KR Maritime Cyber Security

News from KOREAN REGISTER

Apr 2019

Vol. **012**

KR Cyber Security Activities

● SEA ASIA 2019 KR’s cyber security technical seminar

KR’s cyber certification team delivered a successful and well attended cyber security technical seminar to delegates at the SEA ASIA 2019 conference in Singapore. The technical seminar consisted of two sessions. In the first, the major cyber security issues facing the maritime industry were addressed and KR’s cyber security activities were discussed. In the second session, the recently developed KR cyber security system type approval was presented. This is the first time KR has offered a technology seminar at an event like this, and it was very well received. The seminar gave the delegates an opportunity to discuss many cyber security issues and answered by KR’s experts.

The cyber certification team also shared information about its cyber security gap analysis, and its technical services and the cyber security training programs offered by KR.

The importance of cyber security has increased around the world, and the seminar offered a valuable opportunity to address concerns about cyber security issues in the maritime industry through the instant question and answer session. KR is concentrating on strengthening its expertise in the field of cyber security and will share its accumulated experience through this exhibition to the benefit of its customers.

Exceptional Technology Extraordinary Service
CH 1 INTRODUCTION
KR
KOREAN REGISTER
IRCLASS
Why Choose KR as Classification

- **SEA ASIA 2019 KR's cyber security technical seminar**

Sea Asia 2019
Korean Register Cyber Security Technical Seminar

9th – 11th April,
Singapore Korean Register Booth
[No.L1-E01]

▪ Cyber Security Technical Seminar

- Date : **9th to 10th April**
- Place : **Korean Register Booth No. L1-E01**
- Team : Cyber Certification Team
- Contents & Presenter
  1) KR Cyber Security Overview (JK Lim, Senior Surveyor)
  2) KR Cyber Security System Type Approval (SH Choi : Senior Surveyor)

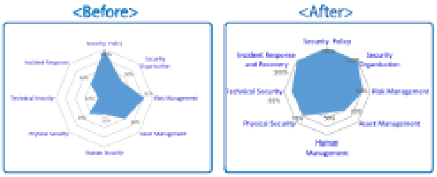
Date	Time	Topic
9th April	14:00 – 14:30	Cyber Security Overview
	14:30 – 15:00	Cyber Security System Type Approval
10th April	10:00 – 10:30	Cyber Security Overview
	10:30 – 11:00	Cyber Security System Type Approval
	14:00 – 14:30	Cyber Security Overview
	14:30 – 15:00	Cyber Security System Type Approval

▪ Provide KR Cyber Security Technical Support (in KR Booth)

1) Gap Analysis for Company & Ship Cyber Security

Korean Register will provide Gap Analysis on 8 main categories* for company & ship cyber security for our client based on KR cyber security checklist.

*Security Policy, Security Organization, Risk Management, Asset Management, Human Security, Physical Security, Technical Security, Incident Response



2) Training Course Introduction

Korean Register will introduce cyber security training course for our client to enhance maritime cyber security capabilities.

● KR issues first certificate of cyber security compliance to T1IT

KR has approved the very first certification of cyber security compliance to be issued to a company in Korea, to T1 Information Technology (T1IT) a specialized IT management company for ships.

The recent emergence of smart ships equipped with the latest Information and Communication Technology makes it easier to control and monitor ship systems, but the risk of exposure to cyber threats is increasing. Accordingly, the International Maritime Organization (IMO) has recommended that ship owners and ship managers incorporate cyber security risk management into their safety management system (SMS) in the International safety management (ISM) code by January 2021.

KR started the inspection and survey process of T1IT's office IT systems and its maintenance system for onboard IT systems in October 2018. The successful certification of cyber security compliance was awarded in March 2019. Kae-myoung Park, general manager in Cyber Certification Team, said "KR issued the first certification of cyber security compliance to a ship management company - Songa Shipmanagement Ltd earlier this year. We now congratulate T1IT on being the first third party company to be certified cyber security compliant, and the very first company in Korea to be recognized in this way."

(주)티원아이티
한국선급(KR) 사이버보안 적합성 인증 획득
- 회사 및 선박 IT 유지보수 -
201 3. 21.(목) 15:30
T1
(주)티원아이티
KR
(사)한

● KR cyber security technical seminar for DSME employees

The KR's Cyber Certification Team has delivered a 'KR maritime cyber security technical seminar' to employees from shipyards, domestic equipment suppliers, and a range of marine policy research institutes such as DSME, KONGSBERG, Marineworks, Hanwha System, LIG Nexone and the Korean Maritime Institute (KMI).

Date	Time	Contents
27th Mar.	13:00 - 13:50	KR Cyber Security Overview
	14:00 – 16:00	Introducing KR's Maritime Cyber Security System (CS ready)
	14:00 – 16:00	Guidance for Cyber Security System Type Approval
28th Mar.	09:00 – 12:00	Cyber Security Risk Assessment

In the seminar, the team has presented and discussed KR's maritime cyber security system Rules (CS ready), KR cyber security system type approval Rules, and the Cyber security risk assessment methods, so that shipyard and equipment suppliers can successfully apply cyber security technical requirements to new ships. The Cyber security risk assessment method has been highly appreciated, it gives a four-step process for evaluating cyber risk which can be applied to actual ships. Looking ahead, KR will continue to offer cyber security technical seminars for its customers as a way to increase value and satisfaction.

The insider threats to maritime IT/OT systems

● The insider threats maritime IT/OT Systems

The marine industry is a vast field that accounts for about 90% of the global supply chain. The maritime transport industry uses various operational technologies (OT) such as GPS, AIS, ECDIS and information technology (IT). Damage to these systems can result in physical damage to the ship as well as data leakage, endangering all life on board. Insider threats, whether intentional or not, are considered one of the biggest cyber threats to business.

1. Human Error - High click rates for phishing campaigns, negligence (leaving technology open and accessible), loss of technology, such as a laptop or a phone;

2. Malicious Insider - Criminal insiders leaking sensitive data, infecting computer systems with malware, abuse of internal privileges and disgruntled employees;

3. Social Engineering - The manipulation of seafarers to gain sensitive information. This can contribute to spear phishing, senior management spoofing, smishing and vishing

● Ways to address

1. The education, training and exercising of the crew and shore based employees enhances their ability to competently react to attacks, find faults, understand the threat
2. A risk management strategy is vital in the assurance of IT/OT system assets. An effective risk management framework can create resilience in people, process and technology.
3. The development of an Incident Response Plan (IRP) should provide the vessel with the ability to respond quickly and effectively in a timely manner.
4. Information sharing with your community is vital. This will inevitably help in optimising the business recovery process, ensuring business continuity at the earliest opportunity.
5. Conduct testing and auditing. Penetration tests by ethical hackers attempt to breach an organisation’s network to expose vulnerabilities.

Ref. : PHISH & SHIPS NEWSLETTER(APR. 2019)

Ultimately, people can become one of the organization's greatest risks if not managed effectively, and they need to be educated and aware of the constantly changing threat environment.

Understanding of cyber threats (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, 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.

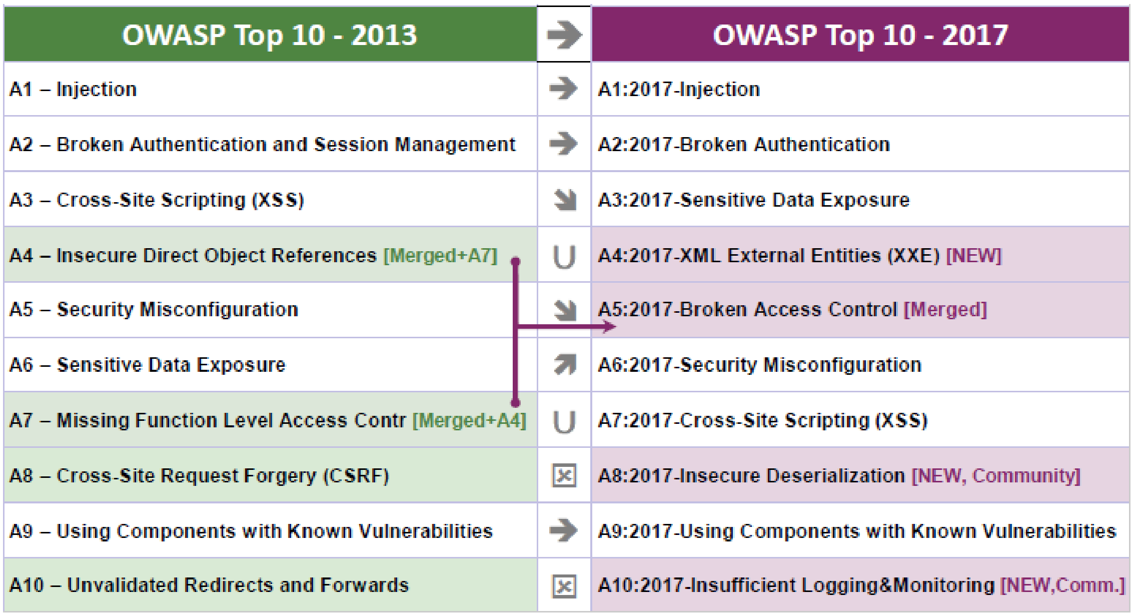
● KR Guidance for Maritime Cyber Security System requirement (CS1)

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, mainly 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 **'A3 : 2017 – Sensitive Data Exposure'**

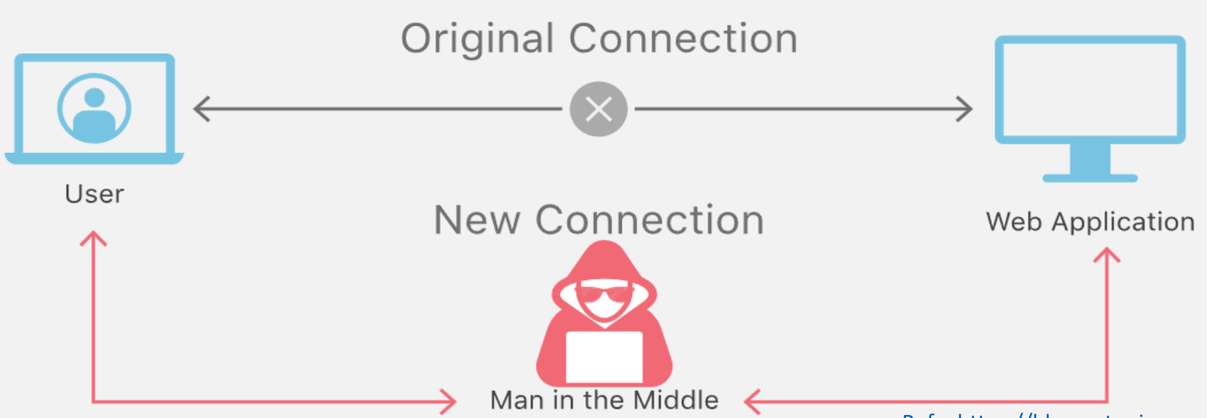


OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities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

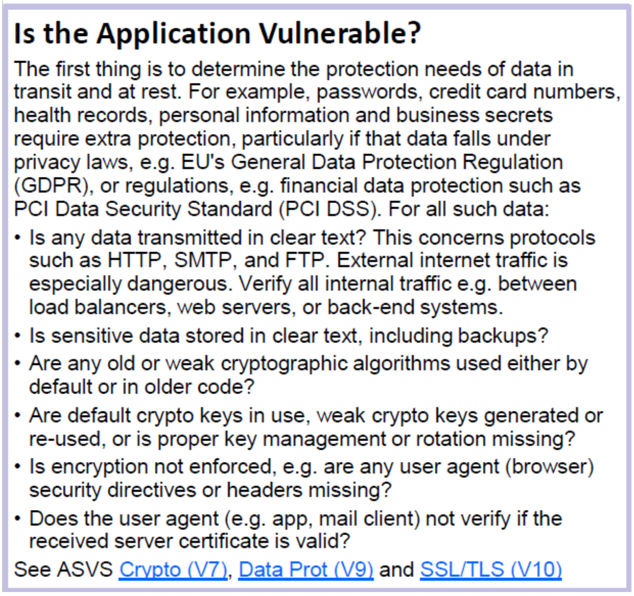
● OWASP Top 10 ‘A3 : 2017 – Sensitive Date Exposure’

When clients and servers communicate, they must use cryptographic protocols (SSL) to protect sensitive information. Also, when users input sensitive information, they must be encrypted and stored. In this case, data processing and encrypted storage should be performed on a server basis. Sensitive data exposure is a vulnerability that occurs when client and server are not using SSL to protect sensitive information when communicating. In particular, if the user does not store encrypted information when entering sensitive information, an attacker can steal information from the medium. In addition, even if data processing and encryption storage are performed by the client, the attacker can take control of the client PC and take the information, so data processing and encryption must be performed on the server side.



Ref. : https://blog.netwrix.com

1. If an attacker intercepts or modifies communication between two devices
2. An attacker can impersonate one of two agents or collect information continuously
3. These attacks target non-website e-mail communications, DNS lookups, and public WiFi

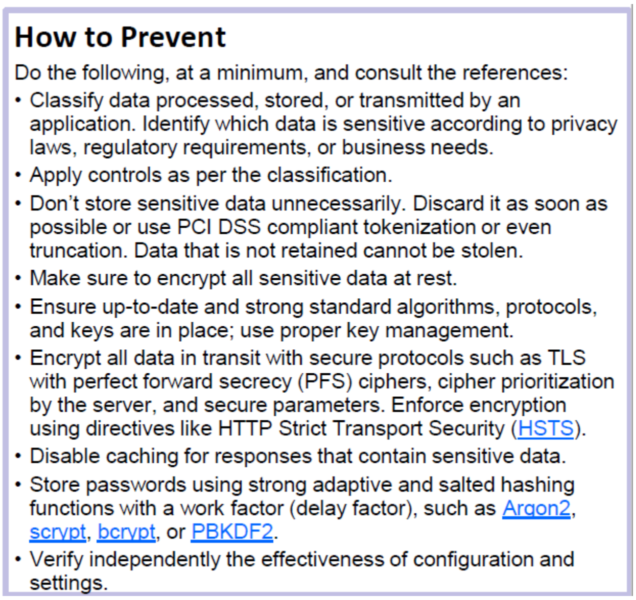


Is the Application Vulnerable?

The first thing is to determine the protection needs of data in transit and at rest. For example, passwords, credit card numbers, health records, personal information and business secrets require extra protection, particularly if that data falls under privacy laws, e.g. EU's General Data Protection Regulation (GDPR), or regulations, e.g. financial data protection such as PCI Data Security Standard (PCI DSS). For all such data:

- Is any data transmitted in clear text? This concerns protocols such as HTTP, SMTP, and FTP. External internet traffic is especially dangerous. Verify all internal traffic e.g. between load balancers, web servers, or back-end systems.
- Is sensitive data stored in clear text, including backups?
- Are any old or weak cryptographic algorithms used either by default or in older code?
- Are default crypto keys in use, weak crypto keys generated or re-used, or is proper key management or rotation missing?
- Is encryption not enforced, e.g. are any user agent (browser) security directives or headers missing?
- Does the user agent (e.g. app, mail client) not verify if the received server certificate is valid?

See ASVS Crypto (V7), Data Prot (V9) and SSL/TLS (V10)



How to Prevent

Do the following, at a minimum, and consult the references:

- Classify data processed, stored, or transmitted by an application. Identify which data is sensitive according to privacy laws, regulatory requirements, or business needs.
- Apply controls as per the classification.
- Don't store sensitive data unnecessarily. Discard it as soon as possible or use PCI DSS compliant tokenization or even truncation. Data that is not retained cannot be stolen.
- Make sure to encrypt all sensitive data at rest.
- Ensure up-to-date and strong standard algorithms, protocols, and keys are in place; use proper key management.
- Encrypt all data in transit with secure protocols such as TLS with perfect forward secrecy (PFS) ciphers, cipher prioritization by the server, and secure parameters. Enforce encryption using directives like HTTP Strict Transport Security (HSTS).
- Disable caching for responses that contain sensitive data.
- Store passwords using strong adaptive and salted hashing functions with a work factor (delay factor), such as Argon2, scrypt, bcrypt, or PBKDF2.
- Verify independently the effectiveness of configuration and settings.

Guidelines for establishing malicious code response

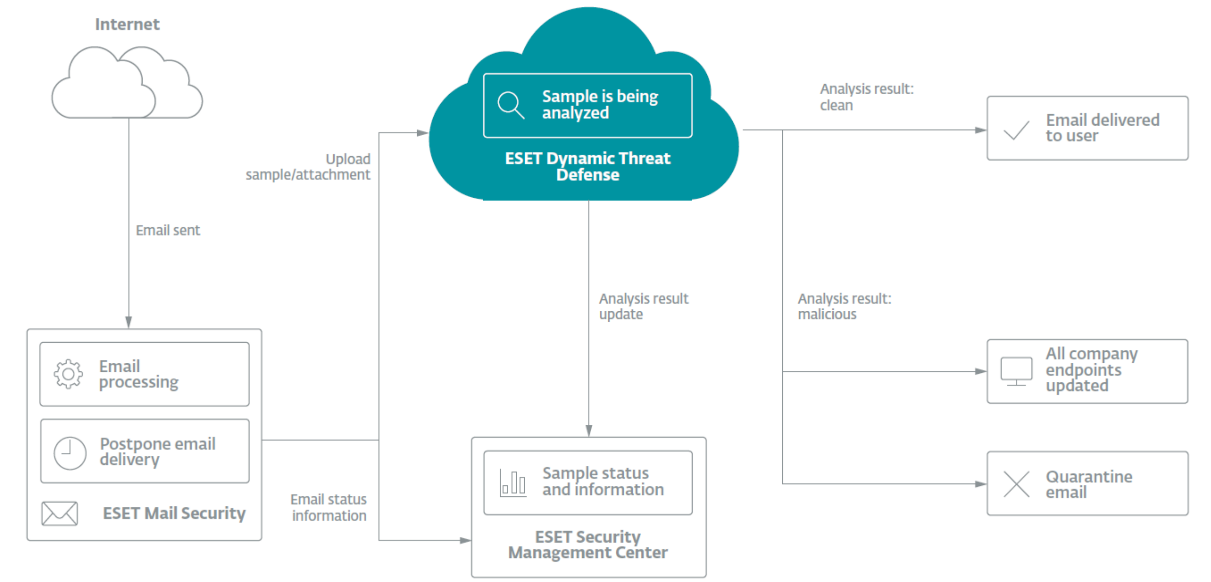
● Necessity of establishing malicious code response

A malicious code is any malicious program intended to cause harm to a user, and any executable form that runs on a computer, such as a macro or script. NotPetya, used in the 2017 Maersk Shipping ransomware infection case, was a variant of the ransomware 'Petya' that requires bitcoin at the cost of decoding the entire MRB (Master Boot Record) file by exploiting Windows Server Message Block (SMB) vulnerability. Such malicious code can have a huge impact on the business operation of the enterprise, and it is necessary to establish appropriate countermeasures. (Norton, McAfee, ESET, etc.), PCs, servers, and mobile terminals, and measures such as sandbox security.

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

Malicious code response (217) : Controls to protect networks, information systems, operating systems, and terminals from malicious code should be provided.

● Sandbox Concept (example)



Ref. : ESET-Solution-Overview-Dynamic-Threat-Defense

Explanation of terms

- **SSL(Secure Sockets Layer)** : SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. To be able to create an SSL connection a web server requires an SSL Certificate. During the SSL Certificate application process, the Certification Authority will validate your details and issue an SSL Certificate containing your details and allowing you to use SSL. Your web server will match your issued SSL Certificate to your Private Key. Your web server will then be able to establish an encrypted link between the website and your customer's web browser.
- **Man in the middle attack(MITM)** : an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example of a MITM attack is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted wireless access point (Wi-Fi) could insert themselves as a man-in-the-middle.
- **Sandbox** : a security mechanism for separating running programs, usually in an effort to mitigate system failures or software vulnerabilities from spreading. It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the host machine or operating system. A sandbox typically provides a tightly controlled set of resources for guest programs to run in, such as scratch space on disk and memory.