21st Annual General Assembly
IAMU AGA21
26th- 28th October 2021

Shipboard ECDIS: Cyber Security Challenges

Boris Svilicic[a], Sam Pecota[b], Jeric Bacasdoon[c], Ahmed K. Tawfik[d]

[a] Faculty of Maritime Studies University of Rijeka, Croatia
[b] California State University Maritime Academy, USA
[c] Maritime Academy of Asia and the Pacific, Philippines
[d] Arab Academy for Science, Technology and Maritime Transport, Egypt

INTRODUCTION

The Electronic Chart Display and Information System (ECDIS) has strongly influenced how ships are navigated. The ECDIS meets the International Maritime Organization (IMO) requirement for the nautical charts carriage and the IMO mandatory ECDIS carriage requirement is currently in force for all SOLAS vessels [1]. The paper charts workload reduction and real-time navigational information provided by the ECDIS have allowed the ship's command to focus on the actual traffic situation, and thus the safety of ship navigation is improved [2]. The ECDIS has been improved for nearly three decades, primarily on the basis of integration and networking, which resulted in development of a complex cyber-physical system.

The IMO has published the Guidelines on maritime cyber risk management, which offers general guidelines for safeguarding the ship navigation from cyber threats and risks [3]. In addition, IMO has imposed that cyber security risks are to be adequately implemented in the International Safety Management (ISM) code and the periodical audit of ships for ISM code by 1st January 2021 [4].

In this work, we present an analysis of cyber security challenges in ECDIS system implemented on board of a ship. The analysis is based on experimental cyber security testing of a shipboard ECDIS with a vulnerability scanning software tool [5]. The tested ECDIS is implemented on the training ship *Kraljica mora* of the Faculty of Maritime Studies Rijeka, University of Rijeka, Croatia.

EXPERIMENTAL DETAILS

Figure 1 Training and research ship *Kraljica mora*.

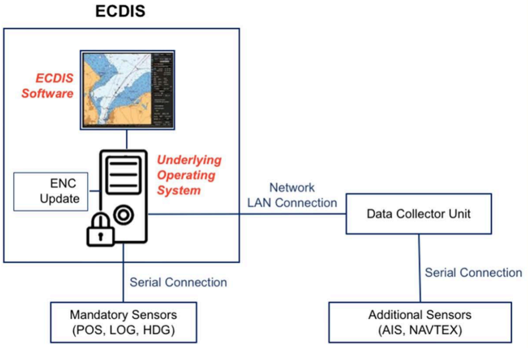


Figure 2 Architecture of the shipboard ECDIS.

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

RESULTS

Testing setup

- Testing was performed using the industry most widely used vulnerability scanner, the Nessus Professional version 8.0.1
- A laptop was directly connected using an Ethernet cross cable
- Despite the fact that the vulnerability scanning is a passive process, the ship was docked during the testing

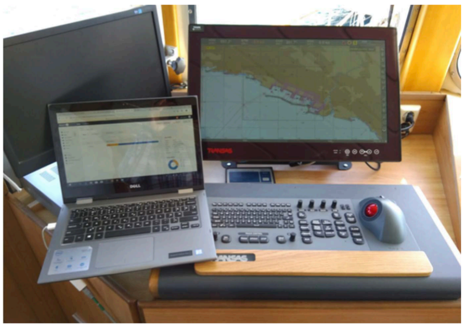
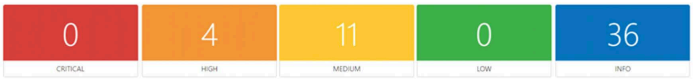


Figure 3 The cyber security testing setup.



0	4	11	0	36
CRITICAL	HIGH	MEDIUM	LOW	INFO

Figure 4 Summary report of the vulnerability scan.

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.	

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

CONCLUSIONS

- The cyber security analysis of the shipboard ECDIS, which is based on the testing with an industry leading vulnerability scanner, is presented.
- 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.
- Future work: testing of ECDISs implemented on training ships *Golden Bear* (CSUMA), *Aida IV* (AAST-MT) and *Kapitan Gregorio Oca* (MAAP)

References

[1] IMO, MSC-FAL.1/Circ.3, 2017.

[2] D. Brčić, et al., *WMU JoMA*, 18 (2019), 359-377.

[3] IMO, MSC-FAL.1/Circ.3, 2017.

[4] O.S. Hareide, et al., *J. of Nav.*, 71 (2018), 1025-1039.

[5] B. Svilicic, et al., *J. of Nav.*, 72 (2019), 1108-1120.

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.