Cyber Security Test Environment for Bridge Systems

***Abstract*—Despite the increase of cyber threats in the maritime domain, there is a serious lack of adequate security testing in maritime systems engineering. To address this gap, we present a holistic, simulative testing environment to instrument cyber attacks and devices for automated testing on soft- and hardware level, which can be integrated already in the development phase.**

Today's commercial shipping industry is largely digitalized and highly networked. However, as a major driver of the global economy, it is by no means immune to cyber attacks. Recently, various cyber threats on maritime systems have been demonstrated to be real, including attacks on integrated bridge systems (IBSs) [2]. Such attacks, particularly those targeting the misleading of vessels' navigation, can have devastating effects and pose serious risks. From an economic perspective, maritime value chains can be disrupted. Much worse, the ecosystem and even human lives can be endangered by ship collisions. Thus, cyber risks are also an issue of safety, which has long been recognized. Maritime cyber security was therefore placed on the agendas of various organizations and governments. Despite training, bridge crew members nevertheless often interpret discrepancies in nautical equipment observed during cyber attacks as merely technical errors.

While raising awareness of cyber threats is the task of all maritime actors, it is a crucial task and challenge for IT security researchers to provide a suitable technology for identifying vulnerabilities in maritime systems. However, current maritime systems engineering does not put emphasis on cyber security. It lacks "security by design" and does not integrate cyber security into its testing. Also, security cannot yet be quantified in this context, as it can be, e.g., by CVSS in other domains. Testing environments for maritime systems do exist, however, most neglect cyber security. Only a very few, such as [3], take security into account, but primarily focus only on the human factor and the need for training of crew members.

Therefore, we present *MCSL*, a *Maritime Cyber Security Lab* that provides a modular environment to assess cyber security of maritime systems. *MCSL* enables automated testing on soft- and hardware level and focuses on the impact of attacks against IBSs. It covers typical nautical protocols, e.g., NMEA 0183 and IEC 61162-450, as typical standards used in modern seagoing vessels. By this means, it greatly supports the development and validation of effective security solutions for maritime systems already in the development phase.

Our framework is composed of individual components implemented in Python with a modular and easily extensible design. Among them, there is i) a maritime simulator, ii) an attack component, and iii) a network analyzer (cf. Fig. 1). The latter can be used to analyze the behavior of a maritime network under cyber attacks. Furthermore, a Wireshark plugin dissects maritime network traffic, automatically captured and processed by the analyzer, and allows investigating attacks

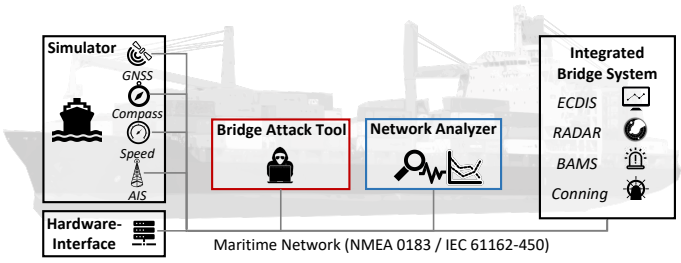

Fig. 1: Conceptual overview of *MCSL* and its components.

exploratively. Each component can be configured and executed on demand for individual test cases.

To operate without hardware sensors or an actual bridge, simulation is used. The simulator is responsible for generating different inputs of sensors comprising typical maritime electronics onboard vessels, ranging from SOG and echo sounders to GNSS and AIS transceivers. Individual sensors can be selectively configured to create a complete, virtual replication of typical ship networks. *MCSL* provides an easy-to-use interface to integrate software applications and additionally also maritime hardware into the simulation environment.

The attack tool is the actual core of *MCSL* offering different implementations of cyber attacks. It includes a graphical user interface allowing to interactively select, configure, combine, and schedule numerous attacks targeting the maritime system under test, e.g., manipulating GNSS data, which was shown to be a serious attack vector in practice [1]. From a technical perspective, the attack tool performs so-called person-on-the-side attacks. Since nautical communication is generally neither authenticated nor encrypted, it enables a network topology analysis and scanning for active devices based on passive network sniffing. The information gained by eavesdropping can then be exploited to actively launch simple or subtle cyber attacks against typical entities within an IBS.

Contribution to MARESEC: Besides a detailed introduction of *MCSL*, its tools and design concepts, we will show exemplary evaluation results from a demonstrative attack on the IBS navigation using the open-source ECDIS, OpenCPN. By doing so, we highlight *MCSL*'s potential, firstly for an assessment of cyber security in IBSs and, secondly, to improve the development of adequate and domain-specific countermeasures for secure and resilient maritime applications.

References

[1] J. Bhatti and T. E. Humphreys, "Hostile Control of Ships Via False GPS Signals: Demonstration and Detection," *Journal of the Institute of Navigation*, vol. 64, no. 1, pp. 51–66, 2017.

[2] M. S. Lund, J. E. Gulland, O. S. Hareide, Ø. Jøsok, and K. O. C. Weum, "Integrity of integrated navigation systems," in *In Proc. of the Conf. on Comm. and Network Security (CNS)*, Beijing, China, 2018, pp. 1–5.

[3] K. Tam, K. Moara-Nkwe, and K. Jones, "The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training," *Mar. Tech. and Research*, vol. 3, no. 1, 2021.