KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 024

April 2020

한국선급 활동

- 영국 선사 관리 선박에 사이버보안 적합성 인증서 최초 수여
- 2020년도 국가인적자원개발 컨소시엄 교육 과정 안내

무선 네트워크의 취약점 분석과 대응방안-2

사이버 위협의 이해(OWASP Top 10 Internet of Things)

KR 해상 사이버보안 형식승인 지침의 이해

용어 설명

영국 송가 쉽매니지먼트 관리 선박에 사이버보안 적합성 인증서 최초 수여

한국선급(KR, 회장 이형철)은 영국 해운선사인 송가 쉽매니지먼트(Songa Ship management)에서 관리하는 'SONGA HAWK' 선박에 사이버보안 적합성 인증서를 수여하였다고 밝혔다. 송가 쉽매니지먼트는 탱커선을 주요 선종으로 관리하는 선사로, 18년 한국선급과 회사 및 선박(23척)에 대한 사이버보안 인증계약을 체결한데 이어 19년 2월에 '회사 사이버보안 적합성 인증'을 획득한 바 있다.

송가 쉽매니지먼트 관리 선박 중 최초로 인증받은 'SONGA HAWK'은 △리스크관리 △자산관리 △사고 대응 및 복구 등 18개 부문의 81개 항목에 대해 한국선급의 검사를 통과하였다. 이번 'SONGA HAWK' 선박의 인증으로 국제해사기구(IMO) 규정, 탱커선 운영사 안전관리 평가(TMSA), 탱커선 안전성 평가(SIRE) 등 화주검사 사이버보안을 모두 만족함은 물론, 회사와 선박 모두 사이버공격 대응 및 보호 체계를 갖추고 있음을 공식적으로 인정받게 되었다.

최근 해사업계는 정보통신기술(ICT)이 폭넓게 적용됨에 따라 선사.항만.선박 등을 대상으로 한 해상 사이버공격 위험이 증가하고 있어 개별 선박 뿐 아니라 선사의 사이버보안 대응 및 관리에 대한 중요성이 점차 높아지고 있다. 또한 2021년부터는 국제해사기구(IMO)의 해사안전위원회 결의안(Resolution MSC 428(98))이 발효되어 선사.선박 사이버 리스크에 대한 요구가 더욱 강화될 전망이다. 박개명 한국선급 사이버인증 팀장은 "고객들이 효율적으로 사이버 리스크에 대응할 수 있도록 한국선급은 신조선 사이버보안 인증, 해상 소프트웨어 적합성 평가 등 관련 기술 서비스를 확대해 나가도록 노력하겠다."고 밝혔다.

해사 사이버보안의 이해

◈ 강좌구성 및 교육내용

강좌명	교육내용	강좌명	교육내용
해사 사이버보안 이해	•해사 사이버보안 개요 •해사 사이버보안 국제 동향(IMO, BIMCO) •사이버보안 공격 사례 •해사 사이버보안 가이드라인(선급) •한국선급 사이버보안 활동	인적 보안	•사이버보안 주요영역 •인적 보안 •인식 제고 및 교육
사이버보안 조직	•사이버보안 관리 체계 •해사 사이버보안 조직 및 역할 •해사 사이버보안 관리체계 통제 항목	물리 보안	•물리보안의 목적 및 방법 •KR 전산실 물리보안(사례) •리스크평가 물리보안(사례)
사이버 자산관리	•사이버 자산 관리 개요 •사이버보안 자산 식별 •자산 중요도 평가	기술 보안	•기술적 보안 : 네트워크 보안 솔루션 •기술 취약점 진단 개요 •PC 보안 취약성 진단 도구 (실적용 사례)
사이버 위협(Threat)	•해사 사이버 위협 •사이버 위협 : 10대 위협(BSI)		

◈ 교육일정

- 2020.05.26 총 8 시간(1일 8 시간) 09:00 ~ 18:00

◈ 교육대상자

- 선사 신입, 중간 관리자급, 기술자 및 연구원
- 선박 승선원(선원 및 사관)

해사 사이버보안 관리실무

◈ 강좌구성 및 교육내용

강좌명	교육내용	강좌명	교육내용
해사 사이버보안 실무 해설	•해사사이버보안개요 •사이버보안조직 •자산관리 •인적 보안 •물리 보안	해사 사이버보안 리스크 평가 이해	•선박 사이버보안과 리스크 평가 이해 •리스크 평가 절차 및 방법 이해 •네트워크 구성도, 리스크 허용기준, 사이버 위협 목록 이해
해사 사이버보안 IT 해설	•네트워크의이해 •네트워크 공격 기법과 보안 솔루션 •기술취약점 진단 개요	해사 사이버보안 리스크 평가 Workshop	•선사/선박 네트워크 구성도 작성 •자산목록 작성 및 평가 (실습) •선사/선박 사이버보안 리스크 평가(실습) •통제항목 비용/효과 평가
해사 사이버보안 IT 실습	•계정 및 권한 관리 실습 •사용자 보안(PC보안) 실습		

◈ 교육일정

- 2020.06.03~04 총 16 시간(1일 8 시간, 2일) 09:00 ~ 18:00

◈ 교육대상자

- 선사 사이버보안 담당자 (안전관리책임자, 보안책임자)
- 선박 사이버보안 담당자 (선장 도는 지정된 자)

한국선급의 국가인적자원개발 컨소시엄 교육은 컨소시엄 체결 기업의 재직자를 대상으로 무상으로 교육을 제공하고 있으며, KR 컨소시엄 홈페이지(http://champ.krs.co.kr)를 통해 확인 할 수 있습니다.

무선네트워크의 취약점 분석과 대응방안-2

본 기획시리즈는 일상생활과 회사, 선박 등에서 널리 사용되는 무선네트워크의 종류와 통신원리에 대해 알아보고, 무선 네트워크의 취약점과 대응방안을 소개하고자 한다. 따라서 본 뉴스레터 2020년 3월호에서는 ***'무선 네트워크의 취약점 분석과 대응방안'***에 대해 소개한다.

기획시리즈 순서

① 무선 네트워크의 종류와 통신원리
② 무선랜(WIFI)의 기술적 보안 취약점과 대응방안-1
③ **무선랜(WIFI)의 기술적 보안 취약점과 대응방안-2**
④ 무선랜(WIFI)의 기술적 보안 취약점과 대응방안-3
⑤ 기타 무선네트워크(Bluetooth, Zigbee 등)의 기술적 보안 취약점과 대응방안
⑥ 해상무선통신의 종류와 기술적 보안 취약점과 보안성 강화방안

사용자 인증의 보안취약점과 보안대책

SSID 기본설정의 취약점

무선랜 사용자 인증 메커니즘이 갖고 있는 취약성을 분석해 보고, 각 취약성의 대응방법을 알아보고자 한다. WIFI 사용자의 접속편의와 WIFI 신호 식별을 쉽게 하기 위해서 SSID 값을 기관의 이름이나 기억하기 쉬운 값으로 설정한다. AP는 기본설정으로 SSID를 브로드캐스팅 하고 있기 때문에 공격자가 단순히 AP 전파 수신영역 안에만 존재하면 , 브로드캐스트하는 SSID 값을 쉽게 알아낼 수 있다.

SSID 설정변경을 통한 보안대책

1. SSID 설정변경

사용자가 AP의 SSID 값을 브로드캐스트 하지 않도록 설정을 변경하면, SSID를 모르는 공격자로부터 AP에 연결 시도를 줄일 수 있다. 즉, 악의적인 공격자가 무선랜 분석도구를 이용하여 일정 무선 데이터를 분석하여야 하는 불편함을 주기 때문에 공격을 포기하도록 유도 할 수 있다.

2. 폐쇄시스템 운영

사용자가 AP의 SSID를 지정하지 않고 NULL 값으로 설정하면, 무선랜 단말기가 자동으로 자신에게 강한 신호를 보내는 AP에 접속을 요청하게 된다. 일부 AP에서는 SSID 값을 NULL로 하여 접속을 시도하더라도 연결요청을 차단하는 기능을 제공하고 있다.

이렇게 SSID 값을 NULL로 설정하여 AP에 접속을 요구하는 사용자를 차단하도록 운영하는 것을 폐쇄시스템이라고 한다.

출처 : KISA, 무선랜 보안 안내서

WEP 인증메커니즘의 취약점

1. 단방향 인증방식 제공으로 인한 취약성

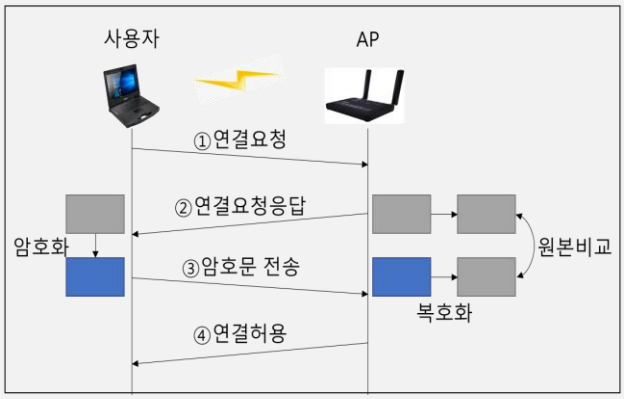
무선랜 WEP인증 매커니즘은 데이터 암호화와 사용자 인증이 편리하게 적용 할 수 있지만 AP에서 사용자를 단방향으로 인증하는 메커니즘 이기 때문에 많은 취약점이 존재한다. 특히 악의적인 공격자가 복제 AP를 이용하여 사용자의 정보를 탈취하는 사례가 발생하고 있다. 복제 AP를 이용한 사이버 공격 시나리오는 아래와 같다.

① 공격자가 정상적인 무선랜 환경에서 서비스를 제공하는 AP의 정보를 수집하여 같은 제조회사의 같은 모델을 이용해 정상 AP와 독같은 설정을 갖는 AP를 복제하여 구성한다.

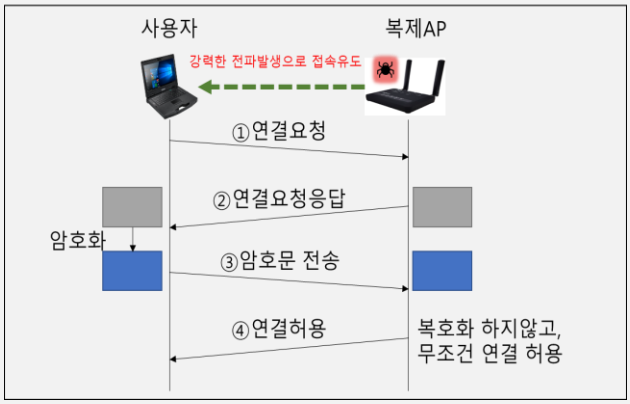
② 복제 AP는 정상 AP보다 더욱 강력한 전파를 송신하여 정상 사용자가 아무런 의심 없이 복제 AP에 접속을 요구하는 메시지를 보내게 만들고, 복제 AP는 응답 메시지를 통하여 거짓 인증요구를 한다.

③ 복제 AP의 공격자는 인터넷 패킷 정보를 수집하여 복제AP에 접속한 정상 사용자의 개인정보 등을 탈취할 수 있다.

<정상적인 WEP 인증절차>



<복제 AP를 통한 WEP인증 회피공격>



2. 고정된 공유키 사용으로 인한 취약성

WEP이 갖는 또 하나의 취약점은 무선랜을 사용하는 기관에서 WEP 키 값을 하나의 고정된 공유키를 사용하는 것이다. 무선랜을 사용하는 모든 장비, 즉 AP와 사용자 단말기 등에 동일한 키 값을 설정하여 서용해야 하고, 같은 값을 갖는 키의 사용으로 인해 WEP 키 값이 외부로 유출될 경우에 많은 보안 문제를 일으킬 수 있다. 예를들어, 무선랜을 사용하는 기관에서 하나의 고정키 값을 설정하여 사용하게 되면, 협력업체 직원, 방문객, 퇴사자 등에 의해서 WEP 값이 외부로 유출될 수 있다. 이러한 위험요소를 줄이기 위해서 WEP 값을 주기적으로 변경하여야 한다. 하지만, 무선랜을 사용하는 기관의 사용자 대부분은 외근을 하는 경우가 많아 변경된 WEP를 알려주는데 어려움이 발생하기 마련이다. 무선랜을 사용하는 기관은 하나의 WEP키를 이용하여 사용자 인증을 수행하기 때문에 WEP키가 외부로 유출될 경우에는 공격자가 습득한 WEP키를 이용하여 접속을 시도하므로 매우 위험하다.

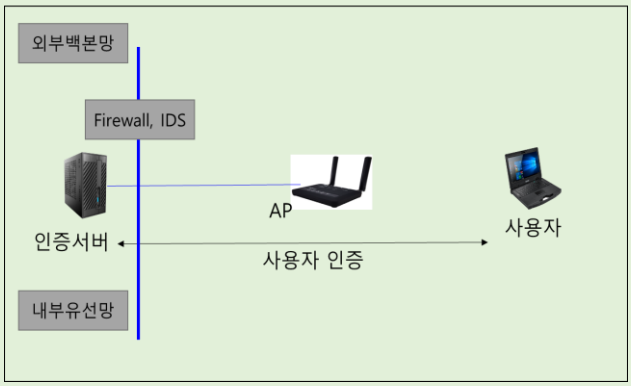
출처 : KISA, 무선랜 보안 안내서

WEP 인증의 보안대책

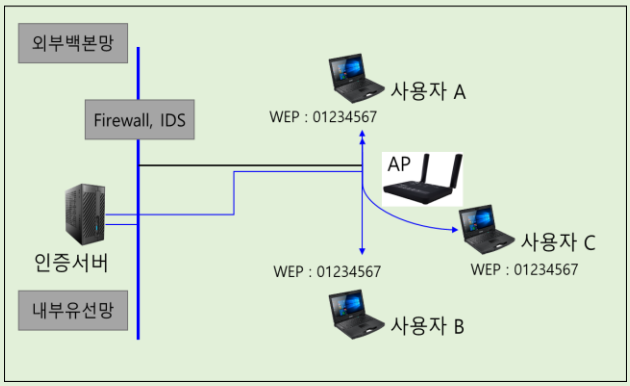
1. 동적 WEP 적용

고정된 공유키 값을 사용하게 되어 보안상 여러 가지 문제점이 발생하게 마련이다. 이러한 문제점을 줄이기 위해서 동적 WEP을 적용하여야 한다. 무선랜 환경에 인증 서버를 적용한 예를 보이고 있다. 인증서버가 사용자가 접속을 시도할 경우에 인증을 수행하고, 기관에서 사용하는 WEP 키의 설정과 갱신 등의 관리를 수행한다.

<인증서버를 이용한 동적WEP 적용>



<동적 WEP을 적용하여 연결을 설정한 예제>



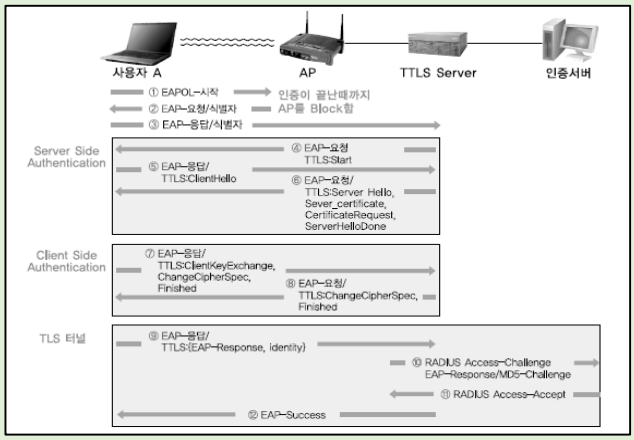
2. EAP-TTLS 인증

EAP-TTLS는 EAP-TLS와 CHAP(Challenge Handshake Authentication Protocol) 또는 OTP 등의 전통적인 암호 기반으로 하는 터널 방식의 인증 메커니즘이다. EAP-TTLS의 인증 절차를 나타내고 있다. TLS 터널을 형성하기 위해서 인증서버 앞단에 TTLS 서버가 이용되고 있다. 하지만 실제로는 TTLS 서버를 별도로 운영하지 않고, 인증서버에서 TTLS 서버의 기능도 함께 수행하는 것이 일반적이다.

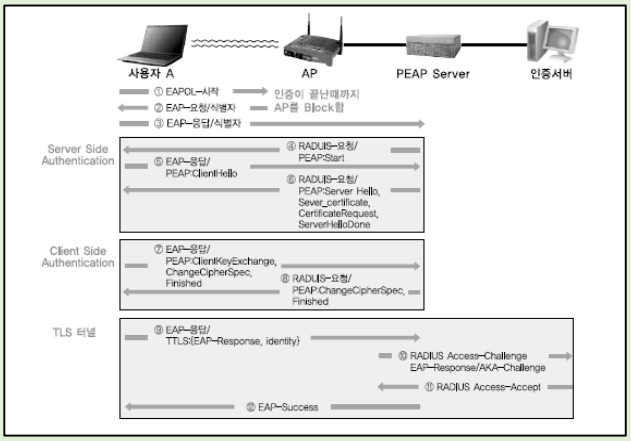
3. PEAP 인증

PEAP은 터널링 방식의 인증 알고리즘으로, 사용자 패스워드를 기반으로 하는 인증 방식이다. PEAP 서버를 이용하여 TLS 터널을 생성하고 이를 통한 인증서버와 사용자간의 인증이 이루어지는 것이 EAP-TTLS와 유사한다.

<EAP-TTLS 인증절차>



<PEAP 인증절차>



출처 : KISA, 무선랜 보안 안내서

사이버 위협의 이해(OWASP Top 10-사물인터넷)

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-사물인터넷 편

OWASP(Open Web Application Security Project)에 따르면 OWASP 사물 인터넷 프로젝트의 목표는 제조업체, 개발자, 소비자가 사물인터넷과 관련된 보안 문제를 더 정확히 이해하고 사용자가 IoT 기술을 구축, 배포 또는 평가할 때 보안 측면에서 더 현명한 의사 결정을 내리는데 도움을 제공하기 위함이다. 2020년 사이버보안 뉴스레터에서는 OWASP에서 선정한 사물인터넷(IoT)의 사이버 위협 Top 10과 대응방안을 살펴보고하 한다.

Top Ten	2014 IoT Top Ten	2018 IoT Top Ten
I1	Insecure Web Interface	Weak Guessable, or Hardcoded Passwords
I2	Insufficient Authentication/Authorization	Insecure Network Services
I3	Insecure Network Services	Insecure Ecosystem Interfaces
I4	Lack of Transport Encryption	Lack of Secure Update Mechanism
I5	Privacy Concerns	Use of Insecure or Outdated Components (NEW)
I6	Insecure Cloud Interface	Insufficient Privacy Protection
I7	Insecure Mobile Interface	Insecure Data Transfer and Storage
I8	Insufficient Security Configurability	Lack of Device Management
I9	Insecure Software/Firmware	Insecure Default Settings (NEW)
I10	Lack of Physical Hardening	Poor Physical Security

안전하지 않은 네트워크 서비스(Insecure Network Services)

사물인터넷(Internet of Things, IoT) 장치에서 안전하지 않은 네트워크 서비스는 정보의 무결성 또는 가용성을 손상시키거나 장치의 무단 원격제어를 위한 관문으로 사용될 수 있다. OWASP에서 IoT장치의 네트워크의 취약점 사례가 아직까지 발표된 사례가 없다. 따라서 IoT Security Foundation의 'IoT Security Compliance Framework(Release 1.0)'에서 선정한 IoT 장치에 대한 네트워크 서비스 보안 요구사항을 통해서 안전하지 않은 네트워크 서비스가 무엇인지와 그에 대한 개발자, 사용자 관점의 보안대책을 살펴볼 수 있다.

Req. No.	Requirement	Applicability
2.3.5.1	The product prevents unauthorised connections to it or other devices the product is connected to, at all levels of the protocols.	Mandatory
2.3.5.2	For products with multiple network interfaces, the uncontrolled ability to forward IP packets between the interfaces is disabled.	Mandatory
2.3.5.3	IP Traffic uses only secure protocols with no publically known vulnerabilities, such as TLS or TLS. Insecure and plaintext application layer protocols (such as ICMP, TELNET, FTP, HTTP, SMTP and NTP) are not used.	Mandatory
2.3.5.4	All the products' unused ports are closed and the minimal required number of ports are active.	Mandatory
2.3.5.5	If a connection requires a password for connection authentication, the default password or factory reset password is unique to each device.	Mandatory
2.3.5.6	Where a wireless interface has an initial pairing process, the passkeys are changed from the default prior to providing normal service.	Mandatory
2.3.5.7	For any WiFi connection, WPA2 with AES or a similar strength encryption has been used and insecure protocols such as WPA and TKIP are disable.	Mandatory
2.3.5.8	Where WPA2 WPS is used it has a unique, random key per device and enforces exponentially increasing retry attempt delays.	Mandatory
2.3.5.9	All network communications keys are stored securely.	Mandatory
2.3.5.10	Where the MQTT protocol is used, it is protected by a TLS connection with no known cipher vulnerabilities.	Mandatory
2.3.5.11	Where the CoAP protocol is used, it is protected by a DTLS connection with no known cipher vulnerabilities.	Mandatory
2.3.5.12	Where cryptographic suites are used such as TLS, all cipher suites shall be listed and validated against the current security recommendations.	Mandatory
2.3.5.13	All use of cryptography by the product, such as TLS cipher suites, shall be listed and validated against the import/export requirements for the territories where the product is to be sold and/or shipped.	Mandatory
2.3.5.14	Where there is a loss of communications it shall not compromise the integrity of the device.	Advisory
2.3.5.15	The product only enables the protocols necessary for the products' normal operation.	Mandatory

출처 : IoT Security Compliance Framework(Release 1.0), 2016

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

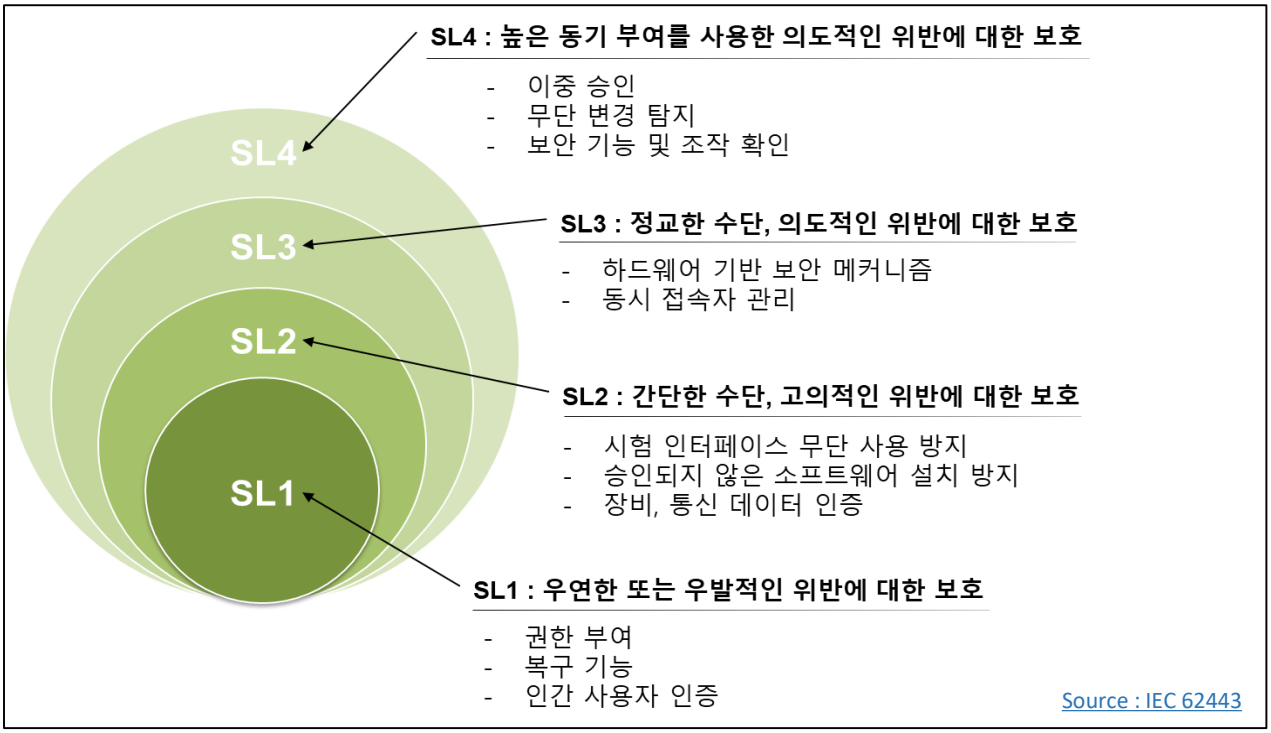
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<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

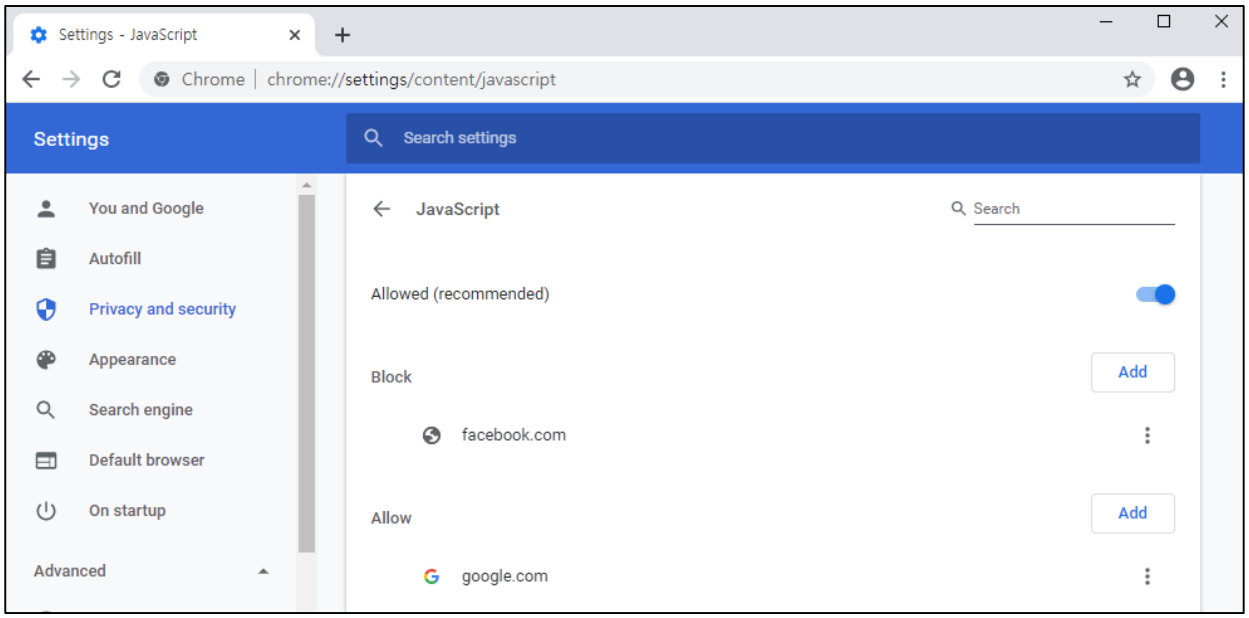
한국선급 해상 사이버보안 형식인증 검사항목

소프트웨어 애플리케이션 요건 – 모바일 코드 (901)

1. 소프트웨어 애플리케이션이 모바일 코드 기술을 이용하는 경우 보안 정책을 시행할 수 있는 기능을 제공하여야 한다.(SL 1)
2. 모바일 코드의 실행을 제어할 수 있는기능을 제공하여야 한다. (SL 2,3,4)

모바일 코드의 보안 통제

이동 코드라고도 불리는 모바일 코드(Mobile Code)는 수신자의 명시적인 설치없이 실행될 수 있는 프로그램을 말하며(출처 IEC 62443 4-2), 인터넷 익스플로러의 Active X, 크롬의 확장 프로그램들이 우리가 주변에서 접할 수 있는 모바일 코드의 예시이다. 모바일 코드 기술이 적용된 경우 해당 소프트웨어 애플리케이션에서는 모바일 코드의 보안 정책을 시행할 수 있는 기능을 제공하여야 한다.



<모바일 코드 보안 정책의 예시 – JavaScript의 실행/차단 기능 제공>

육상에서의 원격 모니터링 기능이 제공되며 모바일 코드 기술을 이용하는 경우 해당 소프트웨어 애플리케이션은 설치 및 실행 전 사용자 확인, 관리자 승인과 같은 실행 통제 기능, 코드의 실행전 무결성 검사와 같은 기능이 제공되어야 한다. 모바일 코드는 명시적인 설치는 없으나 기능을 수행하기 위한 파일들이 없는 것은 아니다.

크롬의 확장프로그램을 기준으로 로컬 드라이브에 저장되는 기본 위치는 다음과 같다.

%LOCALAPPDATA%\Google\Chrome\User Data\Default\Extensions\

윈도우 운영체제의 경우 실행화면(단축키 : 윈도우버튼 + R)을 통해 해당 위치를 입력할 경우 크롬의 확장프로그램이 저장되는 위치를 확인 할 수 있다

용어 설명

응용계층 프로토콜의 설명

- **MQTT(Message Queuing Telemetry Transport)** : MQTT 프로토콜은 대부분 저전력 배터리 등 제한적인 특정 환경에서 동작하기 때문에 낮은 전력, 낮은 대역폭 환경에서 사용할 수 있도록 설계되었다. 이러한 점 때문에 IoT에 사용하기 유용한 프로토콜이다.
- **ICMP(Internet Control Message Protocol)** : TCP/IP에서 IP 패킷을 처리할 때 발생되는 문제를 알려주는 프로토콜이다. 흔히 Ping test라고 부르는 것이 ICMP 프로토콜을 사용하여 네트워크의 연결상태를 모니터링하는데 쓰인다.
- **TELNET** : 포트가 접속 가능한지 확인 하는데 쓰이는 프로토콜이다.
- **FTP(File Transfer Protocol)** : 파일전송 프로토콜ㄹ호서, 서버와 클라이언트 사이의 파일 전송을 하기 위한 프로토콜이다.
- **HTTP(Hyper Text Transfer Protocol)** : WWW 상에서 정보를 주고받을 수 있는 프로토콜이다. 주로 HTML 문서를 주고받는 데에 쓰인다. TCP와 UDP를 사용하며, 80번 포트를 사용한다.
- **SMTP(Simple Mail Transfer Protocol)** : 인터넷에서 이메일을 보내기 위해 이용되는 프로토콜이다. 사용하는 TCP 포트번호는 25번이다.