Cyber-Security of Shipboard Navigational Computer-Based Systems

BORIS SVILICIC
Department of Electrical Engineering,
Automation and Computing
University of Rijeka, Faculty of Maritime
Studies Rijeka,
CROATIA

Abstract: This work presents a cyber-security study of three shipboard navigational computer-based systems, the Electronic Chart Display and Information System (ECDIS), Automatic Radar Plotting Aids (ARPA), and Integrated Navigational System (INS). The systems are implemented on three different ships and are of different manufactures. The cyber-security examination was conducted using a software vulnerability scanner. The results have been studied in the context of security measures that are implemented on the ships. It has been shown that critical level cyber risks origin from the unmaintained operating system, its update and unsecured setup.

Keywords: cyber-security, vulnerability scanning, navigational computer-based system, risk assessment

Received: July 13, 2023. Revised: July 5, 2024. Accepted: August 18, 2024. Published: September 5, 2024.

1. Introduction

The ship navigation heavily relies on the cyber physical systems and on the internet for communications. While the cyber-technologies and the connectivity offer immense advantages in terms of improved safety and efficiency of the ship navigation, they also expose ships to new risks [1-8]. Therefore, the maritime cyber risk management has been taken an important role in the safe navigation of ships [9]. The International Maritime Organization has imposed to ship owners and ship management to implement cybersecurity measures in the safety management system of ships before the first annual verification of the Document of Compliance by beginning of the year 2021 [10].

In this work, a study on origins of cyber vulnerabilities in navigational systems implemented onboard ships engaged in international voyage is presented. The study is conducted on the basis of an experimental examination of cyber vulnerabilities of shipboard navigational systems: (i) Electronic Chart Display and Information System (ECDIS) implemented on the training/research ship *Kapitan Gregorio Oca* (IMO: 9859959), (ii) Automatic Radar Plotting Aids (ARPA) implemented on the oil/chemical tanker *Sepen* (IMO: 9311385), and Integrated Navigational System (INS) implemented on the RoPax ship *Marko Polo* (IMO: 7230599). The sips are shown on Fig. 1. The experimental examination was conducted on the basis of vulnerability scanning using a software tool, and results were studied in the context of security measures that are implemented on the ships.

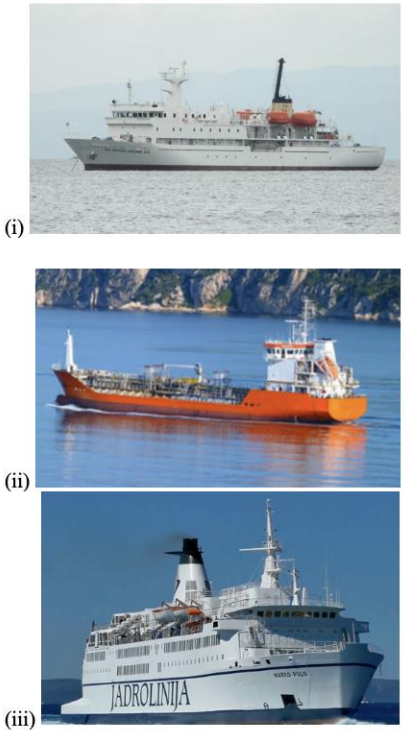

Fig. 1. The ships: (i) *Kapitan Gregorio Oca*, (ii) *Sepen*, and (iii) *Marko Polo*.

2. Experimental Details

The examination of cyber-security vulnerabilities was conducted on three different navigational computer-based systems, the Electronic Chart Display and Information System (ECDIS), Automatic Radar Plotting Aids (ARPA), and Integrated Navigational System (INS). The navigational systems are implemented on three different kind of ships (training/research ship, chemical tanker, Ro-Pax) that are engaged in international voyage. While the navigational systems are of three different manufactures, all the systems are IMO compliant and meets IMO performance standards. The technical details of the systems are given in Table 1.

TABLE I. TECHNICAL DEATILS OF THE SYSTEMS

	Kapitan Gregorio Oca	*Sepen*	*Marko Polo*
Navigational system	ECDIS	ARPA	INS
Manufacturer	Furuno	Japan Radio Company Ltd.	Wärtsilä SAM Electronics
Model	FMD-3200	Alphascan 5925-6X	NACOS MULTIPILOT
Approval date	2017	2016	2017
Installation date	2020	2018	2018

The cyber-security examination was conducted by vulnerability scanning using a widely used software tool, the Nessus Professional version 8.15.2. A laptop with the vulnerability scanner was directly connected to the tested shipboard systems using an Ethernet cross cable (Fig. 2). During the scanning, the ships were docked, and the same scanning model was applied for the testing all the systems.

3. Results Discussion

The vulnerability scanning has resulted in identification of all known cyber security vulnerabilities. The vulnerabilities with the critical severity were detected at ARPA of ship *Sepen* and INS of ship *Marko Polo*. The critical vulnerabilities detected are related to operating system used. In the case of ship *Marko Polo* and INS, the used operating system is Microsoft Windows 7, and in the case of ship Sepen and ARPA, the used operating system is Microsoft Windows Embedded Standard 7. Both operating systems are obsolete since the year 2020, and the third version of the extended security update lasted until October 2023. In addition, on the bot systems, the vulnerable Server Message Block service version 1 (SMBv1) was activated, which correlates to the most known maritime cyber security incident, the NotPetya cyber-attack on the Maersk Line shipping company [11, 12].

(i)

(ii)

(iii)

Fig. 2. Vulnerability scanning of the shipboard systems: (i) ECDIS of *Kapitan Gregorio Oca*, (ii) ARPA of *Sepen*, and (iii) INS of *Marko Polo*.

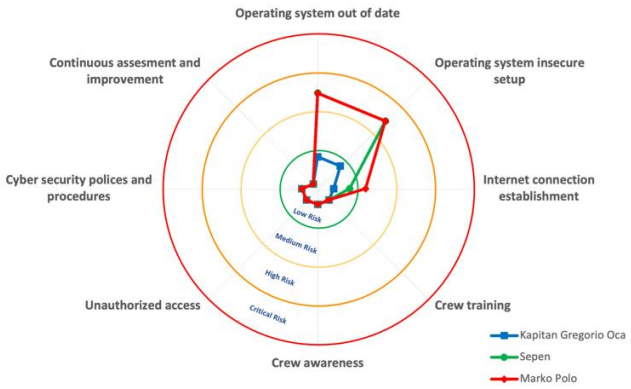

Fig. 3. Origin of cyber risks determined.

While the vulnerability scanning results provides list of all known vulnerabilities detected on the systems, the results could incorrectly reflect real cyber risk level because of the shipboard operating environment specifics [8]. Therefore, the vulnerability scanning results are studied in the context of security measures that are implemented on the particular ship. Information regarding the implemented security measures are collected by interviewing the ship crew. The determined origins of cyber vulnerabilities in the systems are shown on Fig. 3.

The high-level cyber risks are assigned to the obsolete operating system used on ships *Sepen* and *Marko Polo*, and its unsecured setup. The excellent results shown for the ECDIS of the ship *Kapitan Gregorio Oca* are based on the usage of a Linux operating system. It is important to point out that the system are not connected to the Internet. With the systems connection to the Internet, the risk levels would raise to the critical level, requiring immediate mitigation action. The low risk levels, representing acceptable level of risk, are related to the security measures implemented for control of unauthorized access to the navigational systems, implemented security policies and procedures, ship crew continuous training, and continuous assessment and improvement of the systems.

4. Conclusions

The cyber-security study of three shipboard navigational computer-based systems, the ECDIS, ARPA and INS, is presented. The cyber-security examination of the systems, that are implemented on three different ships and are of different manufactures, was conducted using a wildly used software vulnerability scanner. The results have been studied in the context of security measures implemented on the ships. The results obtained suggest that critical level cyber risks origin from the unmaintained operating system, its update and unsecure setup. The results contribute to the knowledge of cyber-security of shipboard navigational systems.

Acknowledgment

The materials and data in this publication have been obtained through the support of the International Association

of Maritime Universities (IAMU) and The Nippon Foundation in Japan.

References

[1] G. Ashraf *et al*., "A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry," IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 2, pp. 2677-2690, Feb. 2023.

[2] X. Huang, *et al*., "A review on risk assessment methods for maritime transport," Ocean Engineering, Volume 279, article 114577, 2023.

[3] K. Tam and K. Jones, " MaCRA: a model-based framework for maritime cyber-risk assessment," WMU Journal of Maritme Affairs, vol. 18, no. 1, pp. 129–163, 2019.

[4] B. Svilicic, M. Kristić, D. Brčić, S. Žuškin, "Paperless Ship Navigation: Cyber Security Weaknesses", *Journal of transportation security*, vol. 13, pp. 1938-7741, 2020.

[5] B. Svilicic, I. Rudan, V. Frančić, D. Mohović, "Towards a Cyber Secure Shipboard Radar", *Journal of Navigation*, vol. 73, pp. 547 - 558, 2020.

[6] B. Svilicic, J. Kamahara, M. Rooks, Y. Yano, "Maritime Cyber Risk Management: An Experimental Ship Assessment", *Journal of Navigation*, vol. 72, pp. 1108-1120, 2019.

[7] B. Svilicic, I. Rudan, A. Jugović, D. Zec, "A Study on Cyber Security Threats in a Shipboard Integrated Navigational System", *Journal of Maritime Science and Engineering*, vol. 7, pp. 364-375, 2019.

[8] Svilicic, B., Kamahara, J., Celic, J., Bolmsten, "Assessing Ship Cyber Risks: A Framework and Case Study of ECDIS Security", *WMU Journal of Maritime Affairs*, vol. 18, pp. 509-520, 2019.

[9] International Maritime Organization (IMO), Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.2, 2022.

[10] International Maritime Organization (IMO), Maritime Cyber Risk Management in Safety Management Systems., MSC 98/23/Add.1., 2017.

[11] United States Computer Emergency Readiness Team, Alert Petya Ransomware, TA17-181A, 2017.

[12] Microsoft, Microsoft Security Bulletin MS17-010 - Critical, 2017.