KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 024

April 2020

KR certifies first cyber security compliant vessel

Korean Register (KR) has completed a comprehensive cyber security survey of the chemical/oil tanker SONGA HAWK and has certified the ship to be fully compliant in all areas, the very first ship to achieve the certification.

KR conducted a cyber security audit of Songa Ship management and certified the company to be fully compliant in all areas in 2019, the first company to achieve this. Two years on from the original contract, SONGA HAWK, has now been certified as ship cyber security compliant by KR, successfully passing the inspection of 81 items in 18 categories including risk management, asset management, technical security and incident response and recovery.

With this certification, Songa Ship management and SONGA HAWK satisfy the international cyber security requirements as outlined by the IMO (International Maritime Organization), TMSA (Tanker Management and Self-Assessment) and SIRE (Ship Inspection Report Program). KR will now inspect the other ships in Songa Ship management's fleet, testing their compliance, with a view to issuing further ship cyber security compliance certificates.

In 2021, the International Maritime Organization's (IMO) Resolution MSC.428 (98) will enter into force, which will increase demand for company and ship cyber risk management services.

KR established its cyber security certification process in line with international security standards such as ISO 27001, IEC 62443, the NIST Framework, IMO and BIMCO cyber security guidelines.

The classification society has provided cyber security certification services for companies and ships since 2018, and cyber security type approval services for ship networks and automated systems in compliance with IEC 62443 4-2 and IEC 61162-460 standards since 2019.

Vulnerability Analysis and Countermeasures of Wireless Networks-2

This series will introduce principles and kinds of wireless network widely used in companies, home, and ships. Also, weakness and countermeasures of wireless network. Therefore, this newsletter in February 2020 introduces 'the kinds of wireless network and communication principle'

Series news

① The principles and kinds of wireless networks

② Technical Security Vulnerabilities and Countermeasures of Wireless LAN (WIFI)-1

③ **Technical Security Vulnerabilities and Countermeasures of Wireless LAN (WIFI)-2**

④ Technical Security Vulnerabilities and Countermeasures of Wireless LAN (WIFI)-3

⑤ Technical Security Vulnerabilities and Countermeasures of Other Wireless Networks

⑥ Kinds of maritime wireless communication, technical security vulnerabilities

Security Vulnerability and Security Measures for User Authentication

Vulnerabilities in SSID default settings

After analyzing the vulnerability of the wireless LAN user authentication mechanism, find out how to respond to vulnerability. In order to make easily the WIFI signal identification of the WIFI user, the SSID value is set up as the name of company as an easy to memorize. Since AP broadcasts SSID as a default setting, if an attacker exists only in the AP coverage, it is easy to find out the broadcast SSID value.

Countermeasures through change of SSID

1. Changes in the establishment of SSID

If the user changes the setting so that the SSID value of the AP is not broadcast, The connection attempt can be reduced from the attacker who does not know SSID to AP. In other words, malicious attackers may abandon attacks because they then must analyze certain wireless data using wireless LAN analysis tools.

2. Operation of a closed system

If the user sets the SSID of the AP as the NULL value without designating it, the wireless LAN terminal automatically requests access to the AP sending a strong signal to the user. Some APs offer the ability to block connection requests even if they try to connect using the SSID value as NULL. It is called a closed system that sets the SSID value as NULL and operates to block users who require access to AP.

Source : KISA, WLAN Security Guidelines

Vulnerability of WEP Authentication Mechanism

1. Vulnerability due to a one-way authentication method

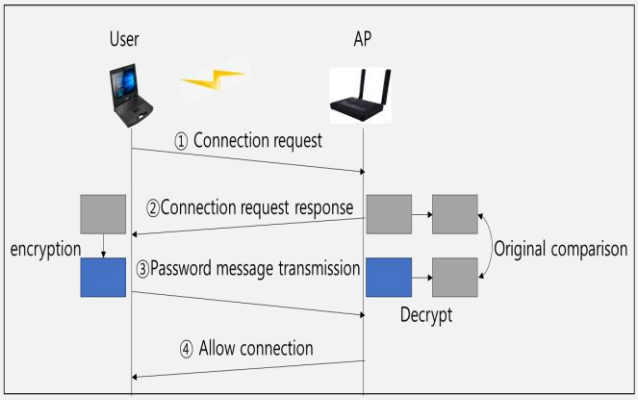
WEP authentication can be applied conveniently to data encryption and user authentication, but there are many vulnerabilities because it is a mechanism that certifies users in a one-way direction in AP. Malicious attackers have been exploiting user information using cloned APs. Some cyber attack scenarios using cloned APs are outlined below.

① The attacker collects the AP providing service information in the normal wireless LAN environment and uses the same model of the manufacturing company to replicate the AP, the normal AP and the poisonous setting then combine.

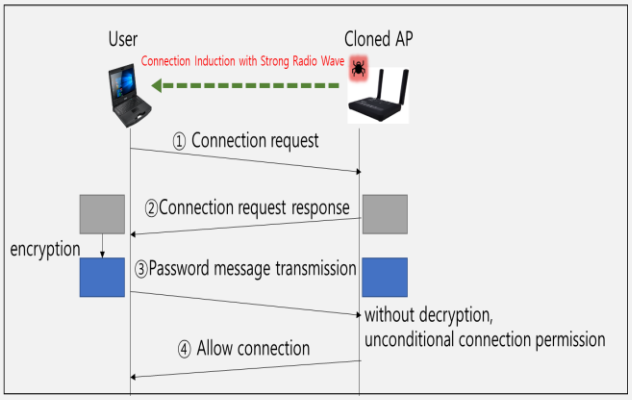
② The cloned AP sends a stronger radio signal than the normal AP, sending a message that the normal user requests access to the replication AP without any doubt, and allowing the replication AP to request a false authentication through the response message.

③ An attacker of a cloned AP can collect Internet packet information and deodorize personal information of a normal user who accesses the cloned AP.

<Normal WEP certification procedure >



<WEP authentication evasion attack through replication AP>



2. Vulnerability due to the use of fixed shared keys

Another vulnerability of WEP is the use of one fixed shared key for WEP key values in institutions using wireless LANs. All of the equipment using wireless LAN have the same key value which is set and used in AP and user terminal, and many security problems are caused when the WEP key value is leaked out, because the same value is being used. For example, if a fixed key value is set and used by an institution using a wireless LAN, a WEP value can be leaked to the outside by a partner employee, a visitor or a leaver. To reduce these risk factors, WEP values should be changed periodically. However, most of the users of the WLAN use the WEP key because they often work externally, so it can be difficult to keep them informed about any WEP changes. The WEP key is used to authenticate the user using the one WEP key.

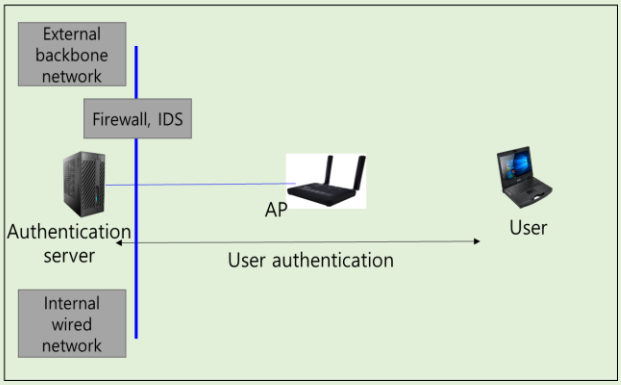
Source : KISA, WLAN Security Guidelines

Countermeasures for WEP authentication

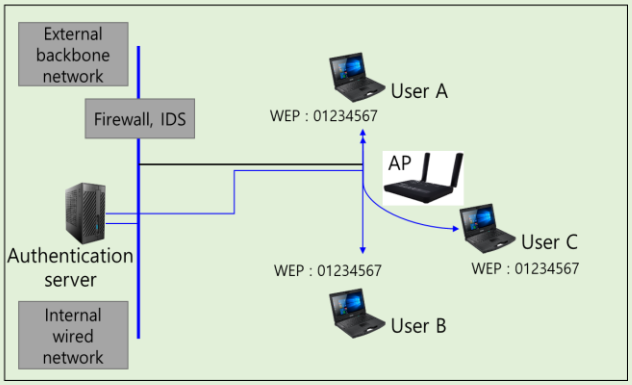
1. Application of dynamic WEP

The fixed shared key value causes various security problems. A dynamic WEP should be applied to reduce these problems. The authentication is performed whenever the certificate server tries to create a connection. This manages the establishment and renewal of the WEP key used in companies.

<Dynamic WEP application using authentication server>



<Example of establishing a connection by applying dynamic WEP>



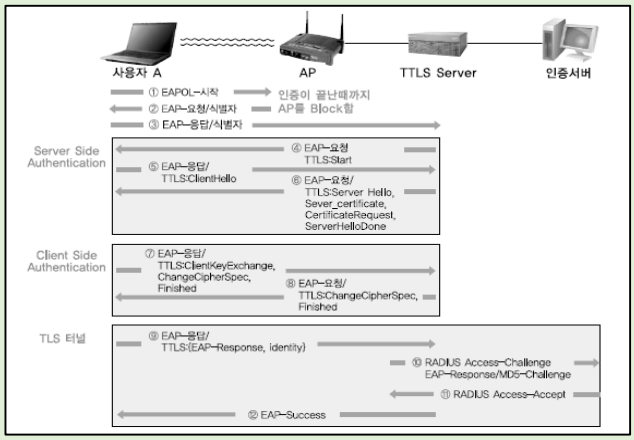
2. EAP-TTLS Authentication

EAP-TTLS is a tunnel-based authentication mechanism based on traditional passwords such as EAP-TLS and Challenge Handshake Authentication Protocol (CHAP) or OTP. EAP-TTLS is an authentication procedure. To form TLS tunnels, TTLS servers are used in front of the authentication server. However, it is common to perform the function of the TTLS server in the authentication server without operating the TTLS server separately.

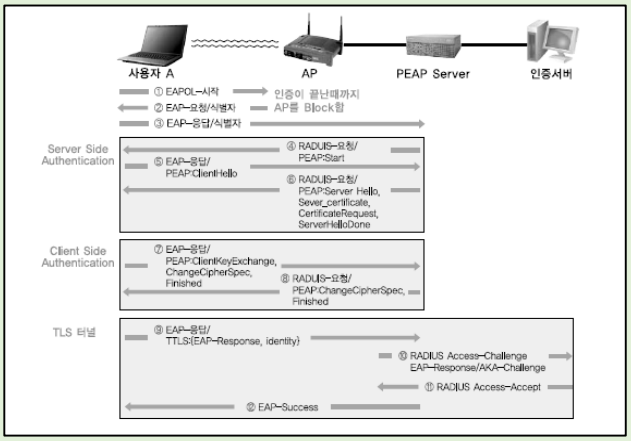
3. PEAP Authentication

PEAP is a tunneling authentication algorithm based on a user password. It is similar to EAP-TTLS in that the TLS tunnel is created by using the PEAP server and the authentication between the certificate server and the user is made through this.

<EAP-TTLS Authentication Procedure>



<PEAP Authentication Procedure >



Source : KISA, WLAN Security Guidelines

Understanding Cyber Threats(OWASP Top 10 IoT)

Understanding cyber threats

A cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, or the nation state through unauthorized access to an information system, causing destruction, disclosure, modification of information, and/or denial of service (source: NIST SP: 800-128). Cyber threats need to be categorized periodically to identify the vulnerabilities of assets, and the potential impact on that asset.

KR Guidance for Maritime Cyber Security System requirement(CS1)

204.1 Risk Management : External environmental factors affecting the environments of internal information technology and operational technology should be identified and cataloged as threats.

OWASP Top 10-Internet of Things(IoT)

The goal of the OWASP Things Internet Project is to help manufacturers, developers, and consumers understand more accurately the security issues associated with the Internet of Things and help users make wiser decisions in terms of security when building, distributing or evaluating IoT technology, according to the OpenWeb Application Security Project (OWASP). IoT)'s cyber threat Top10 and countermeasures are examined.

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

Source : OWASP Top 10 Project

Insecure Network Services

Network services that are not safe in Internet of Things (IoT) devices can be used as gateways to gain unauthorized remote control of the device or to damage the integrity or availability of information. There have been no cases of vulnerabilities for the insecure network service of IoT devices in OWASP. Therefore, through the network service security requirements for the IoT device selected by the IoT Security Framework (Release 1.0) of the IoT Security Foundation, we can look at what unsafe network services are and security measures from developers and users' perspectives.

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

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

Understanding Guideline for Type Approval of Maritime Cyber Security

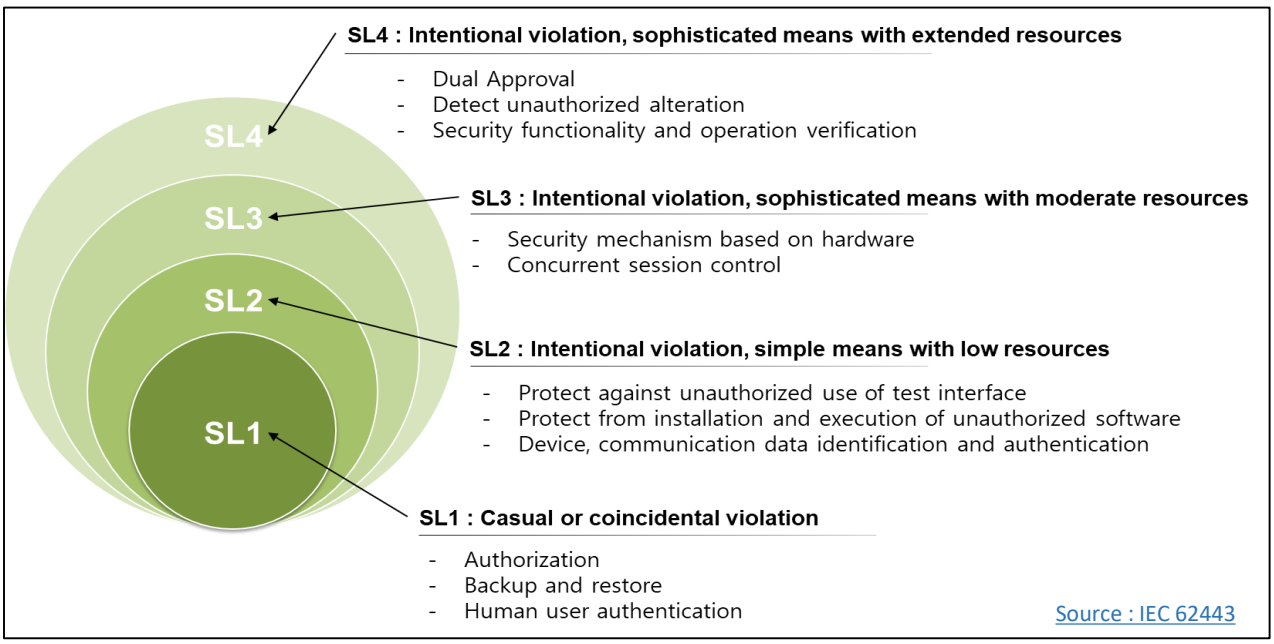
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance before installation on board. The cyber security type approval has been developed based on international standards such as ISA 62443 4-2, IEC 61162-460, and inspect cyber security level and function of cyber systems including remote access equipment, integrated control and monitoring systems on board the ship. The security requirements and their levels are verified on 12 categories and 124 requirements.

< Composition of KR Cyber Security Type Approval Guidelines >

Section 1 General	Section 5 Data Confidentiality	Section 9 Software Application Requirements
Sections 2 Identification and Authentication	Section 6 Restricted Data Flow	Section 10 Embedded Device Requirements
Section 3 Use Control	Section 7 Timely Response to Events	Section 11 Host Device Requirements
Section 4 System Integrity	Section 8 Resource Availability	Section 12 Network Device Requirements

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

Understanding Security Level (SL)



Source : IEC 62443

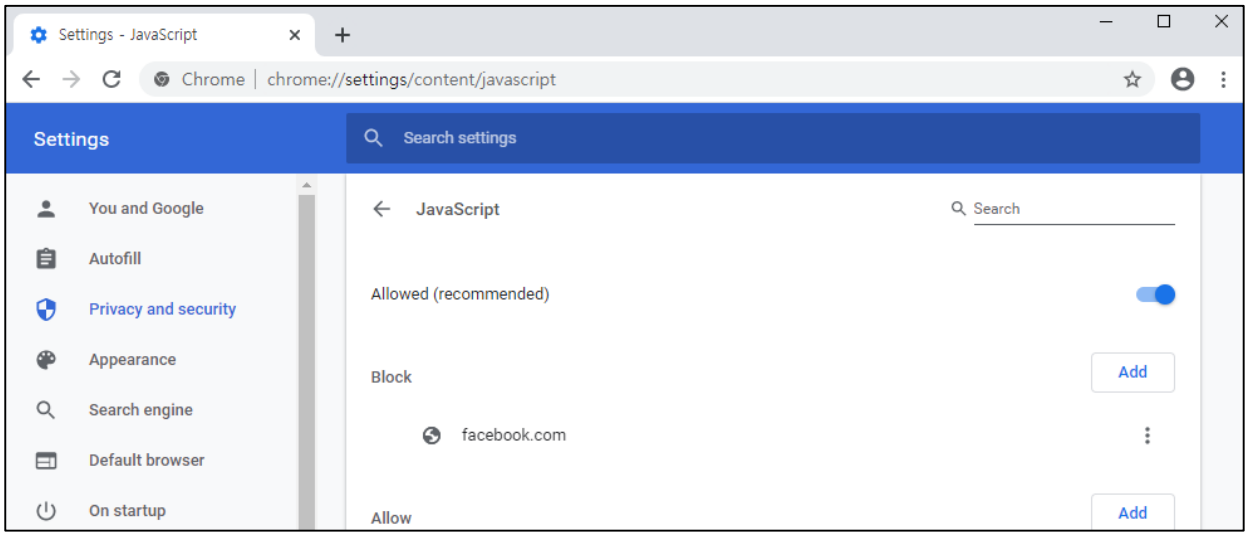
KR Type Approval of Maritime Cyber Security Inspection Items

Software Application – Mobile code (901)

1. In the event that a software application utilizes mobile code technologies, that application should provide the capability to enforce a security policy for the usage of mobile code technologies. (SL 1)
2. The application should provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed. (SL 2,3,4)

Security control of mobile code

Mobile code refers to a program that can be executed without the explicit installation of the recipient (source IEC62443 4-2), ActiveX of Internet Explorer, and Chrome extension programs are examples of it that we can access around. If mobile code technology is applied, the software application should provide the ability to implement the security policy of mobile code.



<Example of Mobile Code Security Policy – Providing the Execution/Cript of JavaScript>

If you use mobile code, the software application must be provided with features such as user identification before installation and execution, execution control such as administrator approval, and integrity check before execution of the code. The mobile code does not seem to install the software, but the file for running this software exists somewhere. For chrome, it is stored in the following locations on the local drive based on the extension program:

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

In the case of the Windows OS, if the corresponding location is entered through the execution screen (short key: Windows button + R), the location where the extension program of chrome is stored can be confirmed.

Explanation of Term

Description of application layer protocol

- **MQTT (Message Queuing Telemetry Transport)** : MQTT protocols are designed to be used in low power and low bandwidth environments because they operate in limited specific environments, such as low power batteries. This is a useful protocol for IoT.
- **ICMP(Internet Control Message Protocol)** : It is a protocol that informs the problem that occurs when processing IP packet in TCP/IP. Commonly called Ping test is used to monitor the network's connection status using the ICMP protocol.
- **TELNET**: It is a protocol used to confirm that the port is accessible.
- **FTP(File Transfer Protocol)** : A file transfer protocol, a protocol for file transfer between servers and clients.
- **HTTP (Hyper Text Transfer Protocol)** : It is a protocol that allows information to be exchanged on WWW, mainly used to exchange HTML documents. TCP and UDP are used. And port 80 is used.
- **SMTP (Simple Mail Transfer Protocol)** : It is a protocol used to send emails on the Internet; the TCP port number used is number 25.