KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 017

September 2019

KR Cyber Security Activities

- e-Navigation Underway Asia-Pacific 2019
- KR provided customized Maritime Cyber Security Awareness Training service for VL Enterprise PLC in Thailand

Malicious Mail Defense Training Can Prevent APT Attacks

[Series news] ② 5G Network Architecture and Cyber Threat

Understanding Cyber Threats(OWASP Top 10)

Guidelines for Type Approval of Maritime Cyber Security

Explanation of Term

KR Cyber Security Activities #1

e-Navigation Underway Asia-Pacific 2019

The Korean Register attended the e-Navigation Underway Asia-Pacific 2019 conference held in Korea from 2-3 September, to monitor trends in international policy and the latest maritime cyber security technological developments.

This conference has discussed the key technologies related to the 4th industrial revolution in the marine sector, such as navigation and communication innovation, cyber security, Autonomous Maritime Surface Ship, and marine digital information and communication service international platform, with the theme of e-Nav. implementation in Asia Pacific region: new digital maritime service. [Session 4] was announced on cyber security in the maritime, and technical trends and policy trends were introduced. In particular, the Danish Maritime Affairs (DMA) has been trying to prevent cyber threats in the maritime sector. The DMA established a department for cyber security and announced roadmap for cyber security at national level. The responsibilities and roles of various stakeholders in the maritime business (Port, Ship owner, 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.

Source : https://www.e-navap.org/cop/bbs/selectENUWinfo.do?cttDiv=ENUWA_000000003&siteId=1

Session	Subject
Session 1	Developing and Delivering Digital Maritime Service
Session 2	2-1. Innovations in Marine Navigation and Communication 2-2. Innovations in Marine Navigation and Communication
Session 3	Cooperation and Capacity Building for e-Navigation
Session 4	Cyber Security in the Maritime Sector
Session 5	Upcoming e-Navigation Underway Conferences
Session 6	Panel Discussion and Wrap up

KR Cyber Security Activities #2

KR provided Customized Maritime Cyber Security Awareness Training Service for VL Enterprise PLC in Thailand

The Korean Register provided cyber security awareness training service for OCIMF TMSA and IMO ISM code preparations to VL Enterprise PLC shipping company in Thailand. This training consists of management security, physical security, technical security related matters and risk assessment understanding process for building cyber security system in a shipping company. It provided guidelines for employees to prepare for maritime cyber security issue and received great acclaim in education satisfaction survey.

On the other hand, cyber threats and vulnerability are increasing due to the development of ICT technology, and the importance of cyber security for shipping industries is getting stronger. The International Maritime Organization (IMO) will adopt the MSC.428 (98) resolution on cyber risk integrated management in the ISM Code Safety Management System (SMS) and will take effect in 2021, and the shipping industry also requires cyber security items in the OCIMF-TMSA/SIRE. Therefore, it is expected that 'Cyber Security awareness training' for staffs is necessary to prepare to these international cyber security requirements. The KR have provided customized cyber security training service to SONGA and San-sho Korea, shipping companies, to prepare TMSA inspection and cyber security system construction. The KR plans to strengthen cyber security customized training services for shipping companies, shipyards and equipment companies for maritime cyber security in the future.

Maritime Cyber Security Awareness Training

19-Sep. at Bangkok, V.L. Enterprise PLC.

Course Introduction and Time Table

Trainer: Jeoungkyu Lim(Korean Register)
Sanghoon Choi(Korean Register)

1 Course Introduction

As the Information and Communication Technology (ICT) applied to shipping industry, cyber threats and vulnerabilities related to digitalization, integration and automation of processes and system in shipping have been emerged. According the IMO Resolution MSC.428(98), administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

This one day awareness training course provides the trainees with the knowledge and method to respond to the maritime cyber security issues.

2 Time Table

Time	Category	Details	Trainer
09:00 - 09:50	Maritime cyber security overview	• Introduction • International response in maritime industry • KR cyber security activities	JK Lim
10:00 - 10:50	Administrative security	• Cyber security management system • Maritime cyber security organization • Human security • TMSA Element 13 : Maritime Security	JK Lim
11:00 - 11:50	Cyber Asset / Cyber Threat	• Cyber asset management overview • Identify asset • Asset criticality • Maritime Cyber threat • Threat list	SH Choi
12:00 - 13:00	Lunch Break		
13:00 - 13:50	Physical security	• Purpose and method of physical security • KR Server room physical security • Physical security by risk assessment	JK Lim
14:00 - 14:50	Technical security	• Network security • Vulnerability diagnosis • PC security vulnerability diagnosis	SH Choi
15:00 - 15:50	Understanding of maritime cyber security risk assessment	• Understanding of maritime cyber security and risk assessment • KR cyber security risk process • Application cases	JK Lim
16:00 - 17:00	Workshop	• Hands-on	SH Choi

Malicious Mail Defense Training Can Prevent APT Attacks

"Do not open a suspicious email," "Do not click on the suspicious Internet address included in the email.", These phrases are always a security rule for e-mail. This is because many people are still opening up suspicious emails and are effective gateways to hackers and cyber criminals.

Phishing VS Spear Phishing

Phishing is one of the most popular forms of fraud (social engineering techniques, social engineering) today, using e-mail or instant messaging to fraudulently obtain information that requires confidentiality, such as password privacy, by masking as a message sent by a trusted group and company.

Especially in the past, if phishing mail with a suspicious and unseen title was the main method of spear phishing, it is constantly evolving to use social issues such as disguised as a similar caller address or disguised as a title related to work or to target specific attacks.

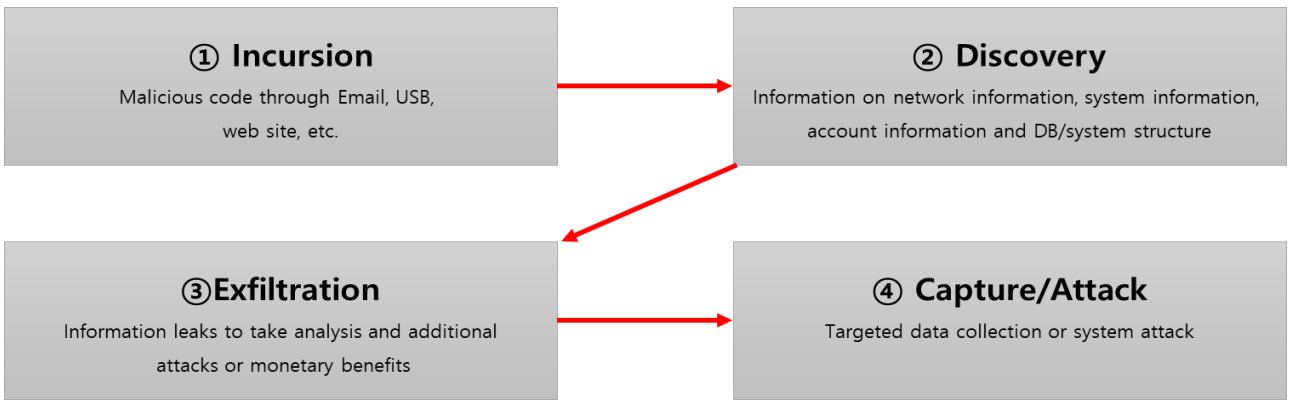
Characteristics of Spear Phishing Mail

- targets targeting specific institutions and businesses, not random
- the severity of malicious code that seeks to leak information, is often far more serious than general advertising and adwords
- The elaboration of the content undoubtedly similar to normal mail

In particular, more than 90% of the APT (Advanced Persistent Threat) attacks that have been revealed so far, depending on overseas statistics, were either started from malicious mail or used for attacks.

Source : https://blog.lgcns.com/2064?category=604440

A Stage of APT Attack



Source : http://cybercafé.tistory.com

Is Spear phishing Mail Really Unpreventable?

When a hacker targets a particular organization or person, the hacker attempts to make a Spear phishing e-mail that is customized with a social engineering technique that impersonates an person or stimulates the interest and curiosity of the person concerned. It is not easy for an individual to distinguish this kind of sophisticated email.

This is because the Spear phishing mail is constantly evolving to spread malicious code to user PCs such as the form of executable file to the form of non-executive file in the form of document, and to avoid detection of security solutions, and is an attack targeting organizational members. However, it is the most effective to prevent damage to Spear phishing mail through the most basic regular security education and to raise awareness of attack threats of Spear phishing mail through a small interest and effort on members. It would be a good defense.

Source : https://blog.lgcns.com/2064?category=604440

For effective malicious mail response training, it should be focused on improving the security awareness of the organization focusing on accident prevention, taking into account internal and external environment of the company all over the company, and the evaluation results of the training should be reflected in the following training and continuously performed.

Subject	Prevention / Detection
Training plan	· Purpose of training, schedule establishment and selection of training subjects · Recently, the case of malicious mail, internal and external environment of the company, and the preparation of scenarios considering the training target · Select evaluation items (input, execution, reporting of security teams, etc.)
Training performance	· Check training environment (securement of security equipment, PC etc.) · Notices through the tracking of the behavior of the training subjects · Write training Statistics and Reports
Training evaluation	· Evaluation of training based on evaluation items and grades · Follow-up selection and information security education
Improvement Plan	· Reflecting the improvement plan according to the evaluation results (education, supplementing the procedure guidelines, etc.) · Reflecting the evaluation results in the follow-up scenario

Source : https://blog.lgcns.com/2064?category=604440

[Series News] ②

5G`s Network Architecture and Cyber Threat

This series will deal with a core infrastructure related to the 4th industrial revolution, the positive ripple effect of 5G on the marine industry, and the cyber threat accordingly. Therefore, this newsletter, Sep. 2019, introduces '5G network structure and network slicing technology.

series news

① What is 5G?

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

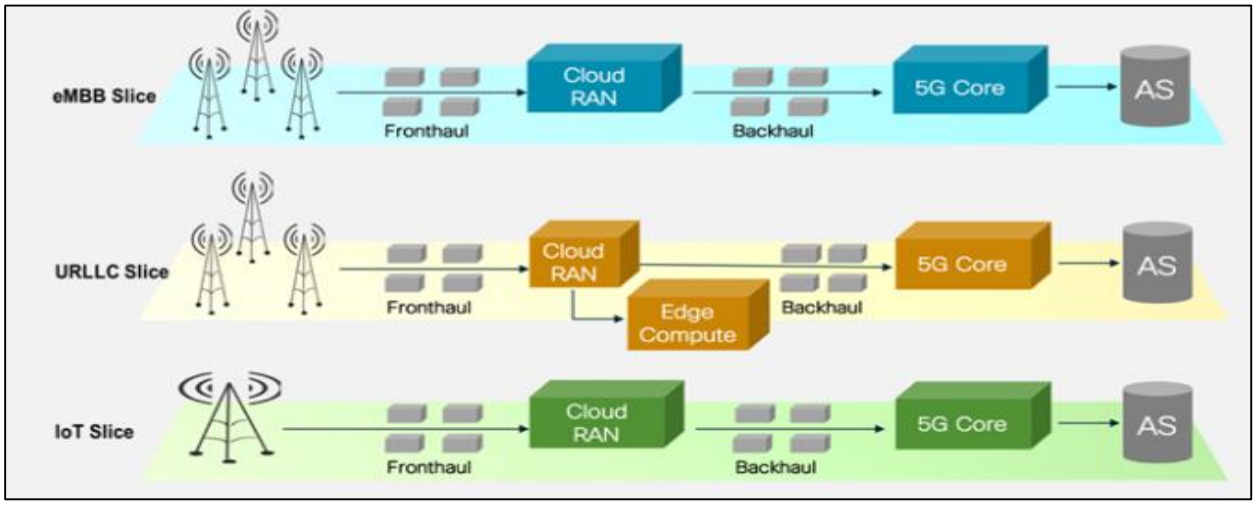
③ Comparison between LTE centralized network and 5G distributed network

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

5G network structure and network slicing

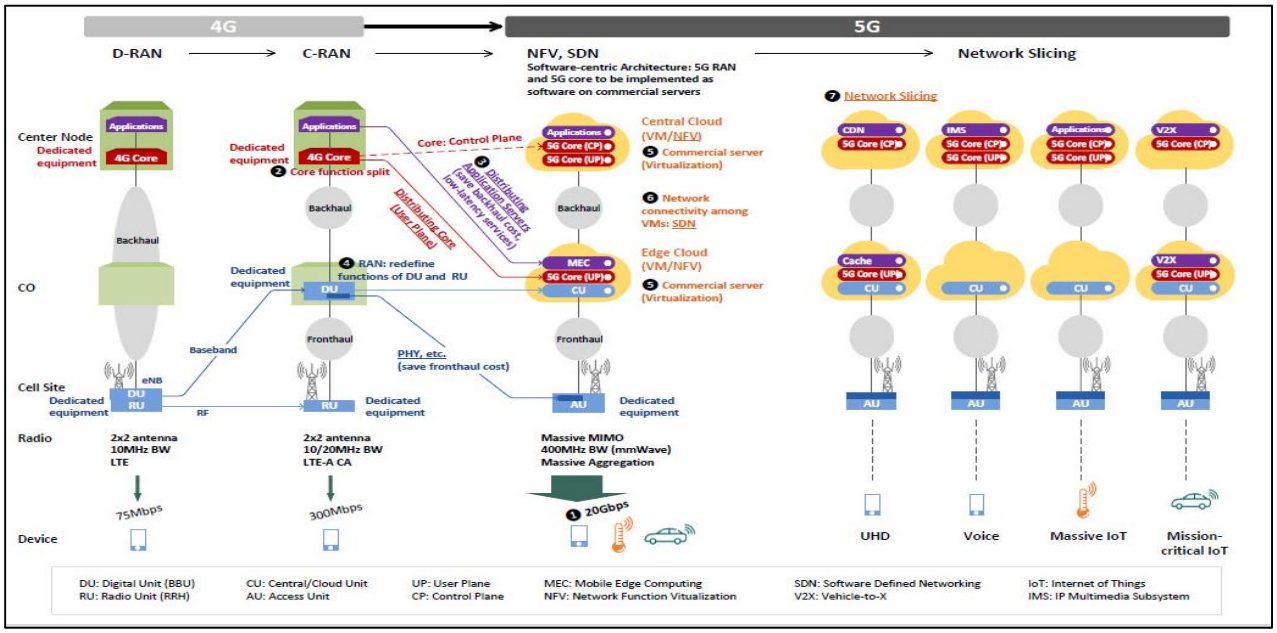
As explained in the August newsletter, 5G has a service-based architecture based on the requirements of each industry. In addition, the separation of CP/UP (Control Plane/User Plane) functions and the modularization of network function (NF) are the main features. The advantages of the 5G network structure are that it can modularize the network functions required by each service such as ships, IoT devices, automobiles, factories, etc., and virtualize them into the optimized network. In this way, a virtual dedicated network technology is called a network slicing technology to divide one physical network into multiple logical networks to guarantee communication performance by service group.



Source : https://www.netmanias.com/en/?m=view&id=blog&no=13311&kw=E2E+Network+Slicing&page=1

5G network structure and network slicing (Continue Page)

In other words, as HDD is partitioned into C and D, it virtualizes the network and provides a dedicated network specialized for the service for various services with different characteristics. For example, in order to respond immediately to the risks that occur on the road, the network associated with autonomous vehicles is most important to perform ultra-low latency of 1 ms. On the other hand, water companies related to Smart City are important for ultra-capacity connection performance that can transmit small amounts of data at the same time on thousands of devices, even though the speed is somewhat slow. So, Is it 5G phone network, 5G Massive IoT network, 5G mission-critical IoT network separately? It is the network slicing technology that reduces the cost by creating several logical networks on one physical delusion.



Source : https://www.netmanias.com/en/?m=view&id=oneshot&no=8393

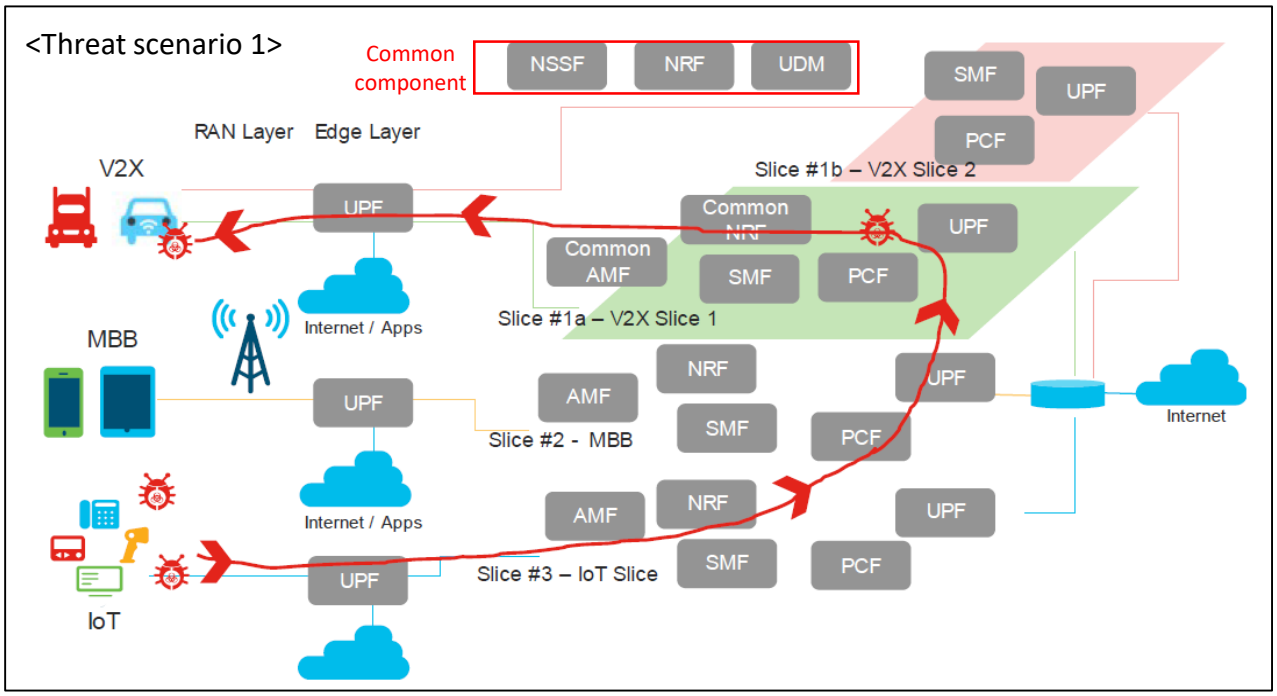
What is the impact of 5G on the marine industry?

In June 2019, the IMO Maritime Safety Commission 101st meeting approved the provisional guidelines for the test operation of Maritime Autonomous Surface Ship (MASS), and the marine industry has been conducting research for the automation and digitalization of existing marine related industries such as MASS, smart port. For the digitalization of the existing marine industry, the development of communication infrastructure is one of the key factors, and international standardization research is also underway to apply 5G. 5G international standardization is carried out in 3GPP. In other words, if the 5G network slicing structure defines the requirements of the marine environment-specific Maritime slice and technology development is carried out, the marine industry is expected to emerge commercial technologies and solutions.

5G Cyber Risk Factors - Threat Factors of 5G Network Slicing Structures

5G makes networks very flexible. They can provide exactly what is required because NFs can be established and removed on a per-need basis and used simultaneously by multiple different slices. Also, network Operations, Administration and Management (OAM) can be simplified and made more flexible. Service providers can utilize automated tools to provide the network services with the predefined redundancy, capacity and other capabilities. Generally, some of these tools and capabilities have been available in the network prior to 5G.

There are common resources and components shared between all the slices, such as the NSSF (Network Slice Selection Function). The rest of the slices may have individual resources assigned, such as AMF, SMF, PCF layers that are dedicated functions catering to specific slices. the attack could be multi-factored by allowing the malware to have the ability to deplete the resources of the slice, therefore causing DoS (Denial of Service) to the actual subscriber. An attacker may also exhaust resources common to multiple slices, causing denial of service or service degradation in other slices as well. This leads to severe degradation in the offered network services. As a cloud native architecture, 5GC (5G Core) has all the functions virtualized that provide the added flexibility required for network slicing. However, this leads to another threat vector. Side channel attacks, coupled with improper isolation between network slices, leads to data exfiltration. This is critical in sensitive parts of the mobile network such as billing, charging and subscriber authentication layers.



Source : The Evolution of Security in 5G, 5G America white paper, July 2019

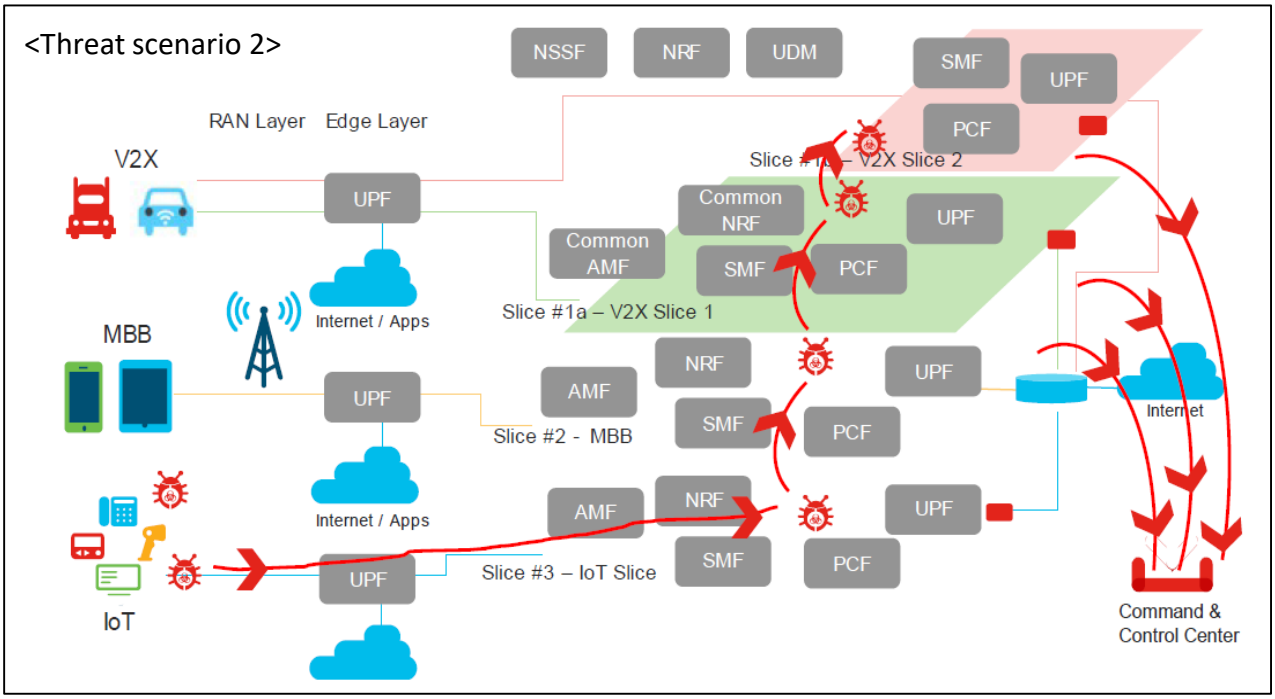
5G Cyber Risk Factors - Threat Factors of 5G Network Slicing Structures

As shown in Figure of threat scenario 2, if the slices and the components within the slice are not adequately isolated, the attacker could access other slice components using the infected device or endpoint in another slice. Figure 4.6 shows the infected device allowing the attacker access to the slice resources. Ultimately, the other slices are exposed and data exfiltration proceeds to an external server (a C&C center, for example).

Once the attacker gathers all the network's information behind the firewall, they could launch an attack on subscribers based on the leaked information. Furthermore, the attacker could use the information for fraudulent financial gains. Network slicing allows operators to offer customized services to customers. It is possible for 5G systems, based on operators' policies, to provide standardized APIs to create, modify, delete, monitor, and update the services of network slices. Slice management also contains critical threat vectors if not secured. Additionally, as per 3GPP standards specifications, the management interface between the Network Slice Management Function (NSMF) and the Communication Service Management Function (CSMF) or between Communication Service Provider (CSP) and Communication Service Customer (CSC) is specified.

Furthermore, interfaces are also specified for the operation phase of management aspects of a Network Slice Instance (NSI), supervision, and performance reporting.

<Threat scenario 2>



Source : The Evolution of Security in 5G, 5G America white paper, July 2019

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

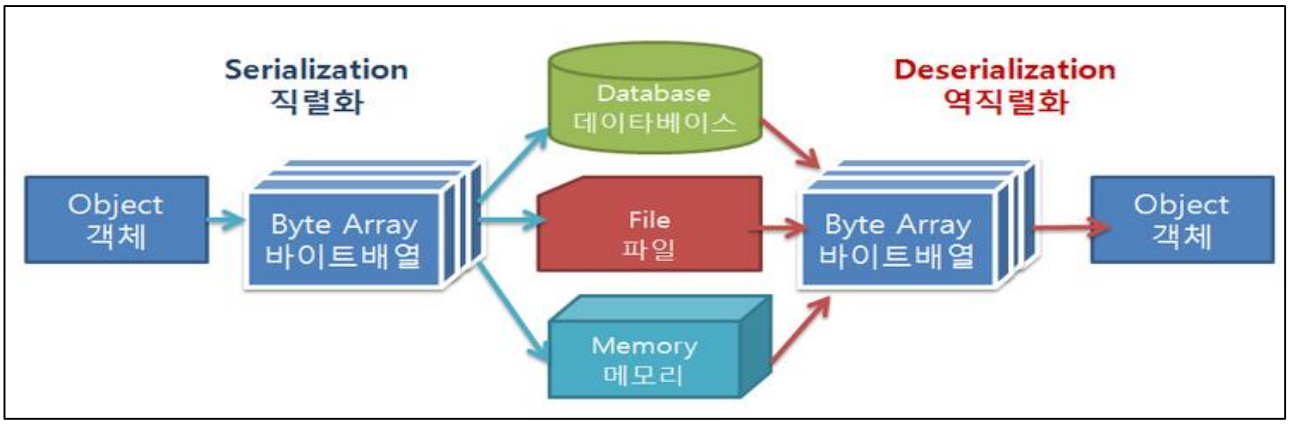
The Open Web Application Security Project (OWASP) is an open source web application security project, researching web exposure, malicious files and scripts, and security vulnerabilities. The OWASP Top 10, which is frequently referred to, highlights the top web application vulnerabilities, it was published in 2004, 2007 , 2010, 2013 and 2017. In this newsletter we will analyze the **'A8 : 2017 – Insecure Desrialization'**

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]	U	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]	U	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 'A8 : 2017 -Insecure Deserialization'

Serialization refers to the process of converting an object into a byte array, which is a combination of 8-bit binary numbers, such as 10100011, and storing the file, memory, or database. In contrast, deserialization is the process of converting a stored object back into an object. Parsing input from untrusted users in applications has traditionally been a major security vulnerability. Deserialization is not much different. This could be because a hacker could force your application to handle malicious forged serialized input. Remote code execution attacks using Object Deserialization in Java are well-known vulnerabilities. Based on the serialization / deserialization principle, the attacker executes the remote code on the server through the TCP / IP protocol. The attacker serializes the command to be executed on the server, converts it into bytes and sends it to the server for deserialization. This is a vulnerability that restores and executes the command received.



Source : https://blog.naver.com/kkson50/220564174258

Is the Application Vulnerable?

Applications and APIs will be vulnerable if they deserialize hostile or tampered objects supplied by an attacker.

This can result in two primary types of attacks:

- Object and data structure related attacks where the attacker modifies application logic or achieves arbitrary remote code execution if there are classes available to the application that can change behavior during or after deserialization.
- Typical data tampering attacks, such as access-control-related attacks, where existing data structures are used but the content is changed.

Serialization may be used in applications for:

- Remote- and inter-process communication (RPC/IPC)
- Wire protocols, web services, message brokers
- Caching/Persistence
- Databases, cache servers, file systems
- HTTP cookies, HTML form parameters, API authentication tokens

How to Prevent

The only safe architectural pattern is not to accept serialized objects from untrusted sources or to use serialization mediums that only permit primitive data types.

If that is not possible, consider one of more of the following:

- Implementing integrity checks such as digital signatures on any serialized objects to prevent hostile object creation or data tampering.
- Enforcing strict type constraints during deserialization before object creation as the code typically expects a definable set of classes. Bypasses to this technique have been demonstrated, so reliance solely on this is not advisable.
- Isolating and running code that deserializes in low privilege environments when possible.
- Logging deserialization exceptions and failures, such as where the incoming type is not the expected type, or the deserialization throws exceptions.
- Restricting or monitoring incoming and outgoing network connectivity from containers or servers that deserialize.
- Monitoring deserialization, alerting if a user deserializes constantly.

Source : OWASP Top 10 - 2017

Guideline for Type Approval of Maritime Cyber Security

Understanding Guideline for Type Approval of Maritime Cyber Security

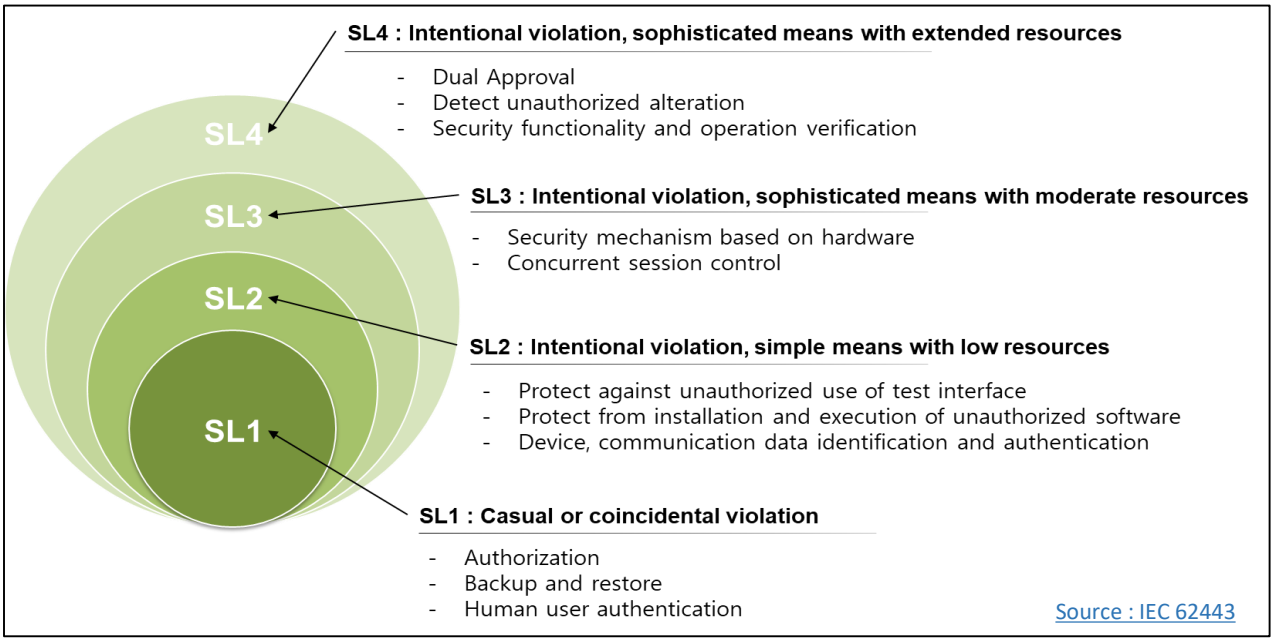
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance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

Authorization enforcement (301)

1. Components should provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities. (SL1)
2. Components should provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.
3. Components should, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all users.
4. Components should support a supervisor manual override for a configurable time or sequence of events.
5. Components should support dual approval when action can result in serious impact on the industrial process. However, dual approval mechanisms should not be employed when an immediate response is necessary to safeguard health, safety and environment consequences, for example, emergency shutdown of an industrial process

The need for empowerment

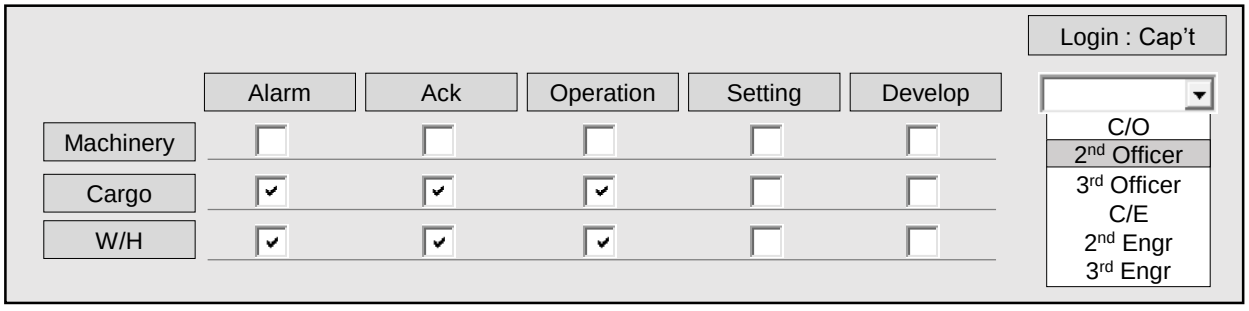
The main purpose of empowerment is to prevent unauthorized work; examples of work include data reading, writing, program downloading and configuration settings. Equipment mounted on a ship should be limited to users who are authorized for safety, but in some cases, specific functions should be opened to emergency measures in a dangerous situation

'**SL 1**' requires each user to be authorized. This prevents unauthorized work by making certain tasks unavailable to unauthorized users.

'**SL 2**' enforces authorization for all users and requires the ability to define and modify roles. Privileges can be managed as a group, but in order to satisfy SL2, all users must be able to map to one or more groups. It should also provide functions for changing and managing roles.

'**SL 3**' requires override. A ship's equipment is provided with safety functions and under normal conditions, a right not normally permitted may be permitted under hazardous conditions. In such cases the manufacturer should define it in advance and make it known to the user.

'**SL 4**' requires dual approval and is the opposite concept of override. Double approval means that two approvals are required to carry out the work. However, it should not apply if an immediate response, such as a safety system, is required



Explanation of Term

Phishing

It is a kind of social engineering technique that tries to get confidential information such as password and credit card information to deny it by pretending to be a message from a reliable company using e-mail or messenger.

Spear Phishing

It is the same as the existing phishing attack disguised as a reliable sender, but it is a phishing that attempts to target a specific person or a specific organization.

Override

When any two systems are present, one system is a software term designed to prioritize another system, which is mainly used to give priority to the safety system in an emergency.

5G Standard related terms

- CP : Control Plane
- UP : User Plane
- NF : Network Function
- 3GPP : 3rd Generation Partnership Project,
- NSSF : Network Slice Selection Function
- AMF : Access and Mobility Management Function
- SMF : Session Management Function
- V2X : Vehicle-to-Everything
- MBB : Mobile Broadband
- IoT : Internet of Things