The 22nd IAMUC
Batumi, 21-22 Oct 2022

Proceedings of the
International Association of Maritime Universities Conference

Towards a Cyber Secure Shipboard ECDIS

Boris Svilicic [1, *], Jeric Bacasdoon [2], Ahmed K. Tawfik [3] and Sam Pecota [4]

[1] *Faculty of Maritime Studies University of Rijeka, Croatia*
[2] *Maritime Academy of Asia and the Pacific, Philippines*
[3] *Arab Academy for Science, Technology and Maritime Transport, Egypt*
[4] *California State University Maritime Academy, USA*
[*] *Corresponding author: boris.svilicic@pfri.uniri.hr; Tel.:* +385-98-529-550.

Abstract: A comparative study of cyber security vulnerabilities in ECDIS systems that are implemented on board of three training ships is presented. The cyber security vulnerabilities have been detected by performing computational testing of the ECDIS systems using a widely used vulnerability scanning software tool. The tested ECDIS systems were chosen from different manufacturers and different underlaying operating systems. The results obtained suggest that the selection of the underlying operating system plays an important role in securing the ECDIS systems. In addition, the results point that the cyber security of ECDIS systems could be significantly violated by exploitation of vulnerabilities in the third-party components of ECDIS software.

Keywords: navigation safety, ECDIS, maritime cyber security, cyber-physical system

1. Introduction

The Electronic Chart Display and Information System (ECDIS) has become a major aid for safe navigation of ships. The ECDIS brings the combination of the paper charts workload reduction and real-time navigational information provision, so the ship's navigational officers can focus on the actual traffic situation, improving the safety of ship navigation (Brčić 2019). The International Maritime Organization (IMO) has setup the requirement for the mandatory ECDIS carriage requirement for all SOLAS vessels (IMO 2017a). With the improvement for nearly three decades, mainly by the integration and networking, ECDIS has developed in a complex cyber-physical system.

The security risks rising from the application of cyber technologies in ECDIS systems has been recognized by the IMO, and therefore the general cyber security guidelines for safeguarding the ship navigation are recently published (IMO 2017b). In addition, the cyber security risks must be adequately implemented in the International Safety Management (ISM) code and periodically audited for ISM code from the beginning of the year 2021 (IMO 2017c).

In this work, we present a comparative study of cyber security threats in ECDIS systems that are implemented on board of three ships, Kraljica mora, Aida IV, and Kapitan Gregorio Oca (Figure 1). In order to perform the comparative study, a computational vulnerability scanning of the ECDIS systems was conducted

(a) (b) (c)

Figure 1. The training ships: (a) *Kraljica mora*, (b) *AIDA IV*, and (c) *Kapitan Gregorio Oca*.

using an industry leading software tool (Svilicic 2020, Svilicic 2019a, Svilicic 2019b, Svilicic 2019c) and by applying the same scanning model. The detected cyber security vulnerabilities are studied and solutions for the risks mitigation are discussed.

2. The Shipboard ECDIS systems

The cyber security vulnerabilities in the current deployment of three ECDIS systems have been studied. The ECDIS systems are implemented on the training ships: (i) Kraljica mora (IMO: 9569358), provided by the University of Rijeka Faculty of Maritime Studies (Croatia), (ii) Aida IV (IMO: 9018775) provided by the Arab Academy for Science, Technology and Maritime Transport (Egypt), and (iii) Kapitan Gregorio Oca (IMO: 9859959) provided by the Maritime Academy of Asia and the Pacific (Philippines). The shipboard EDCIS systems are IMO compliant and meets IMO performance standards. The technical specifications of the ECDIS systems are given in Table 1.

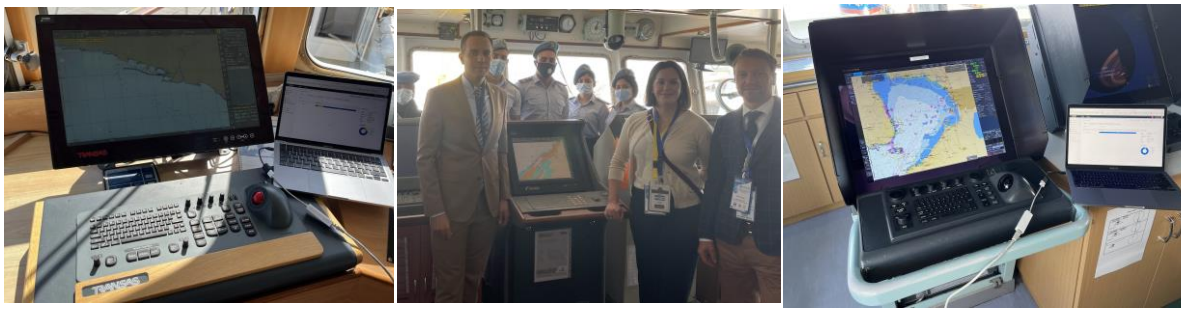
Table 1. Technical specification of the tested ECDIS systems.

ECDIS	*Kraljica mora*	*AIDA IV*	*Kapitan Gregorio Oca*
Manufacturer	Wärtsilä Transas	Transas	Furuno
Model	Navi Sailor 4000	Navi Sailor 4000	FMD-3200
Software version	3.02.350	2.00.012	2450074-03.17
Approval date	2016	2009	2017
Installation date	2019	2010	2020

While the ECDIS system of the training ship AIDA IV is implemented in the stand-alone mode, ECDIS systems of the two other ships are internetworked in a local area network together with a sensor switch. Data from the Global Positioning System (GPS) and Automatic Identification System (AIS) are gathered via serial interfaces. The sensor switch is used for gathering data from radar, gyrocompass, Navtex and other sensors.

3. Cyber Security Testing

The testing of the ECDIS systems was performed by computational scanning for cyber vulnerabilities using a software tool that is most widely used in the industry. The testing software tool used is Nessus Professional, version 8.15.2. (Nessus 2022). The ECDIS systems were tested individually, by connecting a laptop with preinstalled testing software tool to the ships' local area network (Fig. 3).



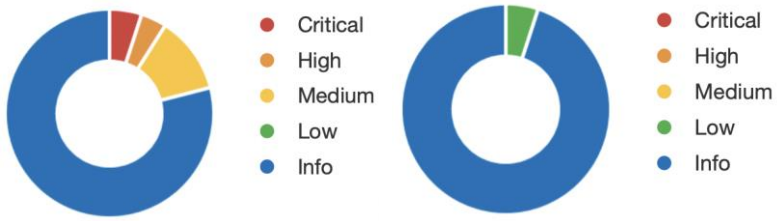
(a) (b) (c)

Figure 2. Cyber security testing of the ECDIS systems implemented on the training ships: (a) *Kraljica mora*, (b) *AIDA IV*, and (c) *Kapitan Gregorio Oca*.

The main objective of the testing is identification of all cyber security vulnerabilities that are known not only to the software developers, but also to potential attackers. The used software tool provides comprehensive database of all known cyber security vulnerabilities, allowing to understand the vulnerability level of the tested ECDIS systems. As the ships are engaged in regular voyage, the tests were conducted is a passive manner, with no disturbance of the ECDIS systems operation, while the ships were docked in a port. The same scanning model was applied for the testing all the ECDIS systems.

4. Results and Discussion

The summary report of the cyber vulnerabilities scanning of the ships Kraljica mora and Kapitan Gregorio Oca are shown on Figure 3. The results obtained indicate high security level of ECDIS systems implemented on the ships Kapitan Gregorio Oca and AIDA IV, while the results show significant vulnerabilities detected on the ECDIS system of the ship Kraljica mora.



(a) (b)

Figure 3. Cyber security vulnerabilities detected: (a) *Kraljica mora*, and (b) *Kapitan Gregorio Oca*.

The ECDIS system on the ship AIDA IV was not tested because the ECDIS software (Table 1) is running on the stan-alone workstation with no hardware for internetworking implemented. However, the ECDIS software is running on the Microsoft Windows XP operating system, which is unsupported by the manufacturer from the year 2014 (Microsoft 2022). The unsupported operating system implies that no new cyber security patches have been released by the manufacturer for about 8 years now. While the ECDIS software is running on the highly vulnerable operating system, the stand-alone implementation with no internetworking ability, provides high level of the cyber security.

The results detected on the ship Kraljica mora (Figure 3a) indicate 3 critical, 2 high and 7 medium cyber vulnerabilities. Exploitation of vulneraries with the critical severity is usually straightforward, meaning that attackers do not need any special knowledge about target systems, and likely results in root-level compromise of target systems. The most critical vulnerability of the ECDIS system is that the ECDIS software is running on the operating system that is unsupported by its manufacturer. In particular, Microsoft Windows 7 Professional operating system has been used, which is not supported by the manufacturer from January 2020 (Microsoft 2022). The remaining critical and high severity cyber security vulnerabilities are related to the vulnerable web server and unsupported version of a system software. In particular, Apache web server version 2.4.49 (Apache 2022) and Python interpreter version 2.7.15 (Python 2022) are running on the ECDIS system. For the both critical vulnerabilities, the support is based on help from members of the communities (Apache and Python communities) who work as enthusiastic volunteers. In addition, the results point out that the significant cyber vulnerabilities exist not only in the software components developed by the manufactures of the ECDIS software (Wärtsilä Transas) or the underlying operating system (Microsoft), but also in the third-party software components (Apache web server and Python interpreter).

The ECDIS system implemented on the training ship Kapitan Gregorio Oca has been shown with low level of cyber security vulnerabilities, having very little impact on the ECDIS operation (Figure 3b). The only vulnerability detected, classified as the low-level, is related to an X11 server running on the ECDIS system. The basis for the excellent cyber security results is in usage of a Linux operating system, which makes the ECDIS system less susceptible to potential cyber security threats. In addition, adequate setup and maintenance of the operating system enhance the level of the ECDIS system cyber security.

5. Conclusions

The cyber security vulnerabilities in the deployment of three shipboard ECDIS systems have been presented. The cyber security testing of the ECDIS system have been done using the industry leading vulnerability scanner. The results obtained show that the highest cyber security level is achieved on the ECDIS system that is based on the Linux operating system, suggesting that the selection of the underlying operating system can play important role to mitigate cyber security risks. In addition, the results point out that the cyber security of ECDIS system could be significantly threaten not only by exploiting vulnerabilities in the

unmaintained ECDIS software and the underlying operating systems, but also by exploiting vulnerabilities in the third-party components of ECDIS software.

Acknowledgements

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

Apache (2019) The Apache Software Foundation. https://www.apache.org/foundation/. Accessed 25 May 2022.

Brčić D, Žuškin S, Valčić S, Rudan I (2019) ECDIS transitional period completion: analyses, observations and findings. WMU J Marit Affairs 18: 359-377. https://doi.org/10.1007/s13437-019-00173-z.

International Maritime Organization (IMO) (2017a) ECDIS—Guidance for Good Practice. https://iho.int/uploads/user/About IHO/International_Organisations/ECDIS-ENC/English/MSC.1-Circ.1503-Rev.1 - Ecdis - Guidance For Good Practice.pdf Accessed 25 May 2022.

International Maritime Organization (IMO) (2017b) Guidelines on maritime cyber risk management. https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf. Accessed 25 May 2022

International Maritime Organization (IMO) (2017c) Maritime cyber risk management in safety manage- ment systems. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf. Accessed 25 May 2022

Microsoft (2022) Microsoft Lifecycle Policy. https://docs.microsoft.com/en-us/lifecycle. Accessed 25 May 2022.

Nessus (2022) Tenable products: Nessus Professional version 8. https://www.tenable.com/products/nessus/nessus-professional. Accessed 25 May 2022.

Python (2022) The Python Community. https://www.python.org. Accessed 25 May 2022.

Svilicic B, Kamahara J, Rooks M, Yano Y (2019a) Maritime cyber risk management: an experimental ship assessment. J Navig 72:1108–1120. https://doi.org/10.1017/S0373463318001157.

Svilicic B, Kamahara J, Celic J, Bolmsten J (2019b) Assessing ship cyber risks: a framework and case study of

ECDIS security. WMU J Marit Affairs 18:509–520. https://doi.org/10.1007/s13437-019-00183-x.

Svilicic B, Rudan I, Jugović A, Zec D (2019c) A study on cyber security threats in a shipboard integrated navigational system. J Mar Sci Eng 7:364–375. https://doi.org/10.3390/jmse7100364.

Svilicic B, Rudan I, Frančić V, Mohović Đ (2020) Towards a cyber secure shipboard radar. J Navig. 73:547-558. https://doi.org/10.1017/S0373463319000808.