KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 016

August 2019

KR, 펜타시큐리티㈜와 선박 사이버보안 업무협약 체결

한국선급과 펜타시큐리티시스템(주)는 지난 7월 31일, 펜타시큐리티 본사에서 양사 관계자가 참석한 가운데 '선박 사이버보안 기술 솔루션 적용 및 검증에 관한 공동연구' 양해각서(MOU)를 체결했다. 이번 협약에 따라 양사는 한국선급의 해상 사이버보안 인증 역량과 펜타시큐리티의 사이버보안 기술역량을 바탕으로 선박에 적용 가능한 사이버보안 솔루션을 검증하게 된다. 또한 국제해사기구(IMO)의 MSC.428(98) 결의안으로 2021년부터 사이버보안 리스크 관리에 대한 요구가 강화될 것으로 예상됨에 따라 사이버보안 시스템의 리스크 분석 및 설계 안전성 평가 부문에서도 협력해나갈 예정이다.
한편 한국선급은 지난해 ISO 27001, IEC 62443 및 NIST Framework 등 국제 보안표준과 IMO 및 BIMCO의 해상 사이버보안 가이드라인 등을 준용하여 해상 사이버보안 인증 체계를 구축하였다. 이를 통해 회사 및 선박에 대한 사이버보안 인증 서비스와 선박의 네트워크 및 자동화 시스템 등에 대해 사이버보안 형식 승인 서비스를 제공하고 있다.
펜타시큐리티는 기업정보보안 분야에서 데이터 암호화, 웹 보안, 인증보안 제품과 서비스를 제공하며 국내 및 아시아-태평양 시장을 선도하고 있다. 2015년부터는 스마트 자동차, 스마트 그리드, 스마트 팩토리 등 사물인터넷 환경에서 필요한 보안기술을 제공하여 차세대 융합보안으로 사업범위를 확장하고 있으며, 최근에는 암호화폐 지갑과 거래소의 보안, 블록체인 기반의 데이터 공유 플랫폼 개발 등을 통해 미래 블록체인 환경에 대한 표준을 제시하고 있다.

해상 사이버 보안의 보험시장 동향

BIMCO, 해상 사이버보안 사고보험의 표준조항 발표

BIMCO(발틱해국제해운협회)는 지난 5월에 해상 사이버사고 보험의 표준조항을 발표하였다. 사이버사고로 인한 전 세계 해운업계의 손실위험을 대비하기 위함이다. BIMCO는 그동안 "선박 사이버 보안에 관한 산업 지침"을 배포하였고, IMO에 적극적으로 참여하여 해상 사이버 보안 이슈를 주도하고 있다. 해운업계의 사이버보안 리스크를 해소하기 위한 노력으로 사이버 보안사고의 책임, 부채 및 의무 등을 사이버사고 보험 계약서에 사용할 수있도록 표준조항을 개발하였다. BIMCO 표준조항의 주요내용은 아래와 같이 세 가지 중요한 기능으로 요약할 수 있다.

첫 번째는 사이버 사고위험에 대한 인식을 높이는 것이다. 두번째는 당사자들이 사이버 사고가 발생할 위험을 최소화하기 위해 절차와 시스템을 마련 할 수있는 메커니즘을 제공하는 것이다. 세번째는 당사자들이 사이버 사고 발생시, 그 영향을 완화하고 해결하는 동시에 서로를 돕기 위해 협력하는 것다. BIMCO의 표준조항은 광범위한 계약에 사용하도록 설계되었다. 브로커와 에이전트 같은 타사 서비스 제공 업체와의 계약을 다룰 수 있을 것이라고 한다. 보험비용 청구에 대한 당사자 간의 책임은 협상 중에 합의 된 금액으로 제한되고, 다른 금액이 삽입되지 않은 경우 미화 100,000 달러가 적용되도록 하였다.

출처 : https://www.bimco.org/news/priority-news/20181121-cyber-security-clause

영국 Beazley보험사, 해상 사이버 보험상품 출시

영국의 해상보험회사 Beazley는 선박 소유자 및 운영자를 대상으로하는 새로운 특정 해상 사이버 보험 상품을 출시하여 해상 사이버 사고가 선박의 운영 능력에 영향을 미치는 경우 물리적 손상 및 고용 손실에 대한 보험을 제공한다고 밝혔다.

이 회사는 자가평가 설문지, 사이버보안 워크숍, 선박 사이버 검사가 포함된 사이버 리스크관리 서비스를 제공할 예정이다. Beazley사는 이번 상품 출시를 통해 사이버 사고 발생 가능성을 줄일 수 있을 것으로 보고 있으며, 이 정보를 국제해사기구(IMO)에 제공함으로써, 2021년 1월 1일 발효예정인 사이버보안 리스크 관리강화에 대한 지침 준수를 지원할 수 있을 것이라고 하였다. 또한, 선박의 OT시스템과 IT시스템이 점차적으로 상호연결됨에 따라 인적오류의 위협도 증가하고 있으며, Beazley사의 사이버보험은 이러한 인적오류로 인한 사고 위험을 줄이고, 보상은 소유자에게 명확한 보상한도를 제공할 예정이다.

출처 : https://smartmaritimenetwork.com/2019/05/17/marine-cyber-insurance-product-launched/

미국 LA항만, 신규 사이버보안 연합센터 설립

미국 LA항만, 신규 사이버보안 연합센터 설립 계획 발표

미국 LA 항만 당국은 LA 항만의 " 사이버 보안 연합센터“ 신규운영을 위한 RFP를 발표하였다. 이는 항만 내 다양한 이해 관계자들의 사이버 방어 활동을 조정하여 사이버 공격으로 인한 위협을 줄이도록 요구하고 있다. 이 센터가 설립되면 터미널 및 다른 항만 파트너가 공격 후 작업을 복원하는 데 사용할 수 있는 정보 리소스를 제공할 예정이다. 이는 실시간 위협 알림과 함께 이해 당사자 의 모바일 장치 등을 통해 액세스 할 수 있는 안전한 사이버 위협 데이터 포털의 형태를 취할 것으로 보고 있다. 항만 경찰서 책임자인 Thomas Gazsi는"사이버 위협 정보를 협력적으로 공유하는 것은 우리 항만의 안전과 보안에 매우 중요하다.“ 라고 하였다. 이 사이버보안 연합센터를 통해 해양 공급망에 위협이 되는 사이버 사고를 종전보다 신속하게 식별하고 완화 될 수 있다. LA 항은 이미 항만 당국의 자체 내부 운영에 중점을 둔 최초의 사이버 보안 운영 센터(CSOC)를 보유하고 있지만, 기존 사이버 센터를 포함하여 항구의 모든 이해당사자가 참여하는 새로운 사이버보안 연합센터를 별도의 조정기관으로 운영하려 한다. 사이버보안 연합센터는 기존 사이버 운영센터(CSOC)를 대체하는 것이 아니며, 항만 내 이해관계자들의 시스템에 대한 간섭, 방해, 부담도 없을 것이라고 한다. 이해당사자들은 사이버보안 연합센터의 정보를 어떻게 사용할지를 결정할 수 있는 통제권을 갖게 될 것으로 보인다.

특히 LA항만의 사이버 보안은 고생산성, 고자동화 컨테이너 터미널에 대한 심각한 고민거리이다. 2018년, 사이버 공격은 롱비치 항구의 Pier J 터미널을 포함한 미국의 여러 지역에서 중국의 해양 운송업체 코스코의 이메일과 전화 시스템에 영향을 미쳤다. 2017년, "Not-Petea" 사이버 공격은 전세계의 여러 항구에서 APM 터미널의 운영을 2주 동안 약 20% 감소시키고 약 2억 달러에서 3억 달러의 경감과 사업 손실을 초래했다.

출처 : https://www.maritime-executive.com/article/port-of-la-stands-up-cybersecurity-coordination-center

[기획시리즈]①

5G와 해양산업의 파급효과, 그리고 사이버 위협

본 기획시리즈는 4차산업혁명과 관련한 핵심 통신인프라인 5G가 해양산업에 미칠 긍정적 파급효과와 이에 따른 사이버 위협에 대해 다뤄보고자 한다. 따라서 본 뉴스레터 2019년 8월호에서는 ***'5G란 무엇인가?'와 5G 기술의 대표적 사이버 위협 시나리오***를 소개한다.

기획시리즈 순서

① 5G란 무엇인가?

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

③ LTE의 중앙집중형 네트워크와 5G의 분산형 네트워크의 비교

④ 5G 표준에서 무선백홀 기술과 5G 위성의 역할

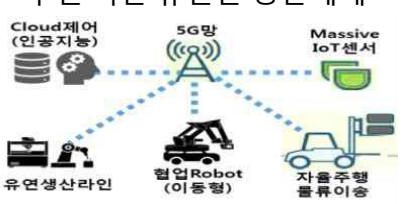
⑤ 선박과 항만에 효과적으로 활용하기 위한 5G 표준의 Private Network 참조모델

5G란 무엇인가?

5G는 데이터 송·수신 용량과 속도 관점에서 유·무선간 차이가 없을 정도의 빨라진 '이동 통신 환경'과 기기 사용에 있어 저전력성 및 많은 기기들이 접속하는 환경에서도 서비스의 안정성을 보장하는 'IoT 통신환경'을 동시에 구현할 수 있는 이동통신 기술 방식'이다.

보통 새로운 세대의 통신 기술이 등장하면 가장 흔하게 등장했던 표현이 "영화 한편 다운로드에 몇 초" 라는 표현이다. 하지만 5G는 단순히 통신속도 향상이 목적인 기술이 아니라 자동차, 철도, 도시, 공장 등 기다양한 산업에서 필요한 요구사항을 기반으로 만들어진 ICT 융합 기술이다.

핵심성능		4G	5G	4G 대비
초고속	최대 전송속도	1 Gbps	20 Gbps	20배
초저지연	전송지연	100분의 1초	1,000분의 1초	1/10
초연결	최대 기기 연결수	십만개/km^2	백만개/km^2	10배

[초고속] 실감미디어	[초저지연] 자율주행차	[초연결] 스마트공장
360° 입체무선 홀로그램	안전한 완전자율주행(Level4)	무선 기반 유연한 생산체계
		

출처 : http://www.gokea.org/bbs/down.php?file_no=20262

5G란 무엇인가?(Continue page)

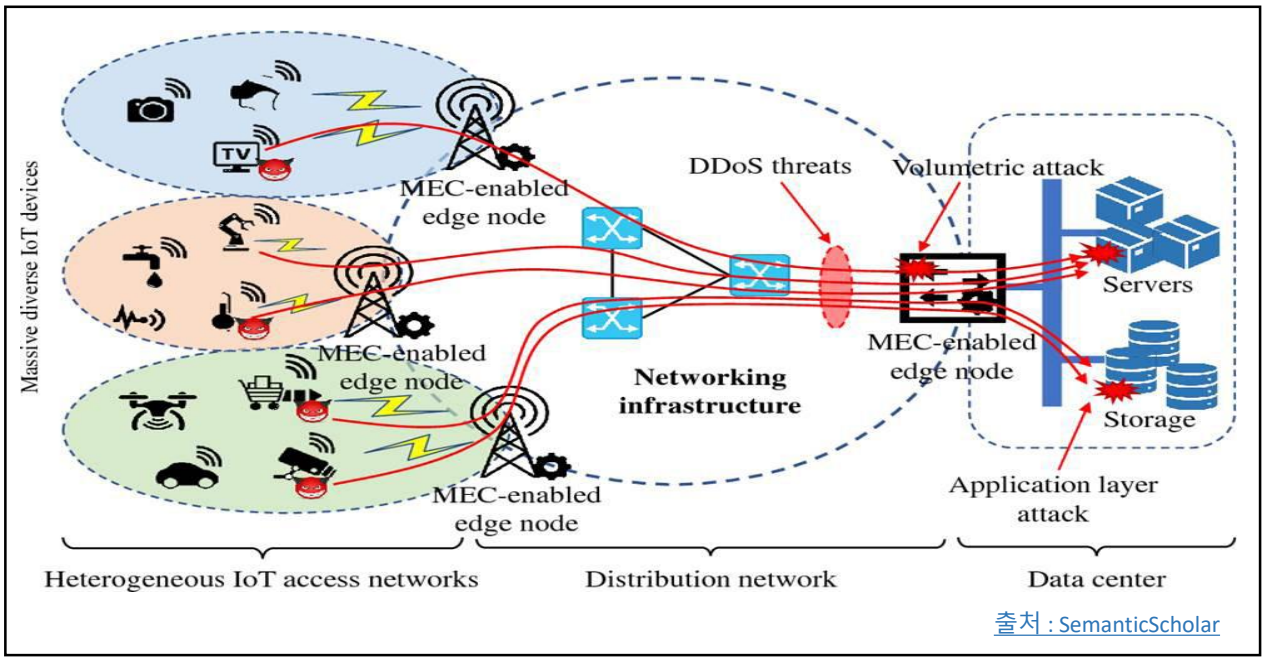
5G가 선박, 해상 IoT, 항만 등에 해상환경에 어떻게 적용될 것인지에 대해 알아보기 위해 5G의 몇 가지 특징을 간단히 소개하고, 다음 뉴스레터 호에서 좀 더 자세히 알아보려 한다.

- **네트워크 슬라이싱(Network Slicing)** : 동일한 물리적 네트워크 인프라에서 가상회되고 , 독립적인 논리 네트워크의 다양화가 가능하며, 해양산업에서는 네트워크 슬라이싱을 통해 선박, 해양 IoT 기기 등 해상환경에 맞는 5G 통신의 요구사항을 가질 수 있다.
- **시간지연에 민감한 서비스(Mission Critical Service)** : 5G의 저지연성과 고신뢰성(URLLC, Ultra Reliable & Low Latency Communications) 기술로 재난통신, 자율주행차, 철도통신 등에 활용하고 있으며, 선박 간 출돌예방을 위한 서비스에 활용이 가능할 것이다.

출처 : https://www.3gpp.org/DynaReport/22819.htm

5G의 사이버보안 위험요소 - 5G의 초연결로 인한 DDOS 공격 가능성

5G 통신망은 기존 통신망이 각 산업별, 용도별 서로 폐쇄적이던 것과 달리, 5G는 모든 산업들이 하나의 통신망으로 연결될 수 있도록 설계되었다. 이를 네트워크 슬라이싱 방식이라 하며, 하나의 망을 통신, IoT, VR, 자율주행 등 가상 전용망으로 나누어 통신한다. 하지만 물리적으로 모든 기기가 5G로 연결되기 때문에 매우 빠른 속도로 악성코드가 전파되거나, 정반대로 감염된 대량의 기기로부터 기지국이 DDoS 공격을 받을 가능성이 높아 지는 것이다. 5G 표준을 제정하는 국제표준단체인 3GPP는 이러한 위협 가능성을 고려하여 5G 네트워크망을 설계하였으나, 점차적으로 진화하는 공격자(Attacker)들로 부터 5G의 초고속, 고밀도 특징을 이용한 사이버 공격을 방어하기 위해 블록체인, 양자암호 등 다양한 방식의 새로운 보안 기술들에 대한 시장이 크게 확산될 것이다.



출처 : SemanticScholar

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 '**A7 : 2017 – 크로스 사이트 스크립팅 (XSS)**' 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 'A7 : 2017 - 크로스 사이트 스크립팅'

1. 크로스사이트 스크립트란?

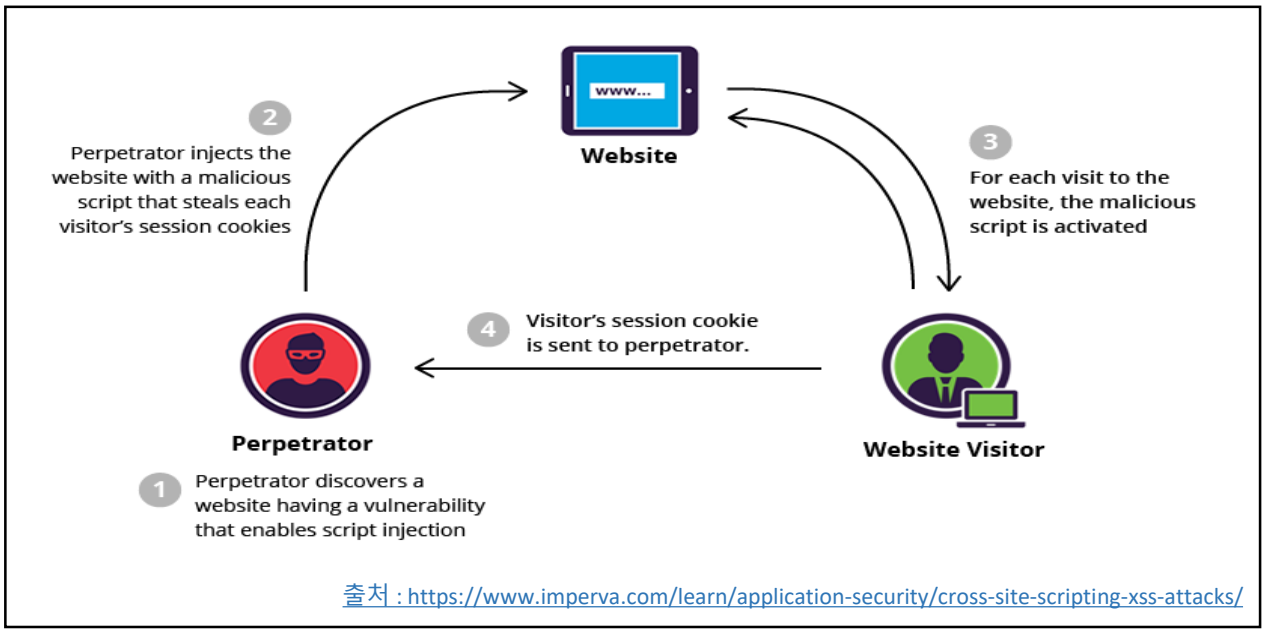
크로스 사이트 스크립팅(XSS)는 애플리케이션에서 브라우저로 전송하는 페이지에서 사용자가 입력하는 데이터를 검증하지 않거나, 출력 시 위험 데이터를 무효화 시키지 않을 때 발생한다"라고 정의되어 있다. 즉 공격자가 의도적으로 브라우저에서 실행될 수 있는 악성 스크립트를 웹 서버에 입력 또는 이것을 출력 시 위험한 문자를 중성화시키지 않고 처리하는 애플리케이션의 개발 과정에서 발생한다. XSS는 일반적으로 자바스크립트에서 발생하지만, VB 스크립트, ActiveX 등 클라이언트에서 실행되는 동적 데이터를 생성하는 모든 언어에서 발생이 가능하다. 이와 같이 XSS 취약점은 비교적 쉽게 공격할 수 있으며 웹 애플리케이션 개발 시 제거되지 않아 매우 광범위하게 분포되고 있다고 할 수 있다. 그래서 이 취약점을 이용한 악성 스크립트 배포 및 이를 통한 악성코드 배포 및 클라이언트 프로그램 해킹 등 현재도 개인 및 조직의 보안에 큰 위협이 되고 있다.

2. 크로스사이트 스크립팅 공격의 종류

1) 저장 XSS 공격

저장 XSS 공격은 웹 애플리케이션 취약점이 있는 웹 서버에 악성 스크립트를 영구적으로 저장해 놓는 방법이다. 이 때 웹 사이트의 게시판, 사용자 프로필 및 코멘트 필드 등에 악성 스크립트를 삽입해 놓으면, 사용자가 사이트를 방문하여 저장되어 있는 페이지에 정보를 요청할 때, 서버는 악성 스크립트를 사용자에게 전달하여 사용자 브라우저에서 스크립트가 실행되면서 공격한다.

출처 : www.kisa.or.kr/uploadfile/201312/201312161355109566.pdf



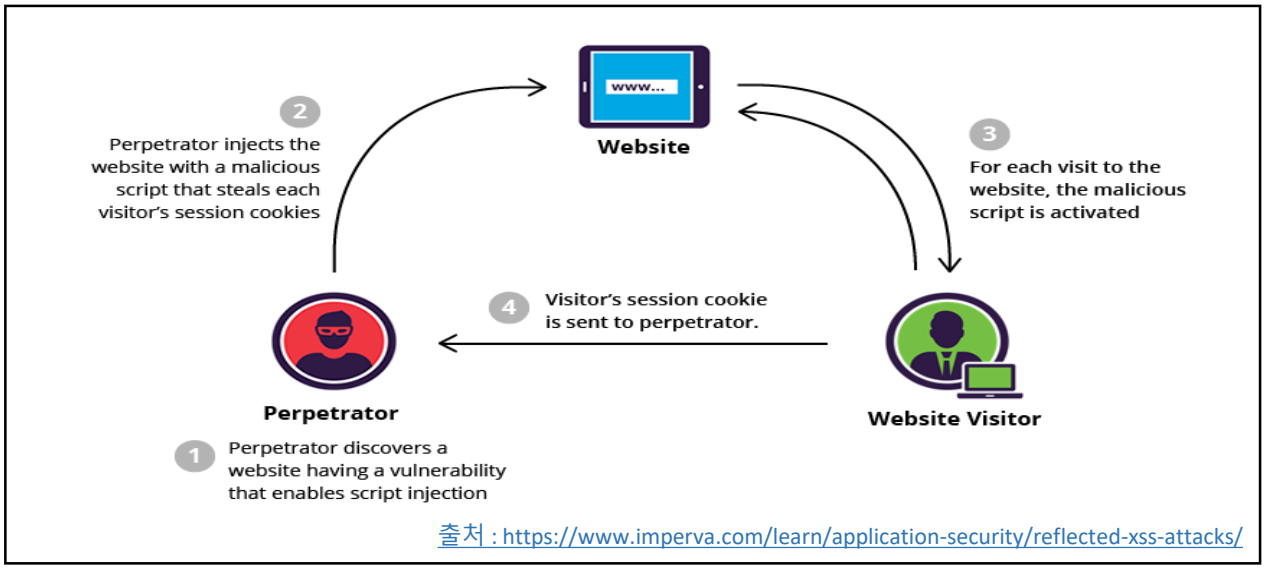
출처 : https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/

2) 반사 XSS 공격

반사식 XSS 공격은 웹 애플리케이션의 지정된 변수를 이용할 때 발생하는 취약점을 이용하는 것으로, 검색 결과, 에러 메시지 등 서버가 외부에서 입력받은 값을 받아 브라우저에게 응답할 때 전송하는 과정에서 입력되는 변수의 위험한 문자를 사용자에게 그대로 돌려주면서 발생한다.

일반적으로 서버에 검색 내용을 입력하면, 검색 결과가 있는 경우에는 결과 값을 사용자에게 전달하지만, 서버에서 정확한 결과가 없는 경우 서버는 브라우저에 입력한 값을 그대로 HTML 문서에 포함하여 응답한다. 이 경우 HTML 페이지에 포함된 악성 스크립트가 브라우저에서 실행이 된다.

출처 : www.kisa.or.kr/uploadfile/201312/201312161355109566.pdf



출처 : https://www.imperva.com/learn/application-security/reflected-xss-attacks/

3) 취약점 확인방법 및 보안대책

취약점 확인 방법

일반적으로 사용자의 브라우저를 목표로 하는 세 가지 형태의 크로스 사이트 스크립팅(XSS)이 있습니다:

리플렉티드 XSS: HTML 출력의 일부로써 유효성이 확인되지 않고, 특수문자가 필터되지 않은 사용자 입력이 애플리케이션 혹은 API에 포함됩니다. 공격이 성공하면 공격자는 피해자의 브라우저에서 임의의 HTML과 자바스크립트를 실행할 수 있습니다. 전형적으로 사용자는 악의적인 워터링 홀 공격을 수행하는 웹 사이트, 광고 사이트 혹은 이와 유사한 공격자에 의해 제어되는 페이지를 가리키는 몇몇 악의적인 링크와 상호 작성을 해야 할 필요가 있습니다.

저장 XSS: 응용 프로그램 또는 API에서 나중에 다른 사용자 또는 관리자가 볼 수 있는 정제되지 않은 사용자 입력값이 저장됩니다. 저장 XSS는 종종 높은 혹은 중대한 위험으로 간주됩니다.

DOM 기반 XSS: 페이지에 공격자가 제어 가능한 데이터를 동적으로 포함할 수 있는 자바스크립트 프레임워크, 한 페이지 애플리케이션, 그리고 API는 DOM 기반 XSS에 취약합니다. 이론상으로 애플리케이션은 안전하지 않은 자바스크립트 API로 공격자가 제어 가능한 데이터를 보내지 않습니다.

전형적인 XSS 공격은 세션 도용, 계정 탈취, 다중 요소 인증 우회, 트로이목마 악성코드 배포 로그인 패널과 같은 DOM 노드 대체 혹은 변조, 악성코드 다운로드, 키 로깅, 그리고 다른 클라이언트 측면의 공격과 같은 사용자 브라우저에 대한 공격을 포함합니다.

보안 대책

XSS를 방지하려면 신뢰할 수 없는 데이터를 사용 중인 브라우저 컨텐츠와 분리해야 합니다. 이것은 다음에 의해 달성될 수 있습니다:

- 최신 Ruby on Rails, React JS와 같이 XSS를 자동으로 필터링 처리하는 프레임워크를 사용합니다. 각 프레임워크의 XSS 보호의 한계를 알아보고 다루지 않은 사용 사례들을 적절히 처리하기 바랍니다.
- HTML 출력(본문, 속성, 자바스크립트, CSS 혹은 URL) 내 컨텍스트 기반으로 신뢰할 수 없는 HTTP 요청 데이터를 필터링하며 리플렉티드 및 저장 XSS 취약점이 해결됩니다. 요구되는 데이터 필터링 기술에 대한 상세 내용은 OWASP 치트 시트 'XSS 방어' 을 참고 바랍니다.
- 클라이언트 측에서 브라우저 문서를 수정할 때 상황에 맞는 인코딩을 적용하면 DOM XSS에 대해 대응할 수 있습니다. 이것으로 방어할 수 없는 경우, OWASP 치트 시트 'DOM 기반 XSS 방어' 에서 기술된 바와 같이 브라우저 API에 유사한 문맥 감지 필터링 기술을 적용할 수 있습니다.
- 컨텐츠 보안 정책(CSP)의 활성화는 XSS에 대한 심층적인 방어 통제입니다. 로컬 파일 첨부(예: 경로 조작 덮어 쓰기 또는 허용된 콘텐츠 제공 네트워크의 취약한 라이브러리)를 통해 악성코드를 배치할 수 있는 다른 취약점이 없는 경우라면 효과적입니다.

출처 : OWASP Top 10 - 2017

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

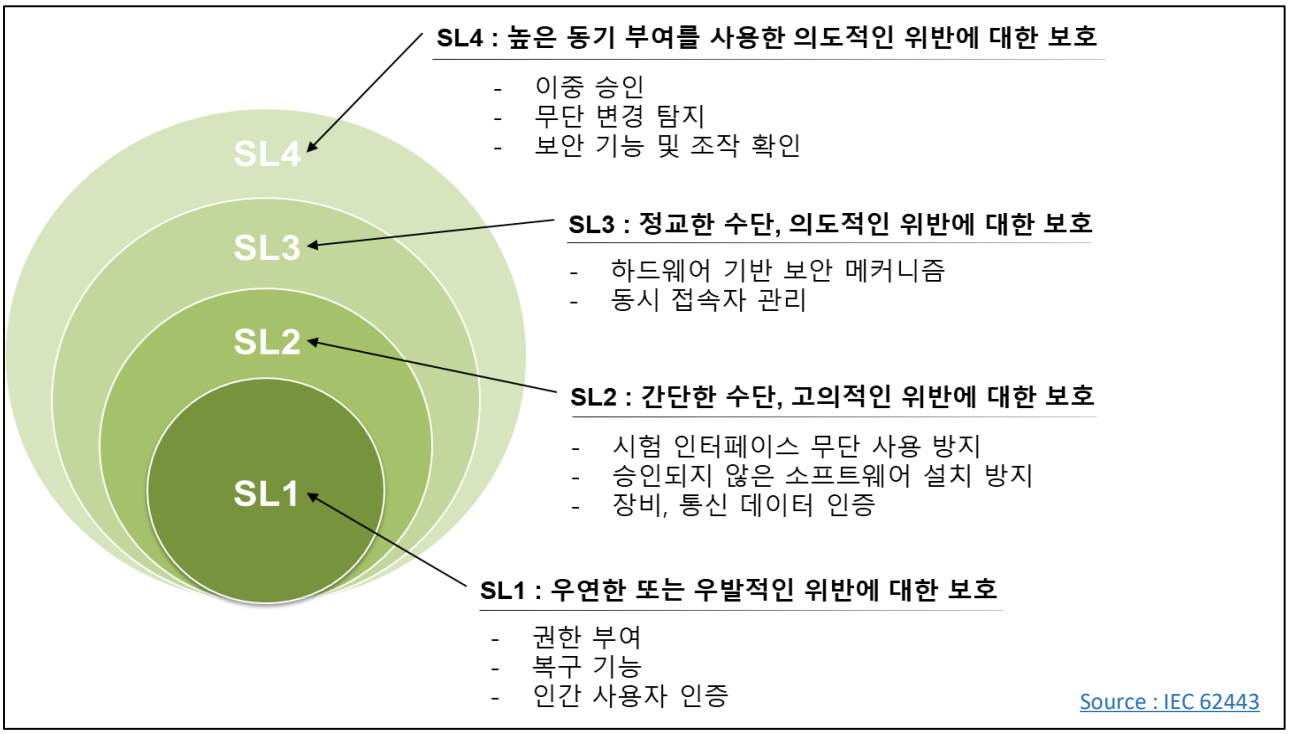
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<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

인간 사용자 식별 및 인증(201)

1. 구성품은 모든 인간 사용자 접속을 지원하는 모든 인터페이스에서 모든 사용자를 식별하고 인증할 수 있는 기능을 제공하여야 한다.(SL1)
2. 사용자 식별 및 인증이 신속한 현장 비상조치를 방해해서는 아니 된다.(SL1)
3. 구성품은 모든 인간 사용자를 고유하게 식별하고 인증할 수 있는 기능을 제공하여야 한다.(SL2)
4. 구성품은 구성품에 접속하는 모든 인간 사용자에 대해 다중요소 인증을 사용할 수 있는 기능을 제공하여야 한다.(SL3,4)

인간 사용자 식별 및 인증이란?

식별자 (Identifier)라 함은 신원을 주장하는 개체를 식별, 표시 또는 명명하는 보안 도메인 내에서 고유한 기호 패턴을 의미하며, 인증은 식별 요청에 대한 증명을 의미한다. 인간 사용자 식별 및 인증에서는 사이버보안 형식승인 대상 장비의 사용전 적합한 사용자 인지를 확인하는 기능을 요구한다.

'SL 1'에서는 우선 인간 사용자 접속이 가능한 모든 인터페이스에서 식별 및 인증을 하도록 요구한다. 이에 장비는 해당 요구사항에 대해 예외를 인정 할 수 있다. 대한 예시로는 HMI(Human Machine Interface)가 될 수 있다.

'SL 2'에서는 'SL 1'에 추가로 모든 인간 사용자를 고유하게 식별함을 요구하고 있다. 사용자 식별 및 인증은 역할기반 또는 그룹 기반일 수 있다. SL2 요건을 만족하기 위해서는 역할기반 또는 그룹기반의 식별자 구성일지라도 사용자 개인에 대한 개별적인 식별자를 만들고 관리할 것을 요구한다.

'SL 3, 4'에서는 추가적으로 다중요소 인증을 요구한다. 인증 팩터는 3가지 팩터로 나누어 진다. 사용자만 알고 있는 것(Something You Know)을 이용한 **지식기반 팩터**(eg. 패스워드, PIN 코드 등), 사용자만 소유하고 있는 것(Something You Have)을 이용한 **소유기반 팩터**(보안카드, OTP 등), 그리고 사용자만의 고유한 속성(Something You Are)을 이용한 **속성기반 팩터**(지문인식, 홍채인식 등)가 있다. 다중요소 인증은 2개 이상의 팩터를 이용하여 인증하는 방식을 의미한다.

지식기반 팩터	소유기반 팩터	속성기반 팩터
		

용어 설명

DDOS

'분산 서비스 거부' 또는 '분산 서비스 거부 공격'이라고도 한다. 여러 대의 공격자를 분산 배치하여 동시에 동작하게 함으로써 특정 사이트를 공격하는 해킹 방식의 하나이다. 서비스 공격을 위한 도구들을 여러 대의 컴퓨터에 심어놓고 공격 목표인 사이트의 컴퓨터시스템이 처리할 수 없을 정도로 엄청난 분량의 패킷을 동시에 범람시킴으로써 네트워크의 성능을 저하시키거나 시스템을 마비시키는 방식이다.

Edge node

에지노드는 클러스터 컴퓨팅에서 다른 노드와 통신하기 위한 최종 사용자 포털 역할을 하는 컴퓨터이다. 에지 노드는 간혹 게이트웨이 노드 또는 에지통신 노드라고도합니다.

HMI

HM(Human Machine Interface)는 사람과 자동화 된 시스템이 서로 어떻게 상호작용하고 , 소통하는가에 대한 모든 것을 말한다. HMI는 오랫동안 전통적인 기계에 국한되었지만, 이제는 컴퓨터와 디지털 시스템, 사물인터넷 (IoT)을 위한 기기와도 연관되어 점점 더 많은 기기들이 연결되고 자동으로 작업을 수행한다.