KR Maritime Cyber Security

News from KOREAN REGISTER

Feb 2019

Vol. 010

KR Cyber Security Activities

● KR delivered certificate of cyber security compliance to Songa

Korean Register (KR, CEO Lee Jung-ki) announced on 12th of February that they had delivered a certificate of cyber security compliance for the company to Songa after completing the cyber security certification audit of Songa Shipmanagement(Songa, CEO Kenneth MacLeod), a leading shipping company in UK.

Songa, a shipping company that manages and operates 23 fleets with tanker ships as main vessels, became the first KR cyber security certified company that has an established cyber security management system for responding to cyber incidents.

The KR, established cyber security certification process last year in accordance with the international security standard such as ISO 27001, IEC 62443, NIST framework and IMO and BIMCO cyber security guidelines, provides cyber security certification services on company and ships.

For Songa's cyber security certification audit over the last six months, the company passed 87 inspection items in 18 categories such as human management, risk management, asset management, response and recovery that satisfies all the requirement of IMO, OCIMF TMSA and RIGHTSHIP under the direction of CCSO(Company Cyber Security Officer) Joanne Pauline. The KR will proceed with the sequential certification of cyber security for 23 Songa vessels in this year.

● e-Navigation International Underway 2019

KR e-Navigation TFT attended the e-Navigation Underway 2019 held in Copenhagen, Denmark in February, and monitored the latest international policy trends and technology development for the marine application of new digital technology.

The conference consisted of four sessions, which led to active discussions among maritime industry experts. The presentations on the development and introduction of new technologies such as drone, cyber security, and blockchain were presented, and the question and importance of cyber security was emphasized in all the sessions.

In particular, on the subject of cyber security, 'The Guidelines on Cyber Security Onboard Ships(Rev.3)' recently published by BIMCO (Baltic and International Maritime Council), Denmark's national strategies and initiatives on maritime cyber security and information security were introduced in [Session 4].

The responsibilities and roles of various stakeholders in the maritime business (Port, Shipowner, Shipyard, Manufacturer, Service provider) should be clearly identified in order to ensure cyber security of ships in the future, and it is expected that maritime industry strategy needs to be established at national level, such as Denmark.

Session	Details
[Session 1] The Industry - Barriers and benefits when being a first mover	Rulemaking is required for new technologies (AI, drones, cyber security) and paradigm shift is needed to share data of maritime industry
[Session 2] Regulation and Standards	Regulations and standards have two-sidedness that can be a barrier and benefit to the growth of autonomous industries and need a role to bring positive results to the maritime industry.
[Session 3] The Port and Coastal State	Introducing cases of application of services and drones to ports of e-Navigation results, EMSA announces new technology application plans to respond to marine safety, security, prevention and marine pollution by ships, South Korea announces strategies for building smart marine logistics systems.
[Session 4] Cyber Security	The Danish Maritime Authority will implement the maritime security roadmap and plan for the maritime sector starting on January 1, 2019, and announce maritime cyber security related proceedings for two years by BIMCO and CIRM.

Ref. : About e-Navigation Underway 2019

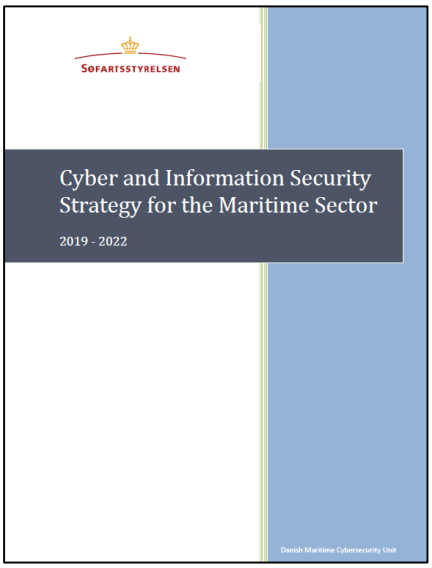
Denmark launches Maritime Cyber Strategy (2019-2022)

● Cyber and Information Security Strategy for the Maritime Sector

As a part of government cyber and information security strategy, the Danish Department of Industry, Business and Financial Affairs announced a new sectoral strategy for the shipping industry. The strategy includes several plans to strengthen IT security and prevent cyber threats at sea. The objective is to ensure the safety of navigation in Danish waters from cyber attacks and the safety of Danish ships, including systems and software for ship operation, propulsion and navigation. It also includes services such as traffic monitoring, warning and information systems, as well as other systems that are connected to the safe operation of the ship. The Danish Maritime Authority will set up the Danish Maritime Cyber security Unit to implement the following strategy step by step.

<Short Term(2019)>

- Establishment of the Danish Maritime Cybersecurity Unit
- EU and international law
- Exchange point between maritime sector players and the CFCS
- Inpatriation of maritime employees to the CFCS
- Increased awareness level through cooperation and knowledge sharing in the maritime sector



<Medium Term(2020-2021)>

- Specific objectives and user-friendly recommendations to maritime sector players
- IT security culture and awareness
- Focus on standardised processes in relation to cyber and information security management
- Ensuring a consistent and robust cyber and information security emergency response in the maritime sector
- Joint emergency response and early warning plan for handling IT security incidents
- Planning and implementation of joint cyber and information security drills

<Long Term(2022)>

- Identify and address the needs and possibilities for developing a digital hub / communications platform where cyber and information security knowledge is made easily accessible to, and searchable by, the authorities and stakeholders of the maritime sector

Ref. : New strategy for cyber security in the Danish maritime sector

UK launches Maritime 2050 Strategy

● Announcing long-term strategy and recommendations for Maritime 2050

The UK government has embarked on technological innovation, a key element of the newly announced Maritime 2050 strategy, including the creation of the Maritime Innovation Hub in an unnamed port by 2030. Maritime 2050 is the first long-term national strategy to set a road map for how the UK government can cooperate with industry to support maritime growth, focusing on seven themes: industry, technology, trade, environment, human resources, infrastructure and security.

The development of SmartPort aims to create new business models to take advantage of digital and automation processes to maximize throughput through seamless connections. The government has also pledged to legislate the framework of autonomous vessels in the country to attract and carry on international business in the UK's territorial waters. Substituting paper-based processes through the transport chain is another explicit statement of strategy, such as the introduction of digital documents to streamline the essential training and verification of crews, and the potential benefits of blockchain.

The UK also aims to regulate the UK's marine spatial digitization centered on transparent data by setting international standards and ensuring system interoperability at IMO, expecting harmonized standards globally by 2050.

Cyber security has attracted attention as an important consideration for the government to maintain strong defenses as development continues across various sectors of the maritime industry. Although the industry is responsible for securing and protecting the resilience of cyber threats across the supply chain, close consultation with the industry is needed for the UK government to assess cyber threats and provide information and advice on threats through the National Cyber Security Center as an overall solution provider for maritime cyber security.

Ref. : UK launches Maritime 2050 strategy

Understanding of Cyber Threat(OWASP Top 10)

● Understanding of cyber threat

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

Open Web Application Security Project (OWASP) is an open source web application security project, mainly researching web exposure, malicious files and scripts, security vulnerabilities. OWASP Top 10, which is frequently used and can give significant impact among web application vulnerabilities, are published in 2004, 2007 , 2010, 2013 and 2017, Following the newsletter in January, we will analyze the '**A1 : 2017 - Injection'.**

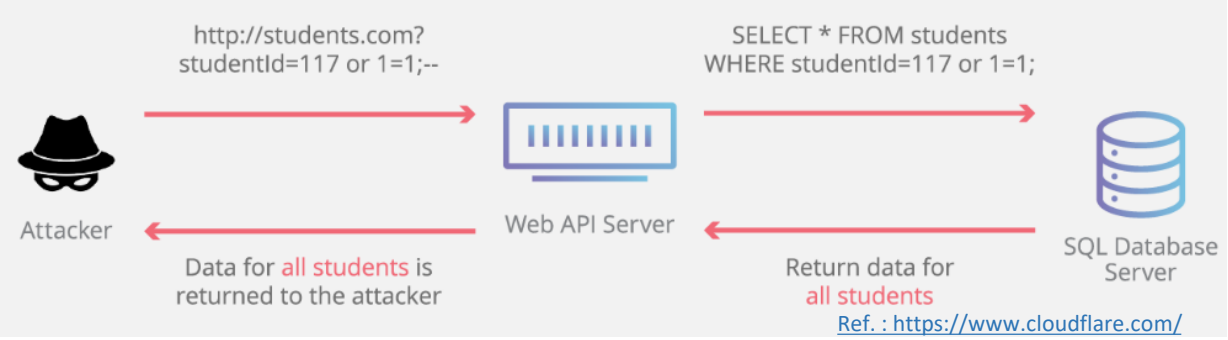
OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities (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.]

Ref. : OWASP Top 10 Project

● OWASP Top 10 'A1 : 2017 - Injection'

Injection is a vulnerability that occurs when an attacker identifies and executes maliciously injected data as part of a normal query of the database in a web application. Injection attacks are possible where data is input or database information is requested. There are different types of injection depending on the attack method and language used: SQL injection, HTML injection, OS command injection, and LDAP.

Structured Query Language (SQL) injection is a code insertion technique used to modify or retrieve data in a SQL database. When an attacker executes a specific SQL command, an unauthorized user can change existing data, modify transactions and balances, and retrieve and / or destroy all server data. The most serious form of SQL injection is that the attacker gets root access to the machine and give it full control.



<Normal SQL query> : Enter '117' in the student ID, the specific student record is returned

<SQL injection query> : Enter '117 or 1=1' in the student ID, the database returns all data in the student table to the attacker, since '1 = 1' is always true.

Is the Application Vulnerable?

An application is vulnerable to attack when:

- User-supplied data is not validated, filtered, or sanitized by the application.
- Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.
- Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.
- Hostile data is directly used or concatenated, such that the SQL or command contains both structure and hostile data in dynamic queries, commands, or stored procedures.

Some of the more common injections are SQL, NoSQL, OS command, Object Relational Mapping (ORM), LDAP, and Expression Language (EL) or Object Graph Navigation Library (OGNL) injection. The concept is identical among all interpreters. Source code review is the best method of detecting if applications are vulnerable to injections, closely followed by thorough automated testing of all parameters, headers, URL, cookies, JSON, SOAP, and XML data inputs. Organizations can include static source (SAST) and dynamic application test (DAST) tools into the CI/CD pipeline to identify newly introduced injection flaws prior to production deployment.

How to Prevent

Preventing injection requires keeping data separate from commands and queries.

- The preferred option is to use a safe API, which avoids the use of the interpreter entirely or provides a parameterized interface, or migrate to use Object Relational Mapping Tools (ORMs).
  Note: Even when parameterized, stored procedures can still introduce SQL injection if PL/SQL or T-SQL concatenates queries and data, or executes hostile data with EXECUTE IMMEDIATE or exec().
- Use positive or "whitelist" server-side input validation. This is not a complete defense as many applications require special characters, such as text areas or APIs for mobile applications.
- For any residual dynamic queries, escape special characters using the specific escape syntax for that interpreter.
  Note: SQL structure such as table names, column names, and so on cannot be escaped, and thus user-supplied structure names are dangerous. This is a common issue in report-writing software.
- Use LIMIT and other SQL controls within queries to prevent mass disclosure of records in case of SQL injection.

Software Development and Test Guideline

● The need for software development security

Software development security is a security activity to develop and operate secure SW through a series of security activities that are carried out at each stage of SW development by removing security weaknesses (developer error, logical error, etc.) that are the cause of cyber attack in advance from SW development stage.

In order to develop and introduce safe software, the roles and responsibilities of each member participating in the project must be clearly defined, security activities must be carried out at each stage of the software development life cycle, and standards for development security must be established.

● KR Guidance for Maritime Cyber Security System requirement (CS1)

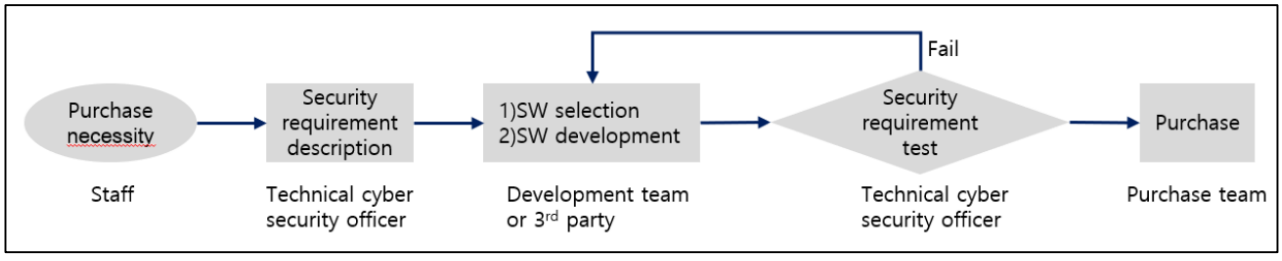
Establish test procedures(212.1) : Procedures should be established to conduct security test before the introduction of software and applications

Security testing (212.2) : Software test should be carried out to identify defects. If the software fails the test, it should be forbidden to apply to the actual operating system

Security acceptance testing (212.3) The environment for test execution should be established and tested according to the procedures

Technical review for operating platform changes (212.4) : The software that has passed the test should be applied to the operating system after obtaining approval from the responsible person

● Software security review procedure (Example)



● Software security checklist (Example)

SW applications security requirements	Result	Remark
Access control		
Is there a function to limit access to certain hosts and networks?		
Connection maintaining times could be set up?		
Is there an encryption capability for remote access?		
User authentication		
Is there a function to limit the minimum number of characters in a password?		
Is there a session lockout function for invalid login attempts?		
Is there a function to set password to include special character?		
Is there a function to set password to change periodically?		
Security function		
Is there a function to restrict anonymous connections?		
Is there a login timeout function?		
Is there backup and recovery capability?		
Availability		
Is there a function to check integrity?		
Is there a function to limit unnecessary services?		
Is there time synchronization capability?		
Is there a function to update software?		
Management and monitoring		
Is there a function to check integrity?		
Is there a capability of process tracking?		
Is there a function to auditing of privilege usage?		

● Software vulnerability check procedures (Example)

Phase	Description
Selection of application	Required module in SW code
Develop checklist	Consider OS version when developing checklist
Perform diagnostics	Check Required and Common Module Targets
Analyze diagnostic results	Create and analyze diagnostic results
Extraction of countermeasures	Prepare countermeasures for diagnosis results
Implementation check	Check for action against vulnerable sources
Create Report	Create diagnostic report

Explanation of Term

NIST Cybersecurity Framework : The US National Institute of Standards and Technology (NIST) has created a security framework in accordance with the Cybersecurity Enhancement Act of 2014 and released version 1.1 of April 2018. The framework provides a flexible way to address cybersecurity, including the impact of cybersecurity on physical cyberspace and human dimensions. This framework is applicable to organizations that rely on information technology (IT), industrial control systems (ICS), cyber physics systems (CPS), and Internet of Things (IoT) technology.

e-Navigation : This refers to the next generation comprehensive marine safety management system for the purpose of safe operation by utilizing real time information and by remote support of ship safety operation combining through advanced ship operation management technology and the advanced ICT in onshore site.

Blockchain : Blockchain is a technology that distributes and stores ledger transactions among all members involved in the transaction. By storing transactions in a distributed to users of the blockchain, there is less risk of falsification and less cost to protect data. The block stores the transaction history for a certain period of time as well as the result of encrypting the previously generated block. Since the previous block, the current block, and the future block are connected by a chain, the longer the block, the more security is enhanced.

SDLC(Software Development Life Cycle) : Software development life cycle refers to a sequence or cycle of information system planning and development, testing, maintenance, and disposal in systems engineering, information systems, and software engineering. Software Development Security or Secure Coding refers to a set of security activities that must be followed during the software development process, such as designing and implementing functions in consideration of security, eliminating potential security vulnerabilities that may exist in source code for safe software development.