Understanding Emerging Cyber Attacks and Vulnerabilities Targeting Maritime Systems

Giacomo Longo[*]

Department of Informatics, Bioengineering, Robotics and Systems Engineering (DIBRIS), University of Genova, Italy

Abstract

This paper provides an overview of the emerging threat landscape in the maritime industry, focusing on recently discovered vulnerabilities and exploits targeting boats and their onboard systems. With increasing reliance on advanced technology for navigation, communication, and automation, maritime vessels have become attractive targets for cyber-attacks. This paper explores various threats that can compromise the integrity, confidentiality, and availability of such critical maritime systems.

Keywords

Maritime Cyber Security, Transportation Security, Critical Infrastructure, Autonomous vessels

1. Introduction

The maritime sector plays a crucial role in the global economy, facilitating international trade and enabling the movement of people and goods across the globe. In recent years, there has been a significant increase in the computerization of maritime systems, with vessels now relying on complex networks of interconnected systems to manage everything from propulsion and navigation to entertainment and communication. While this computerization has brought numerous benefits, it has also introduced new cyber risks to the maritime sector. As ships become more reliant on digital systems, they become increasingly vulnerable to cyber attacks that can disrupt operations, compromise sensitive data, or even pose a threat to safety. A ship is a complex system of systems, with components ranging from industrial ones like propulsion, hydraulics, power generation, and waste disposal, to informatic ones like those found in the bridge for navigation, and even mixed ones like combat management and fire control actuators found in navy vessels and submarines. All of these systems must be operated in concert, generating an enormous number of interdependencies and an associated difficulty in segmenting the underlying networks. Sometimes, these systems can even span multiple ships as in the case of monitoring and combat data exchange systems. Individuals operating these systems might lack formal education about cyber risks, which can further increase the impact of such vulnerabilities. Moreover, there is a trend in the industry towards even more automated or fully autonomous ships, which could exacerbate these risks if adequate cybersecurity measures are not put in place. Finally, ships possess unique sensors, such as radar, sonar, and AIS, as well as systems that pose unique challenges. Understanding the emerging exploits and vulnerabilities targeting maritime systems is critical to ensuring the safety and security of this vital sector.

SEBD 2024: 32nd Symposium on Advanced Database Systems, June 23-26, 2024, Villasimius, Sardinia, Italy

[*] Corresponding author.

giacomo.longo@dibris.unige.it (G. Longo)

0000-0003-0025-7191 (G. Longo)

This paper, presented as part of the “doctoral consortium" session, aims to summarize my in-progress research results related to cybersecurity in the maritime sector, focusing on discovered attack techniques and state of the art methodologies.

2. Emerging Methodologies

2.1. Development of ad-hoc testbeds

In the maritime industry, traditional simulators have been extensively used for training vessel operators with a focus on the physical and operational aspects of the ship.However, these simulators fall short when it comes to cyber security analysis, as they do not accurately reproduce the network layouts and protocols found onboard typical vessels. One of the most promising approaches involves modifying existing simulators to maintain their fidelity while augmenting them with external programs that reproduce network endpoints found in actual ships [1, 2, 3, 4]. They also enable the evaluation of anomaly detection strategies' effectiveness by generating realistic datasets based on simulated scenarios. Simulators are also an essential components of “cyber-ranges", virtual reproductions of systems successfully employed in other sectors for training [5] and educational purposes [6]. They provide hands-on opportunities for experts to familiarize themselves with the devices found onboard vessels. Through immersive, experiential learning, professionals can improve their understanding of potential cyber threats and vulnerabilities while practicing incident response, mitigation strategies, and evidence collection techniques in a controlled environment. These tools provide hands-on opportunities for experts to familiarize themselves with real vessel devices, promoting immersive, experiential learning. Professionals can improve their understanding of potential cyber threats and vulnerabilities while practicing incident response, mitigation strategies, and evidence collection techniques [7] in a controlled environment. Finally, testbeds built using these simulators are crucial for implementing honeypots, which gather intelligence about the capabilities of potential attackers [8, 9, 10, 11]. By observing how attackers interact with honeypots, security teams can better understand the latest cyber threats and develop countermeasures to protect against them. However, developing such simulators is a complex task as it requires catering to both physical fidelity and cyber representativeness, while still being able to run at near real-time speeds [12].

2.2. Establishment of Remote Operation Centers (ROCs) and Security Operation Centers (SOCs)

The maritime industry is seeing a growing trend towards centralized monitoring of fleets to improve efficiency in civil operations and boost operational readiness in naval applications. This shift has prompted some cybersecurity-conscious organizations and navies to incorporate vessel data into their Security Operations Centers (SOCs). However, the unique protocols and systems involved with the maritime domain necessitate that SOC experts be *specialized* through dedicated training programs to optimally utilize this information [13]. Still, the challenge of gathering data from fleets is not a straightforward problem, as ships often lack reliable and fast connections. To enable remote monitoring under poorly performing satellite links, adaptive network compression has been employed as an optimization technique [14]. As the industry moves towards autonomous ships, a single Remote Operation Center (ROC) is expected to manage multiple vessels or even entire fleets. However, in its current stage, standardized secure maritime-specific protocols and procedures for interconnecting ROCs and drone ships have yet to be established, as the current satellite interfaces have already been subject to traffic interception attacks [15]. Establishing these guidelines will be crucial for ensuring seamless communication, maintaining operational efficiency, and securing the data transmitted between ROCs and autonomous vessels.

3. Emerging Threats

3.1. Attacks against RADAR systems

Radar systems are among the most important instrument onboard, used by navigators to gather information about the surrounding traffic and obstacles. For a long time, these systems have been deemed secure from external interference, mainly due to the extensive cost and capabilities required to successfully attack them via electronic warfare techniques. However, recent research has started to instead evaluate potential security vulnerabilities stemming from their computerized implementation. For instance, [16] identified several security weaknesses in the computer systems that run radar software, including misconfigurations, outdated operating systems, and unpatched applications. [17] focused instead on supply chain attacks, which involve compromising the integrity of the antenna hardware before it reaches the end-user. An attacker, while still requiring extensive sabotage capabilities, could potentially compromise the generated images used by radar systems without resorting to electronic warfare techniques. Finally, [18] has described an attack technique involving eavesdropping and taking over a radar video flow over the network, with the capabilities of the attacker being enabled by the peculiarities of the networks usually found onboard. This technique could alter the contents displayed by radar systems to conduct malicious activities, such as simulating the effects of electronic warfare to execute a “cyber false flag" attack [19]. By masquerading as an electronic warfare attack, this exploit aims to deceive naval operators about the actual underlying cause.

3.2. Attacks against automation systems

The literature is rich with examples of attacks targeting bridge systems, highlighting vulnerabilities in almost every device subjected to risk assessments or for which documented exploitation techniques exist. However, automation systems on board ships have received less attention. This discrepancy can be attributed to the low commonality across different ship models and the lack of established tooling and datasets related to automation systems. Although each ship is unique, certain systems, such as the steering gear system, have well-defined architectures that are regulated by standards in detail. For example, the International Maritime Organization (IMO) has established standards for the minimum speed at which the rudder blade must rotate. By combining this external knowledge with data gathered (or exfiltrated [20]) from automation systems, it is possible to identify components from these systems on the onboard network. This has enabled attackers to hijack the steering gear system of a simulated cargo vessel by encoding causal relations [21] between setpoints and measured values within the system [22].

3.3. Attacks against autonomous vessels

Although the maritime sector has not yet witnessed widespread adoption of autonomous ships, the industry is gradually embracing autonomy, starting with decision support systems as a first step. The ultimate goal is to achieve entirely robotic vessels, capable of fully autonomous operation under the supervision of a ROC. To facilitate this transition, some collision avoidance algorithms have already been developed [23, 24], which will enable autonomous guidance in near future applications. These collision avoidance maneuvers have strictly regulated outcomes. Every regulations-compliant algorithm, therefore, follows the same trajectories, as described by these regulations. Similar to the exploits targeting the automation system, this predictability puts attackers in an advantageous position. As a result, attackers have been able to successfully reconstruct a collision avoidance algorithms outputs. This capability allows them to manipulate the autonomous ship trajectory to follow a malicious path [25, 26]. This could result in damage to the ship, increased costs associated with voyages, facilitation of piracy, or causing the ship to violate territorial waters.

4. Conclusion

This paper has provided an overview of several emerging cybersecurity threats in the maritime domain. The industry is shifting towards automation and digitalization, which introduces new attack surfaces that can be exploited by malicious actors. Cyber attacks can now target systems previously considered extraneous from such concerns like RADAR, unexpected areas like the steering gear system, and even near-future technologies like collision avoidance algorithms. As a result, there is a growing need for specialized security professionals trained to address these threats. Furthermore, the development of simulators tailored to maritime systems has gained traction as a method for studying emerging cyber attacks and potential mitigations. The establishment of Remote Operation Centers (ROCs) and Security Operations Centers (SOCs) also plays a crucial role in improving the security posture of fleets, but these initiatives require standardized procedures, secure communication protocols, and network compression techniques to ensure their effectiveness. Finally, as autonomous vessels will become more prevalent, it is essential to consider the potential risks associated with their additional systems and develop appropriate countermeasures. Overall, cybersecurity in the maritime domain remains an ongoing research challenge that requires dedicated tooling, analysis, and constant adaptation to discover and mitigate emerging threats.

References

[1] G. Longo, A. Orlich, S. Musante, A. Merlo, E. Russo, Macyste: A virtual testbed for maritime cybersecurity, SoftwareX 23 (2023) 101426. URL: https://www.sciencedirect.com/science/article/pii/S235271102300122X. doi:https://doi.org/10.1016/j.softx.2023.101426.

[2] K. Wolsing, A. Saillard, E. Padilla, J. Bauer, Xlab-uuv – a virtual testbed for extra-large un-

crewed underwater vehicles, in: 2023 IEEE 48th Conference on Local Computer Networks (LCN), 2023, pp. 1–6. doi:10.1109/LCN58197.2023.10223405.

[3] C. Hemminghaus, J. Bauer, E. Padilla, Brat: A bridge attack tool for cyber security assessments of maritime systems, TransNav: International Journal on Marine Navigation and Safety of Sea Transportation 15 (2021).

[4] G. Potamos, A. Peratikou, S. Stavrou, Towards a maritime cyber range training environment, in: 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, pp. 180–185. doi:10.1109/CSR51186.2021.9527904.

[5] E. Russo, G. Longo, M. Guerar, A. Merlo, Cloud-native application security training and testing with cyber ranges, in: J. Bravo, G. Urzáiz (Eds.), Proceedings of the 15th International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2023), Springer Nature Switzerland, Cham, 2023, pp. 205–216.

[6] E. Russo, M. Ribaudo, A. Orlich, G. Longo, A. Armando, Cyber range and cyber defense exercises: Gamification meets university students, in: Proceedings of the 2nd International Workshop on Gamification in Software Development, Verification, and Validation, Gamify 2023, Association for Computing Machinery, New York, NY, USA, 2023, p. 29–37. URL: https://doi.org/10.1145/3617553.3617888. doi:10.1145/3617553.3617888.

[7] A. Cantelli-Forti, Forensic analysis of industrial critical systems: The costa concordia's voyage data recorder case, in: 2018 IEEE International Conference on Smart Computing (SMARTCOMP), 2018, pp. 458–463. doi:10.1109/SMARTCOMP.2018.00046.

[8] J. Pijpker, S. J. McCombie, A ship honeynet to gather cyber threat intelligence for the maritime sector, in: 2023 IEEE 48th Conference on Local Computer Networks (LCN), 2023, pp. 1–6. doi:10.1109/LCN58197.2023.10223347.

[9] M. Lucchese, F. Lupia, M. Merro, F. Paci, N. Zannone, A. Furfaro, Honeyics: A high-interaction physics-aware honeynet for industrial control systems, in: Proceedings of the 18th International Conference on Availability, Reliability and Security, ARES '23, Association for Computing Machinery, New York, NY, USA, 2023. URL: https://doi.org/10.1145/3600160.3604984. doi:10.1145/3600160.3604984.

[10] F. Lupia, M. Lucchese, M. Merro, N. Zannone, Ics honeypot interactions: A latitudinal study, in: 2023 IEEE International Conference on Big Data (BigData), IEEE Computer Society, Los Alamitos, CA, USA, 2023, pp. 3025–3034. URL: https://doi.ieeecomputersociety.org/10.1109/BigData59044.2023.10386497. doi:10.1109/BigData59044.2023.10386497.

[11] A. Cantelli-Forti, M. Colajanni, Adversarial fingerprinting of cyber attacks based on stateful honeypots, in: 2018 International Conference on Computational Science and Computational Intelligence (CSCI), 2018, pp. 19–24. doi:10.1109/CSCI46756.2018.00012.

[12] E. Russo, G. Costa, G. Longo, A. Armando, A. Merlo, Lidite: A full-fledged and featherweight digital twin framework, IEEE Transactions on Dependable and Secure Computing 20 (2023) 4899–4912. doi:10.1109/TDSC.2023.3236798.

[13] M. Raimondi, G. Longo, A. Merlo, A. Armando, E. Russo, Training the maritime security operations centre teams, in: 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 2022, pp. 388–393. doi:10.1109/CSR54599.2022.9850324.

[14] G. Longo, A. Orlich, A. Merlo, E. Russo, Enabling real-time remote monitoring of ships by lossless protocol transformations, IEEE Transactions on Intelligent Transportation

Systems 24 (2023) 7285–7295. doi:10.1109/TITS.2023.3258365.

[15] J. Pavur, D. Moser, M. Strohmeier, V. Lenders, I. Martinovic, A tale of sea and sky on the security of maritime vsat communications, in: 2020 IEEE Symposium on Security and Privacy (SP), IEEE, 2020, pp. 1384–1400.

[16] B. Svilicic, I. Rudan, V. Frančić, D. Mohović, Towards a cyber secure shipboard radar, The Journal of Navigation 73 (2020) 547–558.

[17] G. Meucci, B. Karahoda, A. H. Oveis, F. Mancuso, E. Jajaga, A. Cantelli-Forti, Naval cybersecurity in the age of ai: deceptive isar images generation with gans, in: 2023 IEEE 48th Conference on Local Computer Networks (LCN), 2023, pp. 1–6. doi:10.1109/LCN58197.2023.10223338.

[18] G. Longo, E. Russo, A. Armando, A. Merlo, Attacking (and defending) the maritime radar system, IEEE Transactions on Information Forensics and Security 18 (2023) 3575–3589. doi:10.1109/TIFS.2023.3282132.

[19] G. Longo, A. Merlo, A. Armando, E. Russo, Electronic attacks as a cyber false flag against maritime radars systems, in: 2023 IEEE 48th Conference on Local Computer Networks (LCN), 2023, pp. 1–6. doi:10.1109/LCN58197.2023.10223370.

[20] A. Cantelli-Forti, M. Colajanni, S. Russo, Penetrating the silence: Data exfiltration in maritime and underwater scenarios, in: 2023 IEEE 48th Conference on Local Computer Networks (LCN), 2023, pp. 1–6. doi:10.1109/LCN58197.2023.10223402.

[21] G. Greco, A. Guzzo, F. Lupia, L. Pontieri, Process discovery under precedence constraints, ACM Trans. Knowl. Discov. Data 9 (2015). URL: https://doi.org/10.1145/2710020. doi:10.1145/2710020.

[22] G. Longo, F. Lupia, A. Pugliese, E. Russo, Physics-aware targeted attacks against maritime industrial control systems, Journal of Information Security and Applications 82 (2024) 103724. URL: https://www.sciencedirect.com/science/article/pii/S2214212624000279. doi:https://doi.org/10.1016/j.jisa.2024.103724.

[23] R. Zaccone, M. Martelli, M. Figari, A colreg-compliant ship collision avoidance algorithm, in: 2019 18th European Control Conference (ECC), 2019, pp. 2530–2535. doi:10.23919/ECC.2019.8796207.

[24] R. Zaccone, Colreg-compliant optimal path planning for real-time guidance and control of autonomous ships, Journal of Marine Science and Engineering 9 (2021). URL: https://www.mdpi.com/2077-1312/9/4/405. doi:10.3390/jmse9040405.

[25] G. Longo, M. Martelli, E. Russo, R. Zaccone, Collision-avoidance capabilities reduction after a cyber-attack to the navigation sensors, Proceedings of the International Ship Control Systems Symposium (2022). URL: http://library.imarest.org/record/10729. doi:10.24868/10729.

[26] G. Longo, M. Martelli, E. Russo, A. Merlo, R. Zaccone, Adversarial waypoint injection attacks on maritime autonomous surface ships (mass) collision avoidance systems, Journal of Marine Engineering & Technology 0 (2023) 1–12. URL: https://doi.org/10.1080/20464177.2023.2298521. doi:10.1080/20464177.2023.2298521.