas la signature acoustique et portons notre étude sur les signatures numériques et radios que nous décomposons en blocs fonctionnels (Figure 2) :

- Fonction Scanner : c'est une des parties Renseignement d'Origine Source Ouverte (ROSO) du projet qui nous permettra de mieux connaître le navire cible et de récolter des informations techniques qui permettront de définir sa signature numérique.
- Fonction Api-Maritime : Cette fonction nous permettra de mieux connaître les interactions avec les plateformes maritimes connues. Cela permettra d'en comprendre les architectures et la méthode pour y déposer des traceurs fictifs.
- Fonction AIS-GSM : Cette fonction concerne l'émission de signaux AIS et GSM

3.1 Les scanners

L'Open source intelligence (OSINT) jadis réservé aux services de renseignement se démocratise de plus en plus et trouve « toute » sa place dans les milieux journalistiques, société de sécurité informatique, hackers en tout genre pour collecter de l'information en source ouverte afin d'élaborer des chemins d'attaques et



FIGURE 1. Les différentes signatures d'un navire

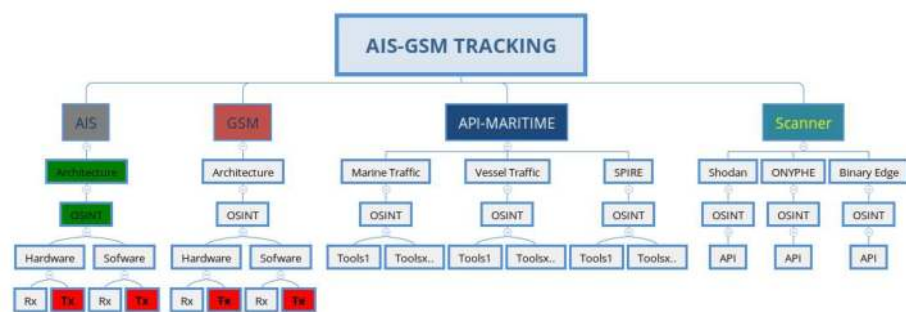


FIGURE 2. Architecture

des empreintes numériques sur des personnes, des biens et des matériels connectés. C'est, appliqué aux environnements maritimes que nous allons confronter ces méthodes. Nous rappelons que le cycle de l'OSINT est itératif et s'applique à des données structurées, non structurées avec des durées de vie sur la toile bien inégales.

Ce qui nous intéresse dans cette fonction de la plateforme c'est d'identifier les outils qui nous permettent de tester l'impact et la réussite ou non de la fonction leurrage de la position AIS par exemple et d'acquérir des données techniques sur les environnements maritimes ciblés par la plateforme.

Un rapide état de l'art des outils et plateformes nous oriente vers des technologies intéressantes :

- les API maritime comme Vessel finder, Marine Traffic, etc..(nous y reviendrons plus loin dans le document).
- Les scanners comme Shodan, Onyphe , Binary edge pour ne citer qu'eux.
- Les bases de données en ligne comme marine-connector.com
- Les réseaux sociaux (image géo localisable de bateau par exemple).

on y voit donc des briques fonctionnelles pour :

- Vérifier le fonctionnement et l'impact sur un trafic réel ou simulé
- Définir des empreintes numériques de système maritime
- Enrichir la connaissance de la plateforme maritime ciblée.

Nous ne traiterons pas l'exhaustivité des outils et des cas d'usage. Mais à des fins d'illustrations et de capacités opérationnelles, prenons comme exemple une recherche en source ouverte sur un équipement de navigation dont les références sont « sailor 900 Vsat ».

Un passage dans un moteur de recherche nous fait comprendre très rapidement que c'est un équipement sensible du bâtiment. Un passage dans un moteur de recherche plus spécialisé nous donne directement des points d'accès sur un système embarqué. Et ceci à des fins de sensibilisation voici quelques exemples d'interface accessible sans déployer d'efforts technologiques. La figure 3 montre l'interface web de communication de l'équipement à bord du navire.

Réinjectons comme données d'entrées les coordonnées GPS dans marine-traffic.com. Nous confirmerons ainsi l'identité du bâtiment se trouvant dans les bases Shodan.

Qui elle nous fait pointer soit sur une interface de réinitialisation d'usine soit une console pour créer des comptes et des autorisations sur le système, soit donner des ordres d'angles de barres (Figure 4).

Nous pouvons ainsi mesurer l'ampleur des vulnérabilités à bord d'un navire. De nombreux scénarios d'attaque peuvent être imaginés en utilisant ce chemin d'attaque.

3.2 API-Maritime

Il est important de comprendre comment un bateau à la côte est visible sur une plate-forme internet , je rappelle ici que notre plate-forme n'est pas imaginée pour la haute mer et que le titre évocateur des « naufrageurs » nous ramène bien

COBHAM

SIGNAL: [Signal strength bars] FINDLAY - SAILOR 900 VSAT

DASHBOARD	
System status	Tracking
GPS position	40°37' N, 80°38' W
Vessel heading	32.5°
Satellite profile	Open Amip
Satellite position	61°W
RX polarisation	Vertical
TX polarisation	X-pol
RX RF frequency	11.730000 GHz
LNB LO frequency	10.750000 GHz
TX RF frequency	13.800000 GHz
BUC LO frequency	12.800000 GHz
Tracking RF frequency	11.730000 GHz
VSAT MODEM	
Model	iDirect Evolution (OpenAMIP)
RX locked status	Locked
Signal level	0 (pwr)
RX IF frequency	980.000000 MHz
TX IF frequency	1000.000000 MHz
TX allowed	Yes
Refresh	

POINTING	
Azimuth, Elevation Geo	151.1° 38.7°
Azimuth, Elevation Rel	121.9° 37.6°
Polarisation skew	-21.6°
TX	
BUC TX	On
BUC output power	[Power level bars]

FIGURE 3. Interface web d'un équipement à bord

ADMINISTRATION

- User login
- User administration
- User permissions
- Export/import config
- Factory default

USER LOGIN

Remember to log out after use

User name:

Current password:

New password:

Retype new password:

[Change](#)

Logout

[Logout](#)

FIGURE 4. Console de ré initialisation

à la côte. Les infrastructures de trafic maritime sur Internet sont enrichies de données par :

- Des données satellitaires
- Des navires équipés d'une balise AIS
- Des antennes côtières
- Des serveurs, de proxy serveur et stockage en réseau
- Des données personnelles de chacun qui peut enrichie la base de données par des photos, des informations techniques.
- D'AISHub et d'AIS dispatcher
- D'internet en général

Nous nous retrouvons donc du plan d'eau au « cloud » en deux clicks de souris. Les inputs sont donc variés pour alimenter ces plateformes et le contrôle d'intégrité et d'authenticité n'est pas aisé ! Faisons un Focus, pour ce module, sur la solution 'AIS-HUB ' et AIS-DISPATCHER. À partir du moment où nous avons notre propre station de réception AIS connecté à internet, nous bénéficions de tout le trafic de la plate-forme AIS-hub.net. Et le trafic qu'il soit réel ou simulé sera repris par cet environnement et sans doute par d'autres. Les solutions proposées, pour certaines sont basés sur des systèmes Raspberry qui couplées à du matériel comme un 'aisHat' et une antenne VHF permettent de monter à moindre coût un 'AISHUB'. Associé à une station côtière, ce système offre également aux autorités portuaires et aux organismes de sécurité maritime la capacité de gérer le trafic maritime et de réduire les risques de la navigation maritime. À savoir également que les flux réseau remontés sont en UDP.

Nous rappelons que l'objectif de la plate-forme n'est pas de récupérer l'intégralité du trafic. Elle a comme cas d'usage d'évaluer la possibilité d'intégrer du trafic simulé dans du trafic réel et éventuellement d'évaluer la possibilité d'avoir un système maritime positionné à plusieurs endroits du globe au même moment voir avec des décalages temporels.

3.3 Module AIS

L'AIS a été développé afin d'améliorer la sécurité de la navigation et un des objectifs était d'améliorer les systèmes d'anticollision. L'analyse de la densité du trafic maritime dans certaines zones maritimes du globe permet de mieux appréhender la nécessité d'un tel système et nous amène son lot de questions si un autre système venait à contrarier les échanges de ces trames de sécurité maritime.

L'AIS est là donc pour améliorer la sécurité de la navigation et ses principales caractéristiques intéressantes pour notre plate-forme sont :

- Les connexions Navire To Navire pour transmettre les AIS.
- Donner des états côtiers pour obtenir des informations sur les navires et cargaisons.
- L'outil VTS (Vesel Traffic System) pour le sens de transmission Navire To Côte

on rappelle que l'AIS souffre de deux maux principaux : la saturation et l'absence de confidentialité pendant l'échange des données.

Afin de pouvoir manipuler des trames AIS il est important de comprendre ce que celles-ci renferment. Une trame AIS est avant tout une trame NMEA qui commence par ‘!AIVDM’ et qui utilise une simple communication série pour transmettre une phrase à un ou plusieurs systèmes en écoute. L’AIS gère l’envoi :

- De la position GPS
- De la vitesse
- Du Cap
- Le Type du canal (A ou B)
- Le lieu et l’heure d’arrivée

Nous ne ferons pas ici une description approfondie des trames AIS le but ici étant d’attirer l’attention du lecteur sur des propriétés intéressantes pour la plate-forme.

Une précision sur le type du canal :

- Type B : Pour les bateaux supérieurs à 300 Tonneaux (passagers, Marine Marchande)
- Type A : Pour les petits bateaux.

De rapides travaux d’OSINT permettront aux lecteurs d’être capables de décoder les messages afin de pouvoir les manipuler.

Nous sommes en présence de trames ASCII. Afin de pouvoir exploiter ces informations dans notre système nous devons être en mesure de les manipuler en réception et en émission c’est-à-dire de pouvoir agir soit sur le format binaire soit sur le format numérique soit sur le format radio. Le but étant de faire du Morphing de trame AIS afin que le trafic simulé soit le plus réel possible. Ce format étant très connu nous trouvons l’ensemble des abaques nécessaires à la transformation des signaux et des trames.

Le module AIS est donc capable d’agir dès que le signal de la trame AIS est transformé en suite binaire. Le système à ce jour n’est pas en mesure de modifier le signal radio, il est cependant bien sûr capable de générer le signal radio et ainsi de construire un ‘base Station AIS’.

3.4 Cas d’étude

L’assemblage de l’ensemble de ces briques permet d’obtenir une plateforme complète de leurrage qui permet à la fois d’agir directement dans le monde de la radio fréquence et dans le monde numérique. Le système est en cours de développement, mais les travaux actuels permettent de mettre en évidence la fragilité des systèmes maritimes à terre et en mer. La figure 5 illustre le fonctionnement général de la plateforme.

La plateforme technique a été réalisée avec un minimum d’investissement, les briques hardwares utilisées peuvent être modifiées et durcis afin d’augmenter les capacités opérationnelles du système. L’idée est d’équiper le système pour caractériser et travailler sur les signatures radio et numérique d’un système naval (nous écartons de ce processus tous les bâtiments militaires ces derniers n’étant pas la cible et plus complexe).

Cet outil se décompose en plusieurs segments :

- Segment réceptions



- Segment émissions
- Segment Manipulation des données
- Segment Récupération des données

Avec cette plateforme expérimentale, il serait possible de :

- Créer des scanners de plate-forme internet de trafic maritime
- Capturer des trames AIS dans un secteur proche du système embarqué
- Scanner la présence d'Access Point Wifi (AP)
- Scanner la présence de Lora, Zigbee
- De ré-émettre via un Hub-AIS des trames AIS sur les ondes radio
- De ré injecter via un Dispatcher-AIS des trames AIS sur les plates-formes de trafic maritime.

Toutes les briques utilisées (hardware et software) sont sur étagères et donc les vulnérabilités présentées sont exploitables.

4 Conclusion

Cette étude des techniques de leurrage d'un navire montre la fragilité des systèmes navals à l'heure actuelle. La multiplication des signaux émis par les bâtiments ainsi que leur grande dépendance à ces données en est la principale raison. La démocratisation des matériels de radio logicielle permet la réalisation de plateformes opérationnelles à moindres frais.

Montrer ces vulnérabilités a pour objectif d'augmenter la compréhension des acteurs des risques ainsi qu'imaginer de nouvelles méthodes de protection. Ces méthodes reposent principalement sur le croisement des informations et aussi et surtout sur la prise en compte des signaux radio.

Afin de contenir les attaques potentielles sur l'AIS et GSM plusieurs solutions sont possibles :

- Croiser les informations ;
- Cartographie et bruits blancs des zones traversées ;
- Nouvelle norme NMEA incluant des champs radio (puissance, type émetteur, indicateur de confiance, . . .) ;
- Formation du personnel aux risques cyber maritimes.

Durcir les protocoles, les normes semble difficile, voire impossible pour certaines applications. Certaines technologies ou certaines applications ne peuvent tout simplement pas être protégées par conception du fait qu'elles doivent être accessibles facilement par le plus grand nombre de personnes. C'est le cas notamment pour le positionnement par satellite ou bien l'identification automatique pour le monde maritime (AIS).

Les travaux en cyberdéfense sont alors à privilégier pour sécuriser les usages de ces systèmes vulnérables. Cela passe dans un premier temps par une meilleure connaissance de l'état cyber des équipements. Cela peut être simple pour certains systèmes, mais la prise en compte de systèmes de systèmes pose rapidement problème. L'évaluation de cette situation cyber et son partage sont l'objet de recherches récentes [6,7,8].

Un aspect important est la détection des tentatives de leurrage afin de redonner de la confiance dans les systèmes de navigation notamment. La détection de cyber attaques est un domaine très actif. Plusieurs travaux s'intéressent au monde maritime en développant de nouvelles approches basées sur l'intelligence artificielle. [9,3]

Références

1. Marco BALDUZZI, Alessandro PASTA et Kyle WILHOIT : A security evaluation of ais automated identification system. *In Proceedings of the 30th annual computer security applications conference*, pages 436–445, 2014.
2. Jahshan BHATTI et Todd E HUMPHREYS : Hostile control of ships via false gps signals : Demonstration and detection. *NAVIGATION : Journal of the Institute of Navigation*, 64(1):51–66, 2017.
3. Clet BOUDEHENN, Jean-Christophe CEXUS et Abdel A. BOUDRAA : A data extraction method for anomaly detection in naval systems. *In 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2020, Dublin, Ireland, June 15-19, 2020*, pages 1–4. IEEE, 2020.
4. Clément IPHAR, Aldo NAPOLI et Cyril RAY : Detection of false ais messages for the improvement of maritime situational awareness. *In Oceans 2015-mts/ieee washington*, pages 1–7. IEEE, 2015.
5. Clément IPHAR, Aldo NAPOLI, Cyril RAY, Erwan ALINCOURT et David BROSSET : Risk analysis of falsified automatic identification system for the improvement of maritime traffic safety. 2016.
6. Olivier JACQ, Xavier BOUDVIN, David BROSSET, Yvon KERMARREC et Jacques SIMONIN : Detecting and hunting cyberthreats in a maritime environment : specification and experimentation of a maritime cybersecurity operations centre. *In 2018 2nd Cyber Security in Networking Conference (CSNet)*, pages 1–8. IEEE, 2018.
7. Olivier JACQ, David BROSSET, Yvon KERMARREC et Jacques SIMONIN : Cyber attacks real time detection : towards a cyber situational awareness for naval systems. *In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pages 1–2. IEEE, 2019.
8. Olivier JACQ, Pedro Merino LASO, David BROSSET, Jacques SIMONIN, Yvon KERMARREC et Marie-Annick GIRAUD : Maritime cyber situational awareness elaboration for unmanned vehicles. *In Maritime Situational Awareness Workshop*, 2019.
9. Nicolas PELISSERO, Pedro Merino LASO et John PUENTES : Naval cyber-physical anomaly propagation analysis based on a quality assessed graph. *In 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2020, Dublin, Ireland, June 15-19, 2020*, pages 1–8. IEEE, 2020.