KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 023

March 2020

싱가포르 선사 대상 맞춤형 사이버보안 교육 실시

한국선급은 2020년 2월 5일 ~ 7일, 싱가포르 해사청(MPA), ADK Maritime, Janus Shipping 등 싱가포르 내 5개 선사 38명의 선원 및 선사직원을 대상으로 맞춤형 사이버보안 인식제고 교육을 실시하였다. 한국선급은 그 동안 사이버보안 교육 활성화를 위해 싱가포르 해사청(MPA)의 교육 보조금 지원사업 참여를 위한 협의를 지속적으로 추진해 왔으며, 지난 1월, 싱가포르 해사청(MPA)에서 한국선급의 사이버보안 인식제고 교육 프로그램을 해양 클러스터 펀드의 교육 보조금 지원사업에 포함시키기로 결정하였다. 이 사업을 통해 싱가포르 내에 위치한 선사들이 한국선급의 사이버보안 인식 제고교육을 신청할 경우, 교육 비용의 50%를 싱가포르 해사청으로 부터 지원 받을 수 있어, 선사들의 교육비 부담을 줄일 수 있게 되었다. 한국선급의 사이버보안 인식제고 교육 프로그램은 사이버보안에 대한 포괄적인 이해, 해사 사이버위협 및 대응 현황, 해사 사이버 리스크 저감 방법 및 실제 적용사례, 사이버 자산 목록 작성 및 사이버리스크 평가 실습을 포함하여 OCIMF의 TMSA, SIRE 검사 외에 IMO 결의안 MSC.482(98)에 대응할 수 있는 정보 및 방법을 제공하고 있다.

한국선급은 선사 뿐만 아니라 조선소, 기자재업체를 대상으로 사이버보안 맞춤형 교육 서비스를 제공하고 있으며, 싱가포르 내에 위치한 회사 중 사이버보안 맞춤형 교육을 희망하는 회사는 2020년 5월에도 한국선급 아태지역본부를 통해 '제 2차 사이버보안 인식 제고 교육'을 신청하면, 저렴한 비용으로 한국선급의 사이버보안 인식제고 교육을 수강 할 수 있다.

싱가포르 해사청(MPA)에서 승인한 KR 사이버보안 교육 프로그램

Module 1. Maritime cyber security overview(1H)

- Understand the background of maritime cyber risks are increasing
- Understand the maritime cyber-attack surfaces : external and internal threat
- Understand the characteristics of ship IT / OT systems
- Understand the maritime cyber-attack cases
- Understand the international maritime cyber security trends such as IMO, BIMCO, IACS, UK Government, DMA (Danish Maritime Sector). OCIMF TMSA/SIRE, RIGHTSHIP, Flag State (Marshall Island)

Module 2. Administrative security(1H)

- Understand what is administrative security and sub-category
- Understand the necessity of establishing cyber security management system (CSMS), consideration and process of establishing CSMS
- Understand the necessity of establishing maritime cyber security organisation including cyber emergency team, role and responsibility through examples
- Understand the requirement of OCIMF TMSA element 13(Maritime security) and learn implementations through examples

Module 3. Cyber asset & cyber threat(1H)

- Identify cyber asset(IT/OT system) to be protected from the cyber threat
- Understand three elements of cyber security : Criticality, Integrity, Availability
- Understand maritime cyber threats and establishing cyber threat list

Module 4. Physical security(1H)

- Understand what is physical security and recognize its necessity
- Learn physical security implementations through best practice(KR server room)
- Learn physical security countermeasures identified through cyber risk assessment
- Understand the physical security requirement of OCIMF SIRE and learn implementations(port blocker, 3rd party control) through examples

Module 5. Technical security(1H)

- Understand what is physical security and recognize its necessity
- Understand network security equipment functionality : firewall, IPS/IDS, VPN
- Learn the difference between penetration test and vulnerability analysis
- Learn the onboard PC vulnerability analysis and implementations through examples

Module 6. Understanding of maritime cyber security risk assessment(1H)

- Learn the difference between general risk assessment and cyber risk assessment
- Learn the KR cyber risk assessment process and could establish own cyber risk assessment method

Module 7. Workshop(1H)

- Exercise each step of KR cyber risk assessment process through hands-on workshop
- Understand cyber threat, cause, consequence, existing control and proposed control through six hands-on scenario

CIRM 선박 항해통신 장비 관련 사이버보안 지침 발표

CIRM, 선박 항해통신 장비 관련 사이버보안 지침 발표

CIRM은 2020년 2월, 선박 항해통신 장비를 위한 사이버보안 가이드라인을 발표하였다. CIRM은 선박의 전자화사들을 위한 주요 국제 비정부기구(NGO)로서, 전 세계 30개국에서 110개가 넘는 회사를 회원으로 보유하고 있으며, 주요 국제회의(IMO, ITU, IEC, IALA 등)에서 폭넓은 활동을 하고 있다. 이번 CIRM의 사이버보안 가이드라인은 국제 해사업계에서 사이버보안에 대한 관심이 점차 증가함에 벤더들이 사이버보안을 구축하는 방법과 참고문서에 대한 정보를 제공하고 있다.

이번 CIRM의 사이버보안 가이드라인은 다음과 같은 두 가지 지침을 발표하였다.

- CIRM Cyber Risk Code of Practice for Vendors of Marine Electronic Equipment and Services
- CIRM Guideline on Implementing the CIRM Cyber Risk Code of Practice

본 규범은 공급업체가 안전한 디지털 해상 환경 구축을 위한을 6 가지 원칙으로 구성되며, 이 규범을 통해 공공급업체는 해양 및 기타 산업에서 파생된 효과적이고 비용효율적인 사이버보안 모범 사례를 구현할 수 있을 것으로 예상된다.

기본 원칙	상세 내용
#1 사이버 위험 표준, 권장 사항 및 지침 준수	▪ IMO, ISO, IEC, IACS에서 제공 한 표준 및 권장 사항을 준수하여 제품 및 서비스를 제공, 유지 및 관리
# 2 기본 사이버보안	▪ 사이버보안 기능이 활성화되도록 제품 및 시스템을 설정
# 3 기밀성	▪ 사이버보안 및 사이버보안 이벤트와 관련된 고객의 데이터 및 정보를 기밀로 취급
# 4 사이버리스크 관리 기반으로서의 품질	▪ 업계 표준 품질 관리 시스템 (예 : ISO 9001)의 원칙과 프로세스를 사용하여 제품 및 서비스를 설계, 개발 및 제공
# 5 소프트웨어 업데이트 및 취약점 처리	▪ 식별된 취약점을 리스크 평가를 통해 적절한 조치를 결정 ▪ 제품 및 서비스에 대한 지원이 제공되지 않는 날짜 공개 • 취약점, 위협 및 사이버 사건에 관한 공유
# 6 지속적인 개발	▪ 사이버 보안 조치 및 산업 표준의 지속적인 개발과 관련된 CIRM 활동에 적극적으로 참여

무선네트워크의 취약점 분석과 대응방안

본 기획시리즈는 일상생활과 회사, 선박 등에서 널리 사용되는 무선네트워크의 종류와 통신원리에 대해 알아보고, 무선 네트워크의 취약점과 대응방안을 소개하고자 한다. 따라서 본 뉴스레터 2020년 1월호에서는 ***'무선 네트워크의 종류와 통신원리'***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

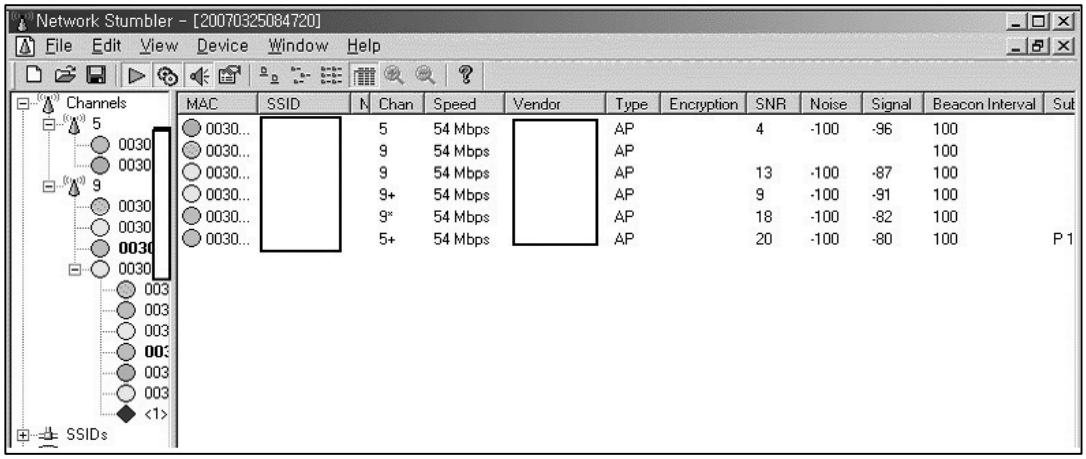
무선랜(WIFI)의 기술적 보안 취약점-1

무선 네트워크 기술 중에서 IEEE(Institute of Electrical and Electronics Engineers) 802.11 제품군에 정의된 무선랜(WIFI)의 기술적 보안위협과 조치방안을 살펴보고자 한다. 무선랜은 공기를 전송매체로 사용하는 서비스의 특성 상 많은 취약점이 존재한다. 또한 불특정 다수의 신호수신이 가능함으로 인해 도청이 가능하고, 무선전파를 전송하는 또한, 무선 장비에 대한 공격이 가능하다. 유선랜에서 존재하는 여러가지 공격 기법이 사용이 가능하다.

위협의 종류	설명
도청	무선랜의 가장 근본적인 문제점이 도청이다. 무선 AP에서 발송되는 전파의 강도와 지형에 따라 서비스가 필요한 범위 이상으로 전달될 수 있다.
서비스 거부(DoS) 공격	무선 서비스를 제공하는 무선 AP장비에 대량의 무선패킷을 전송하는 서비스 거부 공격을 통해 무선랜을 무력화 할 수 있다.
불법 AP(Rouge AP)	공격자가 불법적으로 무선 AP를 설치하여 무선랜 사용자들의 전송 데이터를 수집하는 것으로, 무선의 특성 상 정확한 불법 AP의 위치를 파악하는 것은 쉽지 않다.
취약한 무선 암호화 방식 사용	무선 데이터 암호화 방식으로 많이 사용되고 있는 WEP(Wired quivalency Protocol)는 짧은 길이의 초기벡터(IV)값과 불완전한 RC4 알고리즘의 사용으로 인한 취약점이 존재한다.
비인가 접근	무선랜의 인증절차가 설정되어 있지 않은 경우에는 SSID 값을 획득하고, 획득한 SSID 값을 무선 단말기에 설정하는 것만으로 무선랜 으로의 불법적인 접속이 가능하다.

1. 도청

무선랜의 가장 근본적인 문제점이 도청이다. 무선 AP에서 발송되는 전파의 강도와 지형에 따라 서비스가 필요한 범위 이상으로 전달될 수 있으며, 이 경우 외부의 다른 무선 클라이언트에서 무선 AP의 존재여부를 파악할 수 있고, 더불어 전송 무선 데이터의 수신을 통한 도청이 가능하게 된다. 도청은 기본적으로 무선랜 카드가 탑재된 클라이언트는 모두 가능하며, 도청에 이용되는 별도의 SW는 인터넷을 통해 손쉽게 구할 수 있는데, 이를 이용해 탐지되는 무선랜의 기본적인 구성을 파악할 수 있다. 아래 그림은 'Net Strumbler' 라는 SW로 무선랜의 구성요소인 SSID 정보, 무선랜 암호화 방식, 무선랜 속도, 신호감도 등의 정보를 확인 할 수 있다.



무선랜(WIFI)의 도청 대응방안

1. SSID 설정을 통한 접속제한

SSID는 AP가 제공하는 무선랜 서비스 영역을 식별하기 위해 사용하는 ID이다. 무선랜 서비스에 접속하려고하는 사용자는 현재 자신의 위치에서 접속이 가능한 무선랜 서비스를 식별해야 한다. 만약 SSID를 모르는 사용자는 무선랜 서비스에 대한 정보가 없기 때문에 무선랜 서비스에 접속을 시도할 수 없게 된다. 이러한 특성을 이용하여 무선랜 관리자가 SSID를 브로드캐스트 하지 않도록 설정하고, 인가된 사용자에게는 미리 SSID를 알려주어, 알려준 SSID로 연결을 시도하도록 한다면, SSID를 모르는 공격자로 부터 무선랜 도청을 방지할 수 있다.

2. MAC 주소인증을 통한 접속제한

무선 AP나 라우터에 MAC 주소인증을 통해 비인가자의 접속을 제한함으로써, 공격자로 부터 도청을 예방할 수 있다. 일반적으로 MAC 필터링 기능은 스위치나 AP 자체에서 설정하여 적용할 수 있고, 많은 종류의 AP에서 지원하는 보안기능이다. 또한, 네트워크 장비인 라우터에서 MAC 주소인증 기능을 적용함으로써 비인가자의 접속을 제한 할 수 있다. 다만 이러한 적용방법은 네트워크 장비인 라우터나 스위치에 부하를 가중 시킬 수 있다. 즉, 네트워크 장비가 MAC 주소인증 기능을 수행함으로 인해, 네트워크 장비의 고유의 기능인 경로설정과 데이터 전송의 속도가 저하되는 경우가 발생할 수 있어 실제로 라우터에 적용하는 예는 그리 많지 않다.

출처 : KISA, 무선랜 보안 가이드라인

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

유추할 수 있는 암호의 보안 취약점

비밀번호는 보안을 위한 가장 1차적인 수단이다. PC, 이메일, 휴대전화, 웹사이트 등 비밀번호가 뚫리면, 그 비밀번호로 접속해서 내가 사용가능한 모든 것이 누군가에게 노출될 수 있다. 하지만 많은 사람들이 다른사람이 쉽게 예측할 수 있는 비밀번호를 사용한다. 2015년 이탈리아 보안업체 '해킹팀 ' 이 해킹을 당한 사건이 있었다. 이 회사에서 해킹당한 직원들의 비밀번호는 주로 'passw0rd', 'passw@rd' 등 과 같이 유추하기 쉬운 암호 설정이 그 주요 원인이었다. 이 회사는 감시 및 도·감청용 스파이웨어를 개발·판매하는 업체이다. 프랑스의 비정부기구인 국경없는 기자회가 선정한 5대 해킹기업으로 지목한 곳이기도 하다.

선박용 위성통신 터미널의 하드코딩 된 암호로 인한 보안 취약점

프로그램 코드내부에 하드코딩 된 패스워드를 포함하고,이를 이용하여 내부인증에 사용하거나 외부컴포넌트와 통신을 하는 경우, 관리자 정보가 노출 될 수 있어 위험하다. 선박에서 주로 사용하는 VSAT, Inmarsat, Iridium, Thuraya 등 대 다수의 위성통신 터미널에서도 하드코딩 된 암호 또는 중요정보로 인한 잘 알려 진 보안 취약점들이 있다.

CVE Code	Vulnerability	Description
CVE-2013-6035	Zing protocol	satellite terminals does not require authentication for sessions on TCP port 1827
CVE-2013-6034	hardcoded credentials	satellite terminals has hardcoded credentials, which makes it easier for attackers to obtain unspecified login access via unknown vectors
CVE-2014-0326	hardcoded credentials	Iridium satellite terminals allow remote attackers to read hardcoded credentials via the web interface.
CVE-2014-2964	hardcoded credentials	Cobham Aviator 700D and 700E satellite terminals have hardcoded passwords for the (1) debug, (2) prod, (3) do160, and (4) flrp programs, which allows physically proximate attackers to gain privileges by sending a password over a serial line.
CVE-2014-2941	Hardcoded Credentials	Cobham Sailor 6000 satellite terminals have hardcoded Tbus 2 credentials, which allows remote attackers to obtain access via a TBUS2 command

보안대책

개발자는 패스워드는 암호화하여 별도의 파일에 저장하여 사용하고, sw설치 시 사용하는 디폴트 패스워드, 키 등을 사용하는 대신 "최초-로그인“ 모드를 두어 사용자가 직접 패스워드나 키를입력 하도록 설계해야한다.

데이터 베이스 연결을 위한 패스워드를 소스코드 내부에 상수형태로 하드코딩 하는 경우 , 접속정보가 노출 될 수 있어 위험하다.

안전하지 않은 코드의 예 JAVA

```
public class MemberDAO {
    private static final String DRIVER = "oracle.jdbc.driver.OracleDriver";
    private static final String URL  = "jdbc:oracle:thin:@192.168.0.3:1521:ORCL";
    private static final String USER = "SCOTT"; // DB ID;
//DB 패스워드가 소스코드에 평문으로 저장되어 있다.
    private static final String PASS = "SCOTT"; // DB PW;
……
    public Connection getConn() {
        Connection con = null;
        try {
            Class.forName(DRIVER);
            con = DriverManager.getConnection(URL, USER, PASS);
 ……
```

패스워드는 안전한 암호화 방식으로 암호화 하여 별도의 분리 된 공간(파일)에 저장해야 하며, 암호화 된 패스워드를 사용하기 위해서는 복호화 과정을 거쳐야 한다.

안전한 코드의 예 JAVA

```
public class MemberDAO {
    private static final String DRIVER = "oracle.jdbc.driver.OracleDriver";
    private static final String URL  = "jdbc:oracle:thin:@192.168.0.3:1521:ORCL";
    private static final String USER = "SCOTT"; // DB ID
  ……
    public Connection getConn() {
        Connection con = null;
        try {
            Class.forName(DRIVER);
//암호화된 패스워드를 프로퍼티에서 읽어들어 복화해서 사용해야한다.
            String PASS = props.getProperty("EncryptedPswd");
            byte[] decryptedPswd = cipher.doFinal(PASS.getBytes());
            PASS = new String(decryptedPswd);
            con = DriverManager.getConnection(URL, USER, PASS);
 ……
```

KR 해상 사이버보안 형식승인 가이드라인

사이버보안 형식승인 지침 이해하기

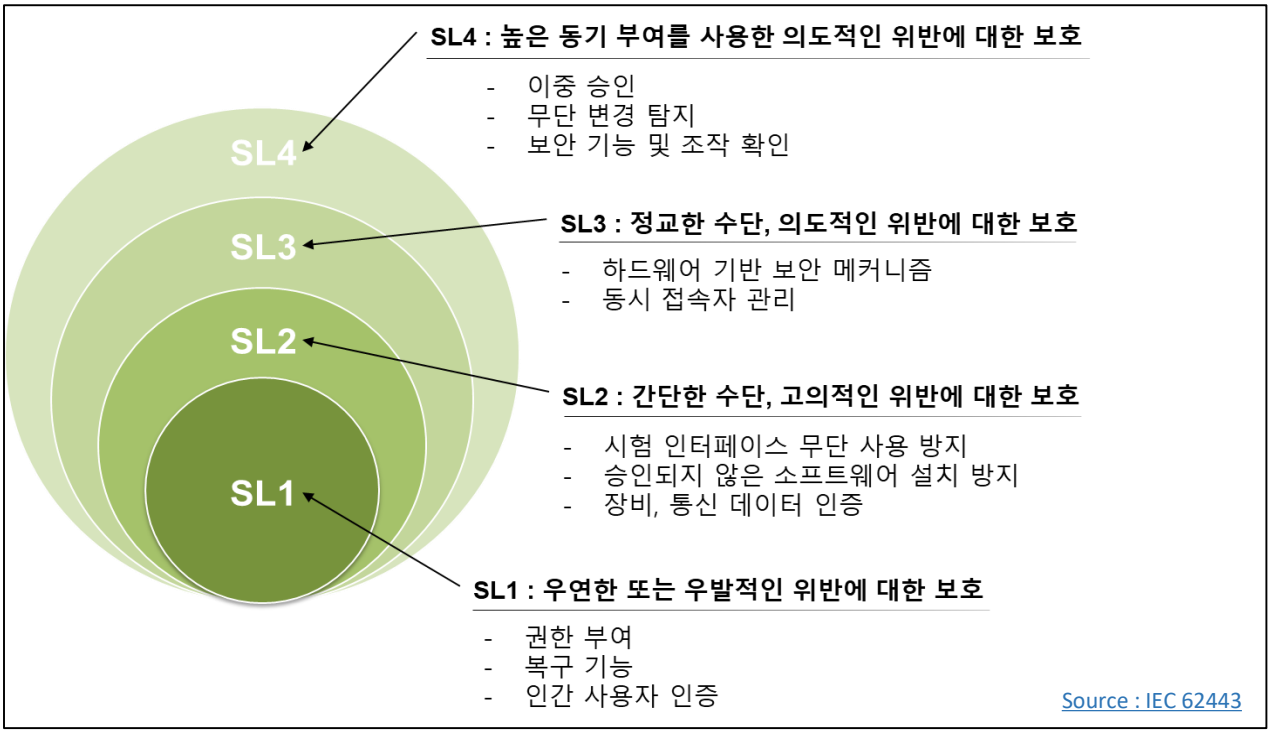
형식승인이란, 선박에 설치하기 전에 제품의 각 형식마다 미리 자료심사 및 승인시험을 하고 만족할 경우 제품이 규정에 적합하다는 것을 제조자에 대해서 증명하는 것을 의미한다. 사이버보안 형식승인은 ISA 62443 4-2, IEC 61162-460과 같은 국제표준을 기반으로 개발되었으며 선박에 탑재되는 원격 접속 장비, 통합 제어 및 모니터링 시스템 등을 포함하는 사이버 시스템의 사이버보안 수준 및 그 수준에 해당하는 요건을 12개의 범주 및 총 124개 항목의 요구 사항에 대한 검증을 통해 보안 기능과 그 수준을 확인한다.

<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



한국선급 해상 사이버보안 형식인증 검사항목

호스트 장비 요건 - 업데이트 지원 (1104)

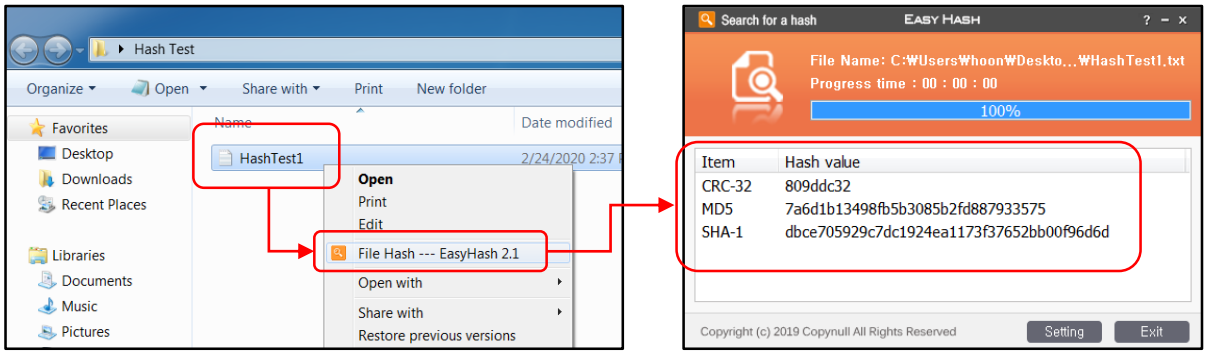
1. 호스트 장비는 업데이트되거나 업그레이드되는 기능을 지원하여야 한다.(SL 1)
2. 호스트 장비는 설치 전에 업데이트 또는 업그레이드의 신뢰성과 무결성을 확인하여야 한다.(SL 2,3,4)

해시값을 이용한 업그레이드 파일의 무결성 확인

동일한 보안 요구사항에 대해 적용 대상의 종류에 따라 기능의 구현 방식이 다르게 적용되어야 할 수 있다. 이러한 요구사항에 대해 사이버보안 형식승인 지침에서는 소프트웨어 어플리케이션, 임베디드 장비, 호스트 장비 그리고 네트워크 장비에 대한 요건으로 구분하여 3장 9절부터 12절까지 총 54개의 요구사항으로 분류하였으며 이번호에는 업데이트 지원과 관련하여 호스트 장비에 대한 요건을 확인해보도록 한다.

호스트 장비는 공급업체로부터 제공된 하나 이상의 소프트웨어 어플리케이션, 데이터 저장 기능을 수행(호스팅)할 수 있는 운영체제 기반의 범용 장치로써일반적인 예시로는 파일 시스템, 프로그래머블 서비스, HMI 등이 있다.(출처 : IEC 62443 4-2)

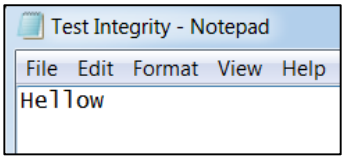
호스트 장비는 업데이트 되거나 업그레이드되는 기능을 지원하여야 하되 SL2 이상을 받고자 하는 업체에서는 업데이트 또는 업그레이드 전 신뢰성과 무결성을 확인할 수 있는 기능을 제공하여야 한다. 무결성에 대한 개념은 2019년 10월 발간된 18호에 기술되어 있으므로 이번호에서는 무결성을 검증하기 위한 방법 및 사례 위주로 설명하고자 한다. 업데이트 파일을 서버로 부터 내려받아 단말기에서 업데이트를 하는 경우 이 파일이 서버로 부터 보낸 원본파일이 맞는지 검증하는 절차(무결성 검사)와 이를 지원하는 기능이 필요하다. 이를 위해 해시 함수를 이용 할 수 있다. 해시 함수는 임의의 데이터에 대해 고정된 길이의 데이터로 매핑하는 함수를 의미하며 호스트 장비등에 저장된 데이터(파일)의 해시 값은 간단한 도구(eg. EasyHash, HashTab 등)를 이용해 확인이 가능하다.



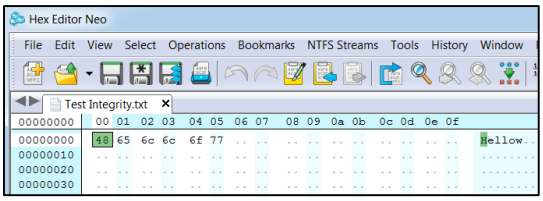
<해시값 확인 방법의 예시 – Easy Hash 프로그램을 이용한 확인>

해시값을 이용한 파일의 무결성 확인

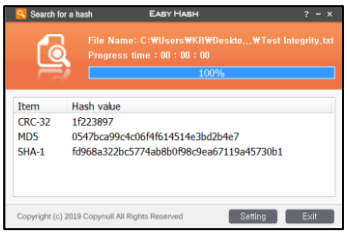
저장된 파일의 변조가 일어났을 경우 해시값을 통해 확인이 가능하다. 테스트를 수행하기 위해 임의의 텍스트 파일을 생성하고, 이에 대한 Hex 값 (PC에 저장되는 바이너리 코드 값)을 확인하기 위해 Hex Editor Neo를 이용하였다. 테스트용 텍스트 파일의 Hash 값 확인을 위해서는 Easy Hash 프로그램을 이용하였다.



<원본 파일>

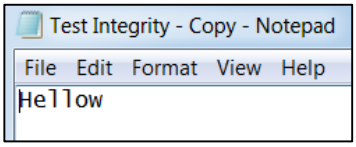


<Hex 값>

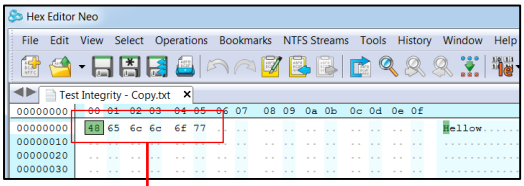


<Hash 값>

저장된 파일의 복사본을 만들고 Hex 값 및 Hash 값을 원본 파일과 비교해 보았으며 원본 파일과 모든 값이 동일함을 알 수 있다. (변조가 이루어 지지 않음)



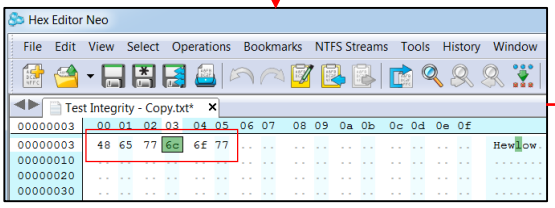
<복사된 파일>



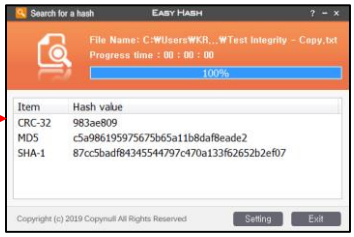
<Hex 값>

<Hash 값>

48 65 **6c** 6c 6f 77 -> 48 65 **77** 6f 77



<Hex 값 - 변조됨>



<Hash 값>

복사된 파일에 변조를 일으켜 보았다. 방식은 Hex 값을 강제로 변경(변조/해킹)한 뒤 Hash 값이 원본 값과 동일한지 비교하였다. Hex 값을 강제로 변경하여 'Hellow'라는 내용의 텍스트 파일이 'Hewlow'로 변경 되었으며 Hash값이 원본과 다름을 알 수 있다. 이러한 방법을 활용하여 업데이트 전 서버로 부터 받은 업데이트 파일의 해시 값을 서버의 원본 파일의 값과 비교하는 기능을 제공함으로써 업데이트 전 무결성을 확인할 수 있음을 알 수 있다.

용어 설명

CIRM(Comité International Radio-Maritime)

선박의 전자화사들을 위한 주요 국제 비정부기구(NGO)로서, 전 세계 30개국에서 110개가 넘는 회사를 회원으로 보유하고 있으며, 주요 국제회의(IMO, ITU, IEC, IALA 등)에서 폭넓은 활동을 하고 있다.

SSID(Service Set Identifier)

SSID는 WIFI 네트워크 이름을 가르키는 용어이다. IEEE 802.11 무선 네트워킹 표준으로 연결할 서비스 세트(네트워크)를 알려주는 식별자이다. SSID는 고유한 이름으로 설계되어있어 특정 무선 랜에 접속하려면 모든 AP나 무선 장치들은 반드시 동일한 SSID를 사용해야만 한다. 특정 BSS의 고유한 SSID를 알지 못하는 그 어떠한 장치도 그 BSS에 접속할 수 없다. SSID는 패킷 상에 부가된 평범한 텍스트 데이터이므로, 충분히 스니프 당할 가능성이 있기 때문에, 네트워크에 대해 어떠한 보증도 하지 않는다.

하드코딩

데이터를 코드 내부에 직접 입력하는 것. 기술적으로는 데이터가 실행 바이너리(exe 파일 등)에 합쳐져 있는 상태를 말한다. 프로그램의 소스코드에 데이터를 직접 입력해서 저장한 경우, 즉 모든 '상수'는 하드코딩이다. '변수'의 초기값이나 기본값도 하드 코딩이다. 기본값 자체를 외부 리소스 파일로부터 읽어서 초기화하는 경우도 있지만 그 '리소스' 파일의 로딩은 실패 확률이 존재하기 때문에 로딩 전까지는 null, 0, nil등의 값이 하드 코딩돼있다.