Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.3, Jun. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.3.657

위협 모델링을 이용한 선박 사이버보안 요구사항 연구

조 용 현,† 차 영 균‡
고려대학교 정보보호대학원

A Study on Cyber Security Requirements of Ship Using Threat Modeling

Yong-Hyun Jo,† Young-Kyun Cha‡
Graduate School of Information Security, Korea University

요 약

최근 운항되고 있는 선박은 전자해도시스템 및 자동위치식별장치 등 다양한 IT, OT 시스템이 사용되고 있어 선박 건조와 항해 환경까지 고려한 보안 요소가 요구된다. 하지만, 선박과 조선 ICT 기자재 산업에 관한 사이버보안 연구는 아직 부족한 현실이며, 위협 모델링을 통한 체계적인 방법론이 부족하다. 본 논문에서는 선박 시스템에 접근하는 이해관계자를 고려하여 Data Flow Diagram을 수립하였다. 선박 시스템들의 보안 취약점과 사례들을 수집한 Attack Library를 기반으로 STRIDE 방법론과 Attack Tree를 활용한 위협 모델링을 통해 선박에서 발생 가능한 위협을 식별하고 선박 사이버보안 대책을 제시하고자 한다.

ABSTRACT

As various IT and OT systems such as Electronic Chart Display and Information System and Automatic Identification System are used for ships, security elements that take into account even the ship's construction and navigation environment are required. However, cyber security research on the ship and shipbuilding ICT equipment industries is still lacking, and there is a lack of systematic methodologies through threat modeling. In this paper, the Data Flow Diagram was established in consideration of stakeholders approaching the ship system. Based on the Attack Library, which collects the security vulnerabilities and cases of ship systems, STRIDE methodologies and threat modeling using the Attack Tree are designed to identify possible threats from ships and to present ship cyber security measures.

Keywords: Threat-Modeling;MASS;Maritime Cyber Security;Ship Cyber Security;Threat Analysis

I. 서 론

지구의 70%를 차지하고 있는 바다를 통한 해양산업은 국가간 교역의 90% 이상을 차지하고 있는 국가의 기간산업이다. 4차 산업 혁명으로 인해 조선·해양 산업에서는 해운은 Shipping 4.0, 항만은 Port 4.0, 조선은 Smart ship 4.0, 해양은 Marine 4.0으로 추진되고 있다[1]. 조선·해양 산업과 ICT 기술을 융합하여 스마트십, 디지털십을 건조했으며 향후 자율운항 선박을 건조할 계획을 추진 중이다. 자율운항 선박은 무인선박, 스마트 쉽, 리모트 컨트롤 선박 및 디지털 선박 등 다양한 명칭이 혼재되어 사용되었으나, 2018년 6월에 개최된 IMO 해사안전위원회(MSC)에서 MASS(Maritime Autonomous Surface Ship)로 정의하였다. 한국해양수산개발원은 자율운항 선박 도입에 따라서 유엔해양법에 따른 관할권 문제, 해상에서의 충돌방지를 위한 규정의 도출, 미래 선원의 문제, 환경보호, 선박의 건조요건 및 기술조건, 책임과 보상 및 보험 이슈, 사이버보안 및 테러에 대한 문제가 있어 대응책이 필

Received(04. 16. 2019), Modified(05. 30. 2019), Accepted(06. 03. 2019)
† 주저자, yhjo13@korea.ac.kr
‡ 교신저자, ykcha@korea.ac.kr(Corresponding author)

요하다고 설명하고 있다. 이처럼 조선·해양 산업에 4차산업 혁명에 따른 패러다임 변화가 일어나고 있으며 선박에 정보통신 기술이 적용되어 운영 중인 각종 항해 장치들이 디지털화되거나 선박과 선박, 선박과 항만, 선박 내 장치와 장치들이 통신망으로 연결되는 연결성이 가속화되고 있다. 이와 같은 변화에 따라 조선·해양 산업의 사이버보안 위협이 증가하고 있으므로 본 연구에서는 조선·해양과 ICT의 융합기술이 접목되고 있는 선박의 위협 모델링을 통해 선박의 사이버보안 요구사항을 도출하고자 한다.

II. 전통적인 선박 보안

해양산업에서는 선박 및 화물의 피랍을 위협요인으로 보아왔으나 최근에는 연안국들의 해적대응 활동 강화로 인해 선원들만 납치 후 도주하여 석방금을 요구하는 형태로 전환되었다. Paul Barnes & Richard Oloruntoba[2]는 해양 보안 위협으로 화물, 선박, 사람이 상호 작용을 하며, VTS(Vessel Traffic Service)와 같은 정보통신 시스템의 증가와 복잡화, 항만에 관계된 많은 공공 및 민간기관의 조정이 어려워 효과적인 보안 프로그램을 수립할 수 없다고 설명하였다. 또한, 주요 위협으로는 화물(Cargo)을 사용하여 밀항하거나 무기를 밀수입하는 형태, 선박(Ship)을 무기 또는 공격 수단으로 사용(침몰, 충돌 등) 하는 형태, 사람(People)을 이용하여 테러 활동을 지원하기 위해 선박에 승선하는 선원 신원정보를 도용하는 형태로 설명하였다.

OECD Maritime Transport Committee[3]은 해양 보안의 범위를 원산지에서 생산자가 세관을 통해 항만에 화물을 전달하고 선박에 화물을 선적하여 도착지의 항만에 하역하여 세관검사를 통과하고 구매자에게 전달되는 일련의 과정으로 설명하였다. 또한, 이 범위에서는 선박 및 항만은 국제해사기구(IMO)의 ISPS(International Ship and Port facility Security Code)에 의한 규정을 적용 받고 원산지 세관부터 도착지 항만까지는 미국 컨테이너 보안 협정(CSI, Container Security Initiative)를 적용받고, 전 범위에서는 9.11 사건 이후 미국의 국가 안보 시스템을 강화하는 목적으로 기획되어 2001년 11월부터 시행된 C-TPAT(Customs Trade Partnership Against Terrorism)를 적용받는다고 설명하였다.

III. 관련 연구

본 장에서는 선박과 선박 사이버보안 관련 표준화 및 관련 규정 제정 현황을 조사하고 선박 취약점과 관련된 연구들을 정리한다. 해양 산업에서의 사이버 피해사례가 2010년부터 발생하여 왔고 이에 따라 선체 내에 사용되는 네트워크 보안 표준 규격이 제정되었고 2016년부터 국제해사기구(IMO) 등에서 사이버보안 가이드라인을 제정하고 2018년부터는 선박 검사항목에 추가되는 등 사이버보안에 관한 요구사항이 증가되고 있다. 알리안츠의 기업 및 특수보험 전문 자회사인 AGCS(Allianz Global Corporate & Specialty)는 전 세계적으로 NotPetya와 같은 악성코드 감염과 같은 사이버 사고가 증가함에 따라 해운 회사들이 사이버 위협을 중대한 리스크로 판단하고 있고, 이전에는 선박이 고립된 환경이었으나 ICT 기술이 적용되면서 위험이 증가했다고 설명하여 해양 보험 산업에서 사이버보험의 인식 중요성을 언급하였다[4].

3.1 사이버보안 위협 분석 연구

종래의 해양 사이버보안 위협에 대한 분석은 금융, IT 등 다른 산업보다는 많지 않다. 그 이유는 선박은 내연기관 및 항해 관련 시스템이 아날로그 방식으로 건조, 운영되다 2000년도에 접어들어 ICT와 융합되기 시작했다. University of Plymouth의 Prof. Kevin D Jones & Dr. Kimberly Tams[5],[6]는 자율운항 선박의 사이버 리스크 평가 방법을 제시하였는데 리스크는 선종과 선체 크기, 위치에 따라 다르므로 이를 Dynamic Risk Profile로 설명하며 자율운항 선박 사이버보안 평가 방법론으로 MaCRA(Maritime Cyber-Risk Assessment Models the three axis)를 제안하였다. 이 방법은 선박의 자율운항 수준, 공격자 보상, 공격 용이성을 5단계로 구분하였다.

3.2 위협 모델링에 관한 연구

위협 모델링은 보안 요구사항을 분석하고 대책을 정의하기 위해 시스템 또는 서비스에서 가능한 모든 위협을 식별하는 것을 의미한다.

Adam Shostack는 Microsoft가 1999년부터 위협 모델링에 대한 문서화를 하였는데 제품 설계와

보안 결함을 찾는데 효과적이라고 하였다[6]. 또한, 위협 모델링을 위해 DFD(Data Flow Diagram)을 가시화하고 Attack list를 STRIDE 방법에 따라 분류하는 것을 기반으로 잠재적 위협을 식별하는 위협 모델링 도구를 개발 하였다[7].

Zhendong Ma 외 1인은 STRIDE를 사용하여 자동차의 취약점을 분석하고 다양한 위협 가능성을 제시하였다[8].

Rafiullah Khan 외 2인은 CPS(Cyber Physical Systems)의 보안 위협을 분석하였는데 다양한 보안 모델링 방법들 중에 STPA-sec는 시스템 안전에 적합하고, HAZOP는 시스템 가용성에 적합하고, SAHARA는 위험 및 보안에 적합하고, PASTA는 공격 시뮬레이션에 적합하다고 하였다. STRIDE는 잠재적 위협 식별이 가능하고, 체계적 접근과 분석이 가능하고, 기술에 기반한 시스템 구성 요소 분석이 가능하여 STRIDE를 이용한 CPS 보안 위협 가능성을 제시하였다[9].

Stijn van Winsen은 미래의 자율주행 자동차의 위협 모델링을 위해 ISO 26262에 포함된 TARA(e Threat Analysis and Risk Assessment)와 SAHARA(The Security-Aware Hazard and Risk Analysis), (SINA)Security in Networked Automotive 방법론에 대해 비교하였다. 그리고 가장 일반적으로 알려진 STRIDE를 사용하여 향후 만들어질 자동차의 위협을 제시하였다[10].

3.3 선박 사이버보안 표준화 작업 동향

조선·해양 분야의 규정(Reguations) 및 표준화(Standard)는 국제해사기구(IMO)를 중심으로 국제통신연합(ITU), 국제수로기구(IHO), 국제전기기술위원회(IEC), 국제표준화기구(ISO)를 중심으로 산업계 표준은 미국해상장비기술위원회(RTCM), 미국선박전자협화(NMEA), 국제항로표지협회(IALA)에서 제정하고 있다. 이 중 선박 네트워크 표준은 2000년 초반 IEC 61162-4 시리즈를 통해 표준화되었고, 보안을 강화한 IEC 61162-460까지 발전하여왔다. 그러나, 아직까지 운항 중인 많은 선박들은 건조 시점에 따라 1983년에 제정된 IEC 61162-3(NMEA-2000) 시리즈에 따라 표준화된 항법장치, 선박 전자장치를 사용하고 있다.

3.3.1 IEC 61162-4 시리즈

2015년에 한국전자통신연구원(ETRI)는 선박에 다양한 사이버보안 위협이 증가함에 따라 선박의 장비와 시스템들을 보호하는 방안을 국제표준으로 제안하여 해양 분야 사이버보안 국제표준으로 채택되었다. 이는 선박 장치, 선박 네트워크, 선박 게이트웨이의 보안 구조와 기능 요구사항을 정의한 국제표준으로 2001년 IEC 61162-4 시리즈가 발표되었고 2011년에 IEC 61162-450이 공표되었다[11].

통합 항해 시스템을 구성하기 위한 안전하고 안정적인 운용을 위한 표준으로 IEC 61162-460(네트워크 안정성 및 보안 표준) 제정되었다.

이광일[12]은 최근에 선박에 VDR(Voyage Data Recorder)와 CAM(Central Alarm Management) 같은 전자장치들의 도입됨에 따라 양방향 통신과 대용량의 선박 네트워크가 필요하게 되었고, 이들 이더넷 기반의 표준화된 인터페이스가 필요하게 되어 제정된 것이 IEC 61162-450으로 LWE(Light-Weight Ethernet)이며, 보안성을 강화하기 위해 IEC 61162-460이 규정되었으며 ETRI에서 2012년에 제안하여 국제표준 초안으로 채택되었다고 설명하였다.

3.3.2 IEC 61162-3 시리즈

Dong-Keun Jeon and Yeonwoo Lee는 선박의 구간별 네트워크 프로토콜 구조를 Ethernet 환경 외에 선박에 탑재되는 통합 항법 시스템은 주로 레이더, GPS 수신기, 자동 항법 시스템(IS) 등 항법 장비 간 양방향 통신은 CAN(Controller Area Network)을 기반으로 IEC 61162-3에서 표준화한 NMEA(National Marine Electronics Association) 2000을 사용하며, 이 표준은 선박의 전자장비들이 상호 인터페이스의 증가로 1983년에 The National Marine Electronics Association에 의해 제정되어 사용 중인 표준인 NMEA 0183 프로토콜이 증가하는 데이터와 물리적인 케이블의 복잡성 등의 문제해결의 한계를 개선하기 위해 제정하였다고 설명하였다[13]. 김창영, 이임건[14]은 전송속도가 4,800bps인 기존의 NMEA 0183에 비해 NMEA 2000은 250kbps를 유지하기 때문에 높은 전송속도를 보장하며 양방향 다중 송수신이 가능하므로 데이터 충돌을 회피할 수

있다. 또한, 정상적으로 동작하는 네트워크에 연결된 한 장비가 고장이 나도 전체 네트워크가 멈추지 않는 특징 때문에 많은 선박 기자재 분야에서 NMEA 2000을 채택하고 이를 이용한 제품이 상용화되고 있다고 설명하였다. 그러나, IEC 61162-3은 50개의 물리적인 장치라는 제한사항을 가지고 있으며, 대형 선박과 같은 복잡한 통합 네트워크를 구성하는 데에는 한계가 있다.

3.3.3 자율운항 선박(MASS)의 사이버보안

2017년 국제해사기구(IMO)의 해사안전위원회(MSC) 제98차 회의에서 자율운항선박을 MASS(Maritime Autonomous Surface Ship)으로 규정하였고, 우리나라 해양수산부에서는 자율운항선박을 통한 경제적 효과가 2025년 약 1,550억달러(한화 약 170조)로 추정하고 있다. 해양수산과학기술진흥원의 자율운항 선박 기술 영향 평가 결과 보고서에 따르면 자율운항 선박이 해킹되어 선박 납치와 화물 탈취와 같은 위험이 예상되고, 악의적인 운항 정보가 입력되어 선박 충돌과 같은 문제를 유발하여 무기화될 수 있는 위협을 제기하였다[15].

3.4 해양 분야 사이버보안 정책 동향

3.4.1 IMO(International Maritime Organization)

해운과 조선에 관한 국제적인 문제들을 다루기 위해 설립된 국제기구인 IMO에서는 선박간, 육·해상간 전자·통신장비 장착 및 가동이 확산되면 육상에서와 마찬가지로 해킹, 정보유출, 사이버테러 등 심각한 해상안전 문제가 발생할 것으로 경고하였다. 이에 산하 조직인 MSC(Maritime Safety Committee) 94차에서 미국, 캐나다는 항만, 선박 해사시설물 및 해운물류 시스템의 다양한 해사 분야에 사이버보안을 강화할 것을 제안하였고 MSC 95차에서 미국, 캐나다 등은 선박 외의 항만, 해사시설물, 장비의 사이버보안 관련 통합지침 개발이 시급함을 주장하였으나, MSC 96차에 제출한 안에는 MSC 95에서의 다른 국가들의 의견을 반영하여 우선 선박 사이버보안 지침안만 포함되었다. 이 지침에는 사이버 위험의 이해, 사이버 위험관리의 필요성과 목적, 위험관리 절차 파악, 선주와 운항자가 위험/보안 관리 시스템에 추가할 활동 목록 제안 등의 내용이 포함되었다.

MSC 98차 회의(2017년 6월 20일)를 통해 사이버보안에 대한 가이드라인을 규정하고 2021년 1월 1일부터 안전관리 시스템에 사이버보안 관리 분야(Maritime Cyber Risk Management)를 포함하는 것을 의무화하였고,이 지침은 업계의 모든 조직을 대상으로 적용된다. IMO cyber security risk management guideline에서는 선박의 취약한 시스템으로 선박 운항 및 화물관리, 승객 관리, 엔진 및 통신 시스템 등을 제시하고 있다. 이 가이드라인에서는 식별-보호-탐지-대응-복구 5단계의 기능으로 효율적인 risk 관리 프레임워크를 제시하고 있다. 이 프레임워크는 NIST의 cyber security framework이다. 최상의 risk 관리를 위해서는 BIMCO(발트해 국제해사기구협의회)의 지침, ISO/IEC 27001, NIST cyber security framework 등 모든 관련 지침 및 표준의 최신 버전을 참조하도록 권고하고 있다.

3.4.2 BIMCO

2016년 2월 1.1버전의 THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS에 이어 2017.6월에 2.0 버전을 발표하였다. 이 버전에는 사이버 침입사고에서 연속성 계획과 대응 및 복구 계획 챕터에서는 선박의 원격 환경을 고려하여 지침이 구체화 되었다. 이 가이드는 사이버 안전관리에 대한 필수 지침을 제공하는 것을 목적으로 하고 있다.

제1장에서는 사이버보안과 안전관리를 다루고 있으며 해양 사이버보안은 탑승한 인원(승객과 선원), 선박과 화물을 무단 접속과 조작/중단, 데이터의 유실로부터 보호한다고 정의하고 있다. 주요 우려 사항으로 선박의 전자분야 디스플레이 및 정보시스템(ECDIS)의 무결성 훼손, 선박용 소프트웨어의 유지관리 및 패치로 발생할 수 있는 장애, 선박의 중요한 센서의 손실 또는 조작으로 위성 네비게이션 시스템을 포함하고 있다.

제2장에서는 해양 사이버보안의 위협을 회사, 선박, 운영과 거래로 식별하고 있으며 금융기관, 공공기관 등 다른 산업에서의 경험이 성공적인 사이버 공격의 경감 사례가 될 수 있음을 제시하고 있다. 또한, 회사의 직원이 해상과 육상에 있을 때 각각 사이버 공격에 노출될 수 있음을 제기한다.

제3장에서는 선박에서 취약점에 노출될 수 있는 시스템을 식별하고 있는데 IMO에서 제시하고 있는 선박 시스템과 같다. 다만 선박과 육상(항만 또는 선박 운영회사, 해운 회사 등)과의 통신이 이뤄지는 시스템인 엔진 성능 모니터링 시스템, 선박 유지관리 시스템, 화물과 승선원 관리 시스템, 항해 관리 시스템 등 육상에서 선박의 운항을 점검하고 관리하기 위해 통신 하는 시스템을 추가로 식별하고 있다.

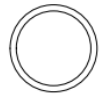
제4장에서는 위험평가에 관한 것으로 K-ISMS, ISO27001 등에서 제시하고 있는 위험평가 가이드 및 통제항목과 같게 위험평가의 책임은 고위 경영진에 있음을 명시하고 있다. 영향 평가를 위해서는 CIA Model을 통해 평가하나 해양산업과 선박의 환경을 고려하여야 한다. 예를 들면 민감한 정보에는 선박 위치, 시스템의 상태 및 판독 값, 화물의 세부사항, 권한, 인증서 등을 포함하도록 하고 있다. 선박의 전력관리 시스템은 SCADA 시스템을 포함하고 있고 선박 전체의 전력 분배와 제어를 담당한다. 이 시스템은 선박의 통신 시스템과 연결되어 육상의 회사에서 모니터링 하도록 구성되어 있다.

제5장에서는 보호 대책에 관한 것으로 위험 평가 결과 나타난 위험에 대해 고위 경영진의 책임으로 보호 대책을 이행하여야 한다. 보호 조치는 절차와 지침으로 구성하고 기술적인 수단과 관리적인 수단을 제시하고 있다. 특히, 보호 대책으로 선박이 위성 및 무선 통신을 이용할 때 위성통신 시스템과 사양을 고려하고, 운항 선박의 불법적인 접속을 방지하는 방법을 고려하여야 한다. 제어 소프트웨어와의 관리 인터페이스는 주로 웹 기반 사용자 인터페이스의 형태로 제공되는데 그러한 인터페이스의 보호는 선박에 설치될 때부터 고려해야 한다.

제6장에서는 업무 연속성 계획에 관한 것으로 선박의 경우 전자 항법 장비의 가용성 또는 탐색의 무결성 데이터 손실, 글로벌 항법 위성 시스템(GNSS)의 가용성 또는 무결성 손실, 해안과의 필수적인 통신의 손실, 세계 해상 조난 안전 시스템(GMDSS) 통신 두절, 선박의 추진 시스템, 보조 시스템 및 산업 제어 시스템을 포함한 산업 제어 시스템의 가용성 손실, 기타 데이터 관리와 제어 시스템의 무결성 손실, 랜섬웨어 또는 서비스 거부공격(DoS)에 대한 손실 등을 고려하여야 한다.

제7장에서는 사고대응 계획에 관한 것으로 그 예로 전자해도시스템(ECDIS)의 악성코드 감염시 원복하는 복구계획, 사고대응 계획, 조사 계획 등을 수립하여야 한다.

Table 1. DFD Symbol description

Symbol	Elements Name	Description
	External Interactor	Input to the system
	Process	Transforms or manipulates data
	Multiple Process	Transforms or manipulates data
	Data Storage	Location that stores temporary or permanent data
	Data Flow	Depicts data flow from data stores, processes or interactors
	Boundary	Machine, Physical, address space or trust boundary

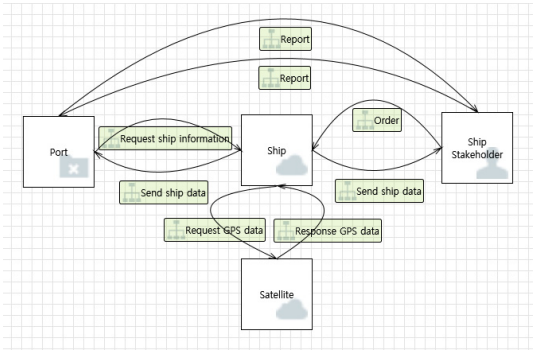


Fig. 1. DFD Context Diagram(Level 0)

3.4.3 OCIMF

국제 정유사 해운포럼(OCIMF)에서는 TMSA Tanker Management & Safe Assessment)에서 기존 TMSA2 효율화 작업의 목적으로 KPI(성과지표) 및 BP(모범사례)를 최신화하였으며, 최근 이슈화 되고 있는 사이버보안을 포함한 Element 13(Maritime Security) 항목을 추가하여 TMSA3를 발행하는 Tanker 선사를 대상으로 2018.1.1.일부터 Cyber Security 17개 항목을 점검하고 있다. SIRE(Ship Inspection Report

Program)에서 Tanker 선사를 대상으로 2018.9.17.일부터 Cyber Security 4개 항목을 점검하고 있다.

3.4.4 RIGHTSHIP 검사

RIGHTSHP에서는 기존 선박 점검표(FOD06(10))에 사이버보안을 포함한 추가 점검사항을 반영하여 RIGHTSHIP 점검표를 최신화(FOD06(11)/2017.05.11.) 하였고, 2017.5.11.부터 시행되었으며 RIGHTSHIP 대상 선박과 관리선사 기준에 따른 High Risk로 분류된 선박 등이 대상이 된다.

3.4.5 선급 검사

한국선급(KR, Korean Register)에서는 선박과 회사가 도입해 운영하는 IT 기술과 서비스에 대해 내외부의 사이버 위협으로부터 안전성을 강화하기 위해 해상 사이버보안 가이드라인을 제정하였다. 이 가이드라인에서는 선박 내부의 IT시스템 외에도 선박 기능과 관련된 OT 시스템도 사이버보안이 필요하며 선박의 OT 시스템은 추진, 발전 및 배전, 조타, 항해, 통신, 평형수, 앵커링, 화물 운영, 화재 및 가스, 점화원 제어, 거주 및 승객, 배수 및 빌지 펌프, 기타 시스템을 포함한다고 하였다. 이처럼 선박은 프로그램 가능 로직 제어기(PLC), 원격단말장치(RTU) 등 OT 시스템과 IT 시스템이 융합된 움직이는 산업제어시스템(ICS, Industrial Control System)임을 고려한 보안대책이 요구될 것이다.

해외 선급인 미국선급협회(ABS), 로이드선급협회(Lloyd's Register)에서도 선박 사이버보안 분야에 대한 선급 검사와 인증을 하고 있다.

IV. 선박 위협 모델링

본 장에서는 설정된 연구 범위에 따라 데이터 흐름도(Data Flow Diagram)을 도출한다. MS Threat Modeling Tool을 이용하여 데이터 흐름도에 따라 개략적인 Attack List를 식별해내고 해당 위협들을 토대로 Attack Tree를 작성해 위험분석을 수행한다. 도구를 사용해 식별한 위협들은 대략적인 정보만을 제공하기 때문에 Attack Library를 작성하여 공격 방법들을 구체화 시킨다.

4.1 DFD(Data Flow Diagram)

본 항에서는 선박의 데이터 흐름도를 도출한다. 데이터 흐름도는 그래픽을 이용하여 시스템에서 각 프로세스를 따라 흐르면서 변화하는 모습을 나타낸다. Table 1은 데이터 흐름도의 구성요소를 나타낸다. 데이터 흐름도는 일반적으로 Context Diagram(Level0)를 포함하여 더욱 구체화 시킨 Level1까지 도출한다. Fig. 1은 선박 운항에 필요한 해양산업을 추상화시킨 Context Diagram이다.

선박(Ship)의 입출항은 선박의 소유주, 운항관리자가 포함되는 선박 이해관계자(Ship Stakeholder)가 선박의 운항 계획을 수립하여 일정에 포함하고 운항 경로 및 탑승자, 화물, 입출항 항구 등 관리한다.

항만(Port)는 한국 해양 관련 법률을 기준으로 선박의 입항/출항 등에 관한 법률에 따라 선장 등이 항만으로 정해진 서식 및 절차에 따라 입/출항 12시간 전에 항만정보시스템 및(PORT-MIS, EDI)을 이용하여 신고하여야 하며, 선박이 입항 또는 출항하거나 이동한 때에는 본선 선장과 도선사 및 예선 선장은 항만 교통관제센터에 무선으로 통보한다. 입항 또는 출항 시 한국 국적선이 아닌 외국 무역선의 경우 관세법에 따라 외국무역선의 입출항 전환 및 승선절차에 관한 고시에 따른다.

위성 통신 시스템(Satellite)은 선박법 및 선박위치 발신 장치의 설치기준 및 운영 등에 관한 규정에 따라 해상보안, 해양안전 및 선박 관리를 위해 선박에 설치된 시스템을 통해 선박의 항해 경로, 속도, 방향, 위치 등을 Ship Stakeholder와 Port로 제공한다. 이 시스템에는 선박 위치정보식별 장치(AIS, Automatic identification system)이 포함 된다.

Fig. 2는 Context Diagram을 보다 구체화 시킨 데이터 흐름도 Level 1을 나타낸다. Level 1은 선박 보안에 위협을 끼칠 수 있는 다양한 요인들을 식별하기 위해서 선박 운항에 필요한 요소를 크게 2가지의 Boundary로 육상(Offshore)과 선박(Ship)으로 분류하였으며, 육상(Offshore)은 다시 7가지의 세부 Boundary로 해운사에서 사용하는 Shipping Management Web Services, 항만에서 사용하는 Port MIS Web Services, 관세청에서 사용하는 Customs Web Services, 항만에서 화물관리를 위해 사용하는 Shipping Mana-

gement, 해양경찰에서 사용하는 VTS System, 해상통신을 위해 사용하는 Marine Satellite Services, 선주사가 해운 계약서를 Shipping Management DB로 관리하는데 이 DB에는 선하증권(B/L) 또는 용선계약서(C/P)가 포함되며 이 정보는 위/변조 또는 삭제 시 화물계약에 따른 비용 청구가 어렵기 때문에 보호 대책이 요구된다.

선박(Ship)은 IT 영역으로 통합항해정보시스템(IBS)과 AIS, ECDIS, VDR로 분류하였으며, OT 영역으로 평형수관리시스템(Ballast water system), 화물관리시스템(Cargo Management System), 엔진시스템(Engine System)으로 분류하였다. 선박은 해상위성통신망을 이용하여야만 육상과 통신이 가능하기 때문에 이러한 IT/OT 영역의 시스템들은 위성통신시스템과 게이트웨이를 통해서만 접근할 수 있다.

선박에 해상위성통신망을 이용하여 접근하는 External Entity로 6개를 분류하였으며 발주사(Ship Customer), 에이전트(Ship Agent), 선주사(Ship Owner), 조선기자재 회사(Ship Equipment Maker), 선박 운영사(Ship Operator)가 포함된다. 이들은 선박의 해상 위성통신을 이용하여 선원들과 통신하여 항해 및 운항정보를 송수신하거나 선체내 시스템의 모니터링을 위해 연결되기 때문에 접근통제 측면에서는 개방되어야 하는 필수적인 곳으로 이와 같은 선박과 신뢰된 접점의 보안 요구가 필요할 것으로 판단된다. 선박내 선원 및 승객이 외부 인터넷망을 사용하다 노출되는 악성코드 감염, 피싱 등의 위협은 선원/승객 네트워크와 선박 내부 IT/OT 네트워크의 분리 되지 않아 악성코드 전이 등에 대한 위협은 해상을 이동하는 선박의 특수한 환경에서는 보안대책이 우선적으로 요구될 것으로 판단된다.

4.2 STRIDE-per-element from DFD

본 항에서는 DFD로부터 위협 모델링에 대한 접근법인 STRIDE를 적용한다. 이 방법은 보안 위협의 6가지 위협의 머리글자를 딴 약어로 서비스의 취약성과 잠재적인 공격 가능성을 식별하는데 도움을 준다. 위협의 6가지는 위장(Spoofing), 변조(Tampering), 부인(Repudiation), 정보유출(Information Disclosure), 서비스 거부(Denial of Service), 권한 상승(Elevation of privilege)이고 Table 2 같은 집합으로 그룹화 하였다.

Table 2. STRIDE list

Attack Property	Security Theme
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-Repudiation
Information disclosure	Confidentiality
Denial-of-Service	Availability
Elevation of Privilege	Authorization

다음의 Table 3에서는 DFD의 각 구성 요소에 따라 나타날 수 있는 위협들을 표시하였다.

Table 3. Threat Mapping by STRIPE

Category	S	T	R	I	D	E
External Entry	O		O			O
Data Store	O	O	O	O	O	O
Process	O		O		O	O
Data Flow	O	O	O	O	O	O

이렇게 도출된 STRIDE를 Table 4와 같이 도출하였다.

Table 4. Threats Importance by STRIDE

Threats by STRIDE	Number of threats found	Importance
Spoofing	41	20%
Tampering	31	15%
Repudiation	45	22%
Information Disclosure	28	14%
Denial Of Service	36	17%
Elevation Of Privilege	25	12%
Sum	206	100%

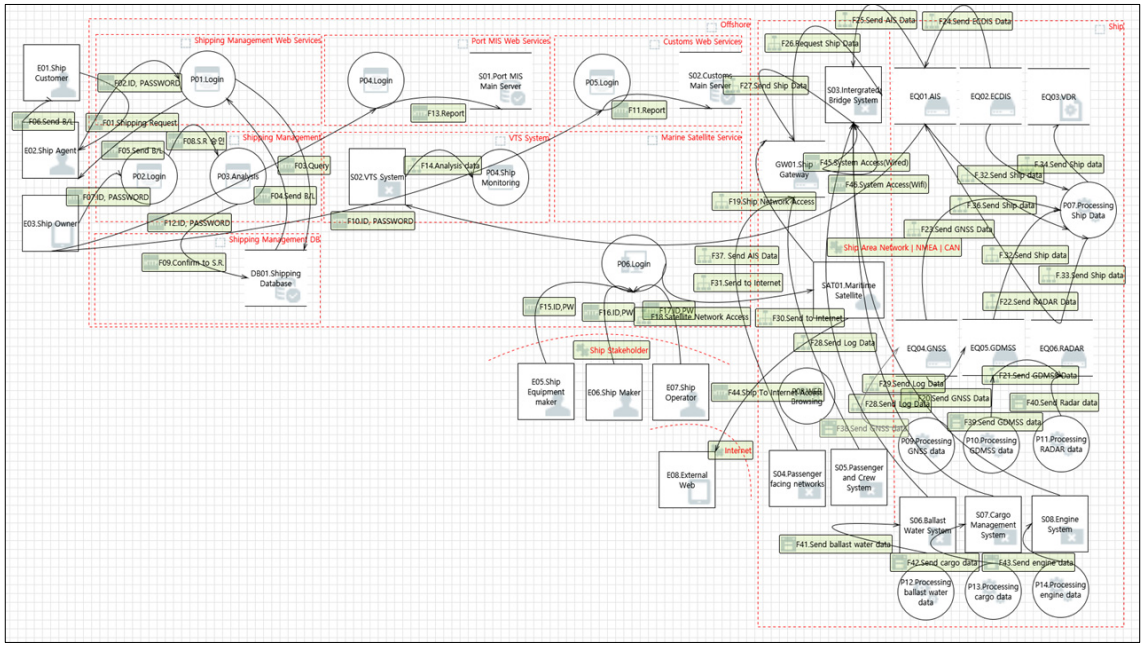


Fig. 2. DFD Context Diagram(Level 1)

4.3 Attack Library 수집

Attack Library는 데이터 흐름도를 작성한 이후 시스템에 대한 위협들을 다양한 자료 조사를 통해 수집한 목록이다. Attack Library 작성을 통해 DFD 상에서 요소마다 발생 가능한 위협을 찾아낼 수 있다. 본 과제에서는 사고사례, 기술보고서, 논문, 컨퍼런스 및 CVE(Common Vulnerabilities and Exposure)를 활용하여 실제 발생하였거나 가능한 공격들을 Table 5와 같이 식별하였다. 사고사례를 수집하기 위해서 국내외 언론보도 자료를 중심으로 수집하였으며 CVE를 확인하기 위해서 조선·해양 및 선박 시스템에서 사용 중인 시스템 목록(예를 들면 VDR과 같은)을 확인하기 위해 선박용 표준 IEC 61162-450과 460을 기반으로 하는 디바이스 목록을 확인하였으며 주요 내용은 다음과 같다.

2013년 Balduzzi는 AIS(Automatic Identification System) 패킷이 인증 또는 무결성 없이 사용되고 있어 공격자가 SDF(Software definced Radio)를 통해 레이더상에서 선박을 감출수 있어 해상안전에 될 소지가 있음을 경고했다[16].

2014년 Dyryvyy는 공격자가 ECDIS의 파일을 대체 또는 삭제하거나 악의있는 콘텐츠를 삽입할 수 있는 심각한 보안 취약점을 소개했다. 2012년 선박과 어선의 충돌사고 후 VDR 음성기록이 삭제되어 수사기관에서 디지털 포렌식을 통해 가해 선박에 탑승한 선원들이 불리한 증거를 훼손하기 위해 파기한 것으로 확인되었다[17]. VDR은 선박 내의 주요 OT시스템 및 브릿지의 음성기록 등 항해 및 거주에 관한 모든 데이터, 음성, 영상 기록이 저장되는 블랙박스와 같은 역할을 하는 장치인데 이 장치는 폐쇄구조가 아니라 원격에서도 접근할 수 있고 Ethernet을 통해서도 접근 가능하고 노트북을 통해 Direct로 접근이 가능하는 등 연결성이 강화됨에 따른 보안 취약점이 다수 발견되고 있다.

2014년 Ruben Santamarta는 BLACKHAT 2014에서 해양 위성통신 장비로 사용하는 주요 업체사의 취약점을 소개하였으며 실제로 일부 기기를 이용해 시연하였다[18].

2014년 IOActive는 선박에서 블랙박스 역할을 하는 VDR(Voyage Data Recorder)에서 Remote에서 데이터를 무단 변조할 수 있는 취약점을 발견하였다[19].

2016년 미국 해안경비대는 선박의 항법(Navigation) 시스템에서 GPS 간섭 또는 방해로 인한 탐색에 잠재적으로 해로운 영향을 미칠 수 있음을 경고(Safety Alert 01-16) 했다[20].

Table 5. Attack Library

Source	Category		Title	Author	Ref.
	sub	item			
Incident Case	3rd Party (Ship Owner)	System (Email)	Nigerian Hacking Group Targets Shipping Firms	The Maritime Executive	[22]
Incident Case	3rd Party (Ship Owner)	System (Email)	Svitzer employee details stolen in data breach	ABC News	[23]
Incident Case	3rd Party (Ship Owner)	System (Infra)	BW Group's computer systems hacked; steps up cyber security	S&P Global	[24]
Incident Case	3rd Party (Ship Owner)	System (Infra)	UK shipping firm Clarkson reports cyber attack	Reuters	[25]
Incident Case	3rd Party (Ship Owner)	System (Infra)	LESSONS FROM THE USS JOHN S. MCCAIN COLLISION	Center for International Maritime Security	[26]
Incident Case	3rd Party (Ship Owner)	System (Infra)	A.P Moller - 2017 Risk Management Report	Maersk	[27]
Incident Case	3rd Party (VTS Maintaenance)	System (VTS)	VTS Hacking by maintenance engineer	yonhapnews	[28]
Conference	Ship	System	CYBER SECURITY FLEET PROTECTION Hackers took 'full control' of container ship's navigation systems for 10 hours	OSM IHS	[29] [30]
Technical Report	Ship	Satellite communications	AmosConnect 8 blind SQL injections	IOActive	[31]
Technical Report	Ship	AIS	A Security Evaluation of AIS	Trend Micro	[32]
Technical Report	Port	System	Antwerp port cyber attack	News	[33]
Technical Report	3rd Party (Ship Owner)	System (Infra)	Pirates hacked shipping company to steal info for efficient hijackings	RISK Labs report	[34]
Technical Report	Ship	VDR	Destroy the VDR digital evidence	Tampere University	[35]
Journal	Ship	AIS	A Security Evaluation of AIS Automated Identification System		[36]
Journal	Ship	AIS	Detection of AIS Spoofing and Resulting Risks	Cyril RAY	[37]
CVE	Ship	Cobham Sea Tel	CVE-2018-5728	MITRE	[38]
CVE	Ship	Cobham Sea Tel	CVE-2018-5267	MITRE	[39]
CVE	Ship	Cobham SAILOR 900 VSAT	CVE-2013-7180	MITRE	[40]
CVE	Ship	Cobham Sea Tel 121 build 222701	CVE-2018-5266	MITRE	[41]
CVE	Ship	Cobham Sea Tel 116	CVE-2018-5071	MITRE	[42]

		build 222429			
CVE	Ship	Cobham Aviator 700D and 700E	CVE-2014-2964	MITRE	[43]
CVE	Ship	Cobham Aviator 700D and 700E	CVE-2014-2942	MITRE	[44]
CVE	Ship	Cobham The thraneLINK protocol	CVE-2014-0328	MITRE	[45]
CVE	Ship	Cobham SAILOR 800 and 900 VSAT	CVE-2018-19393	MITRE	[46]
CVE	Ship	Cobham Sailor 900 and 6000	CVE-2014-2940	MITRE	[47]
CVE	Ship	Cobham Sailor 6000 series satellite terminal contain hardcoded credentials	VU#269991 CVE-2014-2941	KB.CERT. ORG MITRE	[48] [49]
CVE	Ship	NMEA0183	CVE-2013-2038	MITRE	[50]
CVE	Ship	INTERSCHALT Maritime Systems VDR	CVE-2016-9339	MITRE	[51]
CVE	Ship	Auto-Maskin DCU 210E Engine Controller	CVE-2018-5401	MITRE	[52]
CVE	Ship	ICONICS OPC	CVE-2006-6488	MITRE	[53]
CVE	Port	Cargotec Navis WebAccess	CVE-2016-5817	MITRE	[54]
CVE	Ship	Furuno Voyage Data Recorder (VDR) VR-3000/VR-3000S and VR-7000	VU#820196	KB.CERT. ORG	[55]
CVE	Ship	FURUNO FELCOM 250 and 500	CVE-2018-16705	MITRE	[56]
CVE	Ship	FURUNO FELCOM 250 and 500	CVE-2018-16591	MITRE	[57]
CVE	Ship	FURUNO FELCOM 250 and 500	CVE-2018-16590	MITRE	[58]
CVE	Ship	Inmarsat AmosConnect 8 blind SQL injections	CVE-2017-3221	MITRE	[59]
CVE	Ship	Inmarsat AmosConnect 8 Hard-coded credentials	CVE-2017-3222	MITRE	[60]
CVE	Ship	Iridium Pilot and OpenPort contain multiple vulnerabilities, Use of Hardcoded Credentials	CVE-2014-0326	MITRE	[61]
CVE	Ship	Iridium Pilot and OpenPort contain multiple vulnerabilities, Missing Authentication for Critical Function	CVE-2014-0327	MITRE	[62]
CVE	Ship	Auto-Maskin DCU 210E Engine Controller	CVE - 2018-5399	MITRE	[63]
CVE	Ship	Auto-Maskin	CVE - 2018-5400	MITRE	[64]
CVE	Ship	Auto-Maskin	CVE - 2018-5401	MITRE	[65]
CVE	Ship	Auto-Maskin	CVE - 2018-5402	MITRE	[66]
CVE	Ship	Ship Equipment(Using NMEA)	CVE-2018-17174	MITRE	[67]

2016년 9월 17일 US ICS-CERT에서는 ICSA-16-231-01으로 항만 제어시스템인 Navis Webaccess 시스템에 Sql Injection 취약점을 소개했다[21].

Attack Library Source는 사고사례를 수집한 Incident Case, 컨퍼런스에서 소개된 Conference, 기술보고서에서 수집한 Technical Report, 논문지/학회지에서 수집한 Journal, 취약점 데이터베이스에서 수집한 CVE로 분류하였다. Category에서는 보안사고가 발생된 시스템을 분류하기 위해서 선박의 3rd Party, Ship, Port로 구분하고 하위분류 체계에서는 일반적인 System과 선박 전자장치와 장치 모델 분류별로 상세화 하였다.

4.4 Attack Tree

Attack Tree란 자산이나 정해진 목표를 공격하는 시나리오를 제시하는 개념도이다. 이 방법으로 선박의 보안 위협과 취약점을 트리 구조로 구성하기 때문에 어떠한 취약점들이 연계되어 있는지 식별이 용이한 장점이 있다. Attack Tree는 Schneier가 1999년에 공격의 가능성과 위협 식별에 유용한 점이 있음을 증명하였다[68]. 루트 노드부터 자식 노드로 나누어지는 다중 수준으로 구성되어 있다. Fig 3. Attack Tree는 선박과 선박내 ICT 기자재를 공격하는 루트 노드로 설정하였다. 하위 노드는 루트 노드에 위협 요인을 Attack Library를 바탕으로 구성하였다. 이러한 과정을 통해 공격자가 선박을 공격할 방법을 구체화한다. 공격자가 선박의 정보를 획득하거나 선박 가동을 중단시키거나 선박을 공격자의 뜻대로 제어할 방법들을 제시한다.

DREAD 기법(위협을 Damage Potential, Reproducibility, Exploit ability, Affected users, Discover ability로 분류)을 적용하여 1~10까지 점수를 부여하여 우선순위를 결정한다. Damage potential은 잠재적 피해로 공격의 피해량과 범위를 의미한다. Reproducibility는 재현 용이성으로 공격이 쉽게 재현된다면 점수가 높게 부여된다. Exploitability는 공격 가능성으로 공격이 쉽게 성공한다면 위험하다고 판단된다. Affected Users는 공격에 영향을 받는 사용자 수를 의미하고 공격의 파급력을 나타낸다. Discoverability는 취약점이 얼마나 쉽게 발견되는지를 나타낸다.

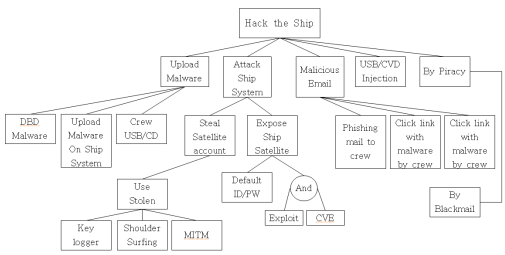


Fig. 3. Attack tree

원격지에서 선박 내부에 침투하여 선체내 시스템을 장악할 수 있는 위협(R1, R4, R9)에 대해서 Damage Potential 점수를 가장 높게 부여하였다. 선박내 시스템에 침투하기 위해서 공격이 재현될 가

Table 6. Risk analysis using DREAD

ID	Threat	D	R	E	A	D	Sum
R1	Unauthorized use of Satellite Network	3	2	1	3	3	12
R2	Attacks by “social engineering”	2	3	3	2	1	12
R3	Unauthorized software or hardware	1	3	2	1	1	8
R4	Malware in programs, documents, e-mail attachments	1	3	3	3	3	13
R5	External attackers masquerading as valid Ship stakeholders	2	1	2	2	1	8
R6	Attack programs allowing external access to Ship devices	2	1	1	1	1	6
R7	Attack programs allowing internal access to Ship system	2	1	1	1	1	6
R8	Unsecured maintenance modes, developer backdoors	1	2	1	1	2	7
R9	Malicious, deliberate damage of information or information processing functions from internal sources	3	1	1	3	3	11

능성이 있는 위협(R2, R3, R4)에 대해서 Reproducibility 점수를 가장 높게 부여하였다. 원격지에서 선박 내부 네트워크와 단말에 침투할 수 있는 위협(R2, R4)에 대해서 Exploitability를 가장 높게 부여하였다. 선박 운항에 직간접적으로 영향을 끼칠수 있는 해상 위성통신과 악성코드 공격 위협(R1, R4, R9)에 대해서 Affected Users 점수를 가장 높게 부여하였다. 선박 취약점이 Attack Library를 통해 식별된(26, 27, 28, 29) 경우 위협(R1, R4, R9)인 경우 Discoverability 점수를 가장 높게 부여하였다. Table 6은 식별된 위협 일부를 DREAD 기법을 이용하여 평가한 표이다.

V. 선박 보안 요구사항 도출

본 장에서는 도출된 위협을 통해 실제로 취약점을 분석하기 위한 체크리스트를 제시한다. Table 7은 선박 취약점 분석을 위한 체크리스트이다. 체크리스트는 상기 Table 5. Attack Library를 통해 식별된 항목들과 Fig. 3. Attack Tree를 통해 도출된 위협에 대한 보안대책을 작성되었다.

System 측면에서는 선박의 위치 정보를 처리하는 AIS, GNSS의 Related Attack와 점검해야 할 보안요소를 도출하였고, 선박의 블랙박스로 사용되는 VDR의 경우 원격 접근이 가능하여 해양사고 발생시에 디지털 포렌식 기술들을 통해 주요 분석대상인 VDR에 저장된 항적 데이터 등이 무결성을 보장하고 파일의 위변조 방지를 위한 방안 도출하였고, 해상위성 통신의 보급으로 먼 바다에서도 인터넷이 가능한 환경에서는 원격지의 공격자가 선박내부에 침투할 수 있는 접점인 VAST의 보안 요구사항을 도출하였다.

Network 측면에서는 선박에서 사용되는 SAN 및 CAN 프로토콜의 위협을 방지 할수 있는 보안 요구사항을 도출하였다.

Application 측면에서는 해상위성통신 시스템인 VAST과 선박에 원격지 접속을 하는 선주, 조선사, 조선IT기자재 회사 등 이해관계자에 대한 보안요구사항을 도출하였다.

Device 측면에서는 선박 내부의 IoT 시스템, OT 시스템 들이 보안 요구사항을 도출하였다.

Physical Security 측면에서는 선박이 대형 이동체이면서 승선하는 선원들의 위협에 따른 보안 요구사항을 도출하였다.

Table 7. Checklist for Ship cyber security

Category	Entry	Related Attack	Checklist
System	AIS, GNSS	Man-in-the-middle attack	Check the system use data
		False Data Injection	Encryption and Data
		GPS spoofing	Obscure antennas
			Add a sensor/blocker
			Extend data spoofing whitelists
			Use more GPS signal types
			Reduce latency
	VDR	Remote File Inclusion	Verify file
		File forgery	Check the system use data
	VSAT	Remote File Inclusion	Use IDS/IPS
		Malicious device	Authorization equipment verification
		Default id/password	Change id/pw
Network	Satellite	Brute forcing attack	Use IDS/IPS
		Password attack	Use password policy
		Command Injection	Use IDS/IPS
	SAN	Ping of Death	Check IP in packet

		Denial-of-Service	Bandwidth limit
	CAN	False Data Injection	Use IDS/IPS
		Hard coding credential	Strongly protected(encrypt.)
Application	VSAT	Sql injection	Verify query
		Default id/password	Change id/pw
	Stakeholder	Spear phishing attacks	Anti malware solution
		E-mail address spoofing	Check Eamil address
		Malware attack	Anti malware solution
Device	Sensor	False Sensor Data Injection	Verify data
		Transmitting Malicious Commands	Verify command
		Denial-of-Service	Bandwith limit
Physical	Onboard	Piracy and Terrorist	Ship's ICT defence system
	Crew	Human error	Awareness and training
	All	Destroy	Video surveillance

VI. 결 론

ICT 융합이 가속화되고 있는 조선·해양산업에서 안전한 선박을 건조 및 운영하기 위해서는 조선·해양 산업 전반에 대한 모든 보안 위협이 파악되어야 한다. 하지만 현재까지 발표된 해양 사이버보안에 대한 위협 도출과 대응방안은 미비한 상태이다. 따라서 본 연구에서는 선박을 중심으로 한 조선·해양 분야의 보안 위협 모델링을 실시하여 선박의 사이버보안 위협을 식별하였다. 이에 대한 위험관리를 위해서는 첫 번째, 항해 중인 선박의 네트워크 아키텍쳐를 변경하기 어려운 환경상 신조 선박의 경우 선박 네트워크 구성을 안전하게 구성하기 위해 IT/OT/Crew 또는 Passenger 구간의 분리 조치 등 선박 사이버보안 요구사항의 표준화가 필요하다. 두 번째, 선박에 탑재되는 시스템의 보안성 평가 제도를 통한 안전성 확보가 요구된다. 세 번째, 선박의 사이버보안 위협을 정기적으로 평가/측정하여야 한다. 네 번째, 선박 또는 선단, 선주사의 사이버보안 위협을 모니터링하고 공유할 수 있는 체계가 요구된다.

다섯 번째, 해양사고의 경우 환경오염, 인명사고 등의 위험 파급력이 높아 관련 업계에서는 위험관리 전략으로 해상보험을 채택하고 있다. 보험 업계에서는 본 논문에서 제기한 선박의 사이버보안 위협과 보안대책의 요구사항을 기반으로 해상 사이버보험이 요구된다. 여섯 번째, 해상 사고 조사에서는 본 논문의 DFD에서 도출된 선박의 주요 데이터 처리와 저장장치에 대해서 디지털 증거수집을 위한 아티팩트 수집에 관한 연구가 요구된다.

추후 자율운항 선박과 같은 IT/OT 의존도가 높은 선박 건조와 선급 검사를 진행할 때에 본 논문에서 제시한 보안위협을 기반으로 보안 요구사항과 보안 체크리스트를 참조할 수 있을 것이다. 하지만 본 논문에서는 분석 범위를 선박을 중심으로 하였기 때문에 선박 운항에 필요한 조선·해양 산업에 관한 범위로 확대하여 보안위협을 식별하고 요구사항을 분석해야 할 것으로 판단된다.

References

[1] Hye-Ri Park, Han-Sun Park and, Bo Ram Kim, A Study on the Policy Directions related to the Introduction of Maritime Autonomous Surface Ship (MASS), Korea Maritime Institute, Aug. 2018

[2] Paul Barnes and Richard Oloruntoba , "Assurance of Security in Maritime Supply Chains," The 6th International Business research Forum, Vol. 11, no. 4, pp. 519-540, Dec. 2005

〔3〕 OECD Maritime Transport Committee, Security in maritime transport: risk factors and economic impact, OECD, Jul. 2003
〔4〕 Joel Whitehead, Safety and Shipping Review 2018, ALLIANZ, Jul. 2018
〔5〕 Kimberly Tam and Kevin Jones, "Cyber-Risk Assessment for Autonomous Ships," 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp.1-8, Jun. 2018
〔6〕 Kevin D. Jones, Kimberly Tam and, Maria Papadaki, "Threats and Impacts in Maritime Cyber Security", Engineering & Technology Reference, pp. 5, Apr. 2016
〔7〕 Adam Shostack, "Experiences Threat Modeling at Microsoft," MODSEC@MoDELS 2008, 2008
〔8〕 Zhendong Ma and Christoph Schmittner, "Threat Modeling for Automotive Security Analysis, Advanced Science and Technology Letters", SecTech 2016, Vol.139, pp.333-339, Nov. 2016
〔9〕 Rafiullah Khan, Kieran McLaughlin, David Laverty and, Sakir Sezer, "STRIDE-based Threat Modeling for Cyber-Physical," 2017 IEEE PES: Innovative Smart Grid Technologies Conference Europe (ISGT-Europe): Proceedings 2017, pp.1-7, Sep. 2017
〔10〕 Stijn van Winsen, "Threat Modelling for Future Vehicles, On Identifying and Analysing Threats for Future Autonomous and Connected Vehicles", Master Thesis, University of Twente, Jan. 2017
〔11〕 Gwang-Il Lee, Jun-Hui Park, and Won-Seok Choe, "International standardization trend of onboard communication", TTA Journal, 126, pp. 45-51, 2009
〔12〕 K.I. Lee and J.H. Park, "Standardization Activities for Ship IT Convergence Technology", ETRI, Electronics and telecommunications trends, 28(4), 2013
〔13〕 Dong-Keun Jeon and Yeon-woo Lee, "TDMA based HR-WPAN Application for a Ship Area Network with Link Transmission Parameters Selection Algorithm", International Journal of Control and Automation, 8(2), pp. 299-310, 2015
〔14〕 Chang-Young Kim and Im-geun Lee, "Design and Implementation of NMEA2000 Protocol Application for Marine Monitoring System", Journal of Korea Institute of Information and Communication Engineering, 19(2), pp. 317~322, Feb. 2015
〔15〕 Ik-roh Yoon, Jung-min Choi, and Kyung Suk Seo, Technology Assessment : Autonomous Ships, 1st Ed., KIMST, Sep. 2018
〔16〕 Dr. Marco Balduzzi, "AIS Exposed Understanding Vulnerabilities & Attacks 2.0," Blackhat asia 2014, 2014
〔17〕 Arstechnica, "Hacked at sea: Researchers find ships' data recorders vulnerable to attack" https://arstechnica.com/information-technology/2015/12/hacked-at-sea-researchers-find-ships-data-recorders-vulnerable-to-attack/, 2019-04-25
〔18〕 Ruben Santamarta, "SATCOM Terminals:Hacking by Air, Sea, and Land," IOACTIVE, 2014
〔19〕 USCG, "Global Navigation Satellite Systems - Trust, But Verify - Report Disruptions Immediately ", https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0116.pdf, 2019-04-23
〔20〕 USCG, "Global Navigation Satellite Systems - Trust, But Verify - Report

Disruptions Immediately ", https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0116.pdf, 2019-04-23
〔21〕 US-CERT, "Navis WebAccess SQL Injection Vulnerability" https://ics-cert.us-cert.gov/advisories/ICSA-16-231-01, 2019-04-15
〔22〕 maritime-executive, "Nigerian Hacking Group Targets Shipping Firms " https://www.maritime-executive.com/article/nigerian-hacking-group-targets-shipping-firms, 2019-04-15
〔23〕 ABC news,"Svitzer employee details stolen in data breach affecting almost half of its Australian employees" https://www.abc.net.au/news/2018-03-15/sensitive-data-stolen-from-global-shipping-company-svitzer/9552600, 2019-04-15
〔24〕 spglobal,"Shipping: BW Group's computer systems hacked; steps up cyber security" https://www.spglobal.com/platts/en/market-insights/latest-news/shipping/101317-shipping-bw-groups-computer-systems-hacked-steps-up-cyber-security, 2019-04-15
〔25〕 reuters,"UK shipping firm Clarkson reports cyber attack" https://www.reuters.com/article/us-clarkson-cyber/uk-shipping-firm-clarkson-reports-cyber-attack-idUSKBN1DT1KO,2019-04-15
〔26〕 cimsec,"CYBERPHYSICAL FORENSICS: LESSONS FROM THE USS JOHN S. MCCAIN COLLISION" http://cimsec.org/cyberphysical-forensics-lessons-from-the-uss-john-s-mccain-collision/35254, 2019-04-15
〔27〕 A.P Moller,"A.P Moller 2017 Risk Management Report" https://www.maersk.com/-/media/ml/about/sustainability/20180209-a-p-moller-maersk-annual-report.pdf, 2019-04-23
〔28〕 YonHapnews, "Court to sentence 2 employees of a company that hacked into Jindo VTS" http://www.yonhapnews.co.kr/local/2014/11/17/0805010000AKR20141117128500054.HTML, 2019-04-15
〔29〕 OSM,"CYBER SECURITY FLEET PROTECTION" https://static1.squarespace.com/static/57a8878837c58153c1897c2c/t/5ab3b85f88251b5549a07357/1521727638547/8PeterSchellenberger_OSM_APM18.pdf. 2019-04-20
〔30〕 rntfnd,"Hackers took 'full control' of container ship's navigation systems for 10 hours - IHS Fairplay" https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay, 2019-04-15
〔31〕 Trendmicro, "Vulnerabilities Found in AmosConnect 8 Maritime Communications Systems" https://www.trendmicro.com/vinfo/dk/security/news/cybercrime-and-digital-threats/vulnerabilities-found-in-amosconnect-8-maritime-communications-systems, ,2019-04-15
〔32〕 Marco Balduzzi, Kyle Wilhoit, and Alessandro Pasta, "A Security Evaluation of AIS," Trend Micro, 2014
〔33〕 Jenna Ahokas and Tuomas Kiiski, "CYBERSECURITY IN PORTS", HAZARD Project Turku School of Economics University of Turku, pp 15, 2017
〔34〕 SOPHOS, "Pirates hacked shipping company to steal info for efficient hijackings" https://nakedsecurity.sophos.com/2016/03/07/pirates-hacked-shipping-company-to-steal-info-for-efficient-hijackings/, 2019-04-20
〔35〕 Marko Helenius , "MARITIME CYBER SECURITY INCIDENT DATA REPORTING FOR AUTONOMOUS SHIPS," Master of Science Thesis, Tampere University of Technology,

Nov. 2017
〔36〕 Marco Balduzzi, Alessandro Pasta, and Kyle Wilhoit, "A security evaluation of AIS automated identification system," ACSAC '14 Proceedings of the 30th Annual Computer Security Applications Conference, pp. 436-445, Dec. 2014
〔37〕 Cyril Ray, Cl´ement Iphar, Aldo Napoli, Romain Gallen, and Alain Bouju. "DeAIS project: Detectionof AIS Spoofing and Resulting Risks," MTS/IEEE OCEANS'15, May. 2015
〔38〕 MITRE,"CVE-2018-5728" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5728, 2019-04-15
〔39〕 MITRE,"CVE-2018-5267" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5267, 2019-04-15
〔40〕 MITRE,"CVE-2013-7180" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-7180, 2019-04-15
〔41〕 MITRE,"CVE-2018-5266" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5266, 2019-04-15
〔42〕 MITRE,"CVE-2018-5071" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5071, 2019-04-15
〔43〕 MITRE,"CVE-2014-2964" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2964, 2019-04-15
〔44〕 MITRE,"CVE-2014-2942" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2942, 2019-04-15
〔45〕 MITRE,"CVE-2014-0328" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0328, 2019-04-15
〔46〕 MITRE,"CVE-2013-7180" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-19393, 2019-04-15
〔47〕 MITRE,"CVE-2014-2940" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2940, 2019-04-15
〔48〕 CERT, "Cobham Sailor 6000 series satellite terminal contain hardcoded credentials", https://kb.cert.org/vuls/id/269991/, 2019-04-15
〔49〕 MITRE,"CVE-2014-2941" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-2941, 2019-04-15
〔50〕 MITRE,"CVE-2013-2038" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-2038, 2019-04-15
〔51〕 CVE Details,"CVE-2016-9339" https://www.cvedetails.com/cve/CVE-2016-9339/, 2019-04-15
〔52〕 MITRE,"CVE-2018-5401" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5401, 2019-04-15
〔53〕 MITRE,"CVE-2006-6488" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-6488, 2019-04-15
〔54〕 CVE Details,"CVE-2016-5817" https://www.cvedetails.com/cve/CVE-2016-5817/, 2019-04-15
〔55〕 CERT, "Furuno Voyage Data Recorder (VDR) moduleserv firmware update utility fails to properly sanitize user-provided input", https://www.kb.cert.org/vuls/id/820196/, 2019-04-15
〔56〕 MITRE,"CVE-2018-16705" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16705, 2019-04-15
〔57〕 MITRE,"CVE-2018-16591" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16591, 2019-04-15
〔58〕 MITRE,"CVE-2018-16590" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16590, 2019-04-15
〔59〕 MITRE,"CVE-2017-3221" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3221, 2019-04-15
〔60〕 MITRE,"CVE-2017-3222" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-3222, 2019-04-15
〔61〕 NVD,"CVE-2014-0326" https://nvd.nist.gov/vuln/detail/CVE-2014-0326, 2019-04-15

〔62〕 MITRE,"CVE-2014-0327" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0327, 2019-04-15
〔63〕 NVD,"CVE-2018-5399" https://nvd.nist.gov/vuln/detail/CVE-2018-5399, 2019-04-15
〔64〕 MITRE,"CVE-2018-5400" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5400, 2019-04-15
〔65〕 MITRE,"CVE-2018-5401" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5401, 2019-04-15
〔66〕 MITRE,"CVE-2018-5402" https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5402, 2019-04-15
〔67〕 NVD,"CVE-2018-17174" https://nvd.nist.gov/vuln/detail/CVE-2018-17174, 2019-04-15
〔68〕 Shim Jae-Suk, Technical and Managerial Study of Personal Information Protection on Smart Grid Service, KISA-WP-2015-0044, KISA, pp. 90, Feb. 2016

〈저자소개〉

조 용 현 (Yong-hyun Jo) 정회원
2004년 8월: 경희대학교 졸업
2007년 2월: 아주대학교 정보통신대학원 정보보호전공 석사
2018년 3월~현재: 고려대학교 정보보호대학원 융합보안학과 박사과정
2002년~2007년: 육군중앙수사단 사이버범죄수사/디지털증거분석 수사관
2009년~2014년: 비씨카드 정보보안실, 신한카드 정보보호팀
〈관심분야〉 디지털 포렌식, 사고대응, 정보보호 정책, 개인정보보호, 융합보안

차 영 균 (Young-kyun Cha) 종신회원
1989년 2월: 고려대학교 수학과 졸업
1992년 6월: 고려대학교 대학원 석사
2012년 8월: 고려대학교 정보보호대학원 박사
2018년~현재: 고려대학교 정보보호대학원 초빙교수
〈관심분야〉 융합보안, 암호학, 물리보안, 금융보안, 정보보호 정책