Multidisciplinary
SCIENTIFIC JOURNAL
OF MARITIME RESEARCH

University of Rijeka
FACULTY OF MARITIME STUDIES

Multidisciplinarni
znanstveni časopis
POMORSTVO

https://doi.org/10.31217/p.33.2.7

Shipboard ECDIS Cyber Security: Third-Party Component Threats

Boris Svilicic, Igor Rudan, Vlado Frančić, Mateo Doričić

University of Rijeka, Faculty of Maritime Studies, Studentska ulica 2, 51000 Rijeka, Croatia, e-mail: svilicic@pfri.hr

ABSTRACT

The Electronic Chart Display and Information System (ECDIS) plays a central role in safe navigation of ships. The ECDIS is basically a software package running on a general operating system that could be comprised of the third-party components. This paper presents an analysis of cyber security weaknesses of a shipboard ECDIS raising from the ECDIS software's third-party components. The analysis is based on the cyber security testing of the shipboard ECDIS using an industry vulnerability scanner. Detected vulnerabilities are analysed regarding the protection measures implemented on the ship. The results suggest that even the type approved ECDIS system with maintained ECDIS software and the underlying operating system could be vulnerable due to weaknesses in the ECDIS software's third-party components.

ARTICLE INFO

Original scientific paper
Received 17 September 2019
Accepted 14 October 2019

Key words:
Navigation safety
ECDIS
Maritime cyber security
Cyber security testing
Third-party threat

1 Introduction

The Electronic Chart Display and Information System (ECDIS) has significantly changed the ship navigation by providing real-time navigational information and reduction of workload from paper charts (Brčić et al., 2019), and thus enhancing the efficiency and safety. The ECDIS development for about three decades into the complex computer-based system has raised a need to protect the safe navigation from cyber threats (Svilicic et al., 2019a; Tam and Jones, 2019; Svilicic et al., 2019b; Hareide et al., 2018; Kessler et al., 2018; Lee et al., 2017). Therefore, International Maritime Organization (IMO) has imposed to include cyber risk assessment in the International Safety Management (ISM) Code by the 1st January 2021 (IMO, 2017a). As well, additionally to the published general guidelines for managing maritime cyber risks (IMO, 2017b), IMO in collaboration with the International Electrotechnical Commission (IEC) is developing a new related standard for maritime navigation and radiocommunication equipment and systems, IEC 63154 "Cybersecurity – General requirements, methods of testing and required test results" (IEC, 2019).

The ECDIS is basically a software package with standardized functionality by IMO performance standards (IMO, 2017c), which is running on a general operating system from a different manufacturer than the system itself. It has been shown that the ECDIS underlying operating system is a source of major cyber threats (Svilicic et al., 2019b; Svilicic et al., 2019c). However, most of the today`s software is comprised of third-party components, which are developed by an entity other than the manufactures of the software or the underlying operating system. While the usage of the third-party software components allows for acceleration and cost reduction of the development process, vulnerabilities existing in these components can represent a critical threat for the system functionality.

In this paper, cyber security of a shipboard ECDIS is tested in order to analyze cyber threats rising from the ECDIS software third-party components. The tested ECDIS was recently implemented on the training and research ship Kraljica mora of the Croatian Ministry of the Sea, Transport and Infrastructure (Figure 1). The testing method is based on the vulnerability scanning of the ECDIS using an industry leading software tool. The detected vul-

Figure 1 Training and research ship *Kraljica mora*.

Source: Ministry of the Sea, Transport and Infrastructure, https://mmpi.gov.hr

nerabilities are analyzed in the context of the shipboard environment and mitigation solutions are discussed.

2 Shipboard ECDIS

The ECDIS that is IMO type approved displays centrally updated Electronic Navigational Chart (ENC) together with sensor data from mandatory position, heading and speed source shipboard sensors (IHO, 2018; IMO, 2017c). Additional sensor data (radar, AIS, Navtex…) are integrated in the ECDIS depending on the ship`s safety and other factors. The ECDIS represents an equivalent to paper charts and with adequate backup arrangement allows for the paperless navigation (IMO, 2017c; Brčić and Žuškin, 2018; Weintrit, 2018). The ECDIS is mandatory for all ships engaged in international trade since the year 2018 (SOLAS, 2009).

The tested ECDIS is of Wärtsilä Transas manufacturer, model Navi Sailor 4000. The ECDIS is type approved in the year 2016 and was installed on board of the ship in March 2019. Technical specification of the ECDIS is shown in Table 1.

Table 1 The shipboard ECDIS specification.

ECDIS	Manufacturer	Wärtsilä Transas
	Model	Navi Sailor 4000
	Software version	3.00.340
	USCG approval	165.123/33/0
	Approval date	July 2016
	Installation date	March 2019
Charts	IHO RNC	IHO S-57
	IHO RNC	IHO S-61
	IHO Chart Content	IHO S-52
	IHO Data Protection	IHO S-63
Interfaces	Serial NMEA	IEC61162-1
	Serial high speed	IEC61162-2
	Network	IEC61162-450
	Chart Update	USB

Source: Authors

Figure 2 shows the architecture of the tested ECDIS. The ECDIS is operating in the stand-alone configuration. The mandatory sensors data (positioning, heading and speed information) are gathered directly via the serial NMEA interfaces (standard IEC 61162) and the additional sensors data (AIS and NAVTEX) are gathered via Ethernet

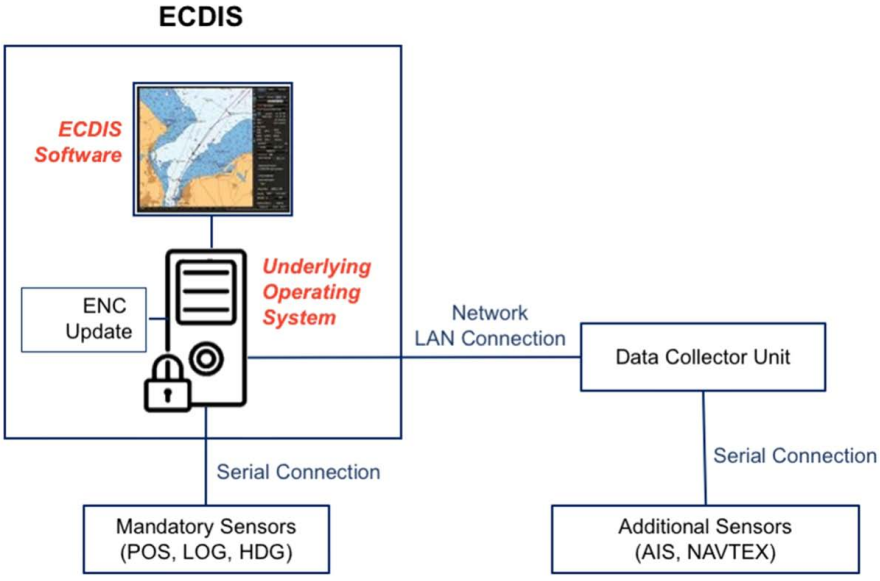

Figure 2 Architecture of the shipboard ECDIS.

Source: Authors

network using a data collector unit for the serial connection of NMEA sensors.

3 Cyber security testing

The cyber security testing of the ECDIS was performed using the industry most widely used vulnerability scanner, the Nessus Professional version 8.0.1 (Nessus, 2019). The vulnerability scanning is a computational method of detecting cyber vulnerabilities, which are known not only to the manufactures of the software and the underlying operating system, but also to potential attackers (Svilicic et al., 2019c; Svilicic et al., 2018). Figure 3 shows the testing setup. A laptop with the Nessus Professional vulnerability scanner is directly connected to the ECDIS using an Ethernet cross cable. Despite the fact that the vulnerability scanning is a passive process, the ship was docked during the testing.

Figure 3 The cyber security testing setup.

Source: Authors

The test results are shown on Figure 4. In total, fifteen vulnerabilities were detected, from which four vulnerabilities were assigned under the high severity and eleven vulnerabilities under medium severity. From 36 pieces of information, the key one is that the ECDIS software is running on the Microsoft Windows 7 Professional operating system. While the underlying operating system was timely updated with the service pack 1 and other security patches, the support for this version of the operating system will end before the end of the current year (Microsoft, 2019). This implies that the manufacturer will not release security patches for newly discovered vulnerabilities.

The detected vulnerabilities are listed in Table 2. All of the detected vulnerabilities with the high severity are related to a web server running on the ECDIS (Table 2, vulnerabilities 1-4). The web server detected is a freely available software provided by the Apache Software Foundation, and in our case represents the third-party component of the ECDIS software. The version of the web server is Apache 2.2, which is obsolete by its provider since December 2017 (Apache, 2019). As in the case of

Figure 4 Summary report of the vulnerability scan.

Source: Authors

Table 2 Detected ECDIS cyber vulnerabilities.

	Service	Vulnerability description	Severity
1-4	Web server	The version of the Apache web server running on the ECDIS is obsolete and no longer maintained the manufacturer.	High
		The version of the Apache web server running on the ECDIS is affected by multiple vulnerabilities. An attacker could cause a denial of service condition, gain unauthorised access or cause the ECDIS to crash.	
5-14	Web server	The version of the Apache web server running on the ECDIS is affected by multiple vulnerabilities. An attacker could cause a denial of service condition, execute code, obtain sensitive information, execute cross-site scripting attacks or cause the ECDIS to crash.	Medium
15	File/printer sharing	Signing is not required on the Microsoft Server Message Block (SMB) service version 1. An unauthenticated, remote attacker can conduct man-in-the-middle attacks against the ECDIS.	
1-36	Underlying operating system	The ECDIS is running Microsoft Windows 7 Professional version of the underlying operating system.	Info
		A file/print sharing service based on Microsoft Server Message Block version 1 protocol is running on the ECDIS.	
		Identification of services running on the ECDIS is possible.	

Source: Authors

Table 3 Cyber threats from ECDIS's third-party components.

	Threat	Description	Possible solution
1	Third-party components abandoned	Allows for the exploitation of well known vulnerabilities of the ECDIS software's third-party components	The third-party components' migration to a version recommended by the manufacturer
2	Third-party components out of date	Allows for the exploitation of well known vulnerabilities of the ECDIS software's third-party components	Patching of the third-party components with the provider's security updates
3	Third-party components insecure setup	Allows for the exploitation of default setup with no security features activated	Secure setup of the third-party components

Source: Authors

Microsoft operating system, Apache community does not provide support for this version of the web server, allowing an attacker to exploit newly discovered and known vulnerabilities. In addition, the support relies on help from the community members who work as volunteers. The provider's recommended solution for the detected vulnerabilities is migration to the actual version of the web server.

From the eleven medium severity vulnerabilities detected, ten are also related to the third-party web server running on the ECDIS (Table 2, vulnerabilities 5-14). One of the medium severity vulnerabilities detected (Table 2, vulnerability 15) is related to the underlying operating system and its standard component, the Server Message Block (SMB) version 1. The SMB provides file/printer sharing service. Despite the fact that the Microsoft operating system is updated with the timely security patches, the manufacturer`s recommendation is to use newer versions of the SMB due to lack of security features implemented in the version 1 (Microsoft, 2018).

4 Results and discussion

Even the cyber security test allows for detection of all know vulnerabilities existing in the ECDIS, the results could reflect incorrectly the real severity of threats due to specifics of the shipboard operating environment. Therefore, the test results are analyzed regarding the implemented protection measures on the ship. The implemented protections were identified by interviewing the ship's navigational ranks. The protections include the physical access controls for unauthorized personnel that are implemented, security procedures that are adhered, the crew is trained by the ECDIS's vendor, ENCs are updated in controlled manner with an USB memory stick provided by the manufacture, and the ship is continuously assessed. The identified cyber threats from the ECDIS's third-party components together with the description and possible solution are listed in Table 3.

In total, three cyber threats are identified, from which all are related to the maintenance of the ECDIS software's third-party components, in particular the fact that the third-party components are abandoned, out of date and insecurely setup. As the ECDIS is operating in the stand-alone configuration without connection to the Internet or an internal ship network, the identified threats represent risks that are acceptable for a short time, but require development of the mitigation plan. The threats' solving solutions include migration from the obsolete to actual version of the third-party components, patching with security updates released by the manufacturer and secure setup of the third-party components. It is important to point out that these maintenance activities not only of the ECDIS software's third-party components, but also of the underlying operating system (in our case in the close future, as shown in Chapter 3) could affect negatively the ECDIS software functionality, and therefore are to be done by the ECDIS manufacturer authorized personnel.

The results show that despite the fact that the shipboard ECDIS is the type approved, with the latest version of the ECDIS software, and running on the updated underlying operating system, significant cyber weaknesses exist on the ECDIS due to unmaintained ECDIS software's third-party components. It is worth noting that the web server features are not necessary needed for the regulated ECDIS software functionality, particularly not for the operation in the stand-alone configuration. This together with the significant risk from the cyber vulnerabilities suggest that the third-party components should not be used in the software's development process of the critical ship navigation systems.

5 Conclusion

The cyber security analysis of the ECDIS software's third-party components is presented. The analysis is based on the cyber security testing of the shipboard ECDIS with an industry leading vulnerability scanner. Three cyber threats identified that require development of the mitigation plan are related to the maintenance of ECDIS software's third-party components, in particular the migration to the actual version, patching with security updates and secure setup. The results suggest that even the ECDIS software and underlying operating system are maintained, the system could be vulnerable due to weaknesses in the ECDIS software's third-party components.

The presented study contributes to development of the upcoming maritime standard IEC 63154 and indicates the testing results that should be targeted. The obtained results contribute to knowledge of ECDIS cyber security and are applicable to any shipboard navigation system.

Acknowledgment

The research was financially supported by the University of Rijeka under the research project Cyber Security of Maritime ICT-Based Systems (grant number: uniri-tehnic-18-68).

References

[1] Brčić, D., Žuškin, S., Valčić, V., Rudan, I. (2019). ECDIS transitional period completion: analyses, observations and findings. *WMU Journal of Maritime Affairs*, 18, 359-377.

[2] Brčić D., Žuškin S. (2018). Towards Paperless Vessels: A Master's Perspective. Pomorski zbornik, 55, 183-199.

[3] Hareide, O.S., Jøsok, Ø., Lund, M.S, Ostnes, R. and Helkala, K. (2018). Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*, 71, 1025-1039.

[4] International Electrotechnical Commission (IEC). (2019). Maritime navigation and radiocommunication equipment and systems – Cybersecurity – General requirements, methods of testing and required test results. IEC 63154 ED1.

[5] International Hydrographic Organization (IHO) (2019). Current IHO ECDIS and ENC Standards. Monaco: IHO.

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

[7] International Maritime Organization (IMO). (2017b). Guidelines on maritime cyber risk management. MSC-FAL.1/Circ.3. International Maritime Organization.

[8] International Maritime Organization (IMO). (2017c). ECDIS – Guidance for Good Practice, Resolution MSC.1/Circ.1503/Rev.1. International Maritime Organization.

[9] International Maritime Organization (SOLAS). (2009). MSC.282(86): Adoption of amendments to the International Convention for the Safety Of Life At Sea, 1974. Annex 1. London: IMO.

[10] Kessler, G.C., Craiger, J.P., Haass, J.C. (2018). A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 12, 429-437.

[11] Lee, Y.C., Park, S.K., Lee, W.K. and Kang, J. (2017). Improving cyber security awareness in maritime transport: A way forward. *Journal of the Korean Society of Marine Engineering*, 41, 738-745.

[12] Microsoft. (2019). Microsoft: Search product lifecycle. Available: https://support.microsoft.com/en-us/lifecycle.

[13] Microsoft. (2017). Microsoft Security Bulletin MS17-010 – Critical. Available: https://technet.microsoft.com/library/security/MS17-010.

[14] Nessus. (2019). Tenable Products: Nessus Professional. Available: https://www.tenable.com/products/nessus/nessus-professional.

[15] Svilicic, B., Kamahara, J., Rooks, M., Yano, Y. (2019a). Maritime Cyber Risk Management: An Experimental Ship Assessment. *Journal of Navigation*, 72, 1108-1120.

[16] Svilicic, B., Brčić D., Žuškin S., Kalebić D. (2019b). Raising Awareness on Cyber Security of ECDIS. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 13, 231-236.

[17] Svilicic, B., Kamahara, J., Celic, J., Bolmsten, J. (2019c). Assessing Ship Cyber Risks: A Framework and Case Study of ECDIS Security. *WMU Journal of Maritime Affairs*, in press. DOI: 10.1007/s13437-019-00183-x

[18] Svilicic, B., Rudan, I., Frančić, V., Mohović, Đ. (2019d). Towards a Cyber Secure Shipboard Radar. *Journal of Navigation*, in press. DOI: 10.1017/S0373463319000808

[19] Svilicic, B., Celic, J., Kamahara, J., Bolmsten, J. (2018). A Framework for Cyber Security Risk Assessment of Ships. *19th Annual General Assembly (AGA) of the International-Association-of-Maritime-Universities (IAMU)*, pp 21-28, Barcelona, Spain.

[20] Swiss Government Computer Emergency Response Team (CERT CH). (2017). Notes About The NotPetya Ransomware. Available: https://www.govcert.admin.ch/blog/32/notes-about-the-notpetya-ransomware#

[21] Tam, K., and Jones, K., (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18, 129-163.

[22] The Apache Software Foundation (2019). Available: https://www.apache.org/foundation.

[23] The Apache Software Foundation (2019b). Apache Web Server 2.2 vulnerabilities. Available: https://httpd.apache.org/security/vulnerabilities_22.html.

[24] United States Computer Emergency Readiness Team. (CERT US). (2017). Alert (TA17-181A) Petya Ransomware. Available: https://www.us-cert.gov/ncas/alerts/TA17- 181A.

[25] Weintrit, A. (2018). Clarification, Systematization and General Classification of Electronic Chart Systems and Electronic Navigational Charts Used in Marine Navigation. Part 1 – Electronic Chart Systems. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 12, 471-482.