Demo: Maritime Radar Systems under Attack. Help is on the Way!

Frederik Basels[°], Konrad Wolsing[°•], Elmar Padilla[°], Jan Bauer[°]

[°]Fraunhofer FKIE
Cyber Analysis & Defense
Wachtberg, Germany

[•]RWTH Aachen University
Communication and Distributed Systems
Aachen, Germany

{frederik.basels, konrad.wolsing, elmar.padilla, jan.bauer} @fkie.fraunhofer.de

***Abstract*—For a long time, attacks on radar systems were limited to military targets. With increasing interconnection, cyber attacks have nowadays become a serious complementary threat also affecting civil radar systems for aviation traffic control or maritime navigation. Hence, operators need to be enabled to detect and respond to cyber attacks and must be supported by defense capabilities. However, security research in this domain is only just beginning and is hampered by a lack of adequate test and development environments. In this demo, we thus present a maritime Radar Cyber Security Lab (RCSL) as a holistic framework to identify vulnerabilities of navigation radars and to support the development of defensive solutions. RCSL offers an offensive tool for attacking navigation radars and a defensive module leveraging network-based anomaly detection. In our demonstration, we will showcase the radars' vulnerabilities in a simulative environment and demonstrate the benefit of an application-specific Intrusion Detection System.**

I. Introduction & Background

Electromagnetic attacks against radar systems have been part of electronic warfare since the military use of radar equipment in World War II and are applied both offensively and defensively. Radiating a high amount of electromagnetic waves onto the enemies' radar antenna can hide or disturb incoming threats and led to an ongoing race of electronic attacks, their counter- and counter-countermeasures [1]. However, modern reconnaissance and surveillance radars interconnected with other systems also open the door to a new type of threat in the form of network-based cyber attacks [2]. Originally, air-gapped systems are now connected to the outside world for remote maintenance, updates over-the-air or the convenience of network access to the staff, enabling attackers to infect systems from outside by software exploits or missing perimeter security. The possibility of targeting radar systems without the need of highly specialized and expensive hardware or physical presence enables non-military groups to launch attacks on radar systems outside the military domain. Civil systems, such as air traffic control or maritime integrated bridge systems (IBSs), utilize radars to secure air traffic or navigation and can now also be targeted by cybercriminals to cause physical or financial harm to individuals or the economy. In the maritime domain, an exemplary scenario could be the deliberate manipulation of a ship's navigation radar to cause collisions or groundings in narrow waterways. The potential far-reaching consequences of such a scenario to the economy were ubiquitously demonstrated by the accident of the Ever Given in 2021, blocking the Suez Canal for six days and leading to a tailback of hundreds of ships [3].

By now, there is no verifiable evidence that a radar system has been targeted by a cyber attack. However, different researchers have demonstrated the feasibility of network-based attacks, due to the lack of basic security mechanisms [4]–[6]. The initial scenario is always a malicious actor with access to the (maritime) radar network, e.g., via a compromised device or gateway on the network (cf. Figure 1), who thus has the capability not only to eavesdrop on radar communication but also to craft and inject manipulated data. Spoofing radar echoes or transmitting control commands to the radar unit enables the attacker to arbitrarily modify the radar image. Such manipulations enable generic denial of service (DoS) attacks, but also more sophisticated attacks, such as creating artificial radar targets or performing false-flag operations [7].

Manipulating parts of the radar screen by message injection is made possible due to the transmission of the radar image over the network. Typically, a radar unit continuously transfers the image in form of scanlines, which can be received and visualized by a radar display, called plan position indicators (PPIs), or integrated into a ship's electronic chart display and information system (ECDIS). Each scanline contains the intensity of the echoes of electromagnetic pulses emitted by the rotating radar antenna in the respective circular sector, which is defined by an angular value in the header field of a radar network message. By injecting spoofed scanlines into the network, researchers were able to arbitrarily change parts of the radar image or jam the entire PPI screen [6]. The format of the transmitted scanlines varies between the

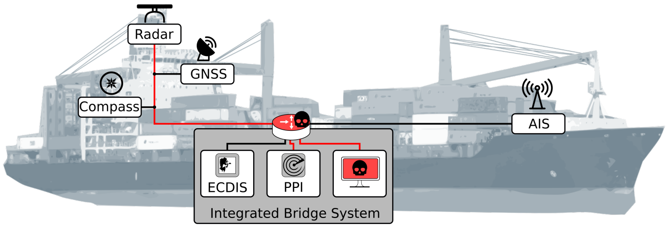


Fig. 1. Broad overview of a ship's network at which all sensor data is collected at the integrated bridge system (IBS). An attacker can either tap into the network in between the radar unit and the receiving devices or can use a corrupted device to inject manipulated data.

DOI: 10.1109/LCN60385.2024.10639793

manufacturers and applications. While the aviation sector usually transmits video data using a standardized protocol named ASTERIX [8], maritime navigation radars often utilize proprietary formats [6]. This diversity complicates the radar security research since the few existing tools and testbeds, e.g., MaCySTe [9] or MaCy [10], only support a limited number of protocols. For this demo, we combine two of our previous research results into one framework to demonstrate a modular Radar Cyber Security Lab (RCSL) that can support researchers in developing and testing defensive mechanisms for radar units and networked radar systems. The lab provides a simulative testbed and a set of tools that can be connected to a physical or simulated radar network individually, to perform offensive and defensive tasks. Furthermore, we demonstrate the live operation of our radar-specific network-based Intrusion Detection Systems (IDSs), which are our first steps in the direction of verifying radar echoes on authenticity to defend radar systems on the network level. To achieve broad compatibility with radars of different manufacturers, each tool is easily adaptable to other protocols and also enables the implementation of protocol-specific solutions. Alongside the scientific purpose, it can support the training of future radar operators to detect cyber attacks against their systems and to react appropriately.

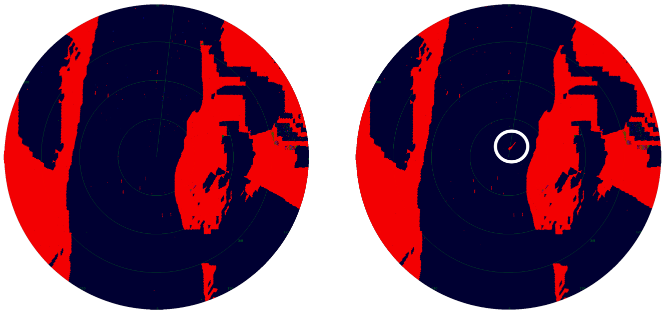
II. Radar Cyber Security Lab

The RCSL that is presented in the demonstration is built up on two contrary modules. First, it contains an offensive tool to perform network-based attacks against maritime navigation radars to cause an incorrect depiction of the ships' surroundings (cf. Section II-A). The second module is a defensive toolset in the form of radar-specific network-based IDSs (cf. Section II-B). Each tool can be configured to operate on different radar protocols and in different positions on the network. For easy setup, all tools are dockerized and can either run in individual containers or on the host system, connected to a simulated or the host's network.

A. Attacking the Radar Network

The offensive module and heart of RCSL is the Radar Attack Tool (RAT) [6], which implements different network-based cyber attacks against maritime navigation radars. RAT can either be configured to operate as machine-on-the-side (MotS) in the network to perform message injection attacks or can run as machine-in-the-middle (MitM) by placing it between the radar sensor and the receiving systems, e.g., a PPI or an ECDIS. The attacks can either be configured in advance by scheduling a list of attack types and their durations, or they can be selected interactively on the running instance using a simple web interface that connects to RAT via an API.

All of RAT's attacks are aimed at giving the radar operator an incorrect assessment of their surroundings and tempting them into actions that endanger the ships' safety. With generic DoS attacks, RAT is capable of rendering the PPI useless, blinding the radar operator. However, blanking or disturbing the whole radar screen or turning off the radar unit is detectable at first sight, even by inexperienced radar operators. Thus, to prevent early detection, RAT includes two more sophisticated attack types, i.e., *transformation* and *object manipulation* attacks [6]. They differ in the proportion of the radar image that is manipulated and the resulting probability of detection. While the transformation attacks change the whole radar screen by rotating, shifting, or scaling the image, object manipulation attacks are more subtle and only target specific areas of the image. To localize objects on the radar screen, RAT listens to other sensor data on the network, e.g., automatic identification system (AIS) and global navigation satellite system (GNSS) messages, which are usually transmitted unencrypted over the ships' networks [5]. The effect of an object manipulation attack is to disguise or move specific radar targets, such as a ship or buoy, or to create artificial ship echoes on the PPI, as shown in Figure 2. To further reduce the probability of detection, RAT is also able to spoof the AIS signals of the targeted ships.



(a) Benign radar image.

(b) Object manipulation attack.

Fig. 2. The PPI screens showing the surroundings of a ship during normal operation (Figure 2(a)) and the effect of an attack that creates radar echoes of a non-existing ship in front of the own position (Figure 2(b)).

B. Network-located Defense of the Radar System

The defensive module of RCSL consists of two network-based IDS solutions inspecting and analyzing the radar data on different levels [11]. The first solution utilizes the nearly constant rotation speed of the radar antenna, which leads to a predictable time between packets and a defined order of scanlines, with successive scanlines covering contiguous circular sectors. Consequently, the angle value in the header fields has to increase between successive packets. Any violation of this behavior indicates the injection of messages by a third party on the network. The consistency enables a description of the packet properties by a set of rules for Snort3 [12], an open-source signature-based IDS. These rules have been proven to be effective against MotS attacks in our previous work [11]. However, in a MitM scenario, an attacker can modify the content of the packets without causing a remarkable change of the network behavior, thereby evading detection. Therefore, RCSL comes with a second IDS solution that analyzes the transmitted radar image based on validated knowledge instead of patterns in the network traffic. As ground truth, the IDS either uses the radar image of the previous rotation (*Image-Delta*) or the verified position of landmarks

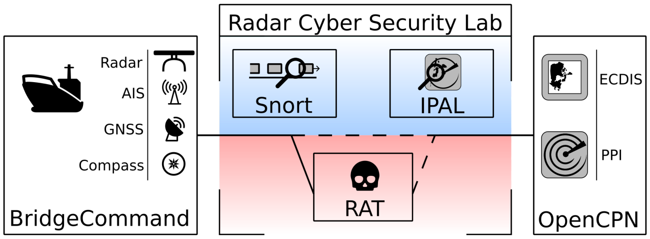


Fig. 3. Overview of RCSL's offensive (🟥) and defensive (🟦) modules and the simulation tools used in our demo. RAT either injects packets as a MotS or modifies transmitted packets in a MitM setup.

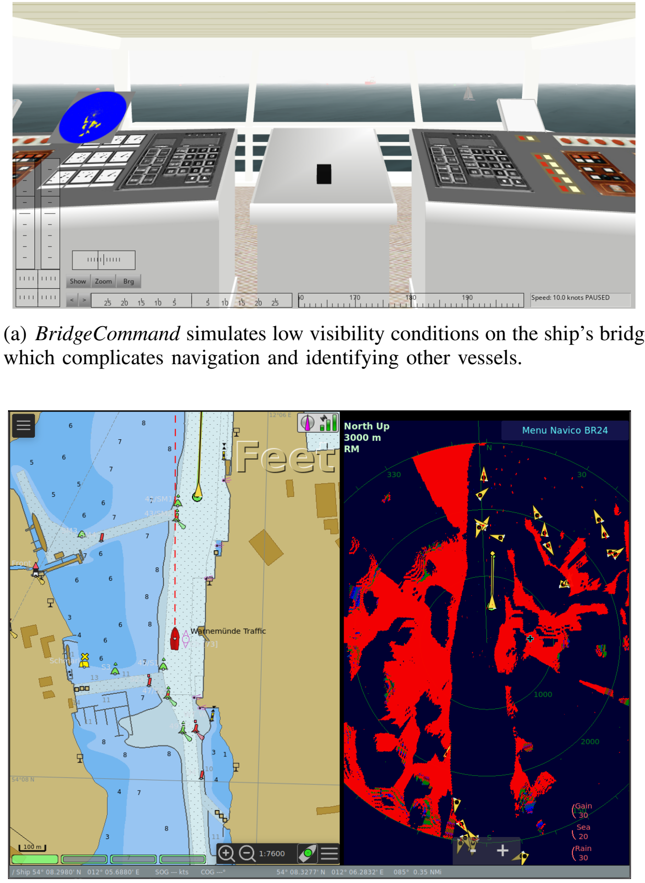
on nautical charts (*Chart-Diff*). Both radar-specific IDSs have been shown to be effective on recorded datasets and represent a first step regarding the feasibility of detecting attacks based on the systemic verification of radar echoes [11].

1) Image-Delta: The main idea of this detection method is based on the assumption that most parts of the radar image are predictable with knowledge about the movement of the ship. After every full rotation, the radar image is stabilized by rotating it into a north-up orientation. Thus, any movement of the ship, reflected in the position of radar echoes, is reversed. The result is compared to the previous radar image, leading to a *delta* value, representing the amount of echoes that are different between both images. To prevent false alerts caused by distortions or inaccuracies on the radar image, the *delta* is compared to a threshold that can be configured or trained in advance. Any *delta* that exceeds this threshold is handled as a malicious change and triggers an alert.

2) Chart-Diff: The second detection method is based on the requirement of ships to utilize up-to-date nautical charts that contain precise positions of landmasses and buoy [11]. Together with GNSS information of the ship, radar echoes can be mapped on these charts to verify their positions with coastlines and other charted objects. Since echoes of other ships and noise can not be validated, the amount of all unverifiable signals have to be compared to a threshold, similar to *Image-Delta*. However, landmasses typically cause distinctive areas on the screen, and their manipulations heavily increase the amount of echoes that do not correspond to objects on nautical charts, leading to exceeding the threshold value. Changes to the echoes of coastlines are thus noticeable, such as the translation or rotation of the radar image.

III. Demonstration

In this demonstration, we present the combination of our offensive and defensive tools from previous research as a framework for future work. After a brief introduction to the setup, we will demonstrate a set of attacks against a simulated ship bridge that utilizes a Navico BR24 navigation radar. An overview of the used tools is shown in Figure 3 and the overall setup is similar to the *radarsec-lab*[1] that was used in our previous work to create the RadarPWN[2] datasets of



(a) *BridgeCommand* simulates low visibility conditions on the ship's bridge which complicates navigation and identifying other vessels.

(b) The surroundings can still be perceived through AIS and radar information visualized by *OpenCPN*'s *radar_pi* plugin.

Fig. 4. Simulated view of the operators' view on the bridge (Figure 4(a)). Caused by the poor weather conditions, the ship's crew is forced to trust the information shown on the ECDIS and PPI (Figure 4(b)).

a maritime bridge system. For visualization, we use the chart plotter navigation software *OpenCPN* [13] together with the open-source plugin *radar_pi* [14]. The plugin adds a radar PPI to the ECDIS screen of *OpenCPN* and implements an interpreter for different radar protocols, including the one used by Navico BR24 radar units [15]. All radar echoes are simulated by *BridgeCommand* [16], which was extended to convert the echoes from the internal representation into Navico BR24 protocol format and transmit them as UDP packets over a network. Further, we use *BridgeCommand* to simulate the movement and network traffic of the targeted ship as well as its environment and all its surrounding objects, i.e., other ships and buoys. To this simulation of an IBS and its environment, we connect RAT as our offensive tool and our defensive toolset, which consists of Snort3 and the radar-specific IDS solutions implemented in the IPAL Framework [17].

Our demonstration covers both types of attacks, i.e., translation of the whole radar image and the object modification (cf. Section II-A), in MotS and MitM configurations. In all cases, the demonstration showcases the scenario of a ship traveling in a narrow waterway under poor visibility conditions, e.g., due to heavy rain, fog, or at night. Steering the

[1] available at https://zenodo.org/records/7188549

[2] available at https://zenodo.org/records/7188636

ship then heavily depends on the ship's sensors, i.e., compass, GNSS, and radar (cf. Figure 4). Playing the part of the attacker, we exploit the dependency on sensor data and use RAT to interfere with the radar image by using different attacks of increasing complexity. During the attacks, we discuss the challenge of their detection by the ships' operators, who can only use the information given on the bridge's systems. A running instance of RCSL's network-based IDS further showcases the capabilities of supporting the operators to detect attacks against radars. At the same time, it demonstrates the limitations of the provided solutions and highlights the need for further research in defending radar systems.

IV. Outlook

One particular area of interest in our future work is the applicability and defense of hybrid electronic warfare in the maritime domain, which combines internal cyber attacks with established external attacks of the electromagnetic spectrum. Longo et al. [7] demonstrated an attack that is on the edge of being part of this hybrid domain. By using packet injection from inside the network, they simulated the effects of external jamming of the radar by creating interference on the victim's PPI. They argued that an intelligent positioning of the jamming patterns, e.g., close to other ships, can lead to false allegations and could be used to perform military false flag operations.

Other researchers were able to use electromagnetic attacks to create unidirectional communication channels from outside into the victim's system. Such external signals are received by a ship's sensors and shared over the network. By exploiting different message fields of AIS radio signals, Amro et al. [18] were able to inject control commands into maritime networks and control malware on ships' systems. Others targeted the victim's radar with jamming sequences, causing patterns on the PPI image which were detected by the malware and initiated malicious actions [19].

With RCSL, we have the base framework to implement the simulation of such hybrid attacks by further extending *BridgeCommand* to inject external adversarial signals to the ships' network and by adding a trigger mechanism to RAT. With the help of this simulator, we strive to further investigate the usability of radar signals for establishing a communication channel with the overall goal to reveal hidden control commands and prevent hybrid attacks.

V. Conclusion

This paper with the described demo investigates the cyber security of modern (marine) navigation radar. Nowadays, interconnecting radar units with other systems eases the operation but introduces vulnerabilities to network-based cyber attacks. Safety-critical areas that require correct and precise radar data, e.g., maritime navigation, thus must implement mechanisms to defend their systems against cyber attacks. The development of protective solutions requires knowledge of radar systems' vulnerabilities and the impact of manipulations, but research on this topic is scarce. For this reason, we presented RCSL as a framework to assist researchers in developing new defense solutions for radar systems while introducing our first results on radar-specific Intrusion Detection Systems.

Acknowledgments

The authors would like to thank Antoine Saillard for his valuable contribution to RCSL. With his research activities, he has significantly supported and fostered the design, implementation, and evaluation of the proposed offensive and defensive components.

References

[1] F. A. Butt and M. Jalil, "An overview of electronic warfare in radar systems," in *Proc. of the Int. Conference on Technological Advances in Electrical, Electronics and Computer Engineering (TAEECE)*, Konya, Turkey, 2013.

[2] S. Cohen, T. Gluck, Y. Elovici, and A. Shabtai, "Security analysis of radar systems," in *Proc. of the ACM Workshop on Cyber-Physical Systems Security & Privacy (CPS-SPC)*, London, UK, 2019.

[3] M.-A. Russon, "The cost of the suez canal blockage," *BBC News*, 2021. [Online]. Available: https://www.bbc.com/news/business-56559073

[4] E. E. Casanovas, T. E. Buchaillot, and F. Baigorria, "Vulnerability of Radar Protocol and Proposed Mitigation," *Journal of ICT Standardization*, vol. 4, 2016.

[5] G. Longo, E. Russo, A. Armando, and A. Merlo, "Attacking (and Defending) the Maritime Radar System," *IEEE Transactions on Information Forensics and Security*, vol. 18, 2023.

[6] K. Wolsing, A. Saillard, J. Bauer, E. Wagner, C. van Sloun, I. B. Fink, M. Schmidt, K. Wehrle, and M. Henze, "Network Attacks Against Marine Radar Systems: A Taxonomy, Simulation Environment, and Dataset," in *Proc. of the 47th IEEE Conference on Local Computer Networks (LCN)*, Edmonton, Canada, 2022.

[7] G. Longo, A. Merlo, A. Armando, and E. Russo, "Electronic Attacks as a Cyber False Flag against Maritime Radars Systems," in *Proc. of the 48th IEEE Conference on Local Computer Networks (LCN)*, Daytona Beach, Florida, USA, 2023.

[8] *Specification for Surveillance Data Exchange – ASTERIX Category 240: Radar Video Transmission*, 3rd ed., https://www.eurocontrol.int/publication/cat240-eurocontrol-specification-surveillance-data-exchange-asterix, EUROCONTROL-SPEC-0149-240, 2015.

[9] G. Longo, A. Orlich, S. Musante, A. Merlo, and E. Russo, "MaCySTe: A virtual testbed for maritime cybersecurity," *SoftwareX*, vol. 23, 2023.

[10] J. Bauer, J. Kutzner, P. Sedlmeier, A. Rizvanolli, and E. Padilla, "*Phish & Ships* and Other Delicacies from the Cuisine of Maritime Cyber Attacks," in *Proc. of the 3rd European Workshop on Maritime Systems Resilience and Security (MARESEC)*, Bremerhaven, Germany, 2023.

[11] A. Saillard, K. Wolsing, K. Wehrle, and J. Bauer, "Exploring Anomaly Detection for Marine Radar Systems," in *Proc. of the 10th Workshop on the Security of Industrial Control Systems & of Cyber-Physical Systems (CyberICPS)*, Bydgoszcz, Poland, 2024.

[12] M. Roesch *et al.*, "Snort: Lightweight intrusion detection for networks." in *Proc. of the 13th Systems Administration Conference (Lisa)*, vol. 99, no. 1, Seattle, Washington, USA, 1999.

[13] OpenCPN, "OpenCPN Chart Plotter," https://github.com/OpenCPN/OpenCPN, 2023.

[14] radar_pi, "Radar Plugin for OpenCPN," https://github.com/opencpn-radar-pi/radar_pi, 2023.

[15] A. Dabrowski, S. Busch, and R. Stelzer, "A Digital Interface for Imagery and Control of a Navico/Lowrance Broadband Radar," in *Proc. of the 4th International Robotic Sailing Conference*, Lübeck, Germany, 2011.

[16] J. Packer, "Bridge Command," https://github.com/bridgecommand/bc, 2023.

[17] K. Wolsing, E. Wagner, A. Saillard, and M. Henze, "IPAL: Breaking up Silos of Protocol-dependent and Domain-specific Industrial Intrusion Detection Systems," in *Proc. of the 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID)*, Limassol, Cyprus, 2022.

[18] A. Amro and V. Gkioulos, "From click to sink: Utilizing ais for command and control in maritime cyber attacks," in *ESORICS*, Copenhagen, Denmark, 2022.

[19] W. C. Leite Junior, C. C. de Moraes, C. E. de Albuquerque, R. C. S. Machado, and A. O. de Sá, "A triggering mechanism for cyber-attacks in naval sensors and systems," *Sensors*, vol. 21, no. 9, p. 3195, 2021.