KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 016

August 2019

KOREAN REGISTER

KR Cyber security Activities

KR signed MOU with Penta security System Inc. for joint development of Ship Cybersecurity Solution

The Korean Register of Shipping (KR) and Penta Security System signed a memorandum of understanding (MOU) on 31 July at the Penta Security Headquarters. Under the agreement, the two companies will verify cyber security solutions for ships, based on KR's maritime cyber security certification capability and Penta Security's cyber security technology. Following the IMO's MSC.428 meeting, the requirement for cyber security risk management is expected to increase significantly from 2021.

The Korean Register of Shipping established its maritime cybersecurity certification system in accordance with international cybersecurity standards such as ISO 27001, IEC 62443, the NIST Framework, and the IMO and BIMCO maritime cybersecurity guidelines.

Through this, the company provides cybersecurity certification services for companies and ships and cyber security type approval services for ship networks and automation systems.

Penta Security is a leading provider of data encryption, web security, authentication security products and services in the field of enterprise information security.

Since 2015, it has expanded its scope of business to include next-generation converged security with security technologies in the IoT environment such as smart cars, smart grids, and smart factories. Penta Security System is also working on a standard for future blockchain environments.

Maritime Cybersecurity Insurance Trends

BIMCO announces new cyber security clause

In July 2019, BIMCO issued a new standard provision for maritime cyber accident insurance. As a result of recent cyber security attacks, BIMCO has developed a new standard Cyber Security clause. BIMCO has been actively participated in the IMO’s international meetings and has been leading maritime cybersecurity issues by distributing “Industrial Guidelines on Ship Cybersecurity”. The standard provisions cover debt and obligations in cybersecurity accident insurance contracts. The main aims of the BIMCO’s clause can be summarized as follows.

The first aim is to raise awareness about cyber incident risk. The second is to provide a mechanism by which parties can arrange procedures and systems to minimize the risk of cyber incidents. The third is for the parties to work together to help each other mitigate and resolve the impact of a cyber incident.

BIMCO's standards are designed for use in a wide range of contracts, including contracts with third-party service providers such as brokers and agents. Liability between the parties for insurance claims is limited to the amount agreed upon during negotiations, and $100,000 is applied if no other amount is inserted.

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

Beazley Insurance launches maritime cyber insurance product

UK insurance company Beazley has created a new marine cyber insurance product targeted at vessel owners and operators, providing insurance for physical damage and loss of hire should a cyber incident impact a vessel’s operational capabilities. There are three elements to the risk management services included in Beazley’s product: a self-assessment questionnaire; a cyber security workshop; and an onboard cyber survey. Beazley Cyber Defence for Marine is based around a risk management services approach, designed to reduce the likelihood of a cyber incident occurring and to assist operators in demonstrating compliance with forthcoming IMO guidelines. The product would support compliance. In addition, as a ship's OT and IT systems are increasingly interconnected, the threat of human error is also increasing. The company's products will reduce the risk of accidents, and compensation will provide clear recompense and limits to owners.

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

Port of LA Sets Up New Cybersecurity Coordination Center

Port of LA Sets Up New Cybersecurity Coordination Center

Los Angeles' harbor department has issued an RFP for a new privately-operated "cyber resilience center" for the Port of Los Angeles. The build / operate / maintain contract calls for a center that would coordinate cyber-defense activity between port stakeholders, reducing the risk of cargo disruption from a cyberattack In addition to defensive measures, the center would provide information resources that terminal and other port partners could use to help restore operations following an attack. In part, this will take the form of a secure cyber threat data portal, accessible through stakeholders' dashboards and mobile devices, along with real-time threat notifications. “Collaborative cyber-threat information sharing is critical to the safety and security of our Port,” said Chief Thomas Gazsi, the head of the port's police department. “This Cyber Resilience Center will allow us to more quickly identify and mitigate cyber incidents that pose a threat to the maritime supply chain.” The Port of LA already has an award-winning, first-of-its kind Cyber Security Operations Center(CSOC) focused on the port authority's own internal operations, but it sees the new Cyber Resilience Center(CRC) as a separate coordinating body for all entities at the port - including the existing cyber center. "The CRC will be a 'system of systems' that the CSOC and stakeholder cyber security systems connect to, but will not replace it, nor will it be intrusive, disruptive or burdensome to stakeholder systems," the port said in its RFP. "Stakeholders will have the control to decide if, and how, to use information from the CRC."

Port cybersecurity is a serious consideration, especially for high-productivity, high-automation container terminals.

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

[Series News] ①

5G`s Effects and Cyber Threats on the Maritime

This series news will discuss the 5G's effects and cyber threats on the maritime industry. The 5G will be the core infrastructure on the 4th Industrial revolution. Therefore, in this issue of newsletter, we will introduce ***'What is 5G?' And representative cyber threat of 5G technology.***

series news

① What is 5G?

② 5G Network architecture, Network Slicing technology, and Affects on the maritime Industry

③ Comparison between LTE centralized network and 5G distributed network

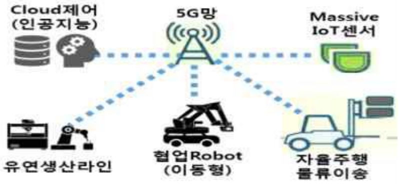
④ Role of wireless backhaul technology and 5G satellites in 5G standards

⑤ The private network reference model in 5G standard for effective use in ships and ports

What is 5G?

5G guarantees data transmission and reception capacity and speed in mobile communication environment, no difference between wired and wireless. Also, the 5G guarantees service stability even in IoT communication environments where many devices are connected and low power in device use. we inquire to a new communication technology "seconds to download movies". However, 5G is not just a technology that aims to improve communication data rates, but an ICT convergence technology that is based on the requirements of a wide range of industries such as automobiles, railways, cities, and factories.

Core Performance		4G	5G	More than 4G
Speed	Maximum transmission speed	1 Gbps	20 Gbps	20 times
Latency	Transmission latency	1 sec / 100 min	1 sec / 1,000 min	1/10
Connectivity	Maximum device connection	100,000/km^2	1,000,000/km^2	10 times

[Speed] Real time Media	[Latency] V2X	[Connectivity] Smart Factory
360° wireless hologram	Full Autonomous Driving(Level 4)	Wireless production system
		

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

What is 5G?(Continue page)

It wants to find out how 5G will be applied to the maritime environment in ships, Maritime IoT and Smart ports. This newsletter will briefly introduce some features of the 5G and explain them in more detail in the next newsletter issue.

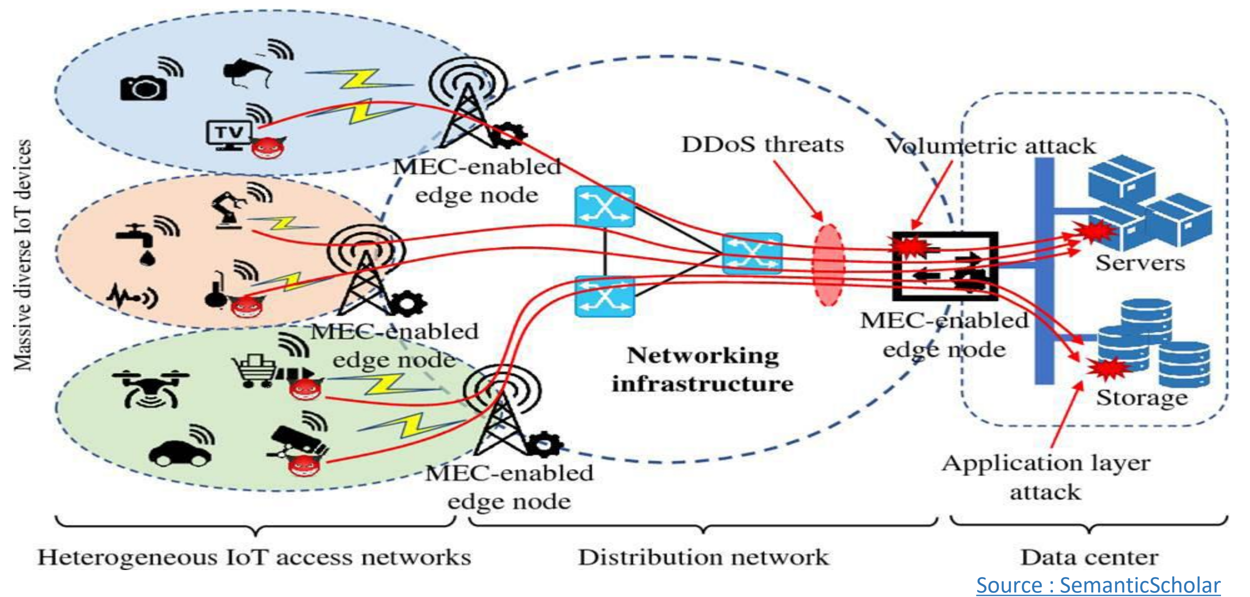
- **Network Slicing** : It is possible to virtualize on the same physical network infrastructure, to diversify independent logical networks, and to have 5G communication requirements suitable for the marine environment, such as ships and marine IoT devices, through network slicing.
- **Mission Critical Service** : 5G's low latency and high reliability (URLLC) technology is used for disaster communication, autonomous driving, railroad communication, and can be used for services for preventing ship collisions.

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

5G`s Cybersecurity risks - Possibility of DDOS attacks

Unlike traditional communication networks, which are closed to each industry and use, 5G is designed to be open and distributed according to use. This is called network slicing, where a network is divided into virtual dedicated networks such as communication, IoT, VR, and autonomous driving. However, because all devices are physically connected to 5G, malware can spread at a very rapid rate, and the base station is likely to be attacked by DDoS attacks from a large number of infected devices.

The market demand for new security technologies such as blockchain and quantum cryptography will spread, to provide a defence against cyberattacks while using 5G's ultra-fast and high-density features.



Source : SemanticScholar

Understanding cyber threats(OWASP Top 10)

Understanding cyber threats

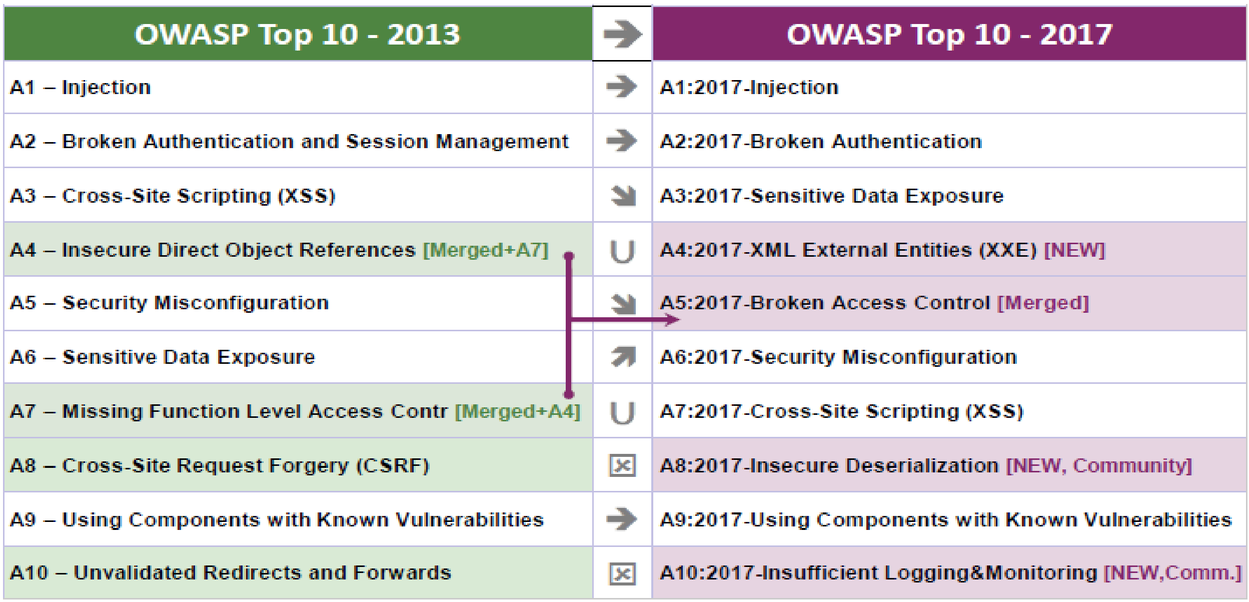
A cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, or the nation state through unauthorized access to an information system, causing destruction, 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

The Open Web Application Security Project (OWASP) is an open source web application security project, researching web exposure, malicious files and scripts, and security vulnerabilities. The OWASP Top 10, which is frequently referred to, highlights the top web application vulnerabilities, it was published in 2004, 2007 , 2010, 2013 and 2017. In this newsletter we will analyze the **'A7 : 2017 – Cross-Site Scripting (XSS)'**



OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	∪	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	☒	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Source : OWASP Top 10 Project

OWASP Top 10 ‘A7 : 2017 -Cross Site Scripting (XSS)’

1. What is Cross Site Scripting?

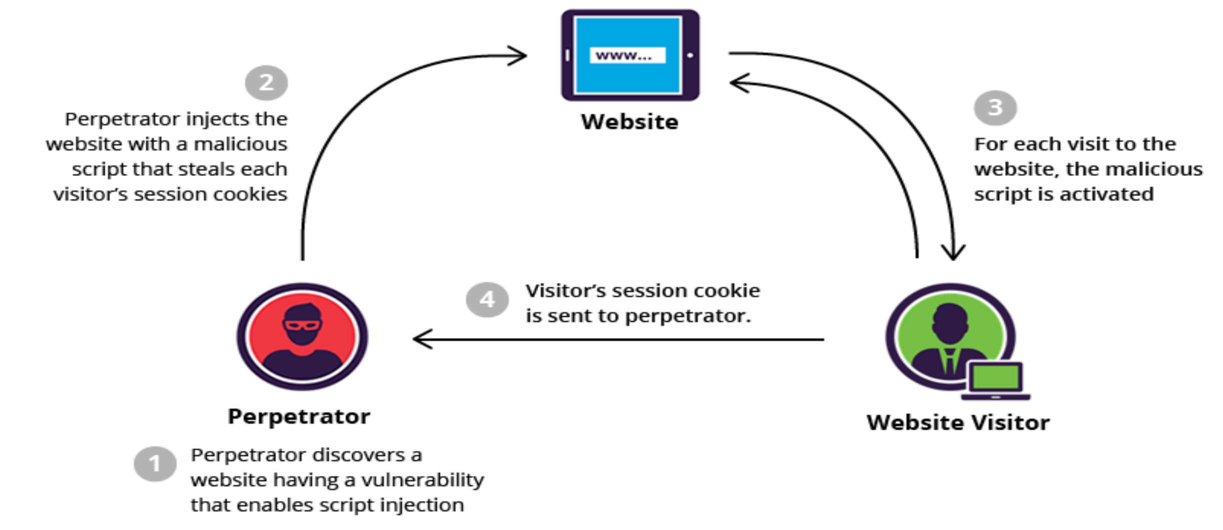
Cross-site scripting (XSS) occurs when a page that an application sends to the browser does not validate the data that the user has entered or invalidates the dangerous data on output. In other words, it occurs during the development of an application in which an attacker intentionally handles a malicious script that can be executed in a browser without neutralizing dangerous characters on the web server or outputting it. XSS generally occurs in JavaScript, but it can occur in any language that generates dynamic data that runs on the client, such as VB scripts or ActiveX. As such, XSS vulnerabilities can be attacked relatively easily and have not been eliminated during web application development. Therefore, the distribution of malicious scripts using these vulnerabilities, the distribution of malicious codes through them, and the hacking of client programs are still a big threat to the security of individuals and organizations.

2. Kinds of Cross Site Scripting Attacks

1) Stored XSS Attacks

Stored XSS attacks are a method of permanently storing malicious scripts on web servers that have web application vulnerabilities. When a malicious script is inserted into the bulletin boards, user profiles, and comment fields of a website, and when a user visits the site and requests information on a saved page, the server forwards the malicious script to the user, attacking the user as the script runs in the user browser.

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


www...
Website
2
Perpetrator injects the website with a malicious script that steals each visitor’s session cookies
3
For each visit to the website, the malicious script is activated
4
Visitor’s session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

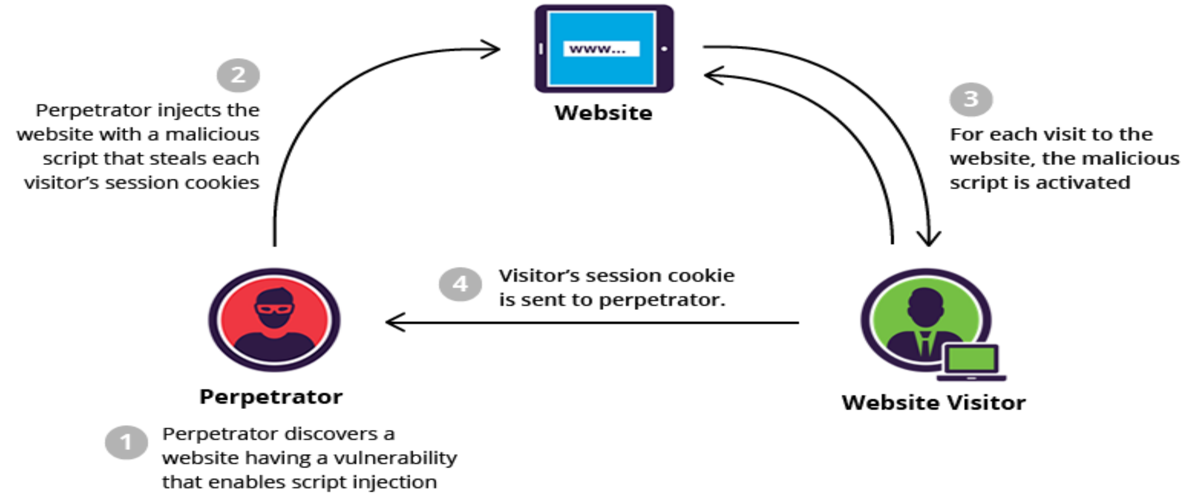
Source : https://www.imperva.com/learn/application-security/cross-site-scripting-xss-attacks/

2) Reflected XSS Attacks

Reflected XSS attacks take advantage of vulnerabilities arising from using specified variables in a Web application, such as search results and error messages, as the server receives externally-entered values and returns the dangerous characters of the variables it enters to the user as it responds to the browser.

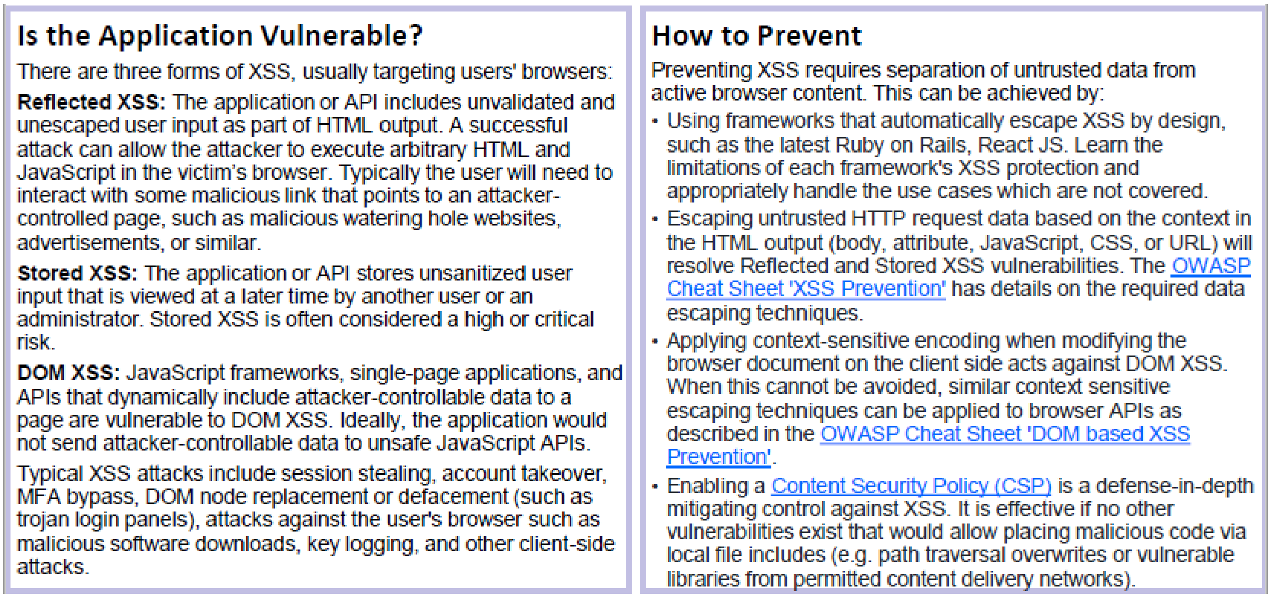
Typically, when you enter a search into a server, it passes the result value to the user if the search results are present, but if the server does not have an accurate result, the server responds by including the value entered in the browser in an HTML document. In this case, the malicious script included in the HTML page is executed in the browser.

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


www...
Website
2
Perpetrator injects the website with a malicious script that steals each visitor's session cookies
3
For each visit to the website, the malicious script is activated
4
Visitor's session cookie is sent to perpetrator.
Perpetrator
Website Visitor
1
Perpetrator discovers a website having a vulnerability that enables script injection

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

3) Vulnerability Check list and Security Measures



Is the Application Vulnerable?

There are three forms of XSS, usually targeting users' browsers:

Reflected XSS: The application or API includes unvalidated and unescaped user input as part of HTML output. A successful attack can allow the attacker to execute arbitrary HTML and JavaScript in the victim's browser. Typically the user will need to interact with some malicious link that points to an attacker-controlled page, such as malicious watering hole websites, advertisements, or similar.

Stored XSS: The application or API stores unsanitized user input that is viewed at a later time by another user or an administrator. Stored XSS is often considered a high or critical risk.

DOM XSS: JavaScript frameworks, single-page applications, and APIs that dynamically include attacker-controllable data to a page are vulnerable to DOM XSS. Ideally, the application would not send attacker-controllable data to unsafe JavaScript APIs.

Typical XSS attacks include session stealing, account takeover, MFA bypass, DOM node replacement or defacement (such as trojan login panels), attacks against the user's browser such as malicious software downloads, key logging, and other client-side attacks.

How to Prevent

Preventing XSS requires separation of untrusted data from active browser content. This can be achieved by:

- Using frameworks that automatically escape XSS by design, such as the latest Ruby on Rails, React JS. Learn the limitations of each framework's XSS protection and appropriately handle the use cases which are not covered.
- Escaping untrusted HTTP request data based on the context in the HTML output (body, attribute, JavaScript, CSS, or URL) will resolve Reflected and Stored XSS vulnerabilities. The OWASP Cheat Sheet 'XSS Prevention' has details on the required data escaping techniques.
- Applying context-sensitive encoding when modifying the browser document on the client side acts against DOM XSS. When this cannot be avoided, similar context sensitive escaping techniques can be applied to browser APIs as described in the OWASP Cheat Sheet 'DOM based XSS Prevention'.
- Enabling a Content Security Policy (CSP) is a defense-in-depth mitigating control against XSS. It is effective if no other vulnerabilities exist that would allow placing malicious code via local file includes (e.g. path traversal overwrites or vulnerable libraries from permitted content delivery networks).

Source : OWASP Top 10 - 2017

Guideline for Type Approval of Maritime Cyber Security

Understanding Cybersecurity Type Approval Guidelines

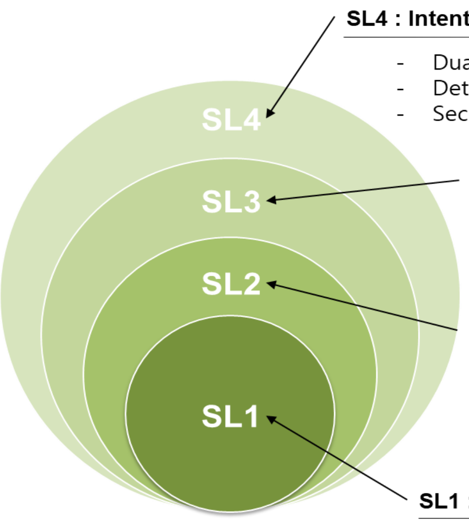
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance 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 Cybersecurity 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)



SL4 : Intentional violation, sophisticated means with extended resources

- Dual Approval
- Detect unauthorized alteration
- Security functionality and operation verification

SL3 : Intentional violation, sophisticated means with moderate resources

- Security mechanism based on hardware
- Concurrent session control

SL2 : Intentional violation, simple means with low resources

- Protect against unauthorized use of test interface
- Protect from installation and execution of unauthorized software
- Device, communication data identification and authentication

SL1 : Casual or coincidental violation

- Authorization
- Backup and restore
- Human user authentication

Source : IEC 62443

KR Type Approval of Maritime Cybersecurity Inspection Items

Human user identification and authentication(201)

1. Components should provide the capability to identify and authenticate all human users on all interfaces capable of human user access. (SL1)
2. User identification and authentication shouldn't hamper fast, local emergency actions.(SL1)
3. Components should provide the capability to employ multifactor authentication for all human user access to the component. (SL2)
4. Components should provide the capability to uniquely identify and authenticate all human users. (SL3,4)

What is Human user identification and authentication?

Identifier means a symbolic pattern unique within the security domain that identifies, displays, or names the entity claiming identity, and authentication means proof of identification request. Human user identification and authentication requires the ability to verify that the user is an appropriate user.

SL1 first requires identification and authentication on all interfaces that allow human user access. An example of this may be a human machine interface (HMI).

SL2 requires that in addition to SL1, every human user is uniquely identified. User identification and authentication can be role based or group based. In order to meet the SL2 requirements, it is necessary to create and manage individual identifiers for individual users, even if they are role-based or group-based identifier configurations.

SL3, SL4 requires multi-factor authentication in addition to SL1, SL2. The authentication factor is divided into three factors. Knowledge-based factors (passwords, PIN codes) using something you know, ownership-based factors(security cards, OTP, etc.) using something you have. There is an attribute-based factor(fingerprint recognition, etc.) that uses its own unique attribute. Multifactor authentication refers to a method of authenticating using two or more factors.

Knowdege based factor	Ownership based factor	Attribute based factor
Enter PIN 3 attempts remaining 1 2 3 4 5 6 7 8 9 0 Cancel	보안카드 일련번호 코드표 10 4567 25 1234 보안카드 일련번호 888888	

Explanation of Term

DDOS

Denial-of-service attack (DoS attack) is a cyber attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Edge node

An edge node is a computer that acts as an end user portal for communication with other nodes in cluster computing. Edge nodes are also sometimes called gateway nodes or edge communication nodes.

HMI

The Human Machine Interface (HMI) is all about how people and automated systems interact and communicate with each other. HMI has long been confined to traditional machines, but now it is also associated with devices for computers, digital systems and the Internet of Things (IoT), where more and more devices are connected and work automatically.