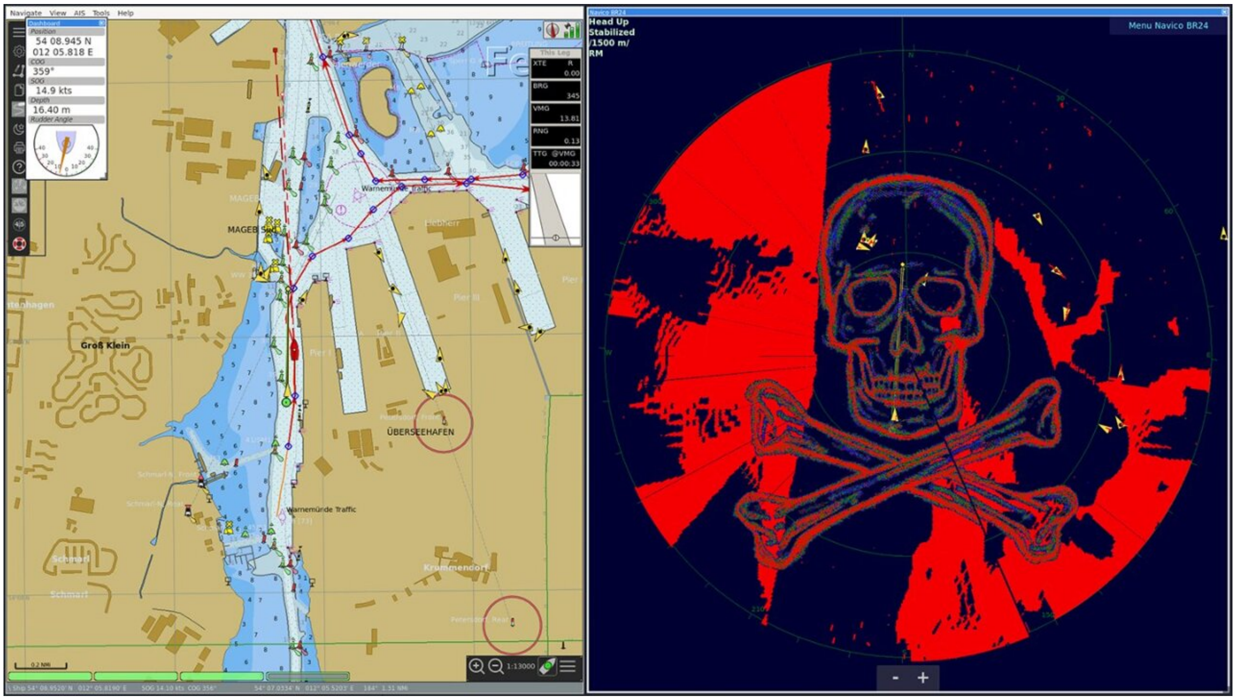
TechXplore

Modular maritime security lab simulates cyberattacks on ships to find ways to detect and defend against them

May 2 2023



Cyberattacks on industry and critical infrastructure are on the rise across the globe. Targets also include ships, which, by transporting billions of tons of goods around the world each year, form part of international supply chains — yet their on-board IT systems often lack secure protection. To raise awareness of the risks of inadequate cybersecurity at sea and to help develop defensive solutions for guarding against cyberattacks, the Maritime Cyber Security research group at the Fraunhofer Institute for Communication, Information Processing and Ergonomics FKIE has teamed up with the Fraunhofer Center for Maritime Logistics and Services CML to set up a modular maritime security lab. This simulates cyberattacks on ships to find ways to detect and defend against attacks. Manipulation of the radar image by the Bridge Attack Tool (BRAT) in a simulation scenario in the Rostock-Warnemünde area. Credit: Fraunhofer-Gesellschaft

For six days in the spring of 2021, the Suez Canal—a narrow waterway connecting the Red Sea and the Mediterranean Sea and an important trade route between locations such as China and Europe—was blocked by the container ship "Ever Given."

A single stricken cargo vessel caused tremendous congestion, with several hundred other container ships stuck as they waited to get through. This in turn had implications for international trade. The resulting delays led to a shortage of containers at ports, threw schedules into several months of disarray and held up shipments.

This incident showed just how dependent we are on maritime bottlenecks like the Suez Canal. As a trading nation, Germany relies on imports and exports running smoothly. If a key trade route is blocked for more than a few days, this has a direct and disruptive impact on production and supply. According to the authorities, the "Ever Given" did not run aground because of a cyberattack, but it is not hard to imagine what could happen in the event of a successful attack on the digital navigation and communication systems on board one or more cargo ships.

Ships as potential targets

Ships increasingly require networking technology in general—whether for finding the best way to navigate routes, monitoring goods or allowing the crew to contact home. This makes maritime systems all the more vulnerable to cyberattacks. Basically, three different kinds of attacks are conceivable, as Dr. Jan Bauer, head of the Maritime Cyber Security research group at Fraunhofer FKIE, outlines, "Generic attacks are not aimed specifically at ships and are therefore the most common threat," explains Bauer, highlighting the example of a USB stick infected with ransomware being connected to the on-board computer.

"Targeted attacks that are carried out with a high degree of expertise and can make ships simply vanish from radar, for example, are far more dangerous," he adds with emphasis. Another possible type of attack involves what is known as electronic warfare. Strictly speaking, this is not actually a cyberattack, but it can have a similar impact in that it affects systems such as GPS by means of interfering transmitters or by using high-frequency radio waves ("jamming" or "spoofing").

Realistic test environment with a stationary ship's bridge

Researchers at Fraunhofer FKIE can simulate these different kinds of cyber-physical attacks, i.e., attacks that impact the real world, in a maritime security lab. The true-to-life stationary ship's bridge under development at the CML in Hamburg is currently being expanded to create a cybersecurity lab as part of the MaCy (maritime cybersecurity lab) project.

This onshore facility features all the tools and systems usually found at sea: the bridge hardware, marine radio and AIS (Automatic Identification System) transceivers, a radar unit and the ECDIS (Electronic Chart Display and Information System), which is used for navigation, among other things. Within this realistic and controlled test environment, the research group is using a variety of developments to detect, investigate and, ideally, avert IT security breaches.

The Bridge Attack Tool (BRAT) makes it possible to carry out effect-based simulations. Developed as an offensive security tool, BRAT has the capability to carry out various attacks itself—such as denial-of-service (DoS) attacks or disrupting and manipulating radar and positioning systems—and show the tangible impact they have on the on-board systems. With a subsequent analysis, the researchers can then highlight existing weaknesses in software systems to industry partners and help them rectify these issues and develop countermeasures by drawing on areas such as cryptography.

To help detect cyberattacks on ships as early as possible, the team has designed a maritime intrusion detection system that automatically spots anomalies. This Cyber Incident Monitor (CIM) evaluates potential attacks and provides information and guidance to the crew over an ergonomic user interface. "In stressful situations, warnings and recommendations for the ship's crew need to be simple and straightforward to implement," says Florian Motz, head of the "organizational ergonomics" research group at Fraunhofer FKIE.

"That's why, when developing CIM, we paid particular attention to ensuring that audible warnings, for example, are only triggered when urgent action is needed, and that alarms and warnings come with information and aids for making decisions—such as advice not to trust the GPS for the time being. The alarm and warning concept is in line with performance standards for bridge alarm management from the International Maritime Organization (IMO)," says Motz.

The team has been working on CIM and parts of the development of BRAT in collaboration with the company BM Bergmann Marine GmbH under the SINAV research project (a study on integrating and processing sensory, navigational, communication and automation information for semi- and fully autonomous ship operation in order to guarantee safe navigation) on behalf of the German Federal Ministry for Digital and

Transport.

Raising awareness and developing measures

The researchers' objective is to use the innovative maritime security lab to raise awareness among companies, authorities and nautical experts of the dangers of cyberattacks at sea and to work with industrial partners to develop protective measures. On the one hand, they can test and upgrade existing systems. On the other, they can provide research data to develop new solutions and thus help establish an approach based on the concept of security by design.

Jan Bauer believes that systematic prevention combined with effective methods for detecting potential cyberattacks offers the best protection from harm. "We mustn't be lured into a false sense of security just because cyberattacks on ships have not been widely reported. Particularly, the systems on older cargo vessels, which have been in use for decades now, are in urgent need of upgrading," he says. The researchers are very clear about the motivation behind their work: With their research findings, they aim to successfully prevent attacks and thus play a small but important part in ensuring IT security and cybersecurity in global supply chains—which in turn are essential to geopolitical security.

Provided by Fraunhofer-Gesellschaft

Citation: Modular maritime security lab simulates cyberattacks on ships to find ways to detect and defend against them (2023, May 2) retrieved 19 April 2024 from https://techxplore.com/news/2023-05-modular-maritime-lab-simulates-cyberattacks.html