Cyber Security Testing of Shipboard Chart Radar

Boris Svilicic [a,*], Igor Rudan [a], Alen Jugović [a], Damir Zec [a]

[a] Faculty of Maritime Studies University of Rijeka,
Studentska ulica 2, HR-51000, Rijeka, Croatia

[*]Corresponding author. E-mail: e-mail: svilicic@pfri.hr.

Keywords: navigation safety, shipboard navigation systems, chart-radar, maritime cyber security, cyber security testing

ABSTRACT
Shipboard navigation systems have been intensively developed for the last two decades, resulting in complex and computer based technology systems. The chart-radar is an onboard navigation system that integrates electronic navigational charts with the full radar functionality, thus allowing improved efficiency and safer navigation. In this work, we present cyber security testing of a chart-radar system implemented on an SOLAS ship sailing on international route. The cyber security testing method aligns with the upcoming maritime standard IEC 63154. The testing was performed using a widely deployed solution for application vulnerability detection. Solving solutions for the identified vulnerabilities are studied.

1. INTRODUCTION

Shipboard navigation systems have been intensively developed for the last two decades by means of digitalization, network integration and software development, which resulted in complex and computer based technology systems. Therefore, safeguarding shipping from cyber threats is gaining increasing relevance in the development of shipboard navigation systems [1-6]. Recently, the International Maritime Organization (IMO) issued the Guidelines on maritime cyber risk management, which offers general recommendations for shipping protection from cyber vulnerabilities and threats. [7]. IMO has also placed to incorporate cyber risk assessment in the implementation of the International Safety Management Code on vessels by start of the year 2021 [8]. In addition, International Electrotechnical Commission (IEC) is preparing a new maritime standard IEC 63154 “Maritime navigation and radiocommunication equipment and systems - Cybersecurity - General requirements, methods of testing and required test results”, which should be published in April 2021 [9].

The radar equipment is considered as a critical navigation system for safe navigation and collision avoidance. With additional integration of electronic navigational charts (ENC) with the full radar functionality (the chart-radar system), the improved efficiency and safety at sea is provided. The chart-radar is, however, essentially a software application running on a standard computer with installed a general operating system. While IMO regulations

standardize radar operational software performance [10], the supporting hardware and software is arranged by ship-owners and implemented by radar equipment manufacturers.

Recently, we presented a cyber risk assessment of a ship based on computational cyber security testing method for identification of cyber threats [1]. In this work, we have tested cyber security of a chart-radar implemented on a SOLAS certified ship sailing on an international route (Figure 1). The chart-radar (which is IMO compliant) was tested by performing vulnerability scanning using a widely deployed solution for application vulnerability detection. The identified cyber vulnerabilities together with possible solutions are studied.

Figure 1. The vessel on-board which cyber security testing was conducted.

2. CHART-RADAR

The tested chart-radar is of Wärtsilä SAM Electronics manufacture, model NACOS RADARPILOT Platinum. The chart-radar is IMO compliant and the radar software meets IMO performance standards. The type approval dates from the year 2017 and chart-radar was installed on the ship in the year 2018. The chart-radar technical specification is given in Table 1.

Table 1. The chart-radar specification.

INS	Manufacturer	Wärtsilä SAM Electronics GmbH
	Model	NACOS RADARPILOT Platinum 2017
	Software version	2.1.02.10
	IMO compliant	Yes
Charts	IHO ENC	IHO S-57 (Edition 3.1.1)
	IHO RNC	IHO S-61 (Edition 1.0)
	IHO Chart Content	IHO S-52 (Edition 6.1.1)
	IHO Data Protection	IHO S-63 (Edition 1.2.0)
Interfaces	Serial NMEA	IEC61162-1
	Serial high speed	IEC61162-2
	Network	Ethernet (LAN)
	Chart Update	USB
	Remote maintenance	Possible

The chart-radar is installed in the stand-alone configuration, with no Internet connection established. Data from radar, GPS, AIS, gyrocompass, log and NAVTEX are

gathered directly via serial interfaces, while the Electronic Navigational Charts (ENC) are updated with an USB memory stick provided by the manufacturer.

3. CYBER SECURITY TESTING

The cyber security testing was performed using a widely deployed solution for application vulnerability detection, Nessus Professional [11]. The vulnerability scanning provides automatic detection of all cyber vulnerabilities that are known not only to software manufactures, but as well to potential attacks [12]. The testing was conducted by directly internetworking a laptop with Nessus Professional scanner to the chart-radar. The testing setup is shown on Figure 2.

Figure 2. Cyber security testing of the chart-radar.

The testing was performed without administrative privileges, while the chart-radar software was running under administrative privileges. Even the testing is a passive process, during the scan the ship was docked in a port.

4. RESULTS DISCUSSION

Summary of the results obtained with the test is shown on Figure 3. In total, 14 risky vulnerabilities were detected. According to the severity level, 2, 1, 9 and 2 were assigned with critical, high, medium and low level respectively.

Figure 3. The test summary report.

List of detected vulnerabilities is given in Table 2. The critical severity vulnerabilities detected (Table 2, vulnerabilities 1 and 2) are related to weaknesses of services running on

the chart-radar underlying operating system, Microsoft Windows 7 Professional Service Pack 1. For the maritime community, Server Message Block (SMB) service vulnerability (Table 2, vulnerability 1) is particularly important because of the NotPetya ransom-ware attack on Maersk container shipping company, in which the NotPetya malicious software was worldwide spreading using the detected vulnerability [13]. In addition to system patching and anti-malware software usage, the preventive solution recommended by the manufacturer (Microsoft) is to disable or block SMB v1 [14].

Table 2. The chart-radar cyber vulnerabilities detected.

	Name	Description	Severity
1	SMB v1 service	Chart-radar is affected by remote code execution vulnerabilities exist in the Server Message Block (SMB) service version 1.	Critical
2	Secure Channel	Chart-radar is affected by a remote code execution vulnerability due to improper processing of packets by Secure Channel security package.	Critical
3	RDP service	An arbitrary remote code vulnerability exists in the implementation of the Remote Desktop Protocol (RDP) on the chart-radar.	High
4	SAM and LSAD protocols	Chart-radar is affected by an elevation of privilege vulnerability in Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols.	High
5	Terminal Service	Remote Desktop Protocol Server (Terminal Service) running on the radar is vulnerable to a man-in-the-middle attack.	Medium
6	Terminal Service	Terminal Services service running on the radar doesn't use Network Level Authentication only.	Medium
7	Terminal Service	Terminal Services service running on the radar is not configured to use strong cryptography.	Medium
8	SMB signing	Signing is not required on the chart-radar through Server Message Block (SMB) service.	Medium
10	SSL certificate	Secure Shell Layer (SSL) certificate of the chart-radar cannot be trusted.	Medium
11	SSL certificate	An Secure Shell Layer (SSL) certificate in the certificate chain has been signed using a weak hash algorithm.	Medium
12	SSL certificate	Chart-radar supports the use of medium strength Secure Shell Layer (SSL) ciphers.	Medium
13	SSL certificate	Secure Shell Layer (SSL) certificate chain for the chart-radar ends in an unrecognized self-signed certificate.	Medium
14	SSL certificate	Secure Shell Layer (SSL) certificate of the chart-radar supports the use of RC4 in one or more cipher suites.	Low

The high severity vulnerabilities detected (Table 2, vulnerabilities 3 and 4) are related to weaknesses of active services on the chart-radar, allowing for possible unauthorized remote code execution and unauthorized access gaining. The recommended solution is installation of security patches released by the underlying operating system provider. The detected medium and low severity vulnerabilities (Table 2, vulnerabilities 5 - 14) are related to the active services' weaknesses that allow for establishment of unauthorized access or cause a denial of service condition of the char-radar. Possible solutions include installation of the provider's security patches and adequate reconfiguration of the underlying operating

system. Implementation of all of the solutions could impact the chart-radar functionality, and therefore is to be conducted only by the chart-radar manufacturer. While the solutions provide protection from know vulnerabilities, protection from newly discovered vulnerabilities would be to disable unnecessary services offered by general operating systems. As it is shown with the cyber security test conducted, source of the detected vulnerabilities (Table 3) is in active services of the chart-radar underlying operating system, which are actually not required for the expected chart-radar functionality.

5. CONCLUSIONS

Cyber security testing of a shipboard chart-radar is presented. The testing method is based on cyber vulnerability detection using a widely deployed solution for application vulnerability detection. The results have shown that cyber vulnerabilities are in active services of the chart-radar underlying operating system, which are all unnecessary for the expected chart-radar functionality. The cyber security testing and obtained results contribute to the knowledge on maritime cyber security and highlights importance for development of the upcoming maritime cyber security standard IEC 63154.

ACKNOWLEGEMENTS

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] B. Svilicic, J. Kamahara, M. Rooks, Y. Yano, "Maritime Cyber Risk Management: An Experimental Ship Assessment," *Journal of Navigation*, 2019, doi:10.1017/S0373463318001157.

[2] K. Tam, K. Jones, "MaCRA: a model-based framework for maritime cyber-risk assessment," *WMU Journal of Maritime Affairs*, Vol. 18, pp 129-163, 2019.

[3] B. Svilicic, D. Brčić, S. Žuškin, D. Kalebić, "Raising Awareness on Cyber Security of ECDIS," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, Vol. 13, No. 1, pp. 231-236, 2019.

[4] A. Goudossis, S.K. Katsikas, "Towards a secure automatic identification system (AIS)," *Journal of Marine Science and Technology*, Vol. 24, pp. 410-423, 2018.

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

[6] G.C. Kessler, J.P. Craiger, J.C. Haass, "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*, Vol. 12, No. 3, pp. 429 - 437, 2018.

[7] International Maritime Organization. 2017. Resolution MSC-FAL.1/Circ.3, Guidelines on Maritime Cyber Risk Management. London: IMO.

[8] International Maritime Organization. 2017. Resolution MSC.428(98), Maritime Cyber Risk Management in Safety Management Systems. London: IMO.
[9] International Maritime Organization. 2007. Resolution MSC.192(79), Adoption of the Revised Performance Standards for Radar Equipment. London: IMO.
[10] International Electrotechnical Commission (IEC). 2019. IEC 63154 Maritime navigation and radiocommunication equipment and systems - Cybersecurity - General requirements, methods of testing and required test results.
[11] B. Svilicic, J. Kamahara, J. Celic, J. Bolstmen, "Maritime Cyber Risk Management: An Experimental Ship Assessment," *19th Annual General Assembly (AGA) of the International-Association-of-Maritime-Universities (IAMU)*, pp. 21-28, 2019.
[12] Tenable, "Tenable Products: Nessus Professional," 2018. Available at: https://www.tenable.com/products/nessus/nessus-professional.
[13] United States Computer Emergency Readiness Team, "Alert (TA17-181A) Petya Ransomware," 2017. Available at: https://www.us-cert.gov/ncas/alerts/TA17- 181A.
[14] Microsoft, "Microsoft Security Bulletin MS17-010 - Critical," 2017. Available at: https://technet.microsoft.com/library/security/MS17-010.