Maritime Cyber Security for Navigation and Control Systems

Ileana Driva
MSc Cyber Security, University of Southampton
20 Duke Street, Southampton, UK
SO14 3ET
id3g15@soton.ac.uk

ABSTRACT

Since shipboard systems have become Internet connected, they enable new technological advances like electronic navigation, digital onboard communications and real-time monitor and control of the ship's performance. However, these systems can be targeted for cyber attacks that can affect any online ICT (Information and Communications Technology) asset. This work was conducted to search the different aspects of cyber security in the maritime sector and propose a generic framework to address cyber security for ship systems in the future.

Keywords

maritime; cyber security; onboard navigation systems; cyber ship attacks

1. INTRODUCTION

Nowadays, due to the fact that ships are connected to the Internet, it is important to investigate if the systems that ships are equipped with are vulnerable to already known cyber threats. That is because a successful cyber attack on a ship is able to cause numerous devastating effects. For instance, if a sophisticated cyber criminal manipulates the online navigation system of a ship the consequences would be disastrous, both for the crew and the environment. In addition, NCC Group [1] detected software vulnerabilities related to the most widely used product for navigation on ships, the Electronic Chart Display and Information System (ECDIS). Thus, ECDIS was found to be vulnerable to web application exploits and so a skilled attacker can take advantage of ship's electronic infrastructure.

Therefore, it is crucial to demonstrate the different approaches concerning cyber security of modern vessels and outline the importance of establishing a framework for reducing cyber security risks related to the shipboard systems and networks.

2. METHODOLOGY

2.1. Categorisation

A categorisation of the recent research studies that have examined maritime cyber incidents, from the view of the maritime organisations, was necessary in order to analyse the different solutions that have been proposed before recommending further actions. The first category includes generic practices, measures and legislations for maritime cybersecurity. The second category covers reviews that followed risk analysis techniques to respond to potential cyber incidents. Finally, the last category involves technical approaches against security vulnerabilities that an adversary could possibly exploit.

Besides these reports, on the subject of cyber security in general, it seemed useful to mention other papers that illustrate the dangers of cyberspace today. With the reality of the high-tech crimes in mind, it would be with fewer difficulties to correlate contiguous crimes compatible to the electronic devices situated on a ship.

2.2. ENISA, IMO

The first report that indicates the ICT risks within the maritime domain was published by the European Network and Information Security Agency (ENISA) [2]. ENISA raised awareness by emphasising the problems of the maritime regulations that have been developed since 2011 and why these security principles have to be modified to improve cyber security. A list of illustrative examples could be perceived as the first step to model a regulatory framework that could guard against various cyber threats and focus on implementing secure systems. A list of illustrative examples could be perceived as the first step to model a regulatory framework that could guard against various cyber threats and focus on implementing secure systems.

In 2014, the International Maritime Organisation (IMO) [3] in the direction of ensuring that ships use secure cyber systems, proposed regulations to plenty of serious issues. In order to address cyber security, a broad guidance was provided on how to manage cyber threats that happen in all kind of marine facilities, together with some corresponding guidelines. In the same report, based on the Canada's Maritime Cyber Security Project released by IMO, a better development of resilient systems would be appropriately achieved if maritime cyber security is divided into five more specific categories: access control, network design, intrusion detection, communication security and governance.

A year after, in response to this submission, ICS, BIMCO, INTERTANKO and INTERCARGO [4] presented guidelines again to enhance maritime cyber security, but this time from the perspective of the maritime industry. Risk scenarios of cyber threats were in detail explained and supplementary guidelines were acquainted from the point of view of the education of the crew to the development of contingency plans and safe practices.

2.3. BIMCO

Baltic and International Maritime Council (BIMCO) [5], likewise IMO, proposed a set of standards and guidelines to be adopted due to safety and security onboard. Furthermore, Security Development Lifecycle (SDL) process was adopted in this approach to introduce general advice of assessing risks faced by the global shipping industry. Cyber incident management procedures consist of a lot of steps that need to be performed to reduce cyber security risks. Such a framework, with technical and management activities for organisations, was published by National Institute of Standards and Technology (NIST) [6] and BIMCO extended it accordingly to be adjust it in the maritime world. Consequently, every organisation that tries to assure the confidentiality, integrity and availability (CIA) model for their systems and data should be prepared and organised in case of the occurrence of any emergency cyber security event.

2.4. NCC

NCC Group [1] detected four software vulnerabilities related the information technology product ECDIS, equipment which is helpful for navigation. ECDIS is connected to shipboard LAN (Local Area Network), which successively is connected to the Internet for online updating the electronic navigational charts (ENC). Thus, ECDIS was found to be vulnerable to web application exploits that allow an unauthorised person to gain access to directories where critical files were stored. The performed actions that were permitted on the ship's web server were mostly HTTP (HyperText Transfer Protocol) exploits which were caused by improper input validation. However, bypassing the access control of the system is not the only result of attacks that are related to dangerous HTTP methods. Untrusted inputs could also lead to the modification of ECDIS chart files and sometimes this means injecting to them a malicious code of the attacker's choice.

The outcomes of this research were clear evidence that the installation of secure patches is vital when trying to achieve safe navigation with the help of the new advanced computer technology. So, despite the fact that ECDIS has advantages when it comes to the navigation, it has also an increasing attack surface because of the fact that allows connectivity to the shipboard network.

2.5. STUXNET

Attacks that aim at the critical infrastructure systems have been reported many times in the past. The most widely known software designed attack of the 21st century is Stuxnet [7]. Back in 2010, Stuxnet, this famous "computer worm" was designed to target Iranian nuclear centrifuges and completely control them by the people who built it and then successfully launched it. The maritime domain could be catastrophically affected from software designed attacks like Stuxnet, as ICSs (Industrial Control Systems) and mainly OT (Operational Technology) environments have been targeted by this kind of malware before. In the same way, the design of a Stuxnet-like malware could be adapted to run on the computer-based control systems such as SCADA (Supervisory Control And Data Acquisition), which is connected to the shipboard LAN and/or WAN (Wide Area Network) and is a crucial system as it enables remote monitoring and control to a lot of other operations. Remotely access to control functions of the OT systems is a cyber security risk that needs to be mitigated because otherwise the utility systems that hold real-time data of the ships can be controlled for profit by prospective attackers. In addition, the unexpected action of maliciously disabling critical systems will also destroy all the safety features which have been applied for ship's infrastructure security.

Although reports about similar incidents on ships have not yet been published, maritime cyber attacks are distinctly possible to occur in the very near future, in a similar way as they are a threat to every physical infrastructure asset no matter if it is a nuclear centrifuge, an oil rig, an aircraft or a vessel.

3. RESULTS

IMO and BIMCO similarly proposed a list of theoretical guidelines regarding the scheme that ENISA had pointed out some years earlier, whereas NCC Group produced a technical presentation on a very specific software product for ship navigation, ECDIS.

When comparing the above reports, the only approach that provided valid facts that actual risks exist on the maritime systems is the one by NCC Group. The other reports signified the importance of creating policies and standards according to the cyber risks that may arise these days.

As a result, to develop an efficient cyber security strategy, firstly it is major to identify the present threats that highly synchronous vessels have to confront, such as the web application security vulnerabilities pointed out by NCC Group. The next step is to consolidate the appropriate security policies to deal with these risks and latter cyber incidents that may emerge. BIMCO risk-based approach could be beneficial to strengthen the right security policies from the list that IMO have already made available.

Moreover, a comparison is that ECDIS is a tool for navigation purposes that could be examined further for vulnerabilities that rely on the network of a ship, while control systems, like SCADA, are part of the critical infrastructure system of the ship and its connections. Maritime network systems (as a section of the general category of the navigation systems) and control systems are both remarkably significant for the right functionality of a ship. Nevertheless, these systems transform each ship to be, up to a certain extent, part of a more complex system that is connected with other systems through the World Wide Web. The distinction between them is fatal when planning defence mechanisms for software security analogous to the type of the probable threats. To illustrate this, a cyber attack on ECDIS can cause access to unauthorised data if secure network protocols have not been installed, while an attack that focuses on an electro-mechanical control system for the main engine of the ship can remotely monitor or change its sea route.

4. DISCUSSION

It has been noticed that guidelines by IMO and SDL process by BIMCO are voluntarily followed by the maritime community on the whole. This is because, until now, there are no obligatory universal legislations, but only regulations that can be adjustable by each maritime company according to their perspective of security. Similarly, this means that these regulations can easily be modified to be more usable for the members of the crew regardless the security implications. Therefore, even if the best protection mechanisms exist, unless somebody with the relevant knowledge applies them in real case scenarios they are not going to be effective. It the same way, compliance with a regulation framework is necessary not only to embed into a universal cyber security culture but because otherwise, shipboard systems are not completely safe against cyber attacks. Even if it is difficult and time-consuming, following specific standards is extremely important and should be taken seriously by the maritime industry. It has to be unambiguous that cyber threats to ships are definitely real, but feasible measures, if are implemented correctly and on time, would undeniably protect the maritime systems and networks in an effective way.

At the same time, all technology segments need to be tested to ensure that current shipboard computer systems are up-to-date and secure against the later cyber crimes. Even if cyber security assessments have been installed some time before, that does not imply that continuous evaluation of the security levels of all components is inessential.

Then, the next step is the installation of practical measures to minimise cyber threats taking place onboard. The non-technical regulations could definitely serve as helpful paths for formulating applicable cyber security protection principles. For instance, if a malware terminates ECDIS activities, a cyber security protection principle should guarantee ship's safe navigation. This may demand also some procedures of the systems to shift from automated to manual mode without impact the performance (e.g to ascertain ship's position). In other words, human-machine interactions should be to a perfect balance to correspond to the interconnected systems and to the systems connected to the rest of the world via the Internet. The result should be a stable implementation of a generic cyber security framework that would enhance the proposed approaches that have been recommended so far.

Likewise IMO, regulations that are included in the International Safety Management (ISM) Code [8] and the International Ship and Port Facility Security (ISPS) Code [9] cover physical threats rather that cyber. Undoubtedly, these guidelines are essential for the building of cyber security tactics and should be complementary to the applied security procedures.

5. CURRENT & FUTURE WORK

Following the above analysis, proposing a framework to address cyber security for the shipboard online computer systems seems urgent. Before that, the main related objectives are to examine the modern architecture of the shipboard online computer systems and investigate any vulnerabilities that can be found in these systems.

The research of this project has been divided into two separate research topics, one for the maritime networks and the other for the maritime control systems (electromechanical control systems). During the maritime networks research, it is important to examine the network system architecture and investigate if any of these networks are vulnerable to already known cyber threats. At the same time, the research on the maritime control systems, such as the Integrated Bridge System (IBS), will provide an examination of the operation of the onboard computer control/data systems. The results can be analysed by conducting a threat analysis and then a risk assessment process for the network vulnerabilities. Additionally, carefully illustrating possible unpleasant future scenarios for the ship critical infrastructure systems can determine suitable information on how to avoid cyber attacks. The last phase will be an overall proposal of some cyber security measures to mitigate the risks and protect the infrastructure assets. This proposal could also fit into a more generic framework that introduces cyber security on ships and could be regarded as an extension of the SSP (Ship Security Plan) accompanied by the Ship Security Assessment (SSA) of a ship.

Finally, this framework aims to be regarded as a manual for all ships. As a consequence, because for ship companies is absolutely fundamental to comply with the common regulations, standards and rules recommended by IMO and international shipping organisations mentioned above, this framework can be used as a guide to implementing them to correspond with the realistic cyber challenges.

6. CONCLUSION

Although cyber attacks in most cases are difficult to predict, a contingency plan for the shipboard network infrastructure is a necessity, especially towards present-day cyberspace. Although it is a challenge trying to secure the cyberspace, as cyber crimes are the kind of unfortunate events that could happen in many different forms in many different ways, it is mandatory to ensure the cyber security of ship's critical infrastructures.

The purpose of this work is to search the different aspects of maritime cyber security and propose a framework to help to address cyber security vulnerabilities in two different ship systems, network and control systems. This framework would be conducted after taking into consideration the guidelines and the standards that already exist. The framework would finally introduce some practical advice, as technical security measures that could mitigate the present cyber risks that target ship systems and protect these systems as much as possible.

7. REFERENCES

1. NCC Group, Preparing for Cyber Battleships – Electronic Chart Display and Information System Security, 2014.
2. ENISA, Analysis of Cyber Security Aspects in the Maritime Sector, 2011
3. IMO, ENSURING SECURITY IN AND FACILITATING INTERNATIONAL TRADE - Measures toward enhancing maritime cybersecurity. Submitted by Canada, 2014.
4. IMO, MEASURES TO ENHANCE MARITIME SECURITY - Industry guidelines on cyber security on board ships. Submitted by ICS, BIMCO, INTERTANKO and INTERCARGO, 2015.
5. BIMCO, The Guidelines on Cyber Security onboard Ship, Denmark, Version 1.0, January 2016.
6. National Institute of Standards and Technology (NIST), "Framework for Improving Critical Infrastructure Cybersecurity," Version 1.0, February 2014.
7. Falliere, N., Murchu, L. O., and Chien, E. (2011). W32. stuxnet dossier. *White paper, Symantec Corp., Security Response,* 5.
8. IMO, INTERNATIONAL SAFETY MANAGEMENT CODE with guidelines for its implementation, 2014 Edition
9. IMO, International Ship and Port Facility Security (ISPS) Code and SOLAS amendments, 2003 Edition