Outdated systems placing maritime vessels at risk of cyber-attack, study suggests

May 24 2016, by Alan Williams

Maritime vessels are under significant threat of cyber-attack because many are carrying outdated software and were not designed with cyber security in mind, according to new research.

But operators could easily mitigate against such dangers by updating security systems, improving ship design and providing better training for

crews, the study led by Plymouth University's Maritime Cyber Threats Research Group suggests.

Traditionally, attacks on marine vessels have included piracy, boarding, theft, and/or destruction, and while these attacks have often been successful and continue, they are well understood.

In contrast, the article says, cyber-attacks are much more stealthy, but have a range of potential implications including business disruption, financial loss, damage to reputation, damage to goods and environment, incident response cost, and fines and/or legal issues.

Professor Kevin Jones, Executive Dean of Science and Engineering, is lead author on the paper which also involved Dr Maria Papadaki, Lecturer in Network Security at Plymouth University, and staff from the Security and Management Lab at HP Enterprise in Bristol. He said:

"In an increasingly connected and technologically dependent world, new areas of vulnerability are emerging. However, this dependency increases the vessel's presence in the cyber domain, increasing its chances of being targeted and offering new vectors for such attacks. Longer term, there needs to be a fundamentally different approach to security of the entire maritime infrastructure meaning there is great need for specific cyber security research programmes focused on the maritime sector."

The article – published in Engineering and Technology Reference – suggests maritime cyber-attacks would most likely target systems responsible for navigation, propulsion, and cargo-related functions, with many incentives for attackers given that over 90 per cent of world trade occurs via the oceans.

It also illustrates the potential severity of the problem by providing scenarios to demonstrate possible attacks, and examples of where

successful cyber-attacks have been launched.

But it says there are easy mitigations to help prevent attacks, by increasing awareness and good practice in the industry, enabling the crew and providing them with the necessary tools to prevent and stop some attacks. The paper adds:

"As things stand, there are fundamental issues with securing the technology used in the maritime industry and the sector is probably the most vulnerable aspect of critical national infrastructure. Both security firms and hackers have found both general flaws and specific, real-world, flaws within the navigation systems of ships, and it seems plausible that similar outdated systems for propulsion and cargo handling may also be compromised and abused by cyber-attackers."

The Maritime Cyber Threats Research Group at Plymouth University has been formed to bring together leading-edge multidisciplinary research and practical expertise. It includes experts in cyber-security and maritime operations, as well as psychology, maritime law and policy, to investigate the marine cyber threat at all levels from theory through to practice.

Provided by University of Plymouth