CYMAR

Cyber at Sea: Issues Concerning the Maritime Sector

Kevin Jones
Faculty of Science and Engineering
University of Plymouth
Plymouth, United Kingdom
0000-0002-7960-0978

Kimberly Tam
School of Engineering, Computing and Mathematics
University of Plymouth
Plymouth, United Kingdom
0000-0003-2840-5715

***Abstract*—Maritime Cyber-security is an area of growing concern and increasing research interest as it becomes increasingly clear that there is global dependency on the sector and vulnerabilities are emerging. This paper summarizes four presentations in a special tract at CYBER 2022: The Seventh International Conference on Cyber-Technologies and Cyber-Systems. This Special track addresses Cybersecurity Issues of Concern to the Maritime Sector (CYMAR). The research work deals with the following key issues:**

(1) Vulnerabilities in maritime systems and how they are relevant to maritime operations.

(2) How to capture malicious behaviors (i.e., real attacker actions) on ships for better threat intelligence.

(3) How to address the human aspect of maritime cyber-security.

(4) Changing human behaviors to reduce cyber-attack surfaces.

Keywords—maritime cybersecurity, cybersecurity, penetration testing, honeypots, threat intelligence, human centered approach, situational awareness

I. Introduction

Global supply chains rely heavily on maritime transportation. This sector is also responsible for providing food and, in the future, may also be a key source of renewable energy. Given the importance and increased digitization of systems at sea, this special track is interested in maritime cyber threats, risks, and safety.

This tract is dedicated to research on cyber-threats in the context of Maritime systems, information technology to operational technology, and offshore to onshore infrastructure. The intention of this tract is to bring together researchers from academia, industry, and government to present ongoing research on the maritime systems of today, but also the threats they may face in the future. However, both areas of cybersecurity (e.g., threat detection, network vulnerabilities, hardware vulnerabilities) and maritime (e.g., operations, transport, logistics, navigation) are expansive and cover technical, social-technical, geopolitics, and legal matters.

As a result, more and more cross-discipline research is necessary to cover a wide range of research topics that are relevant to, and have an impact on, cyber security in the maritime sector.

II. Submissions

A. First submission

The first paper, titled "Investigating the Security and Accessibility of Voyage Data Recorder Data using a USB attack" by Avanthika Vineetha Harish [1]. This looks at specific vulnerabilities in a ship "black box", i.e., the Voyage Data Recorder. This analysis uses real hardware and software and has no software emulator or simulation. In addition, a key part of this paper looks at how this is relevant to the shipping industry, which will make it more likely that those in the sector will understand the threat, and possible actions to mitigate it.

B. Second submission

The second paper, "A ship Honeynet project to collect data on cyber threats to maritime" [2] aims to gather information on current cyber-attacks on vessels using a Honeynet to gather data. This is critical, as not a lot of information on cyber-attacks are recorded in this sector, and so there is little information on the attacks happening now. This uses a network of honeypots (termed a honeynet), and while the concept is not new, using it to simulate and tempt attackers to attack a ship target is novel. This paper explains the beneficial features of a ship Honeynet and it how it can be used to educate the sector on the threats that are happening now.

C. Third submission

The third paper by Allan Nganga, "Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment [3], is in response to both the growing cyber threat landscape and the International Maritime Organization (IMO) guidelines (MSC-FAL.1/Circ.3/Rev.1), part of resolution MSC.428 (98). As the topic suggests, this takes a human-centered approach, rather than a technical approach, addressing how vessel domain awareness can be achieved by people (crew) on the ship. This looks at the interplay between regulator bodies like the IMO, and what people will need to do to satisfy policies and risk appetites. Hence this looks at the wider multi-stakeholder environment instead of focusing on a single perspective.

D. Fourth submission

The fourth and final submission titled "Reducing the cyber-attack surface in the maritime sector via individual behaviour

change" [4], is an early position paper and is less maritime specific, but examines how behavioural changes can be made to reduce cyber-attacks. It does, however, quote that there are a large number of incidences in the maritime sector that relate to human error. This paper argues that training to reduce human error would be an appropriate solution to mitigating cyber-threats in the maritime sector. To do this, this paper looks to understand the conditions necessary to enable people to be more secure.

III. CONCLUSIONS

There is an international presence in these publications, which is appropriate given that shipping is critical to global supply chains, and is therefore an international subject matter. Several of these focus on understanding the cyber threat – some technical and some socio-technical. Some were holistic and cross discipline, looking at how technical vulnerabilities could affect standards and operations, or how regulations can affect human behaviour and jobs. Further research has also been highlighted, as many of these were seen to be initial steps to better understanding of and better provision of cyber-security. In summary, these papers addressed:

- Doing penetration testing on maritime systems in a way that highlights strengths and weaknesses in standards for how systems are designed and implemented. This paper focused on the technical part of how easy it is to penetrate a certain device, later research will make it easier for policy and standard writers to learn from cyber-security penetration test results.
- How we can improve our threat intelligence using technical tools, leading to use of a honeynet to perform an analysis of those findings, providing actual updates to our threat intelligence.
- Examining the relevant players (multi-stakeholder environment) which is a critical first step to scoping the problem, leading to specific suggestions on how individual or sets of stakeholders can act differently and the efficacy of these changes.
- And Finally, and more generic to cyber-security, changing human behaviour to reduce cyber-attacks; with future research ideas to explore how effective this is in the maritime sector, and what tools/techniques are most effective to different sets of people who work in maritime (e.g., crews, management)

ACKNOWLEDGMENT

The authors would like to extend their appreciation to the organization of IARIA and CYBER22 for their interest, help, and advice for this special track.

REFERENCES

[1] Avanthika Vineetha Harish, Kimberly Tam, Kevin Jones, "Investigating the Security and Accessibility of Voyage Data Recorder Data using a USB attack" in Special Track: CyMAR: Cyber at Sea: Issues Concerning the Maritime Sector, along with Cyber2022, Iaria XPS Press, 2022.

[2] JStephen McCombie, Jeroen Pijpker, "A ship Honeynet project to collect data on cyber threats to maritime" in Special Track: CyMAR: Cyber at Sea: Issues Concerning the Maritime Sector, along with Cyber2022, Iaria XPS Press, 2022.

[3] Allan Nganga, Joel Scanlan, Margaretta Lutzhoft, Steven Mallam, " Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment" in Special Track: CyMAR: Cyber at Sea: Issues Concerning the Maritime Sector, along with Cyber2022, Iaria XPS Press, 2022.

[4] Konstantinos Mersinas, "Reducing the cyber-attack surface in the maritime sector via individual behaviour change" in Special Track: CyMAR: Cyber at Sea: Issues Concerning the Maritime Sector, along with Cyber2022, Iaria XPS Press, 2022..