International Journal of Future Generation Communication and Networking
Vol. 14, No. 1, (2021), pp. 1595–1602

An Analytical Study Of Existing Vulnerabilities In The Shipping Industry With Proposed Countermeasures.

Amit Kumar Sinha
Research Scholar, PHD – CSA Department
Sant Baba Bhag Singh University, Jalandhar, Punjab, India.
Email Id – sinha82amit@gmail.com

Dr. Vijay Dhir
Director, Research & Development Department
Sant Baba Bhag Singh University, Jalandhar, Punjab, India.
Email id - research.sbbsu@gmail.com

Abstract
Shipping Industry is not so far from Cyber Attacks and many new incidents held, due to the lack of IT infrastructure security and the competency to handle such incidents. It includes the analytical study of the existing vulnerabilities and the security measures in the shipping Industries. It explains problems with industrial control systems and addresses serious shortcomings in the automatic recognition system, the electronic chart display information system, and the very small aperture terminals. These counter-measures are concerned with the 'defense-in-depth' principle and identify the mechanism and technological solutions. The maritime industry is also targeted and interlinked with cyber threats and attacks. Internet satellite ties on warships, offshore platforms, and even submarines are feasible and omnipresent. It enables services vital in the physically remote environment for protection and rescue operations, navigation, and connectivity. Remote process monitoring and machinery offer safety and productivity advantages and commercial demands force emerging technology to evolve and be adapted. These advances include the convergence of sensors, increased truth, and artificial intelligence, leading to Intelligence and Shipping Automation. Such autonomous ship operations in international waters are expected by 2035. The paper provides the foundation for future study, helps to map risks, and deter cyber-attacks from the maritime environment.
Keywords: *Cyber security in shipping industry, Shipping automation, vulnerabilities, and countermeasures*

I. INTRODUCTION

Geographical isolation exposes sailors to a variety of specific threats, such as unpredicted forecasted weather and avoidance of pirate attacks. Schiff technology plays a vital role in helping to maneuvers these circumstances and in cases of emergency and distress it allows for contact. Regrettably, every technology has its pros and cons and may be used for malicious purposes. The knowledge and culture of cyber security are fresh on the maritime community's agenda but must be taken seriously to prevent disastrous results.

One of the big developments in maritime transport, universal satellite, and data communications, but this involves a multitude of new threats. To ensure safe navigation, communications, emergency response, and traffic control, for example, a range of vital systems onboard are assisted by the Global Navigation Satellite System (GNSS). The Global Positioning System (GPS) can, however, dispose of disturbed or manipulated signals and lead to crashes, landing and environmental disasters. (United States Coast Guard, 2016) states that in 2016, GPS interference was reported by several ships exiting from the US, which led the US Coast Guard to issue 'Protection Warning 01-16 – GNSS – Trust. Immediately report interruptions". (Hambling, D. (2017)) states that in 2017, over 20 vessels reported spoofed the GPS signals placing them approximately 25 nautical miles inside the country. It was a national-state test that was responsible for the origins of the attack. Opponents test the water but have the expertise, the resources, and the incentive to launch attacks with potentially devastating effects. (National Institute of

ISSN: 2233-7857 IJFGCN

Standards and Technology, 2018) states that it is particularly troubling that this applies both to marine vessels carrying advanced arms and to maritime industries, which are part of the vital infrastructure and constitute over 90% of the cargo transported globally.
The next section describes essential vulnerabilities on board in the common IT and ICS systems. This explains the risks associated with the heavy dependency on navigation and communication systems such as the ECDIS, the automatic identification system (AIS), and Very small aperture terminals (VSATs). The Countermeasures section details existing procedural and technical methods for defending maritime assets from malicious attacks.

II. OBSERVATIONS

The various observations are based on identified vulnerabilities depending upon the following criteria are as follows.

VULNERABILITIES

Vulnerabilities are defined as a weakness that exists in the Infrastructure which potentially supports intruders to exploit and attempt attacks. In this section, it brief about the vulnerabilities associated with the range of technologies for IT networks, industrial control systems, navigation, and communication systems are presented.

Information Technology Networks	**Industrial Control System**
• Misconfiguration	• Legacy System
• Old Firewalls and IDS	• High Complexity
• Third-Party Remote Access	• Limitations of Log Parameters
• Connection to onshore business network	• Efficiency/ Convenience vs security
• Shared Resources	• Un-Audited backed running Services
Automatic Identification System	**Electronic Chart Display Information System**
• No integrity Checks	• Run-on Obsolete Systems
• No Authentication	• Input from multiple unsecured sensors
• AIS data publically searchable	• Flaws in the software's and the protocols
• Authorization issues for updates	• Output Compatibilities for Analysis
Very Small Aperture Terminals	**Common Cyber Security Challenges**
• Exposure to Internet	• Monitoring and Surveillance
• Open Ports, Default credentials	• A systematic review of Logs and Backups
• Connected to critical systems	• Activities/ Web access Firewalls
• Authentication and Authorization issues	• Software/ Services Asset Management
• Missing Latest Malware Protection	• Physical Security and Integrity

Table 1: Potential Vulnerabilities and Threats on Ships

Vital marine services aim to ensure the protection of persons, equipment, and the environment. For example, The Global Maritime Distress and Safety System (GMDSS), is a set of guidelines and modules to support vessel search and rescue operations in critical circumstances. A range of vulnerabilities is given for each portion of the GMDSS (e.g. VSAT terminals, AIS transponder). Additional services provide audio, welfare, and entertainment systems, Wi-Fi connectivity for consumers and video surveillance, etc. These devices are seen as less important to safety and operations, leaving them unpatched and vulnerable to attacks regularly. The vital onboard structures susceptible to cyber assaults are summarized in Table 1. In the following pages, the drawbacks of each of these systems are explained.

ISSN: 2233-7857 IJFGCN

a. IT - Information Technology Networks

(Hudson Analytix Inc, 2017), brief that the IT network combines main organization and operating systems onboard and relies on popular databases and other systems. These systems can be used for the management of accounts, cargo, customs and transportation, human resources planning, and management. (Symantec Security Response, 2017) brief that in June 2017, a ransomware outbreak paralyzed global IT networks causing major business upheavals and revenue loss. At first, a malicious upgrade in an accounting software product made the worm "NotPetya" infected computers. It spreads to connected systems, wipes or codes files, and calls for ransom payments. (Mimoso, M. 2017) stats that the Danish shipping business A.P. Moller-Maersk was one of the most affected companies with a loss of $300M due to major system shutdowns and restore efforts across critical infrastructure.

The event highlights the lack of a cohesive strategy for many companies to handle their system's cyber security. Business essential software can only be modified or replaced by other legacy systems or protocols and cannot be updated or replaced. Some companies do not have routine patching or upgrading programs and thus their antivirus software is obsolete or significant security updates for applications are not patched. Networks, especially for third parties, are often inadequately segmented to manage access. IT systems should be closely examined as they give adversaries a broad attack surface and several points of entry. It is necessary to protect all systems and endpoints, which in most cases do not exist. Access by third parties (e.g. equipment deployment, support, and maintenance) often exposes vulnerable systems to the open world.

A safe, corporate IT network and the Internet isolated area should be essential control networks. However, the need for connectivity to the IT network raises economic stresses, regulations, and specifications for remote monitoring and control. The authentication and encryption approach seldom take into account the nature and configuration of connections between IT networks, thus revealing possible vulnerable and legacy Internet systems. IT systems on ships are also linked to on-shore facilities, which further enhances systemic and continuous risk exposure.

b. ICS – Industrial Control Systems

(Wang J. & Zhang, S. M. 2000) brief about, Industrial Control Systems (ICS) on vessels help minimize human errors, improve resource productivity, extend the lifetime of equipment, and provide economic benefits. (Zaghloul, M. S. 2014) explains the ICS control and track onboard parameters such as temperature, pressure, level, viscosity, fluid control, velocity, torque, stress, and current status of machinery and instruments. The various gadgets and protocols from different vendors prepare the process of synchronization to perform interoperability. However, most of those components were planned, programmed, and transmitted in plaintext with no protection in mind. It should be the responsibility of the seller, following a secure development process to ensure that the components are protected, and the operator should configure the components according to industry standards and guidelines. (Shoultz, D. 2017), either party always believes that the other party is responsible and nobody does so, leaving several crucial vulnerabilities to be exploited by the attackers. The system's weaknesses and vulnerabilities to modules and protocols are critical for integrators, implementers, and operators of ICS.

For the safe voyage of the ship, primary controls like (hydraulic, electrical, automatic) are important. They are vulnerable to environmental issues such as pressure, vibration, and moisture. These control systems are incorporated into the IT distributed network of the ship. (Moxa Inc., 2020; Orbcomm, 2020), explains a continuous partnership between IT networks and on-site facilities permits remote access for tracking, identification, and troubleshooting decreases on-site travel costs, and streamlines field data collection and analysis. (Zurich, 2014), A major concern is to systematically disregard protection for convenience and productivity by operators and engineers, which could have an effect on the entire organization. This is due to the lack of expertise and skills, the commercial pressure to save time, and the apparent lack of compliance with security policies.

ISSN: 2233-7857 IJFGCN

c. AIS – Automatic Identification System

According to (Australian Maritime Safety Authority), the AIS is a Very High-frequency (VHF) radio broadcast system based on the ship and shore. It is used for VTS, search and rescue, accident investigation, and weather forecasting. Depending on the information transferred is important for an understanding of the situation and preventing collision at sea. Without authentication or integrity checks, AIS transponders communicate via the air. (Balduzzi, Wihoit, & Pasta, 2013), states that Via SDR, attackers can inject signals and position faux 'man-in-water' light bulbs, invisibly visualize the vessel and generate false weather reports. Depending on the information that may be inaccurate may lead to false decisions and disastrous results.

("VesselFinder Ltd.", 2020) and "Marinetraffic" (MarineTraffic, 2020) states that the data from AIS was made available via websites. (International Maritime Organisation, 2004), define that the International Maritime Organization (IMO) "represents the regrettable publication of the vessel and its route, which may be invaluable for a targeted attack, on the World Wide Web or elsewhere"

d. ECDIS – Electronic Chart Display Information System

The Electronic Chart Display Information System (ECDIS) is required by IMO and normally mounted on the bridge for all commercial vessels. The implementation of ECDIS software has a wide variety of faults. The framework is also operating on old computers (for example Windows XP desktops), for which there is no security update from Microsoft as it is a deprecated operating system. The maps are either loaded via the web or manually via USB or DVD to the device. Feeds from a wide range of other systems onboard, such as Radar, Navigation Telex, ICS, and satellite devices. This offers a broad compromise surface. Dyryavyy, Y. (2014) audited ECDIS commercial software and highlighted some major risks that allow an attacker to substitute, remove, or insert malicious contents on the device. Therefore, manipulated sensor data can be sent to ECDIS which can affect navigation decisions and cause collision or grounding.

e. VSAT – Very Small Aperture Terminal

A Very Small Aperture Terminal (VSAT) is a communications station for sending and receiving information through a satellite network. Mounted above deck in the satellite view, the transceiver provides the interface to a PC and a control unit below deck. VSATs enable numerous services including GMDSS, ECDIS, AIS, phone, internet, cargo management, ships' routing, telemedicine, crew health, tele-training, and weather forecasts. We have also provided a range of communication and security services. Santamarta, R. (2014) checked several different manufacturers' VSATs and determined that at the protocol and implementation level all audited devices are vulnerable. They transmit authentication, encryption, or integrity checks without the transmission in plain text. This may cause an intruder to shut down or corrupt the machine to inject false signals or malicious code that disables the boat from safe navigation.

(Morse, J. 2017), explains that a ship's geolocation is accessible publicly through AIS aggregators, but the actual danger is that VSAT Network Interfaces, such as the Shodan Ship Tracker may be located on the internet. This can disclose fabric names, product codes, and other information that is useful for a future attack. Vendors usually publish default credentials on their sites and several terminals operate unchanged, user names and passwords of the administrator. When an intruder has found an open VSAT GUI, GPS coordinates, settings and software can be modified. This allows more network compromise and can offer up a point of entry into vital control systems. It is concerned that NATO and vital infrastructure are commonly used for these systems, as their use could have disastrous consequences.

f. CCS - Common Cyber Security Challenges

(TrustNet, 2020), explain that, apart from the above mentioned security issues, it has been identified that some common cyber security challenges exist in most of the autonomous ships.

The real-time network and system monitoring and surveillance were generally ignored or carry less priority. Most of the incidents resolved based on the existing logs. However, the existing application generates a very basic level of logs where it is difficult to identify and proceed to any incident response.

ISSN: 2233-7857 IJFGCN

The results used for activities logs are limited in their content and unable to resolve the technical queries. A strong WAF (Web Access Firewall) is also required. It helps to identify the legitimate activities performed by the trusted user(s). Due diligence policies are missing as per the latest IT infrastructure. In most of the operating systems, the list of the tangible and intangible assets are unsynchronized. Malicious applications open the backdoor to transmit the data, where the existing system is incompetents to handle such activities. Onshore the physical security and integrity are also compromised which has to be strictly maintained.

III. COUNTERMEASURES

To several maritime stakeholders, the idea of cyber protection is new and it is time to raise awareness of existing contraindications. A mutual understanding, which includes shared responsibility between maritime stakeholders is important. This section provides a strategic direction for cyber security on ships.

a. Due Diligence policies to prepare a defense in depth

Safety is not a commodity to be purchased off the shelf nor a procedural plan that can be implemented in the same manner by any organization. "Deepening" maritime IT ecosystems produce an all-embracing mantle of security and build resilience to external and internal threats. The approach with procedural and technical countermeasures on each layer (outlined thereafter) helps to create the defense in depth.

Policy: Security starts with the management of the company, the forming of plans, and the making of policies.

Physical Security: The steps to avoid intruders entering the ship by the use of guards, locks, alarms, and control of technical access along with Authentication and Authorization integrity.

Perimeter Security: It includes measures that block attacks via external communication connections from accessing the network. Identify the required ports and services, and allowed to transfer data after filtration only. Some use cases need to be considered and IT audits should be mandated to identify the various perimeters in the logs to respond to any incident.

Network Security: It includes security areas, network segments, and other network-based defense architecture, configuration, and implementation. It is highly recommended to implement network security on all 7 layers of the OSI model to mitigate risk factors on networks.

Host Security: The host layer needs to be protected from the Operating systems vulnerabilities point of view. The layers of backdoor services running on the computers and other endpoints need to be scrutinized. Moreover, the updated Anti-malware applications, Firewalls, and IDPs, etc. also need to be updated as per the opted platform.

Application Security: It eliminates attackers taking advantage of software faults and requires protected development of software, authentication, access control, and application management vulnerability. It is highly recommended to identify the latest application versions and patches to mitigate newly exposed vulnerabilities.

Data Security: Finally, the data protection layer discusses how the information itself is to be secured whether used, transited, or remaining. In the overall protection of vital maritime infrastructure, each layer plays a major role.

b. Security policies and procedures

A diligent employee is the most critical safety asset on board. Policies and procedures provide workers with the tools and instructions they need for their important position in the company. Training and awareness programs encourage workers to understand why and how everyone can help. Clearly articulated, written, and accepted should be policy and procedural documents. Policies must deal with how the material is implemented and the repercussions if it is overlooked. The records need to be periodically checked to ensure that they cover the company adequately in a continuously changing technological environment.

The policies should address and explain at least the following:

ISSN: 2233-7857 IJFGCN

Data recovery capability, backups, redundancy, business continuity, and disaster recovery planning

- Administrator privileges, concepts of least privilege, and the separation of duties
- Remote access control, use of encryption, and Virtual Private Networks (VPN)
- Physical access, removable media controls, “Bring your own device” (BYOD)

Trusted and authenticated personal use of IT systems

- Email, phishing, passwords rules
- The software upgrade, patch, and maintenance schedules
- Anti-virus/-malware software and signature updates
- White- or blacklisting and the use of third party software
- Onshore support and contingency planning
- Equipment disposal, and data destruction
- Implementation of Web Access Firewall.
- Audited permissions to the owner, groups, and guest users.
- Due Diligence logs maintained for the accessibility with the legal compliances as per the visited country.

c. Technical security solutions

Policies require oversight and regulation of physical or technological implementation. Cameras like ECDIS and VSAT are secured against unauthorized use by guards, locks, and protection. The network should be protected in terms of architecture and configuration, to avoid direct exposure on the Internet to devices and ICS. The VSAT hub can be used as an intermediate hop to connect the terminal remotely. Block and control data traffic as firewalls and intrusion systems join the IT network in the ship. The data flow between all network-based nodes, including satellite and radio traffic, must be mapped and encrypted, e.g. by VPN. Thus the enemy could not decipher the message quickly, even though the signals were intercepted.

Network hardening means safe setup and disabling of unused features and accounts of the hardware and software. This refers to firewalls, routers, switches, servers, voice communication, and every other network unit. Hardening involves removing unused ports and facilities, handling updates, patches, and bug fixes, and even installing them. Whenever practicable, you must change default usernames and passwords. The use of complex passwords defends against automatic port scans and dictionary link attempts on the VSAT terminal, for example. To allow users to access only the privileges they need to carry out their work, access control systems should be designed and periodically audited.
Authentication based on the X.509 certificate will guarantee access for approved crew members and visitors to a ship's wireless network. A separate wireless network (Virtual Local Area Network, VLAN) should be built for guests to only allow minimum access to network resources. Where appropriate, the use of secure communication protocols such as ssh, https, and sftp. A further layer of access protection for sensitive systems and applications can be supported by Multi-Factor Authentication (MFA). The whitelist application prevents the installation of unauthorized and potentially malicious programs by the workers. Data loss prevention tools can minimize the possibility of deliberate or accidental data leakage.

IV. CONCLUSION

This paper addressed the existing vulnerabilities and countermeasures to cyber protection in intelligent ship systems. It showed that it is not only probable but immediate to commit a malicious act and events with catastrophic consequences. To guarantee the protection and productivity of operations at sea, the maritime domain leverages cyber technology but boats, platforms, satellites, and offshore facilities are increasingly interconnected and exposed to an abundance of systemic and technical threats.

ISSN: 2233-7857 IJFGCN

To assist the shipping industry with research, instruments, security evaluation, and training programs, the cyber safety community has an urgent responsibility. In such a scenario, the empowerment of the organizations to make informed strategic decisions and allocate resources efficiently to protect every member and the entire maritime community.
Future work based on this paper would aim to map all known threats and set the status quo for the maritime sector's cyber security posture.

REFERENCES

1. Balduzzi, M., Wihoit, K., & Pasta, A. (2013). "Hey captain, where's your ship? attacking vessel tracking systems for fun and profit". Paper presented at the Eleventh Annual Hack in the Box (HITB) Security Conference in Asia. [online] Available at: <http://conference.hitb.org/hitbsecconf2013kul/materials/D1T1%20-%20Marco%20Balduzzi,%20Kyle%20Wilhoit%20Alessandro%20Pasta%20-%20Attacking%20Vessel%20Tracking%20Systems%20for%20Fun%20and%20Profit.pdf> [Accessed 13 Nov. 2020].
2. Dyryavyy, Y. (2014). "Preparing for Cyber Battleships – Electronic Chart Display and Information System Security". [online] Available at: <https://www.nccgroup.trust/au/our-research/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security/> [Accessed 13 Nov. 2020].
3. Hambling, D. (2017). "Ships fooled in GPS spoofing attack suggest Russian cyberweapon. [online] Available at: <https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/#.WZy1mN2_kyQ.linkedin>. [Accessed 13 Nov. 2020].
4. Hudson Analytix Inc. (2017). "Global Threats: Cybersecurity in Ports (Donald Duck, Daughters & Dollars)". Paper presented at the Hemispheric Conference on Port Competitiveness & Security: Finding the Right Balance, University of Miami, Center for International; Business Education & Research. [online] Available at: <http://portalcip.org/wp-content/uploads/2017/03/Max-Bobys.pdf>. [Accessed 13 Nov. 2020].
5. MarineTraffic. (2020). "marinetraffic.com". [online] Available at: < https://www.marinetraffic.com/en/ais/home/centerx:-12.0/centery:25.0/zoom:4> [Accessed 23 Nov. 2020].
6. Mimoso, M. (2017). "Maersk Shipping Reports $300M Loss Stemming from NotPetya Attack". [online] Available at: <https://threatpost.com/maersk-shipping-reports-300m-loss-stemming-from-notpetya-attack/127477/>. [Accessed 11 Nov. 2020].
7. Morse, J. (2017). "Remotely hacking ships shouldn't be this easy, and yet ...". mashable.com. [online] Available at: <http://mashable.com/2017/07/18/hacking-boats-is-fun-and-easy/#mjW1KLCj6aqb>. [Accessed 29 Nov. 2020].
8. Moxa Inc. (2020). "Industrial Ethernet for In-ship Communication". [online] Available at: <https://www.moxa.com/en/solutions/marine>. [Accessed 23 Nov. 2020].
9. National Institute of Standards and Technology. (2018). "Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1". [online] Available at: < https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11>. [Accessed 23 Nov. 2020].
10. Orbcomm. (2020). "SCADA System Monitoring". [online] Available at: <https://www.orbcomm.com/en/industries/natural-resources/scada-system-monitoring>. [Accessed 25 Nov. 2020].
11. Santamarta, R. (2014). "SATCOM terminals: Hacking by air, sea, and land". [online] Available at: <https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf>. [Accessed 25 Nov. 2020].

ISSN: 2233-7857 IJFGCN

12. Shoultz, D. (2017). “Securely Connected Vessels: Vessel Communications and Maritime Cybersecurity”. maritimeprofessional.com. [online] Available at: <https://www.maritimeprofessional.com/blogs/post/securely-connected-vessels-vessel-communications-and-maritime-15176>. [Accessed 01 Dec. 2020].
13. Symantec Security Response. (2017). “Petya ransomware outbreak: Here’s what you need to know”. [online] Available at: <https://www.symantec.com/connect/blogs/petya-ransomware-outbreak-here-s-what-you-need-know>. [Accessed 01 Dec. 2020].
14. TrustNet, (2020). “Cyber Security Checklist - IT Security Audit Checklist – TrustNet”. [online] Available at: <https://www.trustnetinc.com/cyber-security-checklist/>. [Accessed 13 Nov. 2020].
15. United States Coast Guard. (2016). “Safety Alert 01-16 - Global Navigation Satellite Systems - Trust, but Verify”. [online] Available at: <http://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0116.pdf>. [Accessed 05 Nov. 2020].
16. VesselFinder Ltd. (2020). “Vessel Finder”. [online] Available at: <https://www.vesselfinder.com/>. [Accessed 08 Nov. 2020].
17. Wang, J., & Zhang, S. M. (2000). “Management of human error in shipping operations”. Professional Safety, 45(10), 23-28.
18. Zaghloul, M. S. (2014). “Online Ship Control System Using Supervisory Control and Data Acquisition (SCADA)”. International Journal of Computer Science and Application.
19. Zurich. (2014). “Beyond data breaches: global interconnections of cyber risk”. [online] Available at: <https://www.jasadvisors.com/custom/uploads/2014/04/Risk-After-Next-Whitepaper.pdf>. [Accessed 28 Nov. 2020].

ISSN: 2233-7857 IJFGCN