2016-04-15

Threats and Impacts in Maritime Cyber Security

Jones, Kevin

10.1049/etr.2015.0123
Engineering & Technology Reference
IET

doi: 10.1049/etr.2015.0123.
Published 22/04/2016

Title: Threats and Impacts in Maritime Cyber Security

Kevin D Jones Faculty of Science & Engineering, Plymouth University, United Kingdom
Kimberly Tam HP Enterprise, Bristol, United Kingdom
Maria Papadaki School of Computing, Electronics & Mathematics, Plymouth University, United Kingdom

Abstract

In an increasingly connected and technologically dependent world, new areas of vulnerability are emerging. This article explores the unique challenges of maritime cyber security in order to better understand the issues with securing vessels at sea, together with the shore based infrastructure supporting this industry. In particular, this article explores the cyber-attacks possible on maritime-related systems for navigation, propulsion, and cargo-related functions. We illustrate the potential severity of the problem by providing several scenarios to demonstrate the attacks possible once a vessel has been compromised and their attendant consequences.

1. Introduction

There is a long history of maritime operations and a consequent awareness of the threats and consequences in a purely physical space. In recent times, the industry has changed to the point where there is heavy dependence on technology. In this paper we explore modern maritime cyber security, which combines the threat of sophisticated cyber attacks with the disadvantages/advantages of being a sea going vessel (e.g., isolated for long periods of time).

This understanding is significant as the number of cyber threats is rapidly increasing (McAfee, 2015), and the world fleet is still growing (i.e., 3.5% in 2015 (United Nations, 2015)) and becoming more technologically dependent.

2. Modern Maritime Cyber Threats

Traditionally, attacks focused on marine vessels including piracy, boarding, theft, and/or destruction. These attacks were often successful, as it is difficult to call and receive help quickly while travelling across the sea. While these threats continue, they are well understood and there are centuries of experience in mitigation actions. In contrast, today's cyber-attacks are much more stealthy and often kept "under the radar" in order to exploit the compromised vessel for a longer period of time and, hence, for greater profit. Current threat implications of marine-based cyber-attacks include business disruption, financial loss, damage to reputation, damage to goods and environment, incident response cost, and fines and/or legal issues.

3. Modern Maritime Vessels and Vulnerabilities

From the perspective of this article, we can say that the vast majority of marine vessels have two significant capabilities, each supported with specific hardware and software. First, all vessels must have systems for **navigation and propulsion**. Significant technological advances in these areas are becoming more ubiquitous, providing the crew with a more comprehensive view on what is happening inside and outside of the ship, often in real time. These capabilities include, but are not limited to, global positioning systems (GPS), marine Automatic Identification Systems (AIS), and the Electronic Chart Display and Information Systems (ECDIS) and the associated digital nautical charts. As a result, fewer human crewmembers are needed to man modern day ships. However, this dependency on technology increases the vessel's presence in the cyber domain, increasing its chances of being targeted and offering new vectors for such attacks.

For example, the global navigation satellite system (GNSS) signals of GPS tend to be very weak (Royal Academy of Engineering, 2011) and thus deliberate or unintentional interference of the signal can easily deter signal recovery or even overload receiver circuitry. While this may not normally be an issue for a marine vessel on the open sea, if an

attacker were to introduce an interference device, disguised and loaded as cargo, this GPS vulnerability may be exploited. Furthermore, it has been speculated that such a device may cost as little as £40 to build, and may be easily obtained and utilized by an inexperienced hacker (Royal Academy of Engineering, 2011). Researchers at University of Texas at Austin (2013) managed to exploit the lack of authentication of satellite GPS signals, and successfully divert the course of a $80 million yacht with a GPS spoofing device. As the GPS receivers of the vessel did not authenticate incoming signals, it was possible to slowly overpower the authentic ones, and eventually gain control of the vessel's navigational system without being detected or raising any alarms. Low cost GPS spoofing devices have already emerged, with notable example the GPS emulator by Qihoo 360, presented in Defcon 2015 and estimated at a cost of $300 (GPS World staff 2015).

Scenario: An attacker is able to place technology in the cargo to interfer with, or alter, communications to and from the maritime vessel. The attacker's hardware can be smuggled aboard via cyber attacks for altering invoices, control cargo loading machinery, or by infecting port software using social engineering. Once aboard, the hacker's cargo may stay dormant and undetected until the optimal time for attack. As a vessel is more isolated physically and connectivity-wise at sea, that is a valid option.

To summarize, the purpose of navigation and propulsion systems is to accurately position the vessel at all times to avoid getting lost and damaging other vessels and land-based structures. As we shall discuss further later, gaining access to these systems could allow attackers to dictate the path of the vessel, whether by tricking the crew with false sensor readings, or by taking control of the propulsion system directly.

The other set of systems of interest are **cargo-related**, i.e. the loading, unloading handling, tracking, and organisation of goods. Excluding passengers, this is relevant for over 98.3% of the world's fleet as of 2015 (United Nations, 2015). Thus the vast majority of the 1.7 million ships distributing goods, waste, and resources like oil, are vulnerable via their automated systems for handling their cargo, as well as the ports that interact with these systems.

Figure 1 gives an overview of systems mentioned above, as they are often found on modern ships. Other popular monitoring software besides ECDIS includes AIS, as mentioned previously. We shall discuss vulnerabilities of both of these navigational systems in the following section.

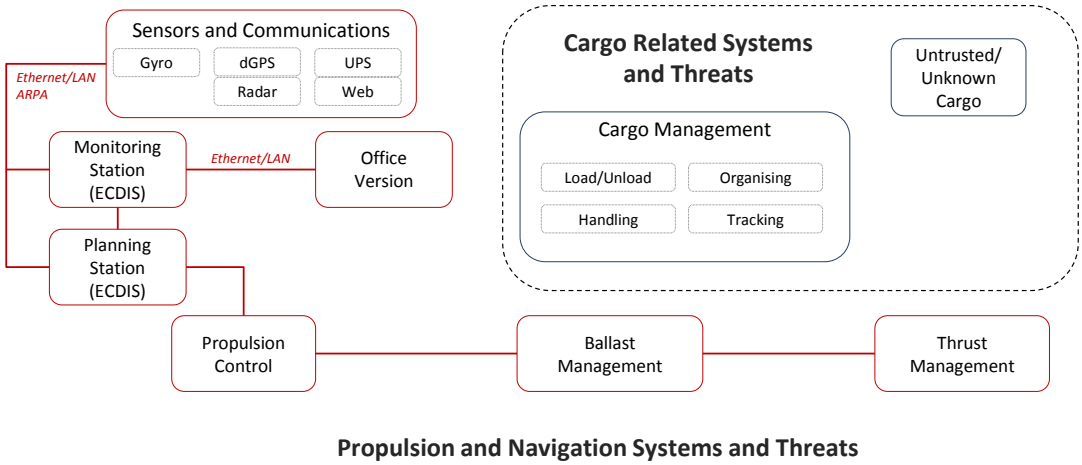

Figure 1.

Overview of navigation, propulsion, and cargo-related systems on a maritime vessel.

For example, in 2013 it was discovered that drug traffickers had hacked the IT system at the Antwerp shipping port in Belgium. This breach gave the organised crime group in-depth knowledge of the security details, and position, of each arriving container, allowing them to steal containers before the arrival of the legitimate owner or overseer. This was ideal for obtaining illegal drugs, hidden amongst legitimate cargo, prior investigations (Bateman, 2014).

Furthermore, the abuse of this particular system, as a result of a cyber-attack two years prior detection, was kept as secretive for as long as possible by the attackers. This is unlike traditional physical maritime attacks. Other scenarios around cyber-attacks on maritime vessels and ports with respect to fraud, such as modifying or sending fake invoices, are also possible (Ott, 2014).

Scenario: There are two possible attacks relating to unsupervised and secret cargo unloading. Firstly, as we have seen in real life, cargo can be stolen if the cyber-attacker had details on the unloading process. Undiscovered theft costs money, but more importantly, it could result in the theft of weapons or materials

that can be weaponized. Secondly, drugs and human trafficking can go unchecked if the systems of either, or both, sending ports and receiving ports are sufficiently compromised.

4. Taxonomy of Maritime Cyber Threat

With an understanding of modern maritime vessels, their systems, and what vulnerabilities they may possess, here we present a taxonomy on maritime cyber threats. While some of these have been implemented in the past, others are likely nefarious activities based on the current technology available to both maritime vessels and attackers.

A. *System vulnerability*

As discussed earlier, ship or port systems may be compromised in order to steal cargo or even hijacked. For example, the ECDIS system that is in charge of displaying digital nautical charts can be compromised (Dyryavyy, 2015) in order to modify files and insert malicious content. This could be a powerful attack, and not only commercial ships are endangered.

In 2013, although by accident, a US navy warship grounded itself on a coral reef due to an error with ECDIS (Dyryavyy, 2015). Studies of this system have found ECDIS to have not been designed securely, e.g. accepting dangerous network methods, and that systems on these ships are often outdated and therefore lacking in some security patches. We discuss the window of vulnerability of maritime systems further on.

Scenario: The malicious version of the incident with the US navy ship could involve an attacker alterting the digital nautical maps, either prior departure or during the voyage at will, to force ships to run aground, into natural formations, or human infastructure. The resulting damange would depend heavily on the vessel size, cargo, and target.

Another system vulnerability has been discovered with AIS, a widely used and mandatory piece of software for vessel positioning and tracking. Security researchers have found ways to abuse the system, such as generating valid commands, changing ship courses, replaying commands, and tracking ships for potential, physical, attacks (Balduzzi, Wihoit, & Pasta, 2013). Again, the general condenses is that these systems are poorly designed at the protocol level, and at the implementation level. As we have seen here, this can result in the hijacking of a ship and/or damaging other ships or structures.

B. Hijacking

Due to cyber-attacks on the various systems on-board a maritime vessel or structure, attackers could control these targets for a number of different outcomes. For example, navigation and propulsion systems may be compromised either with false data, interference, or by encrypting key files or system components. Ransomware has been common to traditional computing systems as well as mobile devices, and could be adapted to the maritime domain. McAfee found that Ransomware is on the rise once again, with a 165% increase of new Ransomware in the first quarter of 2015 (McAfee, 2015) showing that it is a highly profitable and growing sphere of criminal activity.

> **Scenario**: In this scenario, a ship may be compromised via an unsecure network connection. With access to essential systems, an attacker can directly control the ship or encrypt essential system components so that no-one can control the ship. The vessel and any passengers aboard may then be held hostage at sea until some ransom is paid. This is arguably more dangerous, than traditional ransomware due to the isolated nature of ships at sea and their dependency on knowing where they are and being able to travel out harm's way.

Alternatively, a compromised ship may be guided by a hacker to crash into another target either to destroy the ship or another desired target. This attack is viable against other ships, oil rigs, as well as some bridges and possible some land-based structures depending on the situation. Although no such events have happened, given the current level of possible attacks on maritime vessels, it does not seem impossible. For example, although not the same

scenario, there have been reports of an oil rig being shut down after being overwhelmed with malware in 2010. Luckily, the rig was shut off before a possible well blowout, preventing oil spills and an explosion. However, removing all the malware from the rig took 19 days, losing the company potentially up to $700,000 US each day (Shauk, 2013). Similarly, hijacking ships containing bio-hazard material such as dangerous chemicals or causing oil rigs to explode could heavily damage the environment, living things in the area, other valuable resources, and the local economy.

> **Scenario**: Similar to the previous hijacking a scenario, a ship is compromised by a cyber-attack is now under the control of a malicious party. Unlike the previous scenarios, the ship is not the target, but the weapon. The ship itself represents several hundreds of thousands of tons of damage to oil rigs, bridges, other ships, ports etc., as well a carrier of hazardous materials such as nuclear waste to affect a wider area.

C. Outdated Software

There are several reasons why systems on maritime vessels tend to be outdated. Firstly, as large ships are expensive and take a long time to build, many ships were built before cyber security was a major concern. Furthermore, it is not uncommon for new software to be incompatible with older hardware. Therefore, outdated software systems are often kept in use. Just within the US Navy Space and Naval Warfare Systems Command (SPAWAR) over 100,000 workstations run on Windows XP (Gallagher, 2015). In fact, rather than spend the resources to update their systems just as support Windows XP ended, the US Navy opted to pay $9 million US per year to receive support for the older version of Windows (Gallagher, 2015). SWAWAR claimed this to be a temporary measure while the existing hardware and support systems are slowly being updated. This is essential, as outdated software tends to have more vulnerabilities.

Another study by a maritime cybersecurity firm found that 37% of servers running Microsoft failed to download the correct patch and were vulnerable to attacks (Network World, 2015). This demonstrates that, even though the

systems themselves might be up-to-date, they are still vulnerable if not diligent in downloading and applying patches as they become available. Unlike traditional land-based computing, this is particularly challenging for systems isolated at sea. Given that travel times for large vessels tend to be longer, not shorter, due to environmental concerns (Vidal, 2010), the window of attack can last for weeks.

Scenario: If a software vulnerability is discovered just as a target vessel begins its voyage, it may be possible to send a drone to intercept the target and exploit the vulnerability before the ship has a chance to download and apply the patch. This is possible, as the US Navy successfully launched and returned an unmanned under water drone in an undersea mission in 2015 (Martin, 2015). Such a drone could be adopted to deploy exploits or install malware into slow moving, vulnerable, maritime vessels.

D. Cost and Profit

Profit-driven malware are becoming easier and cheaper to manufacture. Tools for malware development and exploit kits are common tools for attackers, so that even inexperience hackers can cause significant damage (Cannell, 2013). Furthermore, the hardware needed to hack maritime systems is often relatively cheap, as the systems they are attacking are often outdated and less sophisticated than other targets. Furthermore, there are many incentives for attacking maritime vessels, as over 90% of world trade occurs via the ocean (United Nations, 2015).

In addition, these large shipments of valuable goods spend long periods of time travelling without top protection and sometimes without human supervision. The cost/benefit to cyber maritime attacks is therefore high and may provide the time needed to remove evidence of the crime. Such attacks are also profitable, as mentioned previously, for smuggling purposes and fraud. As some ships or systems may be at more risk than others, depending on the possible attacks and the value of the vessel and its cargo, it is important to be able to manage risks and to understand what mitigation techniques are suitable to specific scenarios.

Scenario: As seen in the example with the malware-riddled oil-rig, even if an inexperienced hacker attempted to use a kit for an attack and it failed, it is still possible that the systems onboard have been disturbed enough to trigger an accident or shutdown. This could result in the loss of lives, infrastructure, money, and reputation.

5. Mitigation

An essential step to mitigating cyber-attacks on maritime vessels is to begin updating existing ship systems and, more importantly, begin designing ships for increased security. This does not necessarily require fancier, more expensive equipment, but can be achieved with intelligent isolation of different systems and more secure, but still usable, passwords etc. to safeguard these systems. Compromised systems must also be designed to recover quickly and effectively so that the vessel is not left drifting and/or vulnerable. Furthermore, modifying systems to allow valid functions and prevent or flag dangerous options could detect attempted exploits and other cyber-attacks. Resilience of command and control systems is also very important. The US Navy is already developing Resilient Hull, Mechanical, and Electrical Security (RHIMES), which aims to introduce diversity and prevent the same exploit succeeding on multiple controllers (Freeman 2015) However, as these systems are currently limited, and shall be limited until the next generation of ships, it is prudent to take advantage of the human element aboard such ships.

A human crew may be advantageous in many ways in terms of security. Firstly, they may be able to verify that the systems function as intended. Secondly, if systems are modified to query the crew during potential cyber-attacks it is more difficult for an attacker to go undetected. Training on how to keep these systems secure is also important. The use and protection of passwords and access keys, the proper use of the system, what an attack looks like, and how to disable, restart, or suspend certain systems is also useful for keeping the vessel safe.

6. Summary and Conclusions

In general, most maritime vessels are run by outdated software using hardware that was not designed with cyber security in mind. This is the result of the timescale and cost of producing large ships, but results in largely vulnerable systems. Both security firms and hackers have found both general flaws and specific, real-world, flaws within the systems running in the maritime industry. Specifically, several successful cyber-attacks have been launched on the navigation systems of ships. However, as these systems were not designed to be securely isolated, it seems plausible that similarly outdated systems for propulsion and cargo handling may also be compromised and abused by cyber-attackers.

In this article, we discussed several methods an attacker may use to gain access to a maritime vessel (e.g., unprotected network connection, insecure software, hacking kits smuggled aboard) as well as what attacks can be deployed on a ship. We discussed smuggling and theft, as well as hijacking a ship in order to hold it ransom or guide it to collide with another target. As mentioned, there are easy mitigations to help prevent some maritime cyber-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 cyber-attacks. There are fundamental issues with securing the technology used in the maritime industry at this point. This will, of course, become more of a problem if emerging autonomous vessels are not designed with security in mind from the beginning.

Existing cyber expertise from other domains, specifically Industrial Control Systems and other transport sectors, are relevant to the maritime domain and should be applied to mitigate immediate security issues. The sector is probably the most vulnerable aspect of critical national infrastructure and, 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.

References

Balduzzi, M., Wihoit, K., & Pasta, A. (2013). Hey Captain, Where's Your Ship? Attacking Vessel Tracking Systems for Fun and Profit. *Hack in the Box (HITB) Security Conference in Asia.*

Bateman, T. (2014). *Police warning after drug traffickers' cyber-attack*. Retrieved from BBC: http://www.bbc.co.uk/news/world-europe-24539417

Cannell, J. (2013, February). *Tools of the Trade*. Retrieved from Malwarebytes: https://blog.malwarebytes.org/intelligence/2013/02/tools-of-the-trade-exploit-kits/

Dyryavyy, Y. (2015). *Preparing for Cyber Battleships – Electronic Chart Display and Information System Security*. Retrieved from nccgroup: https://www.nccgroup.trust/uk/our-research/preparing-for-cyber-battleships-electronic-chart-display-and-information-system-security/

Freeman, B. (2015, September). *A New Defense for Navy Ships: Protection from Cyber Attacks*. Retrieved from navy.mil: http://www.navy.mil/submit/display.asp?story_id=91131

Gallagher, S. (2015, June). *ArsTechnica*. Retrieved from Navy re-ups with Microsoft for more Windows XP support: {http://arstechnica.co.uk/information-technology/2015/06/navy-re-ups-with-microsoft-for-more-windows-xp-support/

GPS World staff. (2015). *Inexpensive Hack Spoofs GPS in Smartphones, Drones*. Retrieved from gpsworld: http://gpsworld.com/inexpensive-hack-spoofs-gps-in-smartphones-drones/

Martin, A. (2015, July). *TheRegister*. Retrieved from Rise of the swimming machines: US sub launches and recovers a drone: http://www.theregister.co.uk/2015/07/21/us_submarine_launches_and_returns_underwater_drone/

McAfee. (2015, May). Threat Report.

Network World. (2015, May). *Maritime cybersecurity firm: 37% of Microsoft servers on ships vulnerable to hacking*. Retrieved from http://www.networkworld.com/article/2917856/microsoft-subnet/maritime-cybersecurity-firm-37-of-microsoft-servers-not-patched-vulnerable-to-hacking.html

Ott, C. (2014). *Fraud in the Maritime Industry.* Retrieved from Skuld: http://www.skuld.com/documents/topics/cargo/fraud/fraud.pdf?epslanguage=en

Royal Academy of Engineering. (2011). *Global Navigation Space Systems: reliance and vulnerabilities.* London: ISBN 1-903496-62-4.

Shauk, Z. (2013, April). *Malware offshore: Danger lurks where the chips fail*. Retrieved from FuelFix: http://fuelfix.com/blog/2013/04/29/malware-offshore-danger-lurks-where-the-chips-fail/

United Nations. (2015). Review of Maritime Transport. *United Nations Conference on Trade And Development (UNCTAD).* New York and Geneva.

University of Texas at Austin. (2013). *UT Austin Researchers Spoof Superyacht at Sea*. Retrieved from utexas: http://www.engr.utexas.edu/features/superyacht-gps-spoofing

Vidal, J. (2010, July). *TheGuardian*. Retrieved from Modern cargo ships slow to the speed of the sailing clippers: http://www.theguardian.com/environment/2010/jul/25/slow-ships-cut-greenhouse-emissions