KICSP 한국 융합신호처리학회

융합신호처리학회논문지 Vol. 23, No. 4 : 209~215 December. 2022
DOI : 10.23087/jkicsp.2022.23.4.004

해양 사이버 보안사고 및 위험 관리 사항 동향

강동우[1], 김기환[2], 이영실[2*]
[1]한국해양과학기술원 부설 선박해양플랜트연구소, [2]동서대학교 International Collage

Maritime Cyber Security Issues and Risk Management Trends

Dong-Woo Kang[1], Ki-Hwan Kim[2], Young-Sil Lee[2*]
[1]KOREA RESEARCH INSTITUTE OF SHIPS & OCEAN ENGINEERING
[2]Department of Computer Engineering, International Collage, Dongseo University

요 약 국제 해사 환경과 선박 안전을 담당하는 국제해사기구는 국제적 차원 합의와 효율성 향상을 위해 사이버 시스템을 빠르게 추진하여 항해 효율성을 향상시켰다. 그럼에도 불구하고 매년 해양 사이버 시스템 공격 여전히 발생하고 있으며, 특히 2021년 국제 해양 사이버 보안 사고가 2020년과 비교하여 급증하는 양상을 보였다. 본 논문에서는 고도화될 해양 사이버 보안을 강하시키기 위해 고려해야 할 부분을 살펴본다. 이를 위해 2021년 급증한 사이버 공격 사례 중 대표적인 사례를 살펴보고 지속적으로 해양 사이버 보안 사고가 발생하는 원인을 분석한다. 또한, 현존하는 해양 사이버 시스템의 상황과 직면한 문제들에 대하여 해결방안과 고도화될 미래 해양 사이버 시스템을 위해 조치해야 할 사항에 대하여 몇 가지 사이버 체계 방안을 제시한다.

• 주제어 : 해양, 사이버 공격 사례, 국제해사기구, 통합 관리 시스템, OIDC

Abstract The International Maritime Organization, which is in charge of the international maritime environment and ship safety, has rapidly promoted cyber systems for international dimension agreement and efficiency improvement and improved nautical efficiency. Nevertheless, maritime cyber system attacks still occur every year, and in particular, the number of international maritime cyber security incidents in 2021 appeared to increase sharply compared to 2020. This paper discusses the areas that should be taken into account in order to reduce the increasing sophistication of maritime cyber security. To this end, we will look at typical cases of cyber attacks that have increased sharply in 2021 and analyze the causes of the continuous occurrence of maritime cyber security incidents. In addition, we present several cyber system proposals regarding the current state of maritime cyber systems and the solutions to the problems they face, as well as the matters to be addressed for future maritime cyber systems that will be advanced.

• Key Words : Maritime, Cyber Attack Cases, IMO, Integrated Management System, OpenID Connect

Received 01 December 2022, Revised 08 December 2022, Accepted 10 December 2022

*** Corresponding Author** Young Sil Lee, Department of Computer Engineering, Dongseo University, 47, Jurye-ro, Sasang-gu, Busan, Korea.
E-mail: lys0113@gdsu.dongseo.ac.kr

Ⅰ. 서론

문명의 발달과 확장은 해상 무역으로 시작되어 오늘날에는 전 세계 해상 운송 네트워크 통로로 사용되고 있다. 해상 운송의 주요 대상은 각종 화물, 에너지 공급, 승객 및 차량 등 국제 물류의 중추 역할을 수행한다. 2021년 유엔 무역개발회의(United Nations Conference on Trade and Development, UNCTAD) [1]에 의하면 전 세계 100톤 이상의 선박이 99,800척으로 집계되었으며, Fig 1과 같이 2017년 이후로 지금까지 10년 이상 운항 중인 선박 비율은 증가하고 10년 미만 운항 중인 선박 비율은 감소하는 추세로 보고되었다.

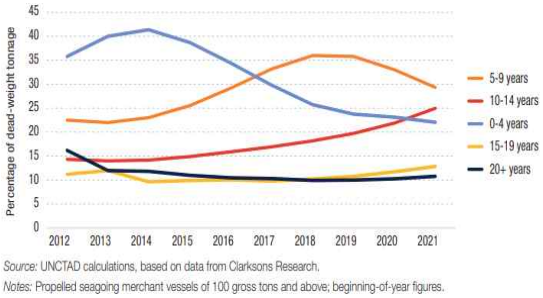

Fig. 1. Age distribution of the global fleet, share of the global carrying capacity, 2012 - 2021.[1]

여기서 주목할 부분은 10년 이상 운항 중인 선박 비율이 줄어들지 않는다는 것이다. 2000년도 당시 선박의 설계에 사이버 보안은 고려되지 않았으므로[2], 이는 현재까지 운항 중인 오래된 선박에서 사용 중인 GPS Plotter, VHF 무선 통신기 등의 항법장치와 AIS, ECDIS 등 항법 보조 장치들은 여전히 사이버 공격의 위험에 노출되어 있음을 시사한다.

한편, 국제 해사 환경과 선박 안전을 담당하는 국제해사기구(International Maritime Organization, IMO)가 2019년 디지털 기술을 활용하여 운항 정보 또는 기후, 항로 등의 정보를 수집하고 통합 및 분석하는 차세대 해상항법 체계 e-Navigation 서비스의 국제표준을 제정하고 채택함에 따라, 이를 위하여 선박 대부분에 선박 작업, 운영 그리고 통신 기능을 지원하는 컴퓨터 장비와 소프트웨어 설치를 적극적으로 추진하였다. 그 결과 오늘날 선박 운항의 대부분은 컴퓨터와 소프트웨어 기술로 자동화되며, 선박 운항에 요구되는 지식과 인력이 낮아짐에 따라 소프트웨어에 크게 의존하고 있다. Allianz[3]는 전 세계에서 코로나 대유행이 시작된 이후 해양 부문 기업들이 사이버 공격 시도가 400% 증가를 보고했다. 또한 해양 산업의 사이버 공격 인식의 변화는 몇 가지 설문 조사 결과와 통계자료 등을 통해 알 수 있다. 2011년 유럽 연합사이버보안국(European Union Agency for Cybersecurity, ENISA) [4]에서 대부분의 해양 업계 종사자들은 낮은 사이버 보안 의식을 가지고 있는 것으로 조사되었다. 다음으로 2018년 영국 Future Nautics에서 발간된 승무원 연결성에 관한 설문 조사[5] 결과, 응답자의 절반 미만이 사이버 공격으로 손상된 선박에서 항해를 수행했다고 보고했다. 2020년 Alcaide[6]는 해양 사이버 보안은 여전히 강화될 필요성이 있으며, 해양 산업 종사자들의 관행과 시스템의 취약성은 여전히 존재하고 있다. 특히 무선 네트워크의 잠재적인 보안 문제는 사이버 보안에서 고려되어야만 할 문제이다[7]. 지난 20년간 대부분의 선박 통신과 소프트웨어 발달로 원격 진단 및 유지 보수가 가능해지면서 사이버 보안 위험성도 증가하게 되었다. 따라서 해양 산업의 관습적, 구조적 특성상 타 산업과 비교하여 사이버 공격에 취약했다. 그 결과 2020년부터 2022년까지는 전 세계 항구와 해사 관련 기업의 공격이 크게 증가하며 크고 작은 사고가 연속되었다. 일련의 사고들은 사람의 실수로 벌어진 일도 존재하였으나 사이버 공격으로 발생된 피해는 대중적으로 인식이 미미하다. 이에 따라 국제해사기구는 미래 해양 사이버 인증 표준으로 Open ID Connect(OIDC) 사용을 기술 표준으로 채택한 상태이며, 2022년 5월 해상 항법 및 무선 통신 장비 및 시스템 데이터 인터페이스 파트 2의 선박과 해안 간 보안 통신(SECOM)이라는 표준을 출간했다. 해당 표준은 지금까지 해상 사이버 보안의 표면적인 정의를 구체적으로 구조화 및 동작 방식을 기술하고 있으며, 기술을 지원하지 않는 장비와의 호환 방법까지 정의하였다. 따라서 해사 사이버 보안에서 가장 심각한 사용자 권한 탈취를 효과적으로 예방할 수 있을 것으로 기대하고 있다. 이에 본 논문에서는 사이버 공격에 대한 심각성을 확인하고 국제해사기구에서 미래 해양 사이버 인증 표준으로 채택한 Open ID Connect(OIDC)를 통해 해양 사이버 보안 문제 해결 방안을 살펴본다.

Ⅱ. 국제 해양 사이버 공격 사례

해양 사이버 공격 횟수는 전 세계적으로 2021년에 2020년과 비교하여 3배가 급증하여, Fig 2처럼 크고 작은 기록적으로 증가했다. 2021년 해양 및 물류 산업은 2020년과 비교하여 선박을 표적으로 공격한 빈도가 33% 증가했으며, 항만 시스템에 대한 공격이 900% 증가하면서 사이버 보안 측면에서 많은 사건이 있었다[4].

2021년 6월 한국 해운사 HMM의 이메일 서버를 표적으로 공격으로 시스템을 오프라인 상태로 만들었다. 서버의 전체 기능을 며칠 이내에 복원하고 공격으로 인하여 민감한 데이터가 손실되지 않도록 신속하게 대응하여 피해를 최소화했다[5].

반대로 2021년 7월 일본 해운회사 가와사키 기선 가이사(Kawasaki Kisen Kaisha)는 자사 컴퓨터 시스템이 "해외 자회사 시스템에 대한 무단 액세스"로 침해되었음을 확인하는 간단한 성명을 발표했다[6]. 이 회사는 불과 3개월 전인 2021년 3월에도 해외 계열사를 통해 유입된 악성코드 감염으로 10일간 시스템 중단이 발생하였다. 외부 전문가를 통해 점검을 수행하였으나 다시 문제가 발생한 것이다.

2021년 7월 남아프리카 공화국의 주요 물류, 철도, 항만을 운영하는 Transnet가 공격[8]당했다. 다행스럽게도 공격은 컨테이너 터미널로 국한되어 회사의 다른 사업부 대부분이 운영되었다. 그러나 공격의 피해는 상당했다. 터미널 클러스터는 일주일 넘게 거의 완전히 마비되었으며, 핵심 운영 시스템은 포렌식 및 격리 중에 중단되고 연결이 끊어져 여러 선박 호출을 생략하기로 결정했다. 이는 수입업체, 수출업체 및 해운업체와 같은 관련 이해 관계자로부터 심각한 법적 결과에 직면할 수 있음을 보여준 사례이다. 모범적인 사이버 공격 대응 사례로 2021년 8월 미국 Houston 항구가 있다[9]. 공격자들이 암호 관리자의 취약점을 악용하여 포트 네트워크를 침입하고 다른 시스템에 대한 접근 권한을 얻기 위해 시도했지만, Houston 항만 IT 팀이 침해를 신속하게 감지하고 이를 완화하기 위한 조치를 취하여 민감한 데이터가 노출되지 않았으며 시스템이 중단되지 않았다. 그러나 자사의 보안이 잘 유지된다고 하더라도 방심할 수 없다. 2021년 9월 프랑스 컨테이너 선사인 CMA CGM은 고객 이름 및 연락처 정보와 같은 비교적 민감한 정보가 유출[10] 당했다. 다행스럽게도 API 모니터링에서 침해를 감지하여 시스템의 중단되지는 않았다. 위와 유사하게 2021년 11월 싱가포르 Swire Pacific Offshore는 IT 시스템에 대한 무단 액세스를 겪었다[11]. 이로 인하여 민감한 독점 상업 정보가 유출되었다. 두 사건은 모니터링을 통해 서비스가 정지하는 심각한 상황을 사전에 예방했으나 민감한 데이터 유출이라는 문제에서 자유로울 수 없었다.

2022년 2월 20일 미국 물류업체 Expeditors가 랜섬웨어 공격을 받았다[1-2]. 이 사고로 약 3주간 서비스를 복구하지 못해 한화 약 7,440억 이상의 손실을 봤다. 유사한 사례로 2022년 2월 21일 뭄바이의 최고 규모의 5개 해양 시설 중 하나인 JNCPT (Jawaharlal Nehru Port Container Terminal)의 관리 정보 시스템(MIS)이 랜섬웨어 공격으로 손상되었다[3]. 이로 인해 복구가 완료될 때까지 수동 작업으로 물류 운반에 영향을 주었다. 이러한 공격에 미리 대처하고 이와 같은 사건이 발생할 때 피해를 최소화하려면 사이버 범죄자가 작동하는 방식과 공격이 발생했을 때 피해를 억제하기 위해 기업이 할 수 있는 일에 대한 깊은 이해가 요구된다. 공격자의 대부분은 경제적 이익을 목적으로 하는 경우이다. 하지만 공격자의 목적이 경제적 이익이 아닌 경우 사태는 심각해질 수 있다. 2021년 특이 공격 사례로 외부 회사를 경유한 공격과 경제적인 목적이 아닌 서비스 파괴행위 등이 있다. 첫 번째로 소프트웨어 플랫폼의 취약점을 사용하여 한 번에 여러 대상을 침해하는 소프트웨어 공급망 공격이 존재한다. 이 공격은 작년에 모든 유형의 산업에서 발생했다.

2021년 11월 그리스 컨설팅 회사 Danaos Management Consultants는 공급망 공격으로 사이버 범죄자들이 이 회사와 거래한 여러 해운회사의 IT 네트워크를 침해했다[12]. 공격자들은 피해자의 데이터를 목표로 금점적인 보상을 요구했다. 이 과정에서 Danaos는 고객의 약 10%가 영향을 받았다. 이 공격은 사이버 복구 능력이 사내뿐만 아니라 타사 시스템에서 발생할 수 있는 위험까지 고려되어야 함을 보여준다. 원격 유지 관리를 실시하는 시설 및 업체의 경우 공격을 감지하더라도 스스로 대응할 방법이 없어 더욱 심각한 문제를 초래한다.

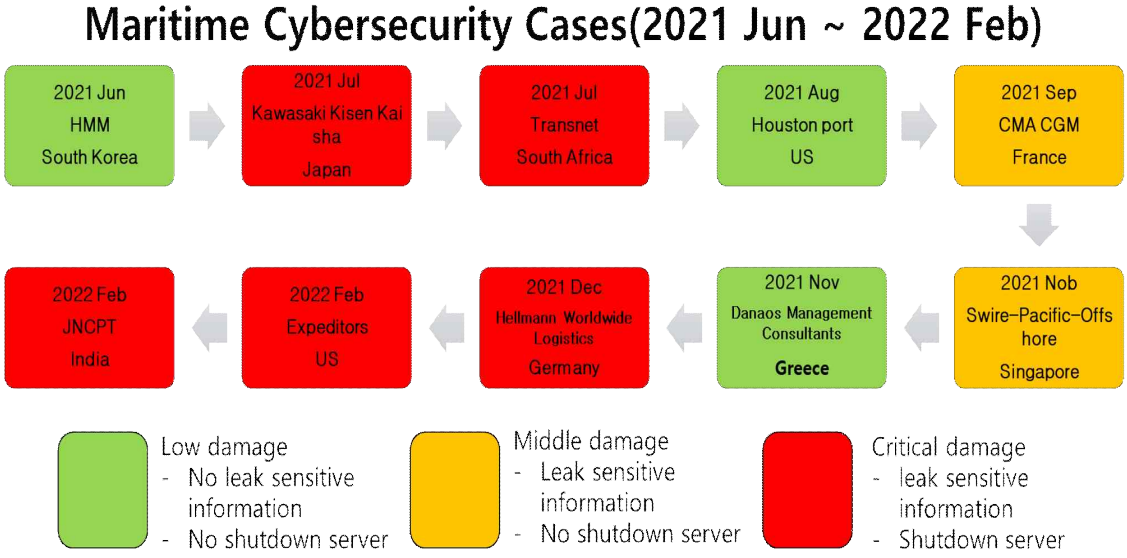

Fig. 2. Maritime Cyber security cases in 2020 ~ 2021.

2021년 12월 독일 물류 회사 Hellmann Worldwide Logistics는 사람들을 속여 민감한 정보를 전달하거나 유해한 소프트웨어를 다운로드하도록 고안된 피싱 공격의 영향을 감지하고 사이버 공격 확산을 막기 위해 서비스 운영을 일시적으로 중단했다[13]. 그 결과 중앙 데이터 센터에 대한 모든 연결이 중단되고 이로 인하여 모든 화물(항공, 해상, 철도, 도로) 운송이 중단되었다. 연쇄적으로 해당 시스템을 이용하는 기업의 서비스까지 일시중단되는 사태가 발생했다. ARGON에서 출간한 소프트웨어 공급망 보안 보고서[14]는 2021년 소프트웨어 공급망 공격량이 3배 급증하였으며, 대부분의 공격이 소프트웨어 공급망 프로세스와 공급자 신뢰를 악용하여 멀웨어 또는 백도어를 배포하면서 피해가 광범위하게 확산되도록 설계되었다는 것이다.

위와 같은 공격으로 국제 물류 공급망이 마비가 심화하였고 결국 2021년 5월 미국 국가 사이버 보안 개선 행정명령 발의, 2022년 1월 백악관에서 오픈 소스 소프트웨어 보안 논의로 해양 물류 공급망 사이버 공격 심각성을 보여주었다[15-16]. 이에 따라 불가피하게 사이버 공격을 당한 경우 최소한 빠른 서비스 복구가 요구된다.

Ⅲ. 사이버 위험 관리

현재 운영 중인 선박의 대부분은 20년 전에 건조되어 낡은 시스템을 업데이트하지 않고 그대로 사용하여 최신 보안 패치가 불가능한 문제를 가지고 있다. 특히 모바일 서비스와 장비의 발달 속도에 20년이 넘은 인터페이스와 시스템을 사용하는 선박은 설계 당시 고려되지 않은 부분들이 많아 최신 보안 패치에 한계가 존재한다. 이에 국제해사기구는 사이버 위험 관리를 “식별, 분석, 평가 및 전달하고 이해 관계자에게 취한 조치의 비용과 이점을 고려하여 수용 가능한 수준으로 회피, 이전 또는 완화하는 프로세스“로 정의한다[17]. 따라서 절차, 인적, 기술적 요인 등 세 가지 주요 요소를 중점적으로 관리할 것을 권장하고 있다.

첫 번째로 인적요인은 사이버 사고는 주로 교육이나 인식 부족으로 인해 발생하며, 모든 요인 가운데 가장 큰 취약성이 나타난다, 사이버 사고는 주로 교육이나 인식 부족으로 인해 발생한다. 즉, 실수로든 아니든 고의든 작업을 허용하는 판단의 주최는 사람이다. TrendMicro의 연구에 따르면 표적 공격의 91%는 사용자가 계속해서 피싱 이메일[18] 때문으로 조사되었다. 피싱 공격과 유사한 사회 공학 공격도 공격자는 단순히 인간 계층을 대상으로 하여 대부분의 기술 제어를 우회할 수 있다. 이러한 이유로 모든 회사는 사

이버 보안 요구 사항 및 정책을 설정해야 할 뿐만 아니라 가장 중요한 것은 이를 직원에게 효율적으로 전달하고 적용할 수 있는 방법을 찾는 것이다. 결과적으로 사이버 보안 인식, 기술 및 잠재적 사이버 위험을 관리하기 위한 역량을 구축하고, 특정 행동이 악용되는 방법을 전달하고, 사이버 보안 위반에 적절하게 대응하도록 사람들을 교육하는 것이다.

두 번째로 절차적 요인은 조직의 프로세스를 설명하고 조직의 특정 운영 및 보안 목표에 따라 직원의 책임과 비즈니스 관행을 정의하는 정책, 절차 및 지침이다. 일반적으로 관리 시스템, 프레임워크, 사이버 보안 모범 사례, 감사제도 등을 반영해야 한다.

세 번째로 기술적 요인은 절차 매뉴얼, 직무 분리, 데이터 분류, 계정 비활성화 정책, 액세스 권한, 사고 대응 계획, 제3자 처리 등 구체적인 정책이 추가되어야 한다. 통합 관리 시스템(Integrated Management System, IMS) 문서가 “사이버 위험“을 적절하게 처리하기 위한 요구 사항을 충족하지만 가장 중요한 것은 효율적으로 전달하기 위함이다. 결과적으로 사이버 보안 인식을 개선하고 규정 준수를 보장하는 가장 효과적이고 즉각적인 방법 중 하나는 사이버 보안 캠페인을 시행하는 것이다. 사이버 보안 캠페인으로 우리는 지속적인 노력과 간단한 지침과 요구 사항을 홍보하고 회사의 모든 직원, 특히 선내 승무원에게 메모 및 이메일 알림을 통해 주기적으로 상기시키는 것으로 자연스럽게 보안 의식을 향상시키고 실천하게 한다.

위와 같은 모든 행위는 궁극적으로 사이버 공격의 핵심은 목적인 사용자 권한 획득으로 원격 제어 권한 탈취에 있다. 즉, 인적, 절차적, 기술적 요인을 모두 고려하여 사용자 인증 권한을 적절하게 관리할 수 있는 방법도 고려되어야 할 사항이다.

사용자 권한 관리는 해사 보안 인증 및 권한 부여를 위한 표준에는 다양한 방법이 있으나 최근에는 PKI 방식을 사용하고 구글, 네이버, 아마존 등 인터넷 서비스 업체의 신뢰성을 이용하여 사이버 보안을 강화하는 방법이 주목받고 있다. 위와 같은 기술을 OpenID Connect(OIDC)라고 하며, 동작 방식은 Fig 3과 같다.

OIDC는 SSO(Single Sign On)로 한 번의 로그인으로 여러 애플리케이션을 이용할 수 있다. 이로 인해 서비스 기관이 다른 경우 빈번한 로그인 피로도가 감소하게 된다. 물론 인증받지 못한 경우 사용이 불가능하도록 설계되었으며, 비인가 사용자가 정상적으로 권한을 획득한 경우 모든 애플리케이션을 이용할 수 있다.

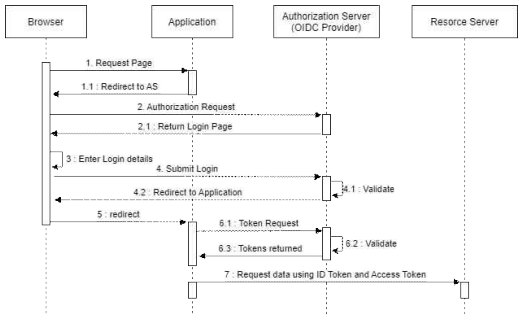

Fig. 3. OpenID-Connect workflow

따라서 OIDC는 통합 인증을 위한 표준으로 오로지 인증을 위해 설계되어 사용자가 간편하게 사용할 수 있다. 또한, 사용자에 대한 부가적인 정보를 id_token으로 전달하는 것이 가능하여 사용자의 정보를 얻기 위해 별도의 통신 과정을 요구하지 않아 데이터 요청이 많은 서비스에서 효율성이 높다. 이와 같은 인증 시스템은 향후 항만 자동화 기술과 자율운항 선박 도입에 있어 항만 운영 효율성 강화와 보안 강화에 기여된다.

Ⅳ. 결론

국제해사기구의 e-Navigation 도입으로 해사 환경에서 다양한 서비스를 창출하고 효율성을 향상시킬 수 있었다. 그러나 다양한 사례를 통해 사이버 공격에 미처 대응하지 못한 경우 선박의 안전까지 금전적 손실로 인한 국가적 피해까지 확대되는 등 결코 좌시할 수 없다. 해사 환경은 대역폭 부족, 복잡한 개발, 신호 범위의 제한과 불규칙한 기상변화로 통신의 한계가 명확히 존재한다. 본 논문에서는 해상 사이버 공격 사례를 기반으로 사이버 보안의 중요성을 강조하고 간편하고 안전한 사용자 인증 기법으로 OIDC 사용을 살펴보았다. OIDC는 모바일에서 권장되는 사용자 인증 기법으로 국제적으로 널리 사용되고 있어 향후 이동성이 높은 해사 클라우드에 도입될 가능성이 크다. 전 세계적으로 해사 클라우드는 2030년까지 해양사고 운항 과실로 인한 피해 감소와 해운 인력 부족 문제를 해결하기 위하여 무인 자율운항 선박 기술에 투자하고 있다. 자

율운항 선박 기술은 사람의 개입이 적은 만큼 장비 인증이 매우 중요하다. 앞서 살펴본 다양한 사례와 같이 해사 환경에서 사이버 보안은 선박의 안전과 재산과 직결되는 만큼 향후 해사 보안 연구도 지속적인 동향 조사와 연구를 진행하여 국내 조선·해운 기술 경쟁력 향상에 기여되어야 할 것이다.

ACKNOWLEDGMENTS

본 논문은 2022년 해양수산부 재원으로 해양수산과학기술진흥원의 지원을 받아 수행된 연구임 (해양 디지털 항로표지 정보협력시스템 개발(2/5) (20210650))

REFERENCES

[1] United Nations Conference on Trade and Development, (2021), Review of Maritime Transport 2021, [Online]. Available: https://unctad.org/system/files/official-document/rmt2021_en_0.pdf

[2] United Nations Conference on Trade and Development, (2020), Review of Maritime Transport 2020, [Online]. Available: https:unctad.orgwebflyerreview-maritime-transport-2020.

[3] Allianz, (2020), Safety and Shipping Review, Munich, [Online]. Available: https://www.agcs.allianz.com/content/damonemarketingagcsagcsreports AGCS-Safety-Shipping-Review-2020.pdf

[4] ENISA, (2011), Analysis of cyber security aspects in the maritime sector. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport

[5] Future nautics, (2015), Crew Connectivity Survey Report 2015, Future nautics Ltd. [Online]. Available: http://www.navarino.co.uk/wp-content/uploads/2018/04/Crew_Connectivity_2018_Survey_Report.pdf

[6] J. I. Alcaide, R. G. Llave, "Critical infrastructures cybersecurity and the maritime sector," Transportation Research Procedia, 2020, pp. 547-554. Available: https://www.sciencedirect.com/science/article/pii/S2352146520302209

[7] H. H. Kim, J. G. Song, Analysis of IoT Security in Wi-Fi 6, The Korea Institute of Convergence Signal Processing, 22(1), 2021, pp. 38-44. Available: https://www.kci.go.kr/kciportal/ci/sereArticleSearch/ciSereArtiView.kci?sereArticleSearchBean.artiId=ART002702545

[8] OFFSHORE ENERGY, (2021) South African port operator Transnet hit by cyber attack, [Online]. Available: https://www.offshore-energy.biz/south-african-port-operator-transnet-hit-by-cyber-attack/

[9] PORT of HOUSTON, (2021) Statement regarding Recent Cybersecurity Attack [Online]. Available: https://porthouston.com/wp-content/uploads/Port-Houston-Statement-_-Cybersecurity-Attack-Thwarted_-Sept-23-2021-_Final-.pdf

[10] SHIP TECHNOLOGY, (2021), CMA CGM reports another cyberattack targeting customer data. [Online]. Available: https://www.ship-technology.com/news/cma-cgm-reports-another-cyberattack/

[11] THE DAILY SWING, (2021) Maritime giant Swire Pacific Offshore suffers data breach following cyber-attack. [Online]. Available: https://portswigger.net/daily-swig/maritime-giant-swire-pacific-offshore-suffers-data-breach-following-cyber-attack

[12] THE MARITIME EXECUTIVE, (2021), Cyberattack Hits Multiple Greek Shipping Firms. [Online]. Available: https://www.maritime-executive.com/article/cyberattack-hits-multiple-greek-shipping-firms

[13] CNBC, (2022) Hackers can bring ships and planes to a grinding halt. And it could become much more commo. [Online]. Available: https://www.cnbc.com//2022/06/27/hackers-can-now-bring-cargo-ships-and-planes-to-a-grinding-halt.html

[14] ARGON, (2021), 2021 Software Supply Chain Security Report [Online]. Available: https://1665891.fs1.hubspotusercontent-na1.net/hubfs/1665891/Assets/Argon%20Security%20-%202021%20Software%20Supply%20Chain%20Security%20Report.pdf

[15] THE WHITE HOUSE, (2021), Executive Order on Improving the Nation's Cybersecurity. [Online]. Available: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

[16] THE WHITE HOUSE, (2022), Readout of White House Meeting on Software Security. [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/13/readout-of-white-house-meeting-on-software-security/

[17] K. H. Moussa, et al. Group Security Authentication and Key Agreement Protocol Built by Elliptic Curve Diffie Hellman Key Exchange for LTE Military Grade Communication, IEEE Access, 10, 2022, pp. 80352-80364. Available: https://ieeexplore.ieee.org/document/9845426

[18] Micro, T. (2012). Spear-phishing email: Most favored APT attack bait. Trend Micro Incorporated Research Paper. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/62/2012/12/21145753/wp-spear-phishing-email-most-favored-apt-attack-bait-1.pdf

저자소개

강 동 우 (Dong-Woo Kang)

2007년 2월 : 동서대학교 컴퓨터정보공학(공학사)
2012년 8월 : 동서대학교 유비쿼터스IT학과(공학석사)
2022년 8월 : 목포해양대 해상운송시스템학과(공학박사)
2012년 ~ 현재 : 선박해양플랜트연구소
관심분야: 수로정보표준, 해양사이버보안

김 기 환 (Ki-Hwan Kim)

2013년 2월 : 동서대학교 정보통신공학과(공학사)
2015년 2월 : 동서대학교 유비쿼터스IT학과(공학석사)
2021년 2월 : 동서대학교 유비쿼터스IT학과(공학박사)
2021년 3월~현재 : 동서대학교 International collage 초빙교수
관심분야 : 딥러닝, 암호학, 부채널

이 영 실 (Young-Sil Lee)

2006년 2월 : 동서대학교 정보네트워크과(공학사)
2010년 8월 : 동서대학교 유비쿼터스IT학과(공학석사)
2015년 8월 : 동서대학교 유비쿼터스IT학과(공학박사)
2017년 4월~현재 : 동서대학교 International college 컴퓨터공학과 조교수
관심분야 : 컴퓨터 보안, 헬스케어, RFID