TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 15
Number 1
March 2021
DOI: 10.12716/1001.15.01.02

BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems

C. Hemminghaus[1,2], J. Bauer[1] & E. Padilla[1]
[1] *Fraunhofer Institute for Communication, Wachtberg, Germany*
[2] *University of Bonn, Bonn, Germany*

ABSTRACT: Today's shipping industry is largely digitalized and networked, but by no means immune to cyber attacks. As recent incidents show, attacks, particularly those targeting on the misleading of navigation, not only pose a serious risk from an economic perspective when disrupting maritime value chains, but can also cause collisions and endanger the environment and humans. However, cyber defense has not yet been an integral part of maritime systems engineering, nor are there any automated tools to systematically assess their security level as well-established in other domains. In this paper, we therefore present a holistic 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 defense.

1 INTRODUCTION

The vast majority of the world's goods flow across the oceans. The shipping industry is, therefore, a major driver of the global economy. The impact of temporary breakdowns in shipping routes and supply chains is illustrated by the recent incident in the Suez Canal, which was blocked for days by the Ever Given golden-class container ship. Although not caused by cyber attacks, a precisely timed execution of an attack could specifically provoke such incidents. Threateningly, incidents attributable to cyber crime are proliferating. Increasingly sophisticated, domain-specific, and targeted attacks on maritime systems are being observed [1, 30], making adequate cyber defense strategies for this sector urgently necessary. In particular, attacks aimed at misleading ship navigation not only pose a serious risk from an economic perspective with massive monetary consequences due to disrupted maritime value chains, but can also cause dangerous collisions of vessels and endanger the environment and human lives. This is why the International Maritime Organization (IMO) placed cyber security on its roadmap and required shipowners to establish cyber risk management by the beginning of 2021 [17]. An operative implementation of cyber risk management for shippers is also supported by industry guidelines [5, 6]. Nevertheless, studies reflecting the current state-of-the-art in cyber security technology for the maritime domain conclude that maritime systems are still highly vulnerable to cyber attacks [7]. This is confirmed by recent incidences, cf. [1].

One reason for high cyber risks correlates with the peculiarities of maritime technology. Maritime systems have a long life cycle. Although they were originally designed for local (air-gapped) networks, they are incrementally interconnected with public interfaces. It has long been known that maritime

systems do not comply with state-of-the-art security practices [3, 25, 27, 28].

However, we believe this is to some extent due to a lack of technology to integrate cyber security into the early stages of systems development, rather than retrofitting and patching. Besides, the resilience of maritime systems in case of cyber attacks is not explicitly assessed and validated, neither in system development nor in certification or operation. Moreover, common cyber risk assessments typically focus on external attacks that target at the availability of different components of maritime systems [30]. However, the class of internal cyber attacks should not be ignored. Physical access is almost impossible to prevent in practice. Changing personnel onboard ships as well as long cable harnesses between distributed electronics result in a large attack surface for internal attacks. Such attacks are inherently more powerful and harmful than external attacks from cyber and physical space. Nevertheless, they are rarely considered in risk analyses and are not supported by automated tools in the context of cyber defense. Overall, in contrast to other domains, a true maritime-specific security tool that also considers application-level properties is still missing.

To close this gap, we present BRAT, a holistic and user-friendly BRidge Attack Tool. It is designed as a modular framework that interactively offers various implementations of cyber attacks targeting the communication of nautical data in Integrated Bridge Systems (IBSs). Those attacks can be individually configured, combined, scheduled, and orchestrated in an automated manner. To the best of our knowledge, BRAT is the first domain-specific tool for internal network attacks against maritime systems. It has the potential to improve security assessments and allows system engineers to systematically identify and verify vulnerabilities in a large number of components. Furthermore, BRAT also enables the development and validation of appropriate cyber attack countermeasures, such as effective detection or preventive authentication. In addition, it is possible to integrate BRAT into the Maritime Education and Training (MET) of bridge crews, thereby increasing awareness and improving their response to cyber threats [11, 12].

The core contributions of this paper are twofold: First, we extend the common threat landscape of maritime systems to include the class of internal cyber attacks. Additionally, we develop an attack model for this kind of threat. Second, based on this attack model, we introduce a bridge attack tool as a comprehensive framework to launch domain-specific cyber attacks against IBSs having the potential to further advance cyber security in the maritime domain.

The remainder of this paper is structured as follows. Section 2 gives a brief background on maritime systems, communication protocols, and cyber security testing. In Section 3, internal cyber attacks on IBS are placed in the overall context of maritime cyber threats and an attack model implemented by our approach is derived. The design concept of BRAT and its architecture are introduced in Section 4, while Section 5 provides a detailed focus on BRAT's attack features and implemented attacks realized in our reference implementation. In Section 6, we then revisit the main use cases of our attack tool and reflect on the results of our approach in a security discussion. A conclusion is finally given in Section 7.

2 BACKGROUND

This section first introduces the main electronic components of maritime systems. The focus is on sensors, which are the interface to the environment and are, therefore, particularly threatened by external attacks. Also, processing systems, which can be deceived by false sensor data, are discussed. Then, the communication protocols for transmitting nautical information are introduced, which offer poorly protected attack surfaces. Finally, we briefly review the current state of security tools and use this to motivate our bridge attack tool.

2.1 *Maritime Systems*

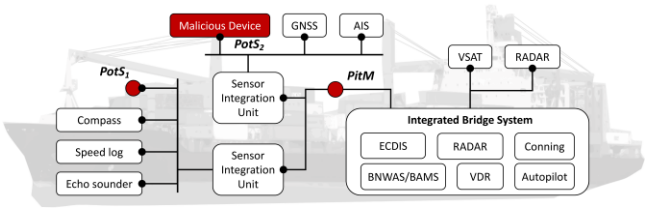

Figure 1. An exemplary architecture of a typical maritime system onboard commercial vessels, cf. [4, 20, 27]. Due to lack of network security features, the maritime system is vulnerable to Person-on-the-Side attacks from injected devices (PotS1) or compromised sensors (PotS2) and Person-in-the-Middle attacks (PitM) from manipulated communication paths.

Typical maritime systems onboard vessels are heterogeneous and distributed IT systems with a plurality of different sensors and actuators. Therefore, they can be understood as CPSs connecting the cyber and physical space. They consist of technical measurement instruments and nautical processing assets, along with systems for external communication and alarms, as schematically shown in Figure 1.

Maritime sensors gather nautical data to provide an accurate navigational situation picture, which is the base for navigational decision-support. Typical sensors are Global Navigation Satellite System (GNSS) receivers, primarily GPS, radars, echo sounders, and compasses with speed logs. More sophisticated sensors not only measure but interpret incoming data, such as maritime radars that often interpret the information stream to recognize and track individual objects. The data gathered by sensors is usually provided via serial interfaces, connected by sensor integration units that often bundle multiple sensors, as exemplarily shown in Figure 1.

Onboard processing systems handle sensor data for either to derive a navigational picture or to control specific actuators such as rudder and propulsion. These systems are interconnected into IBSs, which usually comprise an Electronic Chart Display and Information System (ECDIS) for route planning and monitoring, a conning and a radar display as well as

an autopilot. The Voyage Data Recorder (VDR) is a mandatory equipment for the continued logging of sensor and system states.

External communication systems are used for different purposes. Automatic Identification System (AIS) transceivers exchange messages between other maritime systems in the vicinity for safety and security reasons, including their identity, position, and course information. Incoming AIS messages are usually presented as targets on the ECDIS. Very-Small-Aperture Terminals (VSATs) are used for digital welfare communication, but also navigational needs such as weather and chart updates or route optimization. Further navigational assistance is provided by onboard alarm systems. Bridge Navigational Watch and Alarm Systems (BNWASs) notify crew members when the current officer on watch is unresponsive or unable to perform duties. A central point to monitor and handle alarms from various bridge sources is the Bridge Alert Management System (BAMS), which alarms for unsafe navigation and also monitors sensor integrity to some extent.

2.2 *Maritime Communication Protocols*

Save navigation builds upon a reliable interconnection between bridge components. Hence, the electronic exchange of nautical data is since long standardized. A common standardization is the NMEA 0183 interface standard defined by the National Marine Electronics Association (NMEA) in the 1980s. In this ASCII-based exchange protocol, nautical information is encoded to so-called NMEA sentences, which consist of talker and sentence identifiers, followed by payload fields and a checksum. Nowadays, NMEA sentences are widely established as an encoding format even beyond shipping.

As part of maritime digitization, modern networks use Ethernet technology as transmission medium. There are three common maritime communication protocols based on the IP-stack: Lightweight Ethernet (LWE), NMEA over IP, and NMEA OneNet. The former is a modern communication protocol that was standardized a decade ago with IEC 61162-450 [15]. It is based on the UDP/IP-stack and uses IPv4 multicast with individual receiver groups according to the equipment type. Although the physical communication medium changed to the faster Ethernet, NMEA sentences are still used and encapsulated in UDP datagrams. But LWE also allows the transmission of larger files in a specific binary format. NMEA over IP [26] is a predecessor of LWE, still in use. This protocol is basically a direct portation from the original NMEA 0183 to the IP stack using UDP or TCP. As the protocol is not standardized, the explicit implementation varies between different manufacturers.

At the end of 2020, the first version of the NMEA OneNet standard has been published. OneNet is based on the UDP/IPv6-stack and, in contrast to LWE, supports additional datagram and application security measures. However, as the standardization has just recently been finalized, its market coverage is still very limited. For this reason, our focus is placed clearly on LWE standardized in IEC 61162-450 as the prevailing maritime communication protocol.

2.3 *Cyber Security Testing*

Cyber security is often neglected in maritime systems engineering, leading to inherently insecure systems. Since update cycles and certification processes also take a long time, fixes for identified vulnerabilities do not ship in time. Furthermore, with current methods for testing it is not possible to verify that a weakness causing a vulnerability is actually remedied. Hence, already fixed vulnerabilities may reoccur after system updates or new vulnerabilities may arise from the same weakness. In the maritime domain, this results in a high effort for manufacturers and shipowners in updating, certifying, and deploying new versions of systems after security weaknesses were identified. To reduce the costs, necessary updates to patch security vulnerabilities are left out, which significantly increases the overall cyber risk.

As known from other industries, appropriate tools for comprehensive security testing have an immense benefit. Particularly in the domain of secure software development, automated or semi-automated security testing is a common technique during system development [8]. But security testing has also found its way into a wide range of other domains, e.g., industrial control systems [23] and automotive vehicles [14]. However, in the maritime context, so far only generic tools have been used to support secure systems engineering or identify vulnerabilities.

Sviličić et al. used a generic vulnerability scanner (Nessus) to assess typical maritime components [27–29]. Although their analyses reveal flaws in the systems' underlying operating systems, their assessments do not take into account the maritime-specific context, i.e., the actual maritime applications, data types, and communication protocols. Regarding network security, well-established generic tools like bettercap and yersinia facilitate the testing of common protocol vulnerabilities in the IP stack. On the other hand, several Proofs-of-Concepts (PoCs) on the exploitability of application-level vulnerabilities in maritime systems already exist [3, 4, 20, 22]. However, these PoCs cannot be integrated into system development in an automated manner.

Overall, the maritime sector lacks a true maritime-specific framework that provides adequate tools for testing and assessing cyber security at the application level. Concerning the plurality of components and their interconnection within maritime systems, mentioned in the previous subsections, there is also a large number of attack vectors that need to be addressed by such a framework. The vulnerabilities, from which these attack vectors emerge, will be analyzed in the following section.

3 ANALYSIS OF MARITIME VULNERABILITIES

As Cyber-Physical Systems (CPSs), maritime systems are threatened by attacks from both, physical and cyber space. On the one hand, some maritime sensors

use electromagnetic signals to operate and, thus, are vulnerable to Electronic Warfare (EW). This category of attacks aims to deny the system's access to the electromagnetic spectrum which usually results in a Denial of Service (DoS). Maritime sensors which are known to be prone to EW attacks are GPS, AIS, and radar, cf. [30]. On the other hand, cyber attacks target the information processed in IT systems. They can be categorized by the exploited target which can be a technology, a human, or an organizational process, and by violation of the protection goals availability, integrity, and confidentiality. Our main focus in this paper lies on cyber attacks targeting maritime technology and threatening the availability and integrity of data. This initially excludes supply chain and phishing attacks on employees and suppliers. Nevertheless, cyber attacks that build on successful attacks from these categories, e.g., previously compromised IT systems or corrupt staff members, were considered. The confidentiality of data is neglected because nautical data is rarely classified in civil use cases.

In our threat analysis, we further distinguish between external and internal cyber attacks depending on the attacker's access to the vessel's components. External cyber attacks assume the attacker has access to the communication medium of external interfaces. In the maritime context, this can be a public-facing network interface, a USB port, or even an antenna for radar, VHF, or GPS frequency spectrum. Compared to EW attacks, external cyber attacks do not exclusively target the spectrum, but rather the transmitted information, such as sending fake AIS messages or seemingly valid but interfering GPS signals. Furthermore, they can already be realized with low monetary costs, i.e., less than $400 for VSAT attacks [22] or $2000 for a GPS spoofing [24].

Internal cyber attacks require that the attacker has access to one or more IT components within the internal network. For instance, this can be achieved by a previously compromised component (e.g., via malware) or by injecting an additional malicious device into the network. Compromised components usually have a worse impact on the security of the entire system than external attacks, because the data they provide is generally more trusted by peers.

In [30], Tam and Jones propose a model-based framework for maritime cyber-risk assessment. The authors consider vulnerabilities of both categories, EW (VHF, radar) and external cyber attacks (USB, Internet, satellite). The effects caused are grouped as violations of the protection goals of availability (DoS) and/or integrity (misdirect). Based on this work, our analysis extended the risk assessment to include cyber vulnerabilities of internal cyber attacks, which are neglected as a separate class also in other relevant risk analyses in the literature. Additionally, relevance indices for protecting these systems based on recent incidents according to [1] were added, where applicable. Furthermore, we also include additional maritime system components that are expected to be vulnerable to this new category of attacks, as highlighted in Table 1. As the extension of the original table provided by [30] reveals, internal cyber attacks are expected to expose an additional class of risks to the reliability of maritime systems (emphasized by colored entries in the table). The availability and integrity of these systems may be limited due to a high rate of incoming messages or intentionally manipulated messages sent by a malicious device, for instance. As it has been demonstrated that cyber attacks can have a huge impact on the navigational process, e.g., by distorting the crew's situational picture and provoking a grounding [4, 10, 19, 20], internal cyber attacks must necessarily be taken into account in systems engineering and MET.

Table 1. Internal cyber attacks extend attack vectors on maritime systems according to threat landscape in [30], resulting to further cyber effects, as highlighted in the table. They also have impacts on further components, added in the bottom rows (separated by the dashed line). Systems are ranked by relevance based on previous incidents according to [1].

	Attack Vectors				Cyber Effects	
System	Elec. Warfare	ext. Cyber Attacks	int. Cyber Attacks	Relevance	Availability	Integrity
AIS	✓	✓	✓	19	✓	✓
GNSS	✓	✓		12		✓
ECDIS		✓	✓	10	✓	✓
VDR		✓	✓	9	✓	✓
Radar	✓		✓	5	✓	✓
Speed logs		✓		5	✓	✓
Echo sounder				3		
Compass				–		
Autopilot			✓	–	✓	✓
Conning			✓	–	✓	✓
BNWAS/BAMS			✓	–		✓

3.1 *Attack Model for LWE*

In the case of network attacks, internal attackers can interact with communication by eavesdropping and injecting self-crafted messages. Attackers having these capabilities are called Person-on-the-Side (PotS). If in addition, attackers are able to suppress legitimate messages in existing communication, they are called Person-in-the-Middle (PitM). Note that in the former case, attackers cannot simply prevent the receiving of original messages.

Although PitM attacks can cause more damage and are more difficult to detect, they are also more difficult to execute. PotS attacks, on the other hand, are more realistic and, thus, more likely to occur. In Ethernet networks, a PotS attack can potentially be performed by any compromised component in the maritime system, whereas a PitM attack requires the attacker to obtain a special position in the network, e.g., directly between a sensor's connection to the ECDIS. Both types of attacks could be performed by injecting a malicious sensor, a malicious device (which can be a sensor or a tiny system-on-a-chip device like a Raspberry Pi [21]), or by compromising an existing asset [20]. Our attack model explicitly includes both types of internal cyber attacks, which are integrated into Figure 1 as examples for illustration.

Similar to other established protocols, LWE was not designed to be secure against PitM and PotS attacks. It does not implement supplementary security measures, despite an optional Message Authentication Code using the insecure MD5 hash algorithm by default [13, 15]. However, with the standard IEC 61162-460 [16], new measures to face network security are proposed such as network segregation, firewalls, network access control, and security monitoring. Although this mitigates external and internal cyber attacks, IEC 61162-460 is currently not mandatory and its widespread implementation will take several years. Thus, PitM and PotS attacks will remain relevant in practice.

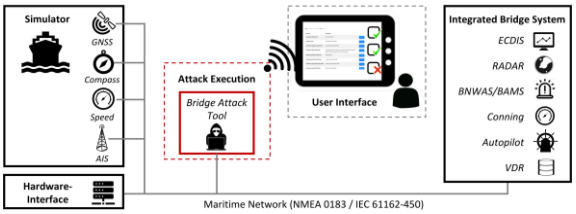

Figure 2. Test- and development environment with sensor input (either using an NMEA/IEC simulator or real maritime electronics) and data consumers, particularly the ECDIS as major HMI device processing and visualizing incoming sensor data.

4 DESIGN AND CONCEPT OF BRAT

The concept of our framework is based on the attack model from the previous section and covers PitM and PotS cyber attacks on maritime networks. BRAT is designed to be integrated into generic development environments together with the maritime application under test. Our reference environment is depicted in Figure 2 and by default provides an IBS consisting of usual components introduced in Section 2.1. A simulator 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.

Attacks against the IBS and other systems in the development environment are conducted by BRAT that is implemented as an ordinary network device. It can launch pre-configured attacks automatically for automated testing or manually be controlled by an operator. For semi-automatic attack execution, attacks can be configured and launched interactively using a graphical Human-Machine Interface (HMI) that is connected via an out-of-band communication channel, e.g., WiFi.

In the setup outlined in Figure 2, BRAT implements PotS attacks against the communication of nautical data in the maritime network. These attacks are performed by capturing legitimate traffic in the network and injecting modified nautical messages that are processed by receivers. For instance, BRAT can inject position-related messages with a relative deviation causing a distorted situation picture. Note that, despite our focus on PotS attacks and LWE in the following sections, BRAT can also be used for PitM attacks as well as for maritime systems supporting NMEA over IP.

4.1 *Architecture*

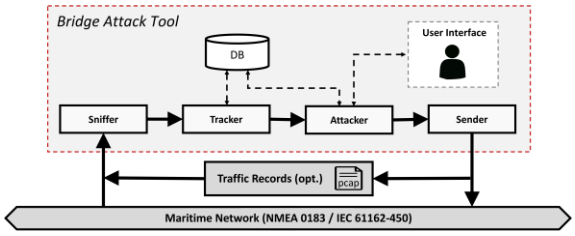

Figure 3. The data flow between BRAT's main components.

The architecture of BRAT consists of four main components whose interaction is visualized in Figure 3. The sniffer captures and filters maritime traffic from the network and provides that data to the tracker. To use BRAT in automated testing of specific scenarios, the sniffer can be configured to use pre-recorded traffic from a file (e.g., in pcap format). The tracker maintains the current navigational state derived from captured packets and stores a history in a database. The attacker module implements the actual attack logic and has access to the database. Based on its configuration and database input, malicious traffic can be generated and finally injected into the network by the sender. Wrappers for nautical payloads provide a convenient language to manipulate nautical data deliberately, e.g., shift the position by the command pos.lon += 1.0. Additional attacks can effortlessly be added to the framework from scratch or by adjusting already implemented attacks (cf. Section 5.2). A user interface allows for configuring, launching, combining, and orchestrating attacks programmatically or interactively. Malicious traffic can also be stored in a file from which it can be replayed or analyzed later.

4.2 *Design Principles*

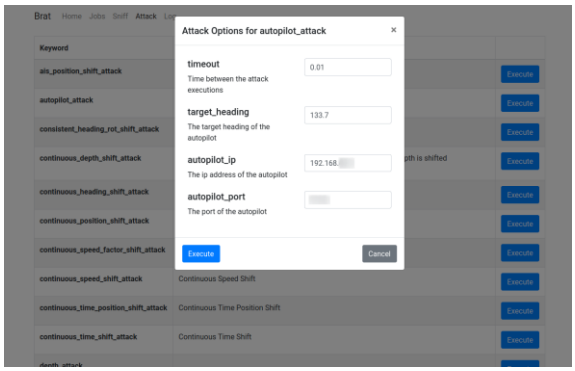

Figure 4. BRAT provides a user-friendly HMI to configure, launch, combine, and orchestrate attacks against the maritime system.

Our design principles include usability, modularity, and reliability. To enhance usability and lower the technical barrier so that also non-technical users can perform security assessments, BRAT comes

with three tailored interfaces. Firstly, 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. Secondly, a command-line interface can be used to interactively launch attacks in security assessments either from scratch or using scripts. Finally, an interactive web-based HMI as depicted in Figure 4 facilitates the use for non-technical users. As use cases and systems change, an attack framework has to be extendable, adjustable, and reusable. Therefore, our architecture follows the modularity principle. In this context, a plugin system is implemented and the functionality of the connection to the maritime network is decoupled from the attack logic. That allows to add customized attacks and support other maritime protocols. Since a security assessment is based on reliable data processing, our framework was implemented together with a comprehensive test suite and logging functionality. This assures dependable application behavior and allows to effortlessly verify modified code sections.

5 IMPLEMENTATION OF ATTACKS

After explaining BRAT's architecture and design principles in the previous section, the following section first introduces BRAT's attack features and provides an overview on possible attacks. Then, it highlights two special attacks to demonstrate the potential of our approach.

5.1 *Attack Features*

Attacks implemented in BRAT aim to alter the presumed and determined navigational state at the receiver. This is achieved by superimposing legitimate traffic by attacker-controlled traffic. To increase the chance of a successful attack, BRAT supports several attack features that are listed in Table 2.

Table 2. Attack features implemented by BRAT to increase the chance of a successful cyber attack.

Attack Feature	Description
Network traffic capturing	Eavesdrop legitimate packets to reckon the current navigational state
Replay attacks	Repeat preceding packets to presume an outdated navigational state
Injection of malicious packets	Produce packets to presume an arbitrary given navigational state
Continuous attacks	Variate data incrementally to obfuscate modification
Parallel attacks	Alter data simultaneously to circumvent possible integrity checks
High frequency	Increase packet frequency to superimpose legitimate traffic
MAC/IP/UDP spoofing	Spoof addresses to veil attacking devices and circumvent integrity checks

The first feature, network traffic capturing, eavesdrops on legitimate packets. From the communicated data, an adversary can estimate the current navigational state to adjust the attacks. Additionally, BRAT can perform replay attacks, which use formerly recorded packets to be resent at a later point in time. Since the original packets were generated by a legitimate source, they are more likely to be accepted by receiving systems. A minimal need for configuration makes these attacks easy to automate.

Instead of just repeating traffic, BRAT can alter packets before emitting them again into the network (injection of malicious packets). It is possible to slightly modify the payload of original packets, which may not attract the attention of the navigator but still impacts navigational decisions. A fixed deviation of the data would be rather obvious. Therefore, BRAT implements continuous attacks with an incrementally increasing variation over time to further obfuscate attacks.

Since modern IBSs support integrity checks of sensor data, the modification of a single nautical data type may be detected by default. For instance, a bogus deviation from the real position may not resonate with the estimated position from the inertial measurement unit causing the integrity check to raise an alert. To circumvent the detection, BRAT supports parallel attacks targeting different sensors simultaneously to enhance the pretended integrity of malicious packets.

As already observed in [19], a high frequency of malicious packets further facilitates cyber attacks. Depending on the actual system, legitimate packets may be discarded or presumed to contain measuring errors, if there are far more packets with nautical data modified by the attacker. Also, the sampling rate of the processing systems may be too slow to process sparsely received benign packets. With BRAT, it is possible to configure the frequency of sending malicious packets.

When standard authentication measures are in place, an active attacker on an IP-based network would rapidly be detected by revealing an unregistered source address. Therefore, BRAT can perform MAC/IP/UDP spoofing, i.e., leave packets up to the transportation layer intact or spoof the identity of explored systems. The ability to arbitrarily change these network addresses can further complicate the identification of malicious packets in existing systems.

5.2 *Implemented Attacks*

As mentioned in Section 3.1, BRAT implements PitM and PotS attacks on the exchange of nautical data in LWEs. According to the attack features from Table 2, cyber attacks can be configured and combined in several ways. For instance, attacks on the availability of the target system may be implemented by using a high frequency of replayed packets for DoS attacks, e.g., by overcharge the receiver or leveraging special malformed packets to trigger parsing errors and crash the receiver. Attacks on the integrity may continuously shift nautical data in multiple messages to spoof several sensors simultaneously and remain undetected by possible integrity checks. NMEA sentences can be parsed, modified, and retransmitted by BRAT. Since many maritime systems support NMEA sentences as input format, our approach can be applied to environments beyond LWE and also to a variety of components, including maritime processing

systems (cf. Table 1) as briefly discussed in the following.

ECDIS, conning, and VDR display and log the current navigational situation and, thus, highly depend on reliable sensor inputs. Interrupted or manipulated nautical data can lead to incorrect estimations and cause the navigator to take wrong and harmful decisions. BRAT's attacks targeting autopilots can send commands, overrule manual steering, and set an intended course. Depending on the autopilot's implementation, it may be possible for an attacker to hijack the autopilot and, thus, to remotely control the vessel. Onboard alarm systems use NMEA sentences to exchange alert information. Hence, BRAT can intercept, manipulate, and suppress raised alerts, but also fake alerts can be generated at a high frequency, e.g., to distract the navigator from forthcoming hazards. Radars use NMEA sentences to deliver located tracks of maritime objects to other devices. As with alarms, these tracks can be intentionally tampered with or injected. Then again, some systems may use traditional IP-based protocols to broadcast radar images, which can be tampered with by non-NMEA-based BRAT attacks. Without loss of generality, in the following, we demonstrate the effectiveness of BRAT's attacks on maritime systems documenting launched attacks against OpenCPN, an open-source chart plotter. Even though it is a free ECDIS that supports only basic functionalities, we would like to emphasize here that we have also tested our attack tool with commercial and well-established products and have come to similar results.

5.3 *AIS Attacks*

AIS attacks can be considered from two perspectives. On the one hand, AIS transceivers consume onboard position and heading information and provide this data to other traffic participants. Indirect attacks on positioning sensors could, thus, imply that transceivers spread incorrect information, which can have a wide variety of effects. On the other hand, a successful AIS attack will result in wrong positions or hidings of targets on the ECDIS, manipulated dimensions of targets, or flooding of "ghost" targets. There are already proposals for securing AIS [2, 9, 18], but an exhaustive implementation is still a long way off. Hence, those systems processing incoming AIS data have to challenge the reliability of that information and implement countermeasures themselves.

BRAT can audit whether an ECDIS application is vulnerable to AIS attacks by simulating a manipulated AIS transceiver and analyzing the application's behavior. Figure 5 shows a successful AIS attack targeting an ECDIS application, which is intentionally obvious for demonstration purpose and inspired by [3]. BRAT manipulates the information sent from the AIS transceiver to flood the chart plotter with fake targets on collision course. Attack options can be adjusted to either hide real targets in a vast number of fake targets or decrement the targets to make the attack less obvious. An unaware navigator may start an evasion maneuver and risk grounding in shallow water.

Modern ECDIS implement radar overlays which makes it possible to validate AIS targets and detect attacks through cross-checking. However, depending on the particular integration of radar tracks, BRAT can circumvent the detection by combining AIS attacks with compatible radar attacks. A more generic approach to disguise fake targets and hide real targets despite radar overlay is subject to our future work.

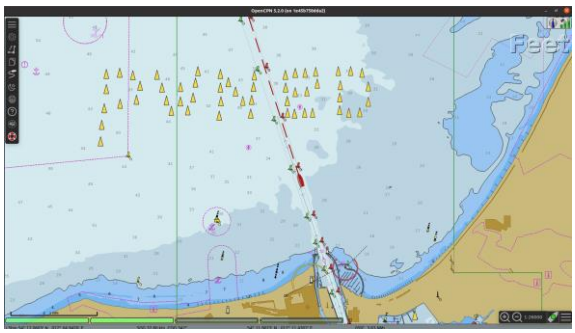

Figure 5. BRAT can launch AIS attacks on the target ECDIS, e.g., to flood the screen of OpenCPN with numerous ghost targets on collision course.

5.4 *Positioning Attacks*

By its very definition, navigation relies on Positioning, Navigation, and Timing (PNT) data. GPS receivers are the central sensors providing not only position and time but also speed and course information. Internal cyber attacks on PNT data have been shown feasible by Lund et al. [20]. Their attack aims to shift the position of the own ship on the ECDIS to make the navigator presumably correct the displayed position, which leads to leaving the actual course. BRAT can simulate such attacks, which is crucial to develop and validate cyber security corresponding countermeasures, but can also be integrated into MET. In Figure 6, the original course displayed by the ECDIS is shifted and injected fake AIS targets fabricate a collision course. In contrast to [20], this is conducted by PotS attacks using an injected device instead of presuming the presence of malware on the ECDIS system as outlined in [19].

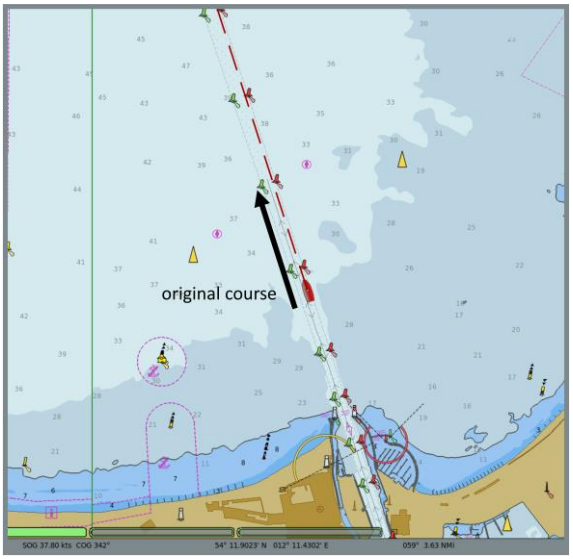

Figure 6a. OpenCPN displays the vessel's original course.

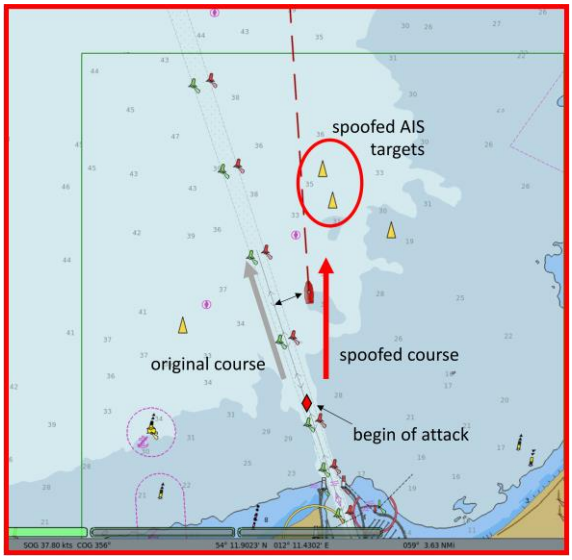

Figure 6b: A cyber attack fabricates a collision course.
Figure 6. PotS attacks on PNT data distort the navigational situation displayed by OpenCPN to fabricate a collision course.

6 SECURITY DISCUSSION

Table 3. Internal cyber attacks (direct) and external cyber attacks (simulative) implemented by BRAT. Due to proprietary radar protocols, simulative radar attacks are only implemented exemplarily, indicated by the bracketed checkmark.

Internal Cyber Attack	AIS	GNSS	ECDIS	VDR	RADAR	Speed Logs	Echo Sounder	Compass	Autopilot	Conning	BNWAS/BAMS
direct	✓		✓	✓	✓				✓	✓	✓
simulative	✓	✓			(✓)	✓	✓	✓	✓		✓

In Section 3, we discussed internal and external attack vectors for maritime systems. BRAT implements attacks addressing these attack vectors. An overview of already implemented attacks on maritime systems is given in Table 3.

Internal cyber attacks use the network interface to attack various system components. Using BRAT complex attacks can be executed targeting AIS, ECDIS, VDR, RADAR, autopilot, conning, and BNWAS/BAMS. With a specially configured PitM attack, BRAT enables full control over the final output of maritime sensors, which makes it further possible to create mock-ups for externally attacked or compromised devices. Thus, external attacks can be "simulated" for all data producers, including AIS, GNSS, speed logs, echo sounder, compass, and BNWAS/BAMS, cf. Table 3.

With respect to related work, it should be emphasized that BRAT is capable of reproducing published cyber attacks, either by executing internal or simulating external attacks. In [19], an attack targeting an ECDIS is proposed. Basically, it uses the injection of malicious packets at a high frequency to attack the integrity of PNT data. This can also be conducted by our approach, as already demonstrated in Figure 6. External attacks targeting AIS are described in [3]. As shown by Figure 5, AIS information displayed in the ECDIS can be arbitrarily manipulated. In this way, the reception of fake AIS data can also be simulated at the same time. Whereas direct attacks on vessels' GNSS receivers cannot be realized by internal cyber attacks, external attacks, particularly GPS spoofing attacks as in [4], are enabled by our tool, as well. For this purpose, internal PitM attacks can mimic the effects of their external counterparts.

As an interactive attack generation framework, BRAT contributes to maritime cyber security in the areas of security assessment, system resilience, attack detection, and security training. BRAT's attacks can be used in penetration tests to assess the cyber security of maritime systems. It uses a common communication interface to attach new systems, provides an interactive HMI to exploratory test launch and combine attack modules, and a scriptable interface to reproducibly trigger identified vulnerabilities. Once defined, those scripts can be automated and integrated into system development cycles to test against vulnerabilities in current and future system versions. This makes it possible to validate the functional behavior and resilience of maritime systems under cyber attacks as part of system development and certification.

As cyber attacks cannot be fully prevented, maritime systems and crews have to be accordingly prepared. A crucial point is the detection of possible attempts on time to prevent the system from further damage. Therefore, security mechanisms, so-called Intrusion Detection Systems, have to be integrated that not only detect cyber attacks but also provide helpful instructions for the navigator to remedy the damage caused by the attack or navigate safely despite flawed systems. BRAT can significantly improve both the development of detection methods and the training of mariners under realistic conditions.

6.1 *Outlook*

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. However, there are complementary onboard protocols to exchange information between IT systems, especially for radar images, chart updates, and automation control. Although not necessarily standardized, some protocol implementations used in operation may reveal flaws similar to LWE, which makes it possible to adapt BRAT to other devices. For instance, the exchange of recorded images in modern radars is based on Ethernet that is vulnerable to the same attacks as LWE unless further security measures are in place. BRAT could, therefore, be enhanced to manipulate those radar images, i.e., inject, replace, delete tracks, by means of internal cyber attacks.

Currently, BRAT's attack model focuses on IBSs onboard commercial vessels. A key assumption in this context is that there is always a human in the loop assessing the navigational situation and validating incoming nautical data. Hence, attacks so far try to

obfuscate malicious behavior primarily in the displayed information to finally decoy the navigator. However, there are other environments in which visual obfuscation is of minor importance. Autonomous surface or underwater vehicles are designed to operate mostly unmanned, eliminating the need and the opportunity for human validation. In consequence, incoming sensor data has an automated impact on how onboard actuators are controlled, which increases not only the likelihood but also the possible damage of a successful cyber attack on the maritime system.

7 CONCLUSION

In this paper, we extended the current threat landscape of maritime systems by internal cyber attacks against integrated bridge systems, which aim to tamper with the communication of nautical data and are usually neglected in existing cyber risk assessments. Moreover, we introduced a BRidge Attack Tool (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. BRAT supports various common network attack features, including packet capturing, replay, and injection attacks along with classical identity spoofing. It can be deployed in common development environments which implement (simulated) sources for nautical data and are compatible to LWE. Thus, it greatly supports existing processes to technically assess, prevent, and detect cyber attacks on maritime systems by using offensive security methods. In addition, Maritime Education and Training can benefit from BRAT as navigators can be trained to adequately react to cyber attacks in realistic scenarios. By using BRAT, we further demonstrated how internal cyber attacks can violate the availability and integrity of common onboard systems and exemplarily highlighted their impacts with regard to AIS and GNSS attacks targeting an ECDIS.

As part of our future work, we plan to extend BRAT's range of applications to support further maritime system interfaces for radar images, chart updates, and automation control. Also, we will widen the context to investigate cyber attacks on autonomous systems.

REFERENCES

1. Awan, M.S., Al Ghamdi, M.A.: Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS). Journal of Marine Science and Engineering. 7, 10, (2019). https://doi.org/10.3390/jmse7100350.
2. Aziz, A., Tedeschi, P., Sciancalepore, S., Pietro, R.D.: SecureAIS - Securing Pairwise Vessels Communications. In: 2020 IEEE Conference on Communications and Network Security (CNS). pp. 1–9 (2020). https://doi.org/10.1109/CNS48642.2020.9162320.
3. Balduzzi, M., Pasta, A., Wilhoit, K.: A Security Evaluation of AIS Automated Identification System. In: Proceedings of the 30th Annual Computer Security Applications Conference. pp. 436–445 Association for Computing Machinery, New York, NY, USA (2014). https://doi.org/10.1145/2664243.2664257.
4. Bhatti, J., Humphreys, T.E.: Hostile Control of Ships via False GPS Signals: Demonstration and Detection. Navigation. 64, 1, 51–66 (2017). https://doi.org/10.1002/navi.183.
5. Bimco: The Guidelines on Cyber Security Onboard Ships, https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships, last accessed 2021/04/19.
6. BSI: IT-Grundschutz Profile for Shipping Companies - Minimum Protection for Ship Operations, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/profiles/Profile_for_Shipping_Companies_Minimum_Protection_for_Ship_Operations.pdf, last accessed 2021/04/19.
7. ENISA: Cyber security aspects in the maritime sector, https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1, last accessed 2021/04/19.
8. Felderer, M., Büchler, M., Johns, M., Brucker, A.D., Breu, R., Pretschner, A.: Chapter One - Security Testing: A Survey. In: Memon, A. (ed.) Advances in Computers. pp. 1–51 Elsevier (2016). https://doi.org/10.1016/bs.adcom.2015.11.003.
9. Goudosis, A., Katsikas, S.: Secure AIS with Identity-Based Authentication and Encryption. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation. 14, 2, 287–298 (2020). https://doi.org/10.12716/1001.14.02.03.
10. Hassani, V., Crasta, N., Pascoal, A.M.: Cyber Security Issues in Navigation Systems of Marine Vessels From a Control Perspective. In: OMAE2017. , Volume 7B: Ocean Engineering (2017). https://doi.org/10.1115/OMAE2017-61771.
11. Heering, D.: Ensuring Cybersecurity in Shipping: Reference to Estonian Shipowners. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation. 14, 2, 271–278 (2020). https://doi.org/10.12716/1001.14.02.01.
12. Heering, D., Maennel, O.M., Venables, O.M.: Shortcomings in cybersecurity education for seafarers. Presented at the 5th International Conference on Maritime Technology and Engineering , Lisbon, Portugal (2020).
13. Hemminghaus, C., Bauer, J., Wolsing, K.: SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures. Presented at the ISNCC-TSP (2021).
14. Huang, T., Zhou, J., Bytes, A.: ATG: An Attack Traffic Generation Tool for Security Testing of In-Vehicle CAN Bus. In: Proceedings of the 13th International Conference on Availability, Reliability and Security. Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3230833.3230843.
15. IEC 61162-450:2018: Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection. (2018).
16. IEC 61162-460:2018: Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and Security. (2018).
17. International Maritime Organization: Guidelines on Maritime Cyber Risk Management MSC-FAL.1/Circ.3., https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx, last accessed 2021/04/19.
18. Kessler, G.C.: Protected AIS: A Demonstration of Capability Scheme to Provide Authentication and Message Integrity. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation. 14, 2, 279–286 (2020). https://doi.org/10.12716/1001.14.02.02.

19. Lund, M.S., Gulland, J.E., Hareide, O.S., Jøsok, Ø., Weum, K.O.C.: Integrity of Integrated Navigation Systems. In: 2018 IEEE Conference on Communications and Network Security (CNS). pp. 1–5 (2018). https://doi.org/10.1109/CNS.2018.8433151.
20. Lund, M.S., Hareide, O.S., Jøsok, Ø.: An Attack on an Integrated Navigation System. Necesse. 3, 2, 149–163 (2018). https://doi.org/10.21339/2464-353x.3.2.149.
21. Michalas, A., Murray, R.: Keep Pies Away from Kids: A Raspberry Pi Attacking Tool. In: Proceedings of the 2017 Workshop on Internet of Things Security and Privacy. pp. 61–62 Association for Computing Machinery, New York, NY, USA (2017). https://doi.org/10.1145/3139937.3139953.
22. Pavur, J., Moser, D., Strohmeier, M., Lenders, V., Martinovic, I.: A Tale of Sea and Sky On the Security of Maritime VSAT Communications. In: 2020 IEEE Symposium on Security and Privacy (SP). pp. 1384–1400 (2020). https://doi.org/10.1109/SP40000.2020.00056.
23. Pfrang, S., Borcherding, A., Meier, D., Beyerer, J.: Automated security testing for web applications on industrial automation and control systems. Automatisierungstechnik. 67, 5, 383–401 (2019). https://doi.org/10.1515/auto-2019-0021.
24. Psiaki, M.L., Humphreys, T.E., Stauffer, B.: Attackers can spoof navigation signals without our knowledge. Here's how to fight back GPS lies. IEEE Spectrum. 53, 8, 26–53 (2016). https://doi.org/10.1109/MSPEC.2016.7524168.
25. Santamarta, R.: White paper: Last Call for SATCOM Security, https://ioactive.com/wp-content/uploads/2018/08/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf, last accessed 2021/04/19.
26. Stripydog: NMEA-0183 over- IP: The unwritten rules for programmers, https://stripydog.blogspot.com/2015/03/nmea-0183-over-ip-unwritten-rules-for.html.
27. Svilicic, B., Kristić, M., Žuškin, S., Brčić, D.: Paperless ship navigation: cyber security weaknesses. Journal of Transportation Security. 13, 3, 203–214 (2020). https://doi.org/10.1007/s12198-020-00222-2.
28. Svilicic, B., Rudan, I., Frančić, V., Mohović, D.: Towards a Cyber Secure Shipboard Radar. Journal of Navigation. 73, 3, 547–558 (2020). https://doi.org/10.1017/S0373463319000808.
29. Svilicic, B., Rudan, I., Jugović, A., Zec, D.: A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. Journal of Marine Science and Engineering. 7, 10, (2019). https://doi.org/10.3390/jmse7100364.
30. Tam, K., Jones, K.: MaCRA: a model-based framework for maritime cyber-risk assessment. WMU Journal of Maritime Affairs. 18, 1, 129–163 (2019). https://doi.org/10.1007/s13437-019-00162-2.