I-ESKIMO 2025

MSC – A3

Development of Cyber Security Standards in Ships and Port Facilities

Introduction:

The degree to which a technology asset could be endangered by a possible situation or event that could lead to operational, safety, or security failures in the shipping industry as a result of data or systems being tampered with, lost, or compromised is known as maritime cyber risk.

The cyber threats are evolving day by day increasing the vulnerability of electronic systems and operational technologies giving us more reasons to adopt and evolve to a further enhanced system to counter such threats.

Need for cyber security in maritime sector:

The cyber threats in the maritime sector are serious issues and are concerning for the developed nations, businesses, stake holders and the working hands.

Following are the major factors caused by cyber threats:

IMPACT ON FINANCES

IMPACT ON OPERATIONS

IMPACT OF SUPPLY CHAIN

IMPACT ON PUBLIC SAFETY

IMPACT ON THE ENVIRONMENT

Cyber Risk Management:

In recognition of these threats, the International Maritime Organization (IMO) passed Resolution MSC.428(98), which mandates that cyber risks be addressed in Safety Management Systems (SMS) by the time the company's Document of Compliance is verified for the first time each year after January 1, 2021. A risk-based approach with an emphasis on governance, identification, protection, detection, response, and recovery is outlined in supporting guidelines like MSC-FAL.1/Circ.3 (Guidelines on Maritime Cyber Risk Management) and outputs from MSC 110/WP.10.

Ship Security Plan (SSP):

In recognition of these threats, the International Maritime Organization (IMO) passed Resolution MSC.428(98), which mandates that cyber risks be addressed in Safety Management Systems (SMS) by the time the company's Document of Compliance is verified for the first

time each year after January 1, 2021. A risk-based approach with an emphasis on governance, identification, protection, detection, response, and recovery is outlined in supporting guidelines like MSC-FAL.1/Circ.3 (Guidelines on Maritime Cyber Risk Management) and outputs from MSC 110/WP.10

Bridge Attack Tool (BRAT):

BRidge Attack Tool (BRAT) that interactively offers various attack implementations targeting the communication of nautical data in maritime systems. This provides system engineers with a tool for security assessments of integrated bridge systems, enabling the identification of potential cyber vulnerabilities during the design phase. Moreover, it facilitates the development and validation of an effective cyber defence.

It is based on a simulator that provides data of general maritime systems via LWE and comprises simulations of common sensors, such as GNSS, compass, and speed logs, but also a simulated AIS transceiver for external nautical information. Our environment can be further extended by real hardware components using Ethernet or serial interfaces, which make it possible to seamlessly connect different IBSs, an autopilot, or other maritime equipment.

BRAT provides a user-friendly HMI to configure, launch and combine attacks against the maritime system.

KEY FEATURES:

An interactive web-based HMI facilitates the use for non-technical users. As use cases and systems change, an attack framework has to be extendable, adjustable, and reusable.

It is possible to use a Python package which makes it easy to investigate security features of maritime systems in an automated test and development environment.

So far, BRAT's underlying attack model exploits security weaknesses in the LWE protocol to manipulate the communication of nautical data in maritime systems using PitM and PotS attacks.

(BRAT) that, to the best of our knowledge, is the first maritime-specific security tool that enables the interactive launch of numerous PitM and PotS cyber-attacks.

It can be deployed in common development environments which implement (simulated) sources for nautical data and are compatible to LWE.

It greatly supports existing processes to technically assess, prevent, and detect cyber-attacks on maritime systems by using offensive security methods.

Proposals to MSC:

For MSC I am hereby proposing a comprehensive study on evolving nature of maritime cyber risk and develop a roadmap plan to counter it which would include specialized training to maritime personals on board ship and port facilities and development of a dedicated technology (combination of software technology, electronic devices and AI) that would have their own

database linked to the ship's owned/managed company and monitored and regulated by the MSC.

Like the AI can be trained, similarly we can train BRAT combining it with AI and make a new OT that would use the algorithms projected by BRAT's attack simulations and based on this, the OT can generate counter measures, warn the bridge, port control tower, company database and nearby coast-guard teams and would present the best actions that should be taken in that situation.

Actions to be taken by MSC:

The MSC should work along with the developed nations and develop a fully functional robust OT that would be the integration of security tool like the BRAT, combining it with AI and integrate the resultant OT with the ships and port facilities.

The MSC should collaborate with the developed nation, stakeholders, registered companies and the member states to develop, train and adapt to a fully functioning robust OT dedicated to counter cyber risk in the industry.

It should be made mandatory by the MSC for all developed nations, shipping companies, member states and port authorities to have certified training programs for their work force based on the model presented by BRAT or the new developed OT.

Request to the committee / sub-committee:

Shifting from "WHAT TO DO" to "HOW TO DO"

Tools such as the Bridge Attack Tool (BRAT) highlight the importance of proactive vulnerability testing, while structured training, regular drills, and classification society certification reinforce resilience. Developed nations, industry stakeholders, and classification societies must lead in applying IMO guidelines rigorously, sharing threat intelligence, and advancing training programs tailored to both shipboard and shoreside personnel with the help of an emerging OT that can further be enhanced to act as the first line of defense against cyber threats in the industry.

The integrated OT (combination of tool like BRAT, AI and electronic devices) can be the key to train the work force of the industry, help us build Ship Security Plans (SSP), suggest us ways to counter the possible cyber threats and can also act as the first line of defense against all kinds of cyber threats.

Thus, with the help of the above discussed OT we can DETECT, PROTECT, REACT AND RECOVER from any form of cyber threats and most importantly, train our work force and make a secure and safe maritime ecosystem capable of providing a safe and efficient environment for trade and commerce in the near future.