KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 019

November 2019

한국선급 활동

- 독일 '해양 사이버보안 인프라 구축 클러스터' 발표
- European Maritime Cyber Resilience Forum 참석
- 싱가포르 선사 사이버보안 맞춤형 교육 수행

[기획시리즈] ④ 5G 표준에서 위성의 역할과 해상에 미치는 영향

사이버 위협의 이해(OWASP Top 10)

KR 해상 사이버보안 형식승인 지침의 이해

용어 설명

독일 '해양 사이버보안 인프라 구축 클러스터' 발표

한국선급은 독일 MCN(Maritime Cluster Norddeutschland)의 초청을 받아 10월 30일 독일 브레머하펜에서 개최한 '해양 사이버보안 인프라 구축을 위한 클러스터'에 참석하였다. MCN은 북부 독일의 해양 산업 연합체로 해양 분야에서의 협력 및 혁신을 촉진시키기 위하여 2011년 창설되었다.

이 포럼에서 한국선급은 해사 사이버보안 동향과 OCIMF, RightShip의 사이버보안 요건에 대해 설명하고, 이에 대응하기 위한 한국선급의 사이버보안 기술 서비스 및 인증 서비스에 대한 활동을 실제 예시를 들어 소개하였다. 다른 흥미로운 발표 내용으로는 Dr. Siv Hilde Houmb가 다른 발표자와 함께 ISO27001 기반 사이버보안 심사가 어떻게 이루어지는지에 대해 라이브 데모를 보여주었다.

한국선급은 2020년, 독일 선사 및 관련 업체들을 대상으로 사이버보안 세미나와 교육을 제공하여 IMO 결의안 MSC.428(98)에 대응할 수 있도록 가이드라인을 제공할 예정이다.

한국선급 활동 #2

European Maritime Cyber Resilience Forum 참석

한국선급은 유럽의 최신 해사 사이버보안 동향 및 기술 정보를 획득하기 위하여 10월 31일 영국 런던에서 개최된 Digital Ship의 European Maritime Cyber Resilience Forum에 참석하였다. (출처 : https://www.london.thedigitalship.com/)

포럼에서는 MAN Energy Solution, UK National Cyber Security Association, Beazley와 같은 해사 업계 전문가들의 활발한 논의가 이루어졌다. MAN Energy Solution에서는 선주, 선원을 비롯한 직원 외에 파트너들 역시 사이버보안 강화할 것을 촉구하였다. 또한, 선박 보험회사인 Beazley 사에서는 선박에 대한 사이버보안 보험에 현황과 서비스에 대한 소개를 하였다.

이 외에 영국의 플리머스 대학에서는 새로운 사이버보안 연구소(Cyber-SHIP Lab)을 설립하였으며, 선박 항해시스템의 시뮬레이션을 통해서 선박 항해시스템과 연결된 다양한 선내시스템에 대한 사이버 영향성을 연구할 것이라고 발표하였다.

한국선급 활동 #3

싱가포르 선사 사이버보안 맞춤형 교육 수행

한국선급은 11월 14-15일 싱가포르의 Diamond Ship Management Pte Ltd, Fleet Ship Management Pte Ltd 및 MSI Ship Management Pte Ltd의 37 명의 감독관을 대상으로 사이버보안 인식제고 교육을 수행하였다. 이 교육은 교육생들에게 사이버 위협을 식별, 사이버 리스크 평가 수행, 사이버 리스크 제어 조치를 구현, 사이버 사고를 탐지, 대응 및 복구하기 위한 기본 지식과 방법을 제공함으로써 IMO 결의안 MSC.428 (98)에 대응할 수 있는 가이드라인을 제공한다.

한국선급은 이번 교육의 고객 만족도 조사에서 교육 내용이 매우 유익하고 실용적이며, 실제 사이버공격 사례와 동영상을 통해 인식제고에 도움이 되었으며, 사이버 리스크 평가 워크샵을 통해 사이버보안 역량강화에 큰 도움이 되었다는 피드백을 수렴하였다. 한국선급은 SONGA 선사, 산쇼코리아㈜, VL Enterprise PLC 등 선사가 국제 사이버보안 이슈에 대응할 수 있도록 맞춤형 사이버보안 교육을 실시한바 있다. 한국선급은 향후 선사와 조선소, 기자재업체를 대상으로 사이버보안 맞춤형 교육 서비스를 강화해 나갈 방침이다.

<Diamond/Fleet SM>

<MSI SM>

Maritime Cyber Security Awareness Training Course Introduction

Maritime Cyber Security Awareness Training

11-15 November, Singapore

Course Introduction and Time Table

Trainer: Jeoungkyu Lim(Korean Register)
Sanghoon Choi(Korean Register)

1 Course Introduction

As Information and Communication Technology (ICT) becomes widely applied to the shipping industry, cyber threats and vulnerabilities related to digitalization, integration and automation of processes and system in shipping have also emerged. According the IMO Resolution MSC.428(98), administrations should ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

This one day awareness training course provides the trainees with the knowledge and method to respond to the maritime cyber security issues.

2 Time Table

Time	Category	Details	Trainer
09:00 - 09:50	Maritime cyber security overview	• Introduction • International response in maritime industry • KR cyber security activities	JK Lim
10:00 - 10:50	Administrative security	• Cyber security management system • Maritime cyber security organization • Human security • TMSA Element 13 : Maritime Security	JK Lim
11:00 - 11:50	Cyber Asset / Cyber Threat	• Cyber asset management overview • Identify asset • Asset criticality • Maritime Cyber threat • Threat list	SH Choi
12:00 - 13:00	Lunch Break		
13:00 - 13:50	Physical security	• Purpose and method of physical security • KR Server room physical security • Physical security by risk assessment	JK Lim
14:00 - 14:50	Technical security	• Network security • Vulnerability analysis • PC security vulnerability analysis	SH Choi
15:00 - 15:50	Understanding of maritime cyber security risk assessment	• Understanding of maritime cyber security and risk assessment • KR cyber security risk process • Application cases	JK Lim
16:00 - 17:00	Workshop	• Hands-on	SH Choi

[기획시리즈] ④

5G 에서 위성의 역할과 해상에 미치는 영향

본 기획시리즈는 4차산업혁명과 관련한 핵심 통신인프라인 5G가 해양산업에 미칠 긍정적 파급효과와 이에 따른 사이버 위협에 대해 다뤄보고자 한다. 따라서 본 뉴스레터 2019년 11월호에서는 ***'5G에서 위성의 역할과 해상에 미치는 영향'***에 대해 소개한다.

기획시리즈 순서

① 5G란 무엇인가?

② 5G의 네트워크 구조와 네트워크 슬라이싱(Network Slicing) 기술, 그리고 해양산업 변화

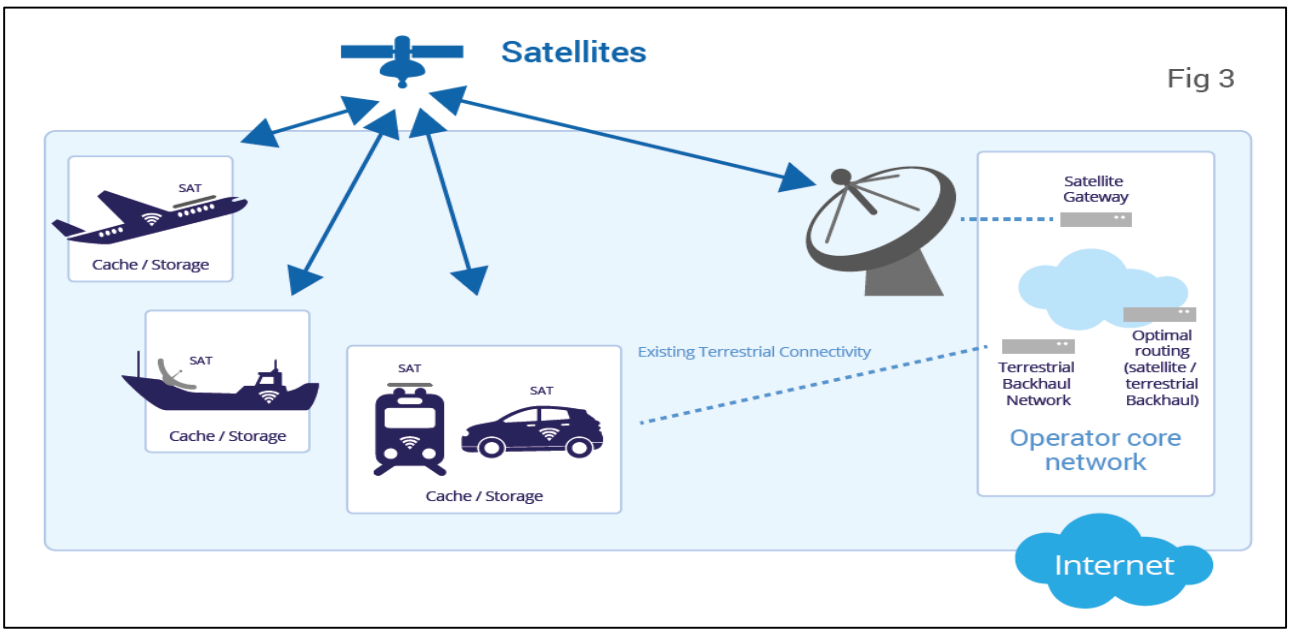
③ LTE의 중앙집중형 네트워크와 5G의 분산형 네트워크의 비교

④ **5G 표준에서 위성의 역할과 해양산업에 미치는 영향**

⑤ 선박과 항만에 효과적으로 활용하기 위한 5G 표준의 Private Network 참조모델

5G표준에서 위성의 역할

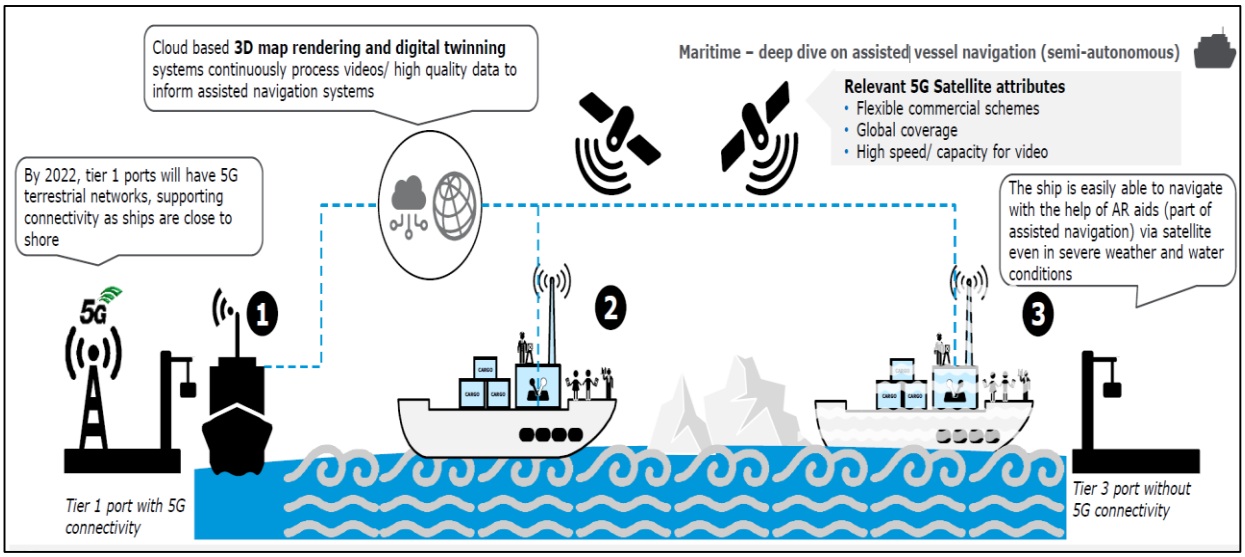
3G, LTE 표준은 지상의 기지국과 지상의 단말 간의 통신을 위해 설계되었으나, 5G를 표준화하고 있는 3GPP(3rd Generation Partnership Project)에서는 위성, 드론, HAPS, 항공기와 같이, 비 지상 네트워크(Non Terrestrial Network)의 구성요소를 포함하여 5G 표준을 설계하고 있다. 즉, 위성은 5G의 non-Terrestrial 기지국으로서, 육상의 기지국과 동일한 형태가 가능해지는 것이다. 이는 지상 기지국만으로 커버할 수 없는 도서산간, 해상, 사막 지역 등에서도 5G를 통해 연결성을 확대시켜 주는 역할을 충분히 할 수 있게 되는 것이다.



출처 : EESA, Satellite for 5G –Tomorrow's connected World 5G Satellite Initiative (S45G)Presentation

5G 위성으로 인한 해사산업에 미치는 영향

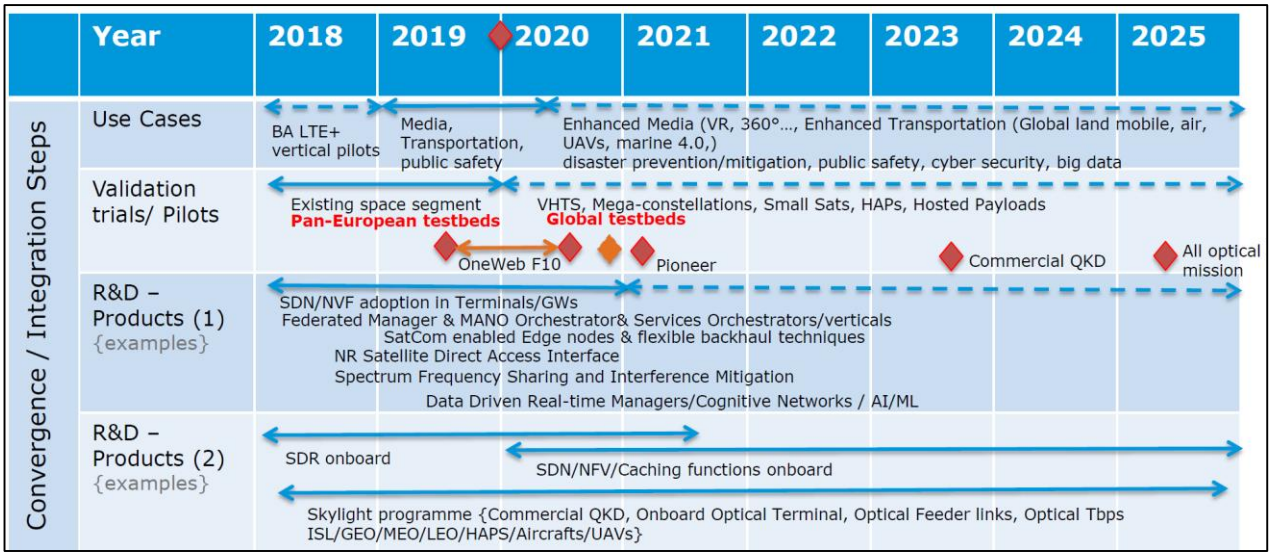
선박에서는 기존에도 VSAT, 인마셋 등 주로 위성통신을 통해 음성통신과 데이터 통신을 하고 있다. 하지만 위성이 점차적으로 5G에 통합되어 상용화가 된다면 높은 통화품질과 성능, 그리고 사이버보안이 강화된 음성, 데이터 통신을 더 낮은 가격으로 사용 할 수 있을 것이다. 특히, 자율운항선박(MASS)에 대한 연구가 전 세계적으로 추진됨에 따라, 지상 네트워크와 위성 네트워크가 통합된 5G 통신은 연결성과 사이버 보안성을 강화시켜주는 데 중요한 역할을 할 것으로 본다.



출처 : EESA, Satellite for 5G –Tomorrow's connected World 5G Satellite Initiative (S45G)Presentation

유럽우주국(EESA)에서 발표한 5G위성의 이행계획에 따르면, 2020년 까지 시범 운용을 실시하고, 2025년 까지 Marine 4.0을 위한 Use case 개발을 이행할 예정이라고 한다.

따라서 선사, 기자재 업계 등 기존 해사업계 들도 5G 위성의 도입으로 연결성향상에 따른 새로운 디지털 서비스 개발을 지금부터 준비할 필요가 있다.



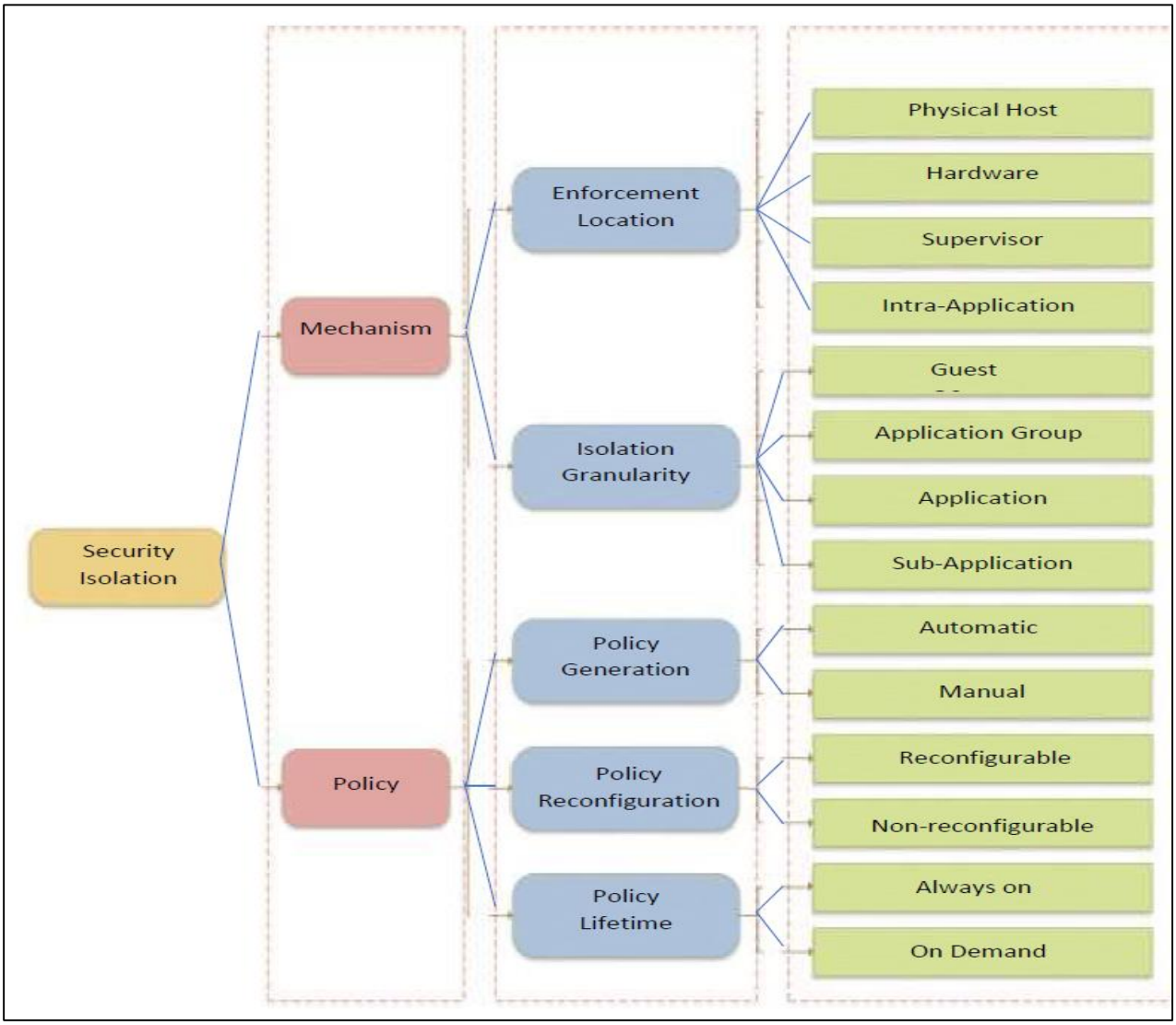
출처 : EESA, Satellite for 5G –Tomorrow's connected World 5G Satellite Initiative (S45G)Presentation

5G기술에 적용된 IoT 기기에서 완화될 수 있는 사이버보안 위협

앞서 설명한 바와 같이 5G는 위성 뿐 아니라 유선 네트워크 까지 기술을 통합해 나가고 있다. 따라서 5G표준에서 사이버보안 위협을 완화시키기 위해 적용한 모델을 기반으로 선박, 회사 등에서 사이버 위협 요소를 해결하기 위해 참조모델로 소개하고자 한다.

특히 선박의 경우 IT 시스템과 OT시스템의 보안 격리 조치가 필요하다. 이러한 보안 격리를 달성하기 위해서는 5G에서는 아래와 같은 모델을 적용하였따. 일반적으로 보안 격리 문제는 위협 모델에 따라 두 가지 방식으로 구성 할 수 있다.

기술적 매커니즘을 통해 보안 격리를 해결하는 방법이다. 메커니즘에 고려되는 설계 하위 범주는 시행 위치 및 격리 세분성이 있다.또 다른 방법으로 정책적인 설계를 적용하는 방법이다. 선박 설계단계에서부터 사이버보안 요소를 고려한다면 OT 시스템에 무거운 사이버보안 솔류션 설치 등 시스템에 영향없이 정책적인 설계로 사이버보안 위협을 줄여 나갈 수 있을 것으로 본다.



출처 : The Evolution of Security in 5G, 5G America white paper, July 2019

사이버 위협의 이해(OWASP Top 10)

사이버 위협 이해하기

사이버 위협이란, 조직 운영, 조직 자산, 개인, 기타 조직 또는 국가에 대해 사이버 시스템을 통한 무단 액세스, 파괴, 공개, 정보 수정 또는 서비스 거부와 같은 잠재적으로 악영향을 미칠 수 있는 상황이나 사건을 의미한다. (출처 : NIST SP : 800-128)

사이버위협은 ICT 기술이 발전함에 따라 자산에 미치는 영향이 변화하므로 자산의 취약점을 파악하기 위해 주기적으로 목록화 할 필요가 있다.

한국선급 해상 사이버보안 시스템 인증 검사항목(CS1)

204.1 위험관리 : 내부 정보기술 및 운영기술 환경에 의한 영향을 미치는 외부 환경 요인을 위협으로 식별하고 목록화하여야 한다.

OWASP Top 10

OWASP(Open Web Application Security Project)는 오픈소스 웹 어플리케이션 보안 프로젝트이다. 주로 웹에 관한 정보노출, 악성 파일 및 스크립트, 보안 취약점 등을 연구하며 웹 어플리케이션 취약점 중에서 빈도가 높고, 보안상 영향을 크게 줄 수 있는 10대 항목(OWASP Top 10)을 2004년, 2007년, 2010년, 2013년, 2017년 기준으로 발표하였다. 1월 뉴스레터에 이어 **'A10 : 2017 – 불충분한 로깅 및 모니터링'** 를 분석하고자 한다.

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – 인젝션	→	A1:2017 – 인젝션
A2 – 취약한 인증과 세션 관리	→	A2:2017 – 취약한 인증
A3 – 크로스 사이트 스크립팅 (XSS)	↘	A3:2017 – 민감한 데이터 노출
A4 – 안전하지 않은 직접 객체 참조 [A7 항목과 병합됨]	∪	A4:2017 – XML 외부 개체 (XXE) [신규]
A5 – 잘못된 보안 구성	↘	A5:2017 – 취약한 접근 통제 [합침]
A6 – 민감한 데이터 노출	↗	A6:2017 – 잘못된 보안 구성
A7 – 기능 수준의 접근 통제 누락 [A4 항목과 병합됨]	∪	A7:2017 – 크로스 사이트 스크립팅 (XSS)
A8 – 크로스 사이트 요청 변조 (CSRF)	☒	A8:2017 – 안전하지 않은 역직렬화 [신규, 커뮤니티]
A9 – 알려진 취약점이 있는 구성요소 사용	→	A9:2017 – 알려진 취약점이 있는 구성요소 사용
A10 – 검증되지 않은 리다이렉트 및 포워드	☒	A10:2017 – 불충분한 로깅 및 모니터링 [신규, 커뮤니티]

출처 : OWASP Top 10 Project

OWASP 10대 위협 'A10 : 2017 - 불충분한 로깅 및 모니터링'

불충분한 로깅 및 모니터링은 언제든지 발생한다. 로그인, 로그인 실패 및 중요한 트랜잭션과 같은 감사 가능한 이벤트는 기록되지 않으며, 경고 및 오류는 로그 메시지를 생성하지 않거나 부적절하거나 명확하지 않다. 의심스러운 활동에 대한 애플리케이션 및 API 로그는 모니터링 되지 않고, 로그는 로컬에만 저장된다. 따라서 적절한 조치를 취할 수 있도록 특정 경고가 트리거되었거나 특정 경고 임계 값에 도달 한 경우 경고하는 자동화된 프로세스가 필요하다. (예 : SIEM)

또한 로그가 백업되어 다른 서버에 동기화되어 있는지 확인이 필요하다. 공격자는 서버를 해킹 한 후 모든 로그를 지울 수 없어야 한다. 시스템을 검토하고 중요한 조치가 기록되었는지 확인한다. 향후 포렌식에 사용될 수 있도록 로그인, 중요한 거래, 비밀번호 변경 등이 포함되어야 한다.

시나리오#1

소규모 팀이 운영하는 오픈소스 프로젝트 포럼 소프트웨어가 소프트웨어 내 결함으로 해킹당했다. 공격자들은 다음 버전과 모든 포럼 내용이 포함된 내부 소스코드 저장소를 제거하였다. 소스코드를 복구할 수 있었지만, 모니터링, 로깅, 혹은 경고의 부재는 훨씬 더 큰 불이익을 초래하였다.

출처 : hackeone.blogspot.com

시나리오#2

공격자는 공통 암호를 사용하는 사용자를 찾기 위해 스캔을 한다. 이 암호를 사용하여 모든 계정을 탈취할 수 있다. 다른 모든 사용장의 경우, 이스캔은 단지 하나의 잘못된 로그인 기록만을 남긴다. 며칠 후 다른 비밀번호로 이 작업을 반복할 수 있다.

출처 : hackeone.blogspot.com

취약점 확인 방법

불충분한 로깅, 탐지, 모니터링과 유효한 응답은 언제나 발생합니다:

- 로그인, 로그인 실패, 그리고 높은 가치를 가진 트랜잭션들과 같은 감사해야 할 이벤트들이 기록되지 않습니다.
- 경고 및 오류에 대해 로그 메시지가 없거나, 불충분하거나 불명확합니다.
- 의심스러운 활동에 대해 애플리케이션과 API의 로그를 모니터링하지 않습니다.
- 로그를 단지 로컬에만 저장합니다.
- 적절한 경고 임계값과 응답 에스컬레이션 프로세스가 적절하지 않거나 효과적이지 않습니다.
- DAST 도구(예: OWASP ZAP)를 통한 침투 테스트 및 검사는 경고들을 추적하지 않습니다.
- 애플리케이션은 실시간 혹은 거의 실시간으로 유효한 공격을 탐지, 에스컬레이션 또는 경고할 수 없습니다.
- 사용자나 공격자에게 로깅이나 경고 이벤트가 보여질 수 있다면, 정보 유출에 취약합니다. (**A3:2017-민감한 데이터 노출**을 보십시오).

보안 대책

애플리케이션에 의해 저장되거나 처리되는 데이터의 위험에 따라:

- 모든 로그인, 접근 통제 실패, 그리고 서버 측면의 입력값 검증 실패 등이 의심스럽거나 악의적인 계정을 식별할 수 있는 충분한 사용자 문맥으로 기록될 수 있는지 확실히 하십시오. 그리고 지연된 포렌식 분석을 허용할 수 있는 충분한 시간을 확보하십시오.
- 중앙 집중적 로그 관리 솔루션에 의해 쉽게 사용될 수 있는 형식으로 로그가 생성되는지 확실히 하십시오.
- 부가 가치가 높은 거래에는 단지 추가만 가능한 데이터베이스 테이블 혹은 유사한 것과 같은 변조나 삭제를 방지하기 위한 무결성 통제 기능을 갖춘 감사 추적 기능을 확실히 하십시오.
- 의심스러운 활동이 적시에 탐지되고 대응될 수 있도록 효과적인 모니터링 및 경고를 설정하십시오.
- NIST 800-61 rev 2 이상과 같은 사고 대응 및 복구 계획을 수립하거나 채택하십시오.

OWASP AppSensor와 같은 상용 혹은 오픈소스 애플리케이션 보호 프레임워크, OWASP ModSecurity 핵심 룰셋을 가진 ModSecurity와 같은 웹 어프리케이션 방화벽, 그리고 개별 대쉬보드와 경고를 갖는 로그 상관분석 소프트웨어가 있습니다.

출처 : OWASP Top 10 - 2017

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

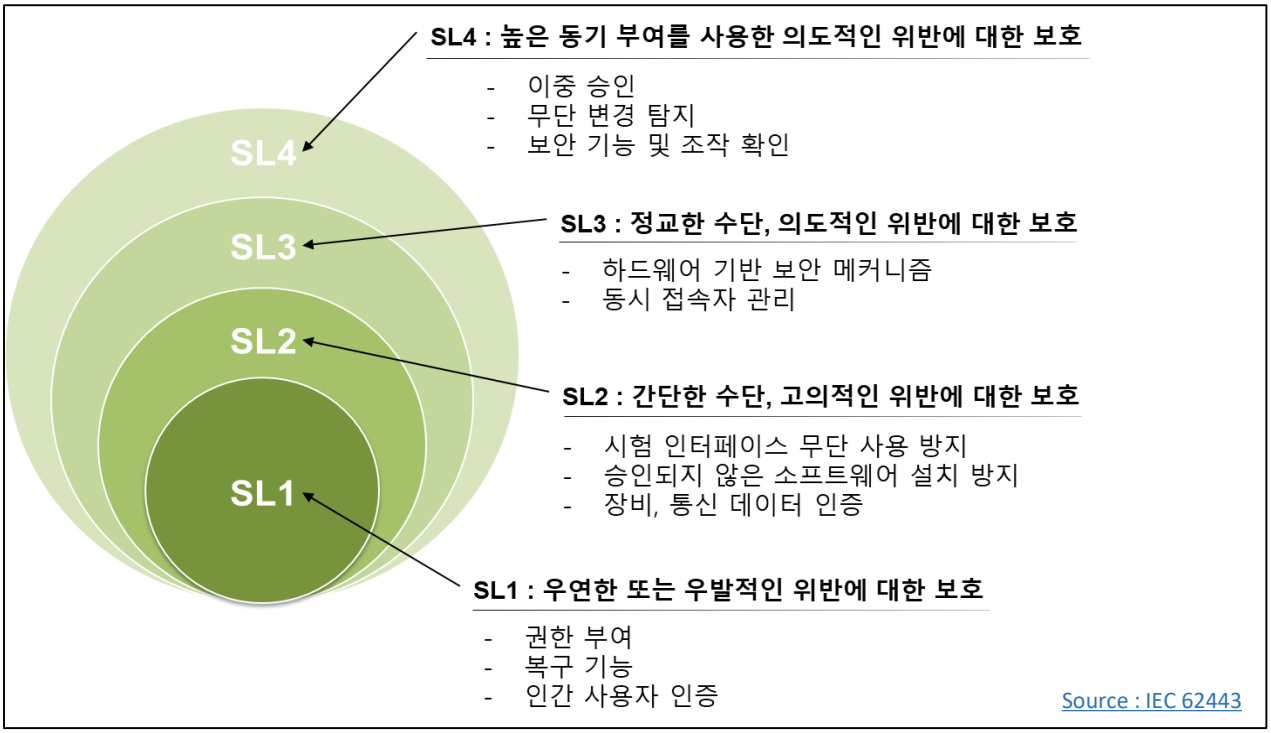
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<KR 사이버보안 형식승인 지침의 구성>

제1절 : 일반사항	제5절 : 데이터 기밀성	제9절 : SW 애플리케이션 요건
제2절 : 식별 및 인증	제6절 : 제한된 데이터 흐름	제10절 : 임베디드 장비 요건
제3절 : 사용 제어	제7절 : 사고에 대한 적시 대응	제11절 : 호스트 장비 요건
제4절 : 시스템 무결성	제8절 : 리소스 가용성	제12절 : 네트워크 장비 요건

Source : http://www.krs.co.kr/KRRules/KRRules2019/data/data_other/ENGLISH/gc31e000.pdf

보안등급(SL, Security Level)의 이해



Source : IEC 62443

한국선급 해상 사이버보안 형식인증 검사항목

암호화 사용 (503)

암호화 적용 시 국제적으로 인정되고 입증된 보안 관행 및 권장사항에 따라 암호화 보안 메커니즘을 사용하여야 한다. (SL1,2,3,4)

암호화 적용을 위한 가이드라인

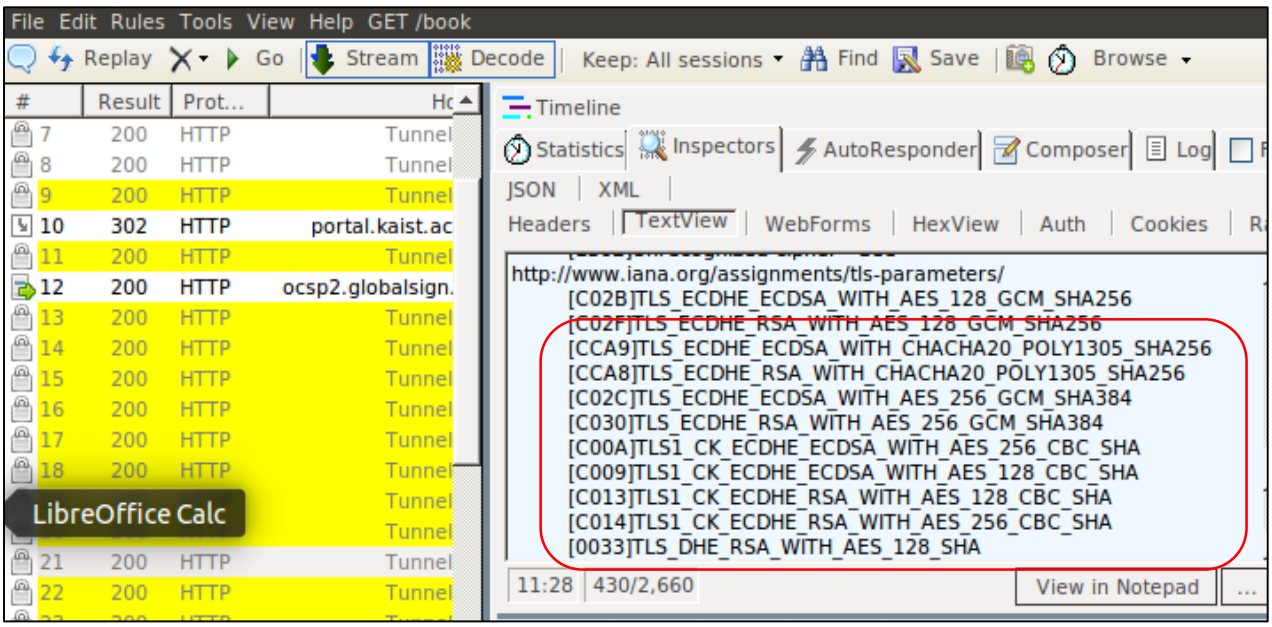
암호화(encryption)는 데이터의 원래 의미를 확인하거나 사용하지 못하도록 암호를 이용하여 그 형태를 바꾸는 것을 의미하며 복호화(decryption)은 암호화된 데이터를 원래의 상태로 복원하는 변환을 의미한다. (출처 : NIST SP : 800-82)

암호화는 중요 데이터의 저장, 내외부 통신 데이터, 백업 등 여러 부문에서 사용될 수 있으며 기밀성을 보호하기 위한 좋은 방법이지만 취약한 것으로 판명된 알고리즘은 사용하지 않아야 한다.

암호화 사용에 대한 최소 요구 사항은 다음과 같다.

1. 취약한 것으로 판명된 알고리즘(MD5, SHA-0, SHA-1, DES, 3DES)은 사용되지 않아야 한다.
2 비대칭키를 사용하는 경우 2048 bit 이상의 키 길이를 사용하고 RSA 혹은 그 이상의 강도로 암호화 하여야 한다.
3 대칭키를 사용하는 경우 256 bit 이상의 키 길이를 사용하고 AES 혹은 그 이상의 강도로 암호화 하여야 한다.

암호화 사용에 대한 요구 사항은 SL 1,2,3,4 공통 요구 사항으로써 한국선급에서는 사이버보안 형식승인을 받고자 하는 시스템은 취약한 것으로 판명된 암호화 알고리즘이 사용되지 않았음을 입증하도록 요구하고 있다.

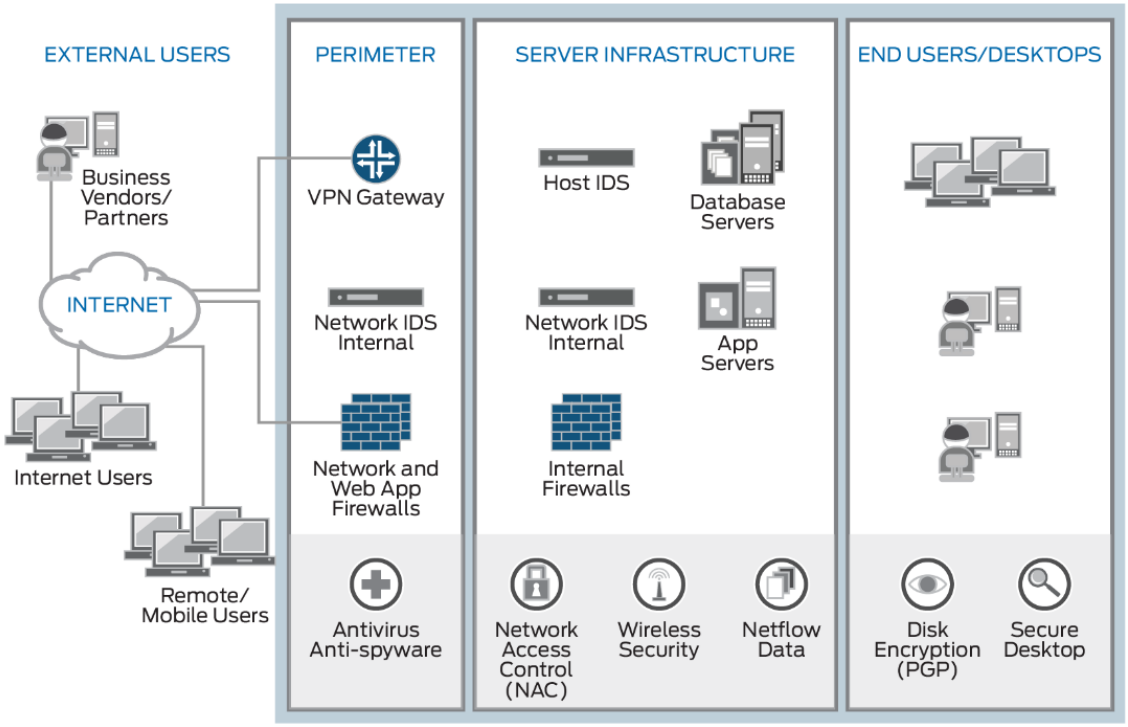


<암호화 진단 도구 중 하나인 FIDDLER를 이용한 암호화 확인의 예시>

용어 설명

SIEM

SIEM(Security Information and Event Management) 소프트웨어는 경계부터 최종 사용자까지 전체 범위에서 로그를 수집, 저장 및 분석한다. 종합적인 보안 보고 및 규제 준수 관리와 함께 신속한 공격 탐지, 차단 및 응답을 위해 보안 위협을 실시간으로 모니터한다. SIEM 소프트웨어는 네트워크 전반의 소스에서 생성되는 이벤트 레코드를 로깅함으로써 보안 이벤트의 장기적 분석과 함께 실시간 보고 기능을 통해 조직의 IT 보안에 대한 포괄적 방어 체계를 제공한다. 출처 : https://www.juniper.net



암호화

- 해쉬함수(복호화 불가) : 임의길이 정보를 입력 받아, 고정된 길이의 암호문(해쉬값)을 출력하는 암호기술로 암호화된 정보는 복호화가 불가능한 특징을 가진다. 저장된 암호문(해쉬값)을 가지고 원래의 사용자 비밀번호를 알 수 없기 때문에 안전한 비밀번호 관리가 가능해진다. (예 : SHA-512)
- 블록암호 알고리즘(복호화 가능) : 주민등록번호, 계좌번호 등을 일정한 블록 크기로 나누어, 각 블록을 송수신자간에 공유한 비밀키를 사용하여 암호화하는 방식이다. (예 : AES 256)

출처 : KISA, 암호기술 구현 안내서