When a BRAT fools your bridge: A Cyber Security Test Environment for Integrated Bridge Systems

Merlin von Rechenberg°•, Mari Schmidt°, Christian Hemminghaus°•, Jan Bauer°, Elmar Padilla°

°Fraunhofer FKIE
Cyber Analysis & Defense
Wachtberg, Germany

•University of Bonn
Security and Networked Systems
Bonn, Germany

{merlin.rechenberg, mari.schmidt, christian.hemminghaus, jan.bauer, elmar.padilla}
@fkie.fraunhofer.de

***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. Our environment consists of a network attack tool targeting bridge systems of seagoing vessels as well as various security components allowing to evaluate the impact of an attack and to develop effective countermeasures to protect maritime systems. In our demonstration, we will exemplarily showcase prominent cyber attacks against safe navigation, introduce possible security means, and discuss potential use cases.**

I. Introduction & Background

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) [6]. Such attacks, particularly those targeting the misleading of vessels' navigation, e.g., by exploiting the automatic identification system (AIS), can have devastating effects and pose serious risks [5]. From an economic perspective, maritime value chains can be disrupted. Much worse, the ecosystem and even human lives can be endangered by ship collisions and groundings. 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 maritime education and training (MET), bridge crew members nevertheless often misinterpret discrepancies in nautical equipment observed during cyber attacks as merely technical errors [2].

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 places far too little 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 the Common Vulnerability Scoring System (CVSS) known in other domains. Testing environments for maritime systems do exist, however, most neglect cyber security. Only a very few, such as [7], take security into account, but primarily focus only on the human factor and the need for MET.

Therefore, we present *MCSL*, a *Maritime Cyber Security Lab* that provides a distributed and 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 network protocols, e.g., NMEA 0183 and IEC 61162-450, as common 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.

II. MCSL Framework

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) a virtualized IBS, and iii) a security lab including an attack tool as well as different security components (cf. Fig. 1). The latter can be used to analyze the behavior of a maritime IT network under cyber attacks and will be described in separate subsections in the following. Each component can be configured and executed on demand for individual test cases. All components are deployable and ready to use either individually via Docker containers in a virtual network or as a compound in a single virtual machine.

To operate without hardware sensors or an actual bridge, simulation is used. The scientific simulator is responsible for generating different inputs of sensors comprising common maritime electronics onboard vessels, ranging from speed over ground (SOG) sensors and echo sounders to AIS transceivers and global navigation satellite system (GNSS) receivers. 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 supplementary software applications, additionally also maritime hardware, or real-world trace-files (pcaps) into the simulation environment. Furthermore, a Wireshark plugin[1], specially developed to dissect maritime network traffic, allows investigating cyber attacks exploratively.

[1] available at https://github.com/fkie-cad/maritime-dissector

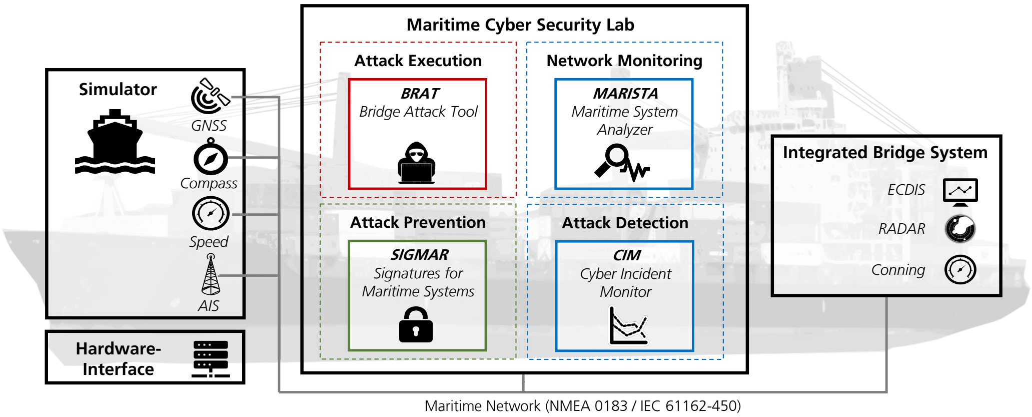


Fig. 1. Conceptual overview of *MCSL* and its modular and distributed network components.

BRAT: The *BRidge Attack Tool (BRAT)* [3] is the actual core of *MCSL*, offering different implementations of cyber attacks on maritime systems. 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 is known to be a serious attack vector in practice [1]. From a technical perspective, the attack tool performs so-called person-on-the-side (PotS) 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.

SIGMAR: Some of the security issues tackled and exploited by *BRAT* could have been technically prevented by conventional security solutions for integrity and authenticity protection that, however, have usually not yet been implemented in practice. Therefore, we developed *SIGMAR* [4] that enables digital *SIGnatures for MARitime systems*. Taking into account the typically long lifecycles of commercial vessels, it provides a low-cost solution to retrofit authentication of nautical data based on asymmetric cryptography. By extending the IEC 61162-450 standard, it offers backward-compatible security that is integrated as proof-of-concept into *MCSL*.

MARISTA: The *MARItime SysTem Analyzer (MARISTA)* captures and processes network traffic to analyze the architecture of maritime systems, its network topology, and existing communication patterns automatically. In addition, *MARISTA* provides the user with a graphical visualization of the network and delivers statistical information derived from the traffic analysis to other components of *MCSL*.

CIM: Finally, we introduce a *Cyber Incident Monitor (CIM)* for securing nautical communication that is tailored for navigational IBSs. The core of *CIM* is a maritime network-based Intrusion Detection System (NIDS), which is, to the best of our knowledge, the first domain-specific NIDS that is capable of detecting PotS attacks within maritime systems. Three fundamental methods are utilized for the anomaly and misuse detection on the application layer: i) protocol-based approaches identifying DoS attacks (e.g., flooding) and unusual frequency of message delivery, ii) content-based approaches checking the plausibility of values and deviations between their payloads, and iii) structure-based approaches using a defined or learned topology (provided by *MARISTA*) to be expressed as a set of rules. Deviations from such rules, e.g., induced by malicious devices, are detected. An additional unique feature of *CIM* is its ergonomic human machine interface (HMI) designed for nautical operators. Alarms and possible detections are presented to the operator in a familiar manner, combined with specific instructions on how to respond adequately to individual cyber incidents.

III. Demonstration & Example Attack Scenarios

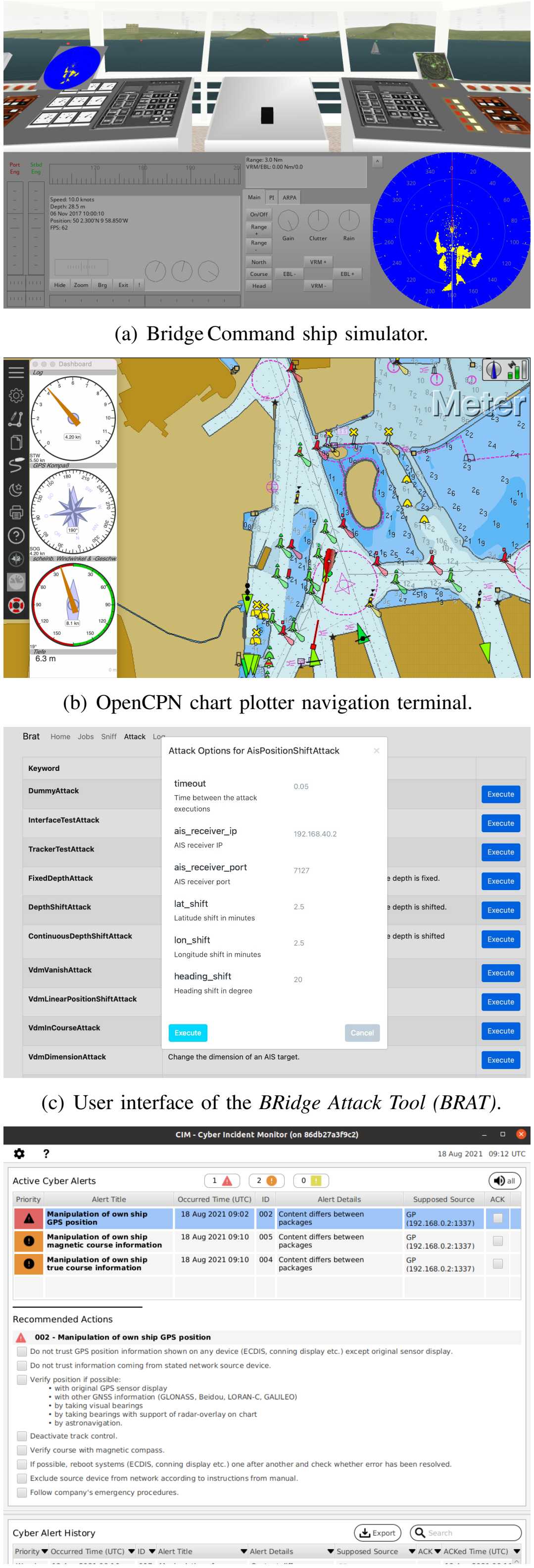
Besides a detailed introduction of *MCSL*, its tools, and design concepts, we will exemplary show demonstrative attacks on the IBS navigation visualized by the open-source chart plotter navigation software *OpenCPN*[2]. By doing so, we highlight *MCSL*'s potential, firstly, for a security assessment of IBSs and, secondly, to improve the development of effective and domain-specific countermeasures for secure and resilient maritime applications.

Utilizing the modular design of our framework, the interactive and open-source ship simulator *Bridge Command*[3] is used in the demonstration, instead of our own more technical simulator. This allows for an active controlling of the ship with a steering wheel and throttle lever, cf. Fig. 2. Two scenarios with a cyber attack will be exhibited in the demonstration. These scenarios, among others, can be fully simulated within *MCSL* to test the behavior of an IBS and/or train nautical personnel w.r.t. cyber security.

A. Scenario 1: AIS Modification

Two ships are traveling in opposite directions on a dense waterway and are about to pass each other. Using *BRAT*, an attacker with access to ship A's network manipulates the AIS position of ship B (only visible for ship A). The spoofed position of ship B is placed exactly in course, a bit ahead of ship A.

[2] https://opencpn.org
[3] https://www.bridgecommand.co.uk



(a) Bridge Command ship simulator.

(b) OpenCPN chart plotter navigation terminal.

Brat Home Jobs Sniff Attack Log

Attack Options for AisPositionShiftAttack

timeout 0.05
Time between the attack executions

ais_receiver_ip 192.168.40.2
AIS receiver IP

ais_receiver_port 7127
AIS receiver port

lat_shift 2.5
Latitude shift in minutes

lon_shift 2.5
Longitude shift in minutes

heading_shift 20
Heading shift in degree

Execute Cancel

Keyword		
DummyAttack		Execute
InterfaceTestAttack		Execute
TrackerTestAttack		Execute
FixedDepthAttack	e depth is fixed.	Execute
DepthShiftAttack	e depth is shifted.	Execute
ContinuousDepthShiftAttack	e depth is shifted	Execute
VdmVanishAttack		Execute
VdmLinearPositionShiftAttack		Execute
VdmInCourseAttack		Execute
VdmDimensionAttack	Change the dimension of an AIS target.	Execute

(c) User interface of the *BRidge Attack Tool (BRAT)*.

CIM - Cyber Incident Monitor (on 86db27a3f9c2)

18 Aug 2021 09:12 UTC

Active Cyber Alerts 1 2 0 all

Priority	Alert Title	Occurred Time (UTC)	ID	Alert Details	Supposed Source	ACK
▲	**Manipulation of own ship GPS position**	18 Aug 2021 09:02	002	Content differs between packages	GP (192.168.0.2:1337)	□
●	**Manipulation of own ship magnetic course information**	18 Aug 2021 09:10	005	Content differs between packages	GP (192.168.0.2:1337)	□
●	**Manipulation of own ship true course information**	18 Aug 2021 09:10	004	Content differs between packages	GP (192.168.0.2:1337)	□

Recommended Actions

002 - Manipulation of own ship GPS position

□ Do not trust GPS position information shown on any device (ECDIS, conning display etc.) except original sensor display.
□ Do not trust information coming from stated network source device.
□ Verify position if possible:
  - with original GPS sensor display
  - with other GNSS information (GLONASS, Beidou, LORAN-C, GALILEO)
  - by taking visual bearings
  - by taking bearings with support of radar-overlay on chart
  - by astronavigation.

□ Deactivate track control.
□ Verify course with magnetic compass.
□ If possible, reboot systems (ECDIS, conning display etc.) one after another and check whether error has been resolved.
□ Exclude source device from network according to instructions from manual.
□ Follow company's emergency procedures.

Cyber Alert History Export Search

Priority	Occurred Time (UTC)	ID	Alert Title	Alert Details	Supposed Source	ACK	ACKed Time (UTC)

(d) *Cyber Incident Monitor (CIM) for navigators.*

Fig. 2. Demo setup. The ship simulator (a) generates sensor input that is transferred to the chart plotter (b) for nautical visualization. In case an attack is launched using *BRAT* [3] (c), its impact can be observed in the plotter display. If the attack is detected by the maritime IDS, *CIM*'s HMI (d) alerts the bridge crew and instructs them with appropriate responses.

This might trigger an automatic collision avoidance alert. However, if operator of ship A initiates an evasive maneuver, this might endanger both and possibly other ships or block the waterway. Depending on the ship type and severity, this could take hours to weeks to recover from. While this attack can be detected effortlessly under clear visibility conditions, at night, in fog or heavy seas, the crew has to rely on additional electronic instruments, but these can also be tampered.

B. Scenario 2: Modification of Position and Heading

A cargo ship with a large draft is traveling along a coast in a waterway enclosed by shallow water. Using *BRAT*, an attacker slowly, but continuously alters the ship's GNSS position and heading. The electronic chart display and information system (ECDIS) will indicate the ship to be off course. Once the operator adjusts the spoofed course, the ship will actually leave the safe waterway and enter shallow water, endangering the ship to grounding hazards.

C. Response to Cyber Attacks

In both scenarios, *CIM* is capable of warning and instructing the operator not to place false trust in the potentially attacked electronic components. In case of AIS modification, the position provided by the AIS signal should be verified by other means, e.g., using the automatic radar plotting aid (ARPA), whereas the indicated position and heading should be crosschecked with a magnetic compass and by comparing the displayed water level with the output of the echo sounder.

ACKNOWLEDGMENTS

The authors would like to thank Julian Spravil and Lucca Ruhland for substantially supporting the development of *MCSL* and valuable discussions, and Nina Rößler and Albert Baumhauer for *CIM's* HMI.
This work was partially funded by the German Federal Ministry of Economic Affairs and Energy (BMWi) within the Program "Maritime Technologies of the Next Generation" (03SX448C) and Project Management Agency Karlsruhe (PTKA). The authors are responsible for the contents of this publication.

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] D. Heering, O. M. Maennel, and A. N. Venables, *Shortcomings in Cybersecurity Education for Seafarers*. CRC Press, 2021.
[3] C. Hemminghaus, J. Bauer, and E. Padilla, "BRAT: a Bridge Attack Tool for Cyber Security Assessments of Maritime Systems," *Int. Journal on Marine Navigation and Safety of Sea Transportation (TransNav)*, vol. 15, no. 1, pp. 35–44, 2021.
[4] C. Hemminghaus, J. Bauer, and K. Wolsing, "SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures," in *Proc. of the Int. Symposium on Networks, Computers and Communications (ISNCC)*, Dubai, UAE, to appear 2021.
[5] G. C. Kessler, J. P. Craiger, and J. C. Haass, "A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System," *Int. Journal on Marine Navigation and Safety of Sea Transportation (TransNav)*, vol. 12, no. 3, pp. 429–439, 2018.
[6] M. S. Lund, J. E. Gulland, O. S. Hareide, Ø. Jøsok, and K. O. C. Weum, "Integrity of Integrated Navigation Systems," in *Proc. of the Conf. on Comm. and Network Security (CNS)*, Beijing, China, 2018, pp. 1–5.
[7] 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.