Cyber Secuirty New threat for Maritime Industry in Bangladesh

Tawhidur Rahman, MCiiSM

C|CISO, CFIP, CCTA,CHFI, Lead Auditor, CCIP, CCII, Team Leader, BGD e-Gov CIRT

The shipping sector is growing digitally. Shipping companies need to understand the risk this causes in light of hacking and cyber-attacks. With cyber security attacks an increasing threat to technology used not just in shore-based organizations, but also on-board modern ships, the IMO issued guidelines relating to cyber risk management in June 2017. Ship owners and managers must incorporate these guidelines into their safety management systems by 1 January 2021.

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).

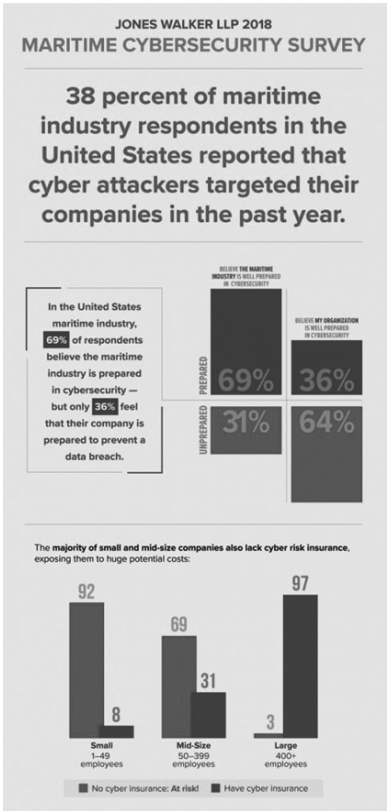
Modern Maritime Cyber Threats

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.

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.

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).

Taxonomy of Maritime Cyber Threat

With an understanding of modern maritime vessels, their systems, and what vulnerabilities they may possess, here we ▸

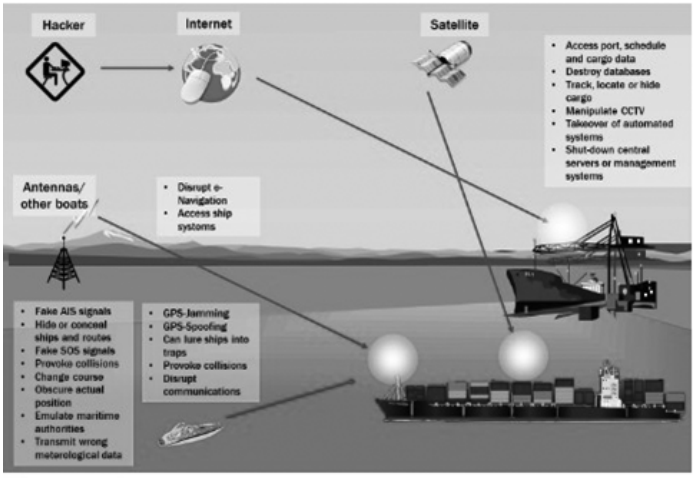
present a taxonomy on maritime cyber threats. While some of these have been implemented in the past, others are likely nefarious activities based on the current technology available to both maritime vessels and attackers.

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



Potential threats against vessels and ports by cyber attacks[3]

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.

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.

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.

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).

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.

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.

International Ship and Port Facility Security (ISPS) should be expanded beyond safety and physical security aspects. Revisions to national and international legal regulatory frameworks necessary to adapt to cyber-related maritime threats. Clarification of responsibilities and tasks between governmental and private key stake-holders in maritime security