ISOLA : an innovative approach to cyber threat detection in cruise shipping

Pedro Merino Laso, Loic Salmon, Maya Bozhilova, Ivan Ivanov, Nikolai Stoianov, Grigor Velev, Christophe Claramunt, Yantsislav Yanakiev

ISOLA : an innovative approach to cyber threat detection in cruise shipping

Pedro Merino Laso[1,2], Loic Salmon[1], Maya Bozhilova[3], Ivan Ivanov[3], Nikolai Stoianov[3], Grigor Velev[3], Christophe Claramunt[1], and Yantsislav Yanakiev[3]

[1] Naval Academy Research Institute, Brest, France,
first-name.name@ecole-navale.fr,
[2] French Maritime Academy (ENSM), Nantes, France
pedro.merino-laso@supmaritime.fr,
[3] Bulgarian Defence Institute, Bulgaria
firstcharactersname.lastname@di.mod.bg,

Abstract. Cruise ships nowadays can carry more than 5,500 passengers and 2200 crew members for an average time of seven days per trip. The cruising industry makes up a large proportion of the tourism market, and demand is on the rise. Despite the large numbers of people on board, crime reporting on cruise ships is so far relatively low. While the ship itself faces security threats, activities on board and on shore provide many opportunities for targets and security flaws to be exploited. With the proliferation of activities and data sensors on board there is an urgent need to develop data fusion algorithms in order to provide a global view of an information environment. The research presented in this paper develops an analysis of current cyber risks at sea, with a specific focus on cruising ships, currently under development with the scope of the H2020 ISOLA project. Several fusion algorithms are described and discussed, while further needs for more secure cyber environments are finally discussed.

Keywords: Cruise shipping, Cyber threats detection, Maritime awareness, Data fusion

1 Introduction

Cruise ships today can carry more than 5,500 passengers and 2200 crew members for an average time of seven days per trip. The cruising industry makes up a large proportion of the tourism market, and demand is on the rise. Large ocean liners and cruise ships are being built to accommodate new travel routes as well as high volumes of passengers. The cruise industry contributed to a record €47.86 billion to the European economy in 2017 which represents a significant increase as compared to the previous years.

Cruise operators are challenged to develop competitive cruise packages for potential clients through developing new itineraries, high-quality on board amenities, as well as shore-based excursions giving access to various cultural sites and

activities in the countries where the ships dock. While the delivery of such large services presents unquestionable advantages for clients on board, this opens the room for many security threats. Despite the large numbers of people on board, crime reporting on cruise ships is so far relatively low. While the ship itself faces security threats, activities on board and on shore provide many opportunities for targets and security flaws to be exploited by individuals or groups with motivation to do so. For instance one of the main issues concerns organized groups that intentionally plan to attack vessels at sea, usually piracy or terrorism acts [9]. To address these risks, the Safety of Life at Sea (SOLAS) Convention has included in 2002 an amendment called International Ship and Port Facility Security (ISPS) Code. This code defines minimum security arrangements for ships, ports and government agencies. Therefore, cruise companies nowadays take security threats more seriously, with the objective of designing and implementing the most appropriate strategies and solutions to provide passengers the best security policies and ensure the cruise and its activities are not endangered by any security threats. Furthermore, cyber security has become a major concern in shipping. International Maritime Organization (IMO) has recalled that International Safety Management (ISM) Code demands to achieve and maintain high standards of safety and environmental protection and today maritime companies needs to address cyber security risks [5]. IMO also encourages administrations to ensure that cyber risks are appropriately addressed in safety management systems [4] no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

The aim of this position paper is to introduce current threats and challenges specifically related to cyber risks at sea, and with a specific focus on cruising ships. We first survey current existing protocols and solutions closely associated to threats at sea, as well as the range of suspicious activities on board. The work is part of the European project ISOLA (Innovative and Integrated Security System on Board Covering the Life Cycle of a Passenger Ships Voyage) developed under the scope of the Horizon2020 program. The main objectives of ISOLA are to develop, integrate, test, deploy, demonstrate and validate a systematic and fully automated security approach by incorporating innovative technologies for sensing, monitoring, data fusion, alarming and reporting real-time during illegal incidents at sea. Amongst many objectives, the project explores a collaborative architecture for monitoring and detecting security incidents and events, and early warning methods for the ship security crew to prevent security issues. The approach should take into account the large range of different types of sensors and smart devices deployed in several areas of the ship. In order to provide comprehensive alert systems to the crew, a crucial objective is to develop data fusion algorithms, reasoning and reporting capabilities.

2 Cyber risks in cruising ships

Cruising ships can be considered as small cities on water. They represent an important target to attackers with different goals such as theft or terrorism.

This type of vessel can be a privileged target due to its very large size and information infrastructures on board, lack of cyber security experts on board, isolated networks not specially secured and the difficulty to interact with remote experts too. This section describes the main cyber risks and contingency plans that should be addressed.

2.1 Cyber risks: from threats to vulnerabilities and contingency plans

It has been long recognized that maritime cyber security encompasses an urgent need to raise awareness on cyber threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks. This implies to develop safe practices in ship operations and a safe working environment, assessment of all identified risks to ships, personnel and the environment, establishment of appropriate safeguards, and continuous improvement of safety management skills of personnel ashore and aboard ships.

Maritime cyber risk can be defined as a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures, as a consequence of information or systems being corrupted, lost or compromised. The most important vulnerable systems of a given ship cover a large range of items from ship management and propulsion systems to administrative crew and passenger networks.

Two types of threats generally arise: malicious actions (e.g., hacking or introduction of malware) and unintended consequences of actions (e.g., software maintenance or user permissions). In general, both actions expose vulnerabilities (e.g., outdated software or ineffective firewalls) or exploit a system vulnerability. Effective cyber risk management should consider both kinds of threat. Cyber safety incidents can arise as the result of for instance a cyber security incident, that might affect the availability and integrity of a ship, for example corruption of chart data held in an Electronic Chart Display and Information System (ECDIS), a failure occurring during software maintenance and patching, loss of or manipulation of external sensor data, critical for the operation of a ship – this includes but is not limited to Global Navigation Satellite Systems (GNSS).

When establishing an evaluation of cyber threats, a series of actions should be taken. A first step is the identification of threats and motives of organizations and individuals to exploit cyber vulnerabilities (e.g., obsolete operating systems and networks), inadequate security configurations and practices. A second step is to identify vulnerabilities. A third step is to assess risk exposure, while a fourth step is to develop protection and detection measures. In order to protect critical systems and data, multiple layers of protection measures, which take into account the role of personnel, procedures and should take into account technical (e.g. network, communications and services) and procedural measures (e.g. maintenance, people access, training and awareness). Contingency plans should be implemented. This measures should be also implemented in teleoperated security systems as drones [8]. This includes disconnecting an operating ship from

shore network connection. Disconnecting is likely to prevent the attacker from being able to manipulate safety critical systems or take direct control of the system. Disconnecting could also take place to avoid malware spreading between networks. Finally, a series of measures should be taken to and recover from cyber security incidents.

2.2 Cyber risks at sea

While maritime monitoring capabilities have been largely extended over the past few years, AIS malicious actions are still possible and range from falsification of transmitted data to disappearance of AIS tracks [10]. The detection of deliberate piracy actions clearly requires the implementation of a vessel monitoring system whose objective will be to identify anomalies and abnormal behaviours potentially. In [3], the authors addressed and discussed computational issues associated to the integration of large maritime data flows in order to identify and visualize some phenomena of interest such as regular and abnormal behaviours. Within the scope of the Datacron project [14], and in order to real-time monitor maritime data, ontologies provide appropriate appropriate information representation mechanisms at the conceptual and representation levels to generate relevant data summaries that can be extracted from database implementations.

However, there is also a need to develop and implement some specific real-time algorithms for tracking and categorize the large extent of vessel trajectories anomalies that can reveal some piracy threats or current unfriendly actions. Amongst the potential behaviours that can denote some anomalies and then potential piracy acts that happen at sea let us mention an abnormal change of position, usurpation of identity (or AIS Spoofing) [10]. Some boats can also no longer transmit their positions during a given time intentionally (or Going Dark) [7] and are difficult to detect considering [12] signal loss for AIS data. In order to address all these issues in a timely manner, not only a sound analysis of AIS data should be provided as most of the above approaches do, but also integration of additional sensor-based capabilities provided by Unmanned Aerial Vehicle (UAVs), semi-autonomous or more conventional systems (radars, human observations etc.).

2.3 Cyber risks on board

Ship's cyber security systems are configured individually without a holistic approach so security engineers can mainly have a bird's eye view on the ship's security posture. Network resources (WiFi, bandwidth) are not always separated between individual critical systems, passengers or personnel. Malicious actors can easily target remote assets on a ship to gain access to the main network and compromise the ship's systems. The potential impacted systems are numerous. Some of them are location-based maritime systems as GPS, ECDIS, AIS as mentioned in the previous section, to ship management and control systems such as industrial command and control modules, safety and security systems. Others are specific for cruising shipping and client specific services such as leisure (e.g.,

video, music, video games, internet...) and boarding systems. For instance, the ISOLA security platform under development is addressing a series of information systems such as cameras, drones, RFID as well as external observation systems (e.g., drones).

Updating or redesigning a current ship system security for a standard update or even to counterbalance a given risk might be done on a specific mode, but this is error prone and leads to an increase on the attack surface of the ship's systems. This implies to evaluate these system update operations and for instance to organise these information manipulation operations and techniques on centralised platform as explored by the ISOLA platform under development. These constraints to take into account have to integrate as much information as possible from IP addresses, network ports, domain names, user names, to services running on the ship's infrastructure. Based on this preliminary set of information nodes and data flows, the next step should trigger a probe for weaknesses. Theses weaknesses include software/hardware flaws that can occur from system configurations, outdated software and firmware. They can be identified using open-source tools commonly used by security researchers. For instance, the ISOLA platform objective is to detect probing attacks and exploitation efforts from the previous step by dynamically detecting any vulnerabilities that can be exploited. The ISOLA platform will notify security administrators on the actions they need to take in order to prevent a system compromise.

3 The ISOLA architecture

This section introduces the ISOLA architecture and a practical example of how incoming data can be fused for threat evaluation.

3.1 ISOLA principles

ISOLA integrates a number of heterogeneous modules with the objective to ensure high level of security among all passengers, crews and overall the vessel functions. The ISOLA framework is integrated in the general Ship Security Plan. Each sensor module (Fig. 1 red) is a specialized component whose objective is to detect some predetermined events Fig. 1.

Incoming data is collected and processed with specialised modules. They operate data fusion mechanisms to improve detection mechanisms and improve situation awareness. They support visual analysis, passenger localization, crowd monitoring and sensor processing. Other modules can be activated if needed as by the dispersion module. The emerging semantics of all detected events are harmonised thanks to an ontology. Security situational awareness is achieved thanks to different visualization systems composed by specific interfaces and 3D visualizations. These systems take advantage of the knowledge generated by three modules: threat recognition, crisis classification and decision support.

The ISOLA framework provides additional services and information to passengers and crew thanks to a mobile phone application adapted to particular events. All data and events are stored to create intelligent reports on demand.

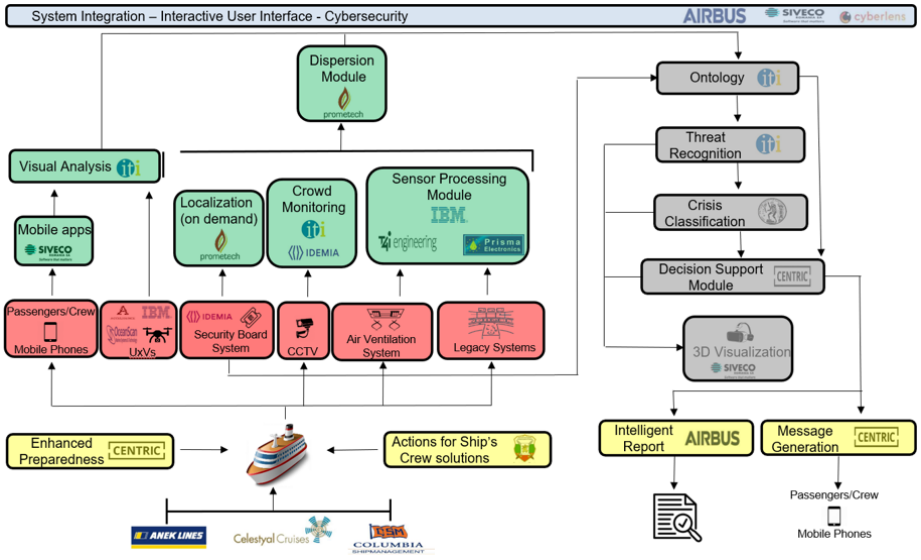

Fig. 1. ISOLA's system architecture.

3.2 Towards Ships data fusion

On the one hand, different heterogeneous data integration solutions have been so far developed for a sound monitoring of vessel trajectories. For instance, Hidden Markov models have been applied to radar-based data and AIS signals to detect suspicious activities [1] while others suggest to combine AUV videos with AIS data [15]. Despite the interest of these approaches the main limitation is that they mainly combine two specific sources of data and cannot cover for example the large range of sensors potentially available, this being specifically the case for large vessels such as cruising ships or very large merchant ships.

On the other hand, different solutions have been developed for detection of threats on airports or on board of vessels, and can be used in the context of cruise shipping. For detection of intrusion of malicious people on board, techniques for people tracking and recognition can be applied [11] [2]. Other works concern also the detection of cyber threats on board, for instance in [13], the authors describe computational vulnerability scanning by using Nessus an industry-leading software.

Different threats on board are to be taken into account. An example of major physical threat is the case of a malicious person who can try to enter the cruising ship. Another threat related to the cyber context lies in is a person on board that may attack network resources and/or to have access to either critical ship systems or passengers' personnel devices. Such malicious actors can easily target remote assets on a ship to gain access to the main network and compromise the ship's systems. At the maintenance level, updating or changing the current system security needs to be done on a device to device form

in manual manner, which is error prone and leads to an increase on the attack surface of the ship's systems. AI algorithms for dynamic detection of vulnerabilities will operate as the main security mechanism of ISOLA. ISOLA security dashboard that will inform security administrators of security issues on their systems and what actions they need to take to mitigate them. At the same time embedded passenger's registration bracelet detectors might locate the presence of the shoplifter and notify the platform accordingly. Holistic security control to assess the security posture of all the ship's infrastructure. Security analysts will be able to assess the security posture of all the systems that the ISOLA platform can have access. Prevent cascading attacks by isolating compromised components. The isolation of components will allow security administrators to resolve security issues by minimizing the impact of those issues have on the rest of the infrastructure.

Under the scope of the ISOLA project, the system to be implemented should integrate a series of state-of-the-art technological achievements from multidisciplinary fields, namely sensors, Internet of Things as well as additional processing mechanisms such as semantic reasoning, high-level analytics, decision support systems, crisis management and situational awareness focusing on passenger's ship security sector and beyond. The objective of the ISOLA monitoring system composed by legacy system of the boat (AIS/GPS and Radar) completed by a fleet of unmanned UxVs, IoT and cameras streams as part of interoperable modalities to detect, assess, evaluate and locate threat actions within existing ships.

The data obtained from ISOLA sensor networks and those from the existing infrastructure of the ships themselves will be processed by the innovative threat detection algorithms and high-level multimodal fusion techniques. By utilising bespoke visual analytics tools, the outcome will be presented to ship security officers and captains via the ISOLA's interactive User Interface. Security officers, authorities, crew, first responders and maritime companies will be enabled to employ the ISOLA's Early Warning and Decision Support System, which also incorporates functionalities for monitoring for external and internal threats in different places of the ship.

The goal is to provide to the officers seamless and valid assessments of the crisis causing by internal or external threats. ISOLA will be deployed and validated in different ship types and different sea border areas (e.g., Mediterranean Sea, North Sea). This prolonged piloting and demonstration process will serve as means to test and refine the deployed approach, including the effectiveness of the innovative technologies, the robustness of the ISOLA platform and its modules, to ensure the interoperability of ISOLA across all demonstrations and finally, to standardise the processes for maritime security.

The interest of the ISOLA approach is that it allows to fuse data from different sources, this providing a sound approach to detect abnormal situations. For instance, when a vessel changes its MMSI or switch off intentionally its signal, this could be detected by comparing AIS data with other data sources such as UAVs videos or radar. If some malicious actions occur on board, the system

raises some alerts to crew members with the help of UAV videos as well a DVATS (Dynamic Vulnerability Assesment and Testing Service) whose aims to reveal the presence of vulnerabilities on the ship. However, there is still a large range of issues that should be further addressed and discussed, from the development of appropriate sensing architectures at large, to data fusion algorithms for cyber detection and threats classification at sea, as well as visualization interfaces still to be developed for both maritime authorities and crew members.

4 Discussion on further needs

To achieve the project's objectives, ISOLA will be developed a number of accurate and reliable components collecting data and process in order to produce knowledge. These tools vary from people localization and area authorization to visual analysis, crowd monitoring for security incidents, and chemical dispersion model. For example, the movements of passengers and crew will be tracked throughout the ship using the Cruise ID. In that way, a tracking infrastructure at critical passageways on board will allow movements to be mapped and crowd densities to be calculated in different areas on the ship. Another component will deal with crowd monitoring from visual content. Within the context of this activity and towards an innovative threat detection toolbox, visual content from video streams will be processed in order to provide the system a higher level of conceptual information that refers to multiple individuals, meaning a crowd analysis framework. This analysis refers to limited cases that include multiple detected individuals and can raise an alert when a suspicious and violent event occurs.

In addition to the previously discussed approaches for enhancing a maritime monitoring capabilities, still there is a range of cyber security capabilities gaps on board of passenger ships that should be addressed. The gaps and suggestion for solutions how to fill these gaps are based on the analysis of user requirements.

The first capability gap is related to lack of dynamic updates of cyber security vulnerability assessment on board. As a solution, ISOLA plan to develop and test a cyber security vulnerability assessment tool. For example, in [13], the authors describe computational vulnerability scanning of the ship's Electronic Chart Display and Information System (ECDIS). There is also a need to scan and assess these risks dynamically, and for all electronic and information systems on board.

The second capability gap concerns security personnel incompetency in strictly following suggested deter actions in case of cyber security incident on board. One possible solution is the system for security alerting, which should provide in real time to the security personnel on board, suggestion about security incidents classification, reaction table, and deter actions escalation, depending on threat criteria and offender's behaviour.

The third capability gap is related to inaccuracy in reporting as regards to all data needed according to formal follow-up report templates. There will be a need to develop and test a system that gives relevant suggestions in real-time to

the security personnel on board about reported data needed, according to the formal follow-up templates, as well as security incidents' timetable and vessel' status and geographic location.

In fact, the second and third capability gaps should be addressed by the development of the ISOLA early warning and decision support system, which will be empowered with enhanced functionalities for visualization and crisis management.

5 Conclusion

As noted at the 2019 SAFETY4SEA London Forum [6], cyber security in maritime is not only an IT issue. For ships specifically and ports, if the issue is a cyber breach, it will have physical consequences – a ship running aground, a collision, or even loss of life. It is not just a loss of data. In that context, it is important to develop and test new approaches by incorporating innovative technologies for sensing, monitoring, data fusion, alarming and reporting real-time during illegal incidents. This will ensure high level of security among all passengers of the ship and augmentation of the Ship Security Plan.

The ISOLA project aims to address the cyber security challenges in a comprehensive end-to-end security way. Starting from the risk and threat analysis in a multi-tier environment, through a network of sensors and C3 (Command, Control and Communications systems) that feeding algorithms with fused information, ISOLA platform will advise and support timely and effectively on board security during the normal routine and also in crisis situations. In fact, building resilience against cyber risks at sea and on board is a challenging and never-ending task.

Acknowledgments

The research leading to these results is part of the ISOLA project that has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement No 883302.

Bibliography

[1] Andersson M, Johansson R (2010) Multiple sensor fusion for effective abnormal behaviour detection in counter-piracy operations. In: 2010 International WaterSide Security Conference, pp 1–7, DOI 10.1109/WSSC.2010.5730221

[2] Bharti Y, Saharan R, Saxena A (2019) Counting the number of people in crowd as a part of automatic crowd monitoring: A combined approach

[3] Claramunt C, Ray C, et al (2017) Maritime data integration and analysis: recent progress and research challenges. In: Proceedings of the 20th International Conference on Extending Database Technology, EDBT 2017, Venice, Italy, March 21-24, 2017, pp 192–197, URL https://doi.org/10.5441/002/edbt.2017.18

[4] International Maritime Organization (IMO) (2017) Guide-lines on maritime cyber risk management. Msc-fal.1/circ.3

[5] International Maritime Organization (IMO) (2017) Maritime cyber risk management in safety management systems. Msc 98/23/add.1

[6] Kapalidis C (2019) Cyber security challenges for the shipping industry URL https://safety4sea.com/cm-cyber-security-challenges-for-the-shipping-industry/ ,accessedon20/01/2021

[7] Kontopoulos I, Chatzikokolakis K, Zissis D, Tserpes K, Spiliopoulos G (2020) Real-time maritime anomaly detection: detecting intentional AIS switch-off. Int J Big Data Intell 7(2):85–96, DOI 10.1504/IJBDI.2020.107375, URL https://doi.org/10.1504/IJBDI.2020.107375

[8] Merino Laso P, Brosset D, Giraud MA (2019) Defining role-based access control for a secure platform of unmanned surface vehicle fleets. In: OCEANS 2019-Marseille, IEEE, pp 1–4

[9] Møller B (2009) Piracy, maritime terrorism and naval strategy. DIIS Report 2009:02, Copenhagen, URL http://hdl.handle.net/10419/59849

[10] Ray C, Iphar C, Napoli A, Gallen R, Bouju A (2015) Deais project: Detection of ais spoofing and resulting risks. OCEANS 2015 - Genova pp 1–6

[11] Ren S, He K, Girshick RB, Sun J (2015) Faster R-CNN: towards real-time object detection with region proposal networks. CoRR abs/1506.01497, URL http://arxiv.org/abs/1506.01497, 1506.01497

[12] Salmon L, Ray C, Claramunt C (2016) Continuous detection of black holes for moving objects at sea. In: Proceedings of the 7th ACM SIGSPATIAL International Workshop on GeoStreaming, IWGS@SIGSPATIAL 2016, California, USA, October 31 - November 3, 2016, ACM, pp 2:1–2:10, DOI 10.1145/3003421.3003423

[13] Svilicic B, Kamahara J, Rooks M, Yano Y (2019) Maritime cyber risk management: An experimental ship assessment. Journal of Navigation 72(5):1108–1120, DOI 10.1017/S0373463318001157

[14] Vouros GA, Andrienko et al GL (2020) Big Data Analytics for Time-Critical Mobility Forecasting, From Raw Data to Trajectory-Oriented Mobility Analytics in the Aviation and Maritime Domains. Springer, DOI 10.1007/978-3-030-45164-6, URL https://doi.org/10.1007/978-3-030-45164-6

[15] Zhou F, Pan S, Jiang J (2019) Verification of ais data by using video images taken by a uav. Journal of Navigation 72(6):1345–1358, DOI 10.1017/S0373463319000262