KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 023

March 2020

KR Cyber Security Activities

- KR established cyber security training course in Singapore

CIRM Releases cyber security Guidelines

Vulnerability Analysis and Countermeasures of Wireless Networks

Understanding Cyber Threats(OWASP Top 10 Internet of Things)

Guidelines for Type Approval of Maritime Cyber Security

Explanation of Term

KR Cyber security Activities #1

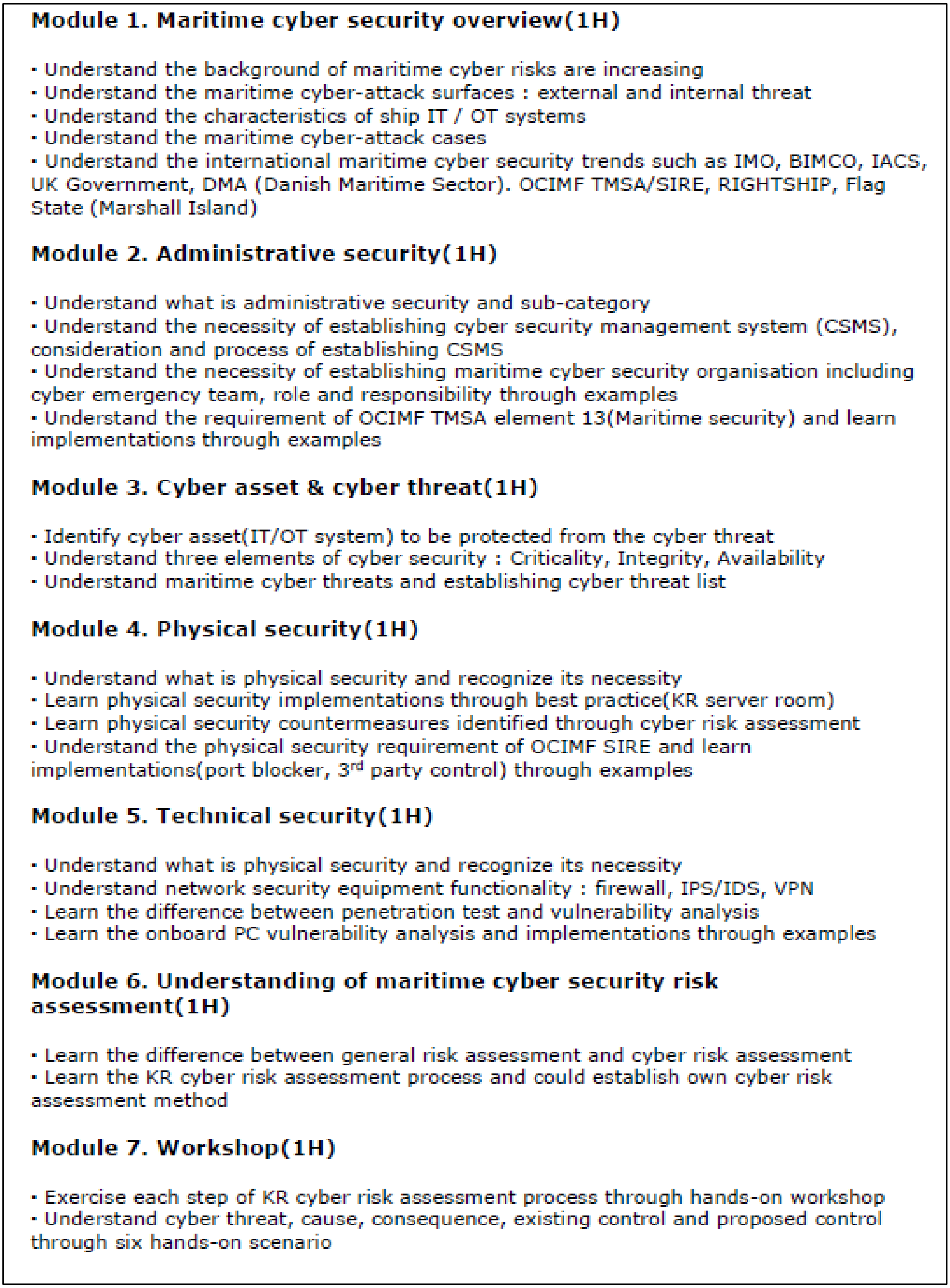
KR established cyber security training for shipping companies in Singapore

At the beginning of February 2020, KR provided customized cyber security awareness training for 38 sailors and employees from a range of ship management companies in Singapore, including the Singapore Maritime Authority (MPA), ADK Maritime, and Janus Shipping.

KR has been working with the Singapore Maritime Authority (MPA), discussing the inclusion of cyber security awareness into their educational support program, as part of the Maritime Cluster Fund. This project offers Singapore-based companies a 50% reduction on the training costs for KR's cyber security awareness training, made possible Singapore Maritime Authority. KR's Cyber Security Awareness Training Program includes The Oil Companies International Marine Forum's (OCIMF) Tanker Management and Self-Assessment (TMSA) program. The TMSA program offers companies a comprehensive understanding of cyber security, maritime cyber threats and responses, maritime cyber risk reduction methods and practical applications, cyber asset inventory and cyber risk assessment practices. In addition to Ship Inspection Report Program (SIRE) testing, it provides information and ways to address IMO Resolution MSC.482 (98).

KR provides customized cyber security training services for shipyards and equipment companies, as well as shipping companies. From May 2020, companies with staff taking the first and second courses in cyber security awareness training can benefit from subsidized costs

KR approved by Singapore MPA regarding training course



Module 1. Maritime cyber security overview(1H)

- Understand the background of maritime cyber risks are increasing
- Understand the maritime cyber-attack surfaces : external and internal threat
- Understand the characteristics of ship IT / OT systems
- Understand the maritime cyber-attack cases
- Understand the international maritime cyber security trends such as IMO, BIMCO, IACS, UK Government, DMA (Danish Maritime Sector). OCIMF TMSA/SIRE, RIGHTSHIP, Flag State (Marshall Island)

Module 2. Administrative security(1H)

- Understand what is administrative security and sub-category
- Understand the necessity of establishing cyber security management system (CSMS), consideration and process of establishing CSMS
- Understand the necessity of establishing maritime cyber security organisation including cyber emergency team, role and responsibility through examples
- Understand the requirement of OCIMF TMSA element 13(Maritime security) and learn implementations through examples

Module 3. Cyber asset & cyber threat(1H)

- Identify cyber asset(IT/OT system) to be protected from the cyber threat
- Understand three elements of cyber security : Criticality, Integrity, Availability
- Understand maritime cyber threats and establishing cyber threat list

Module 4. Physical security(1H)

- Understand what is physical security and recognize its necessity
- Learn physical security implementations through best practice(KR server room)
- Learn physical security countermeasures identified through cyber risk assessment
- Understand the physical security requirement of OCIMF SIRE and learn implementations(port blocker, 3rd party control) through examples

Module 5. Technical security(1H)

- Understand what is physical security and recognize its necessity
- Understand network security equipment functionality : firewall, IPS/IDS, VPN
- Learn the difference between penetration test and vulnerability analysis
- Learn the onboard PC vulnerability analysis and implementations through examples

Module 6. Understanding of maritime cyber security risk assessment(1H)

- Learn the difference between general risk assessment and cyber risk assessment
- Learn the KR cyber risk assessment process and could establish own cyber risk assessment method

Module 7. Workshop(1H)

- Exercise each step of KR cyber risk assessment process through hands-on workshop
- Understand cyber threat, cause, consequence, existing control and proposed control through six hands-on scenario

CIRM releases cyber security guidelines

CIRM releases cyber security guidance for Ship's electronic equipment

CIRM Guideline

GL-002

IMPLEMENTING THE CIRM CYBER RISK CODE OF PRACTICE
FOR VENDORS OF MARINE ELECTRONIC EQUIPMENT AND SERVICES

Edition 1.0
February 2020

Comité International Radio-Maritime (CIRM)
202 Lambeth Road, London, SE1 7JW, United Kingdom
Tel: +44 (0) 20 3411 8344
Email: office@cirm.org
www.cirm.org

The Comite International Radio-Maritime (CIRM) took a step towards tightening cyber security in shipping by issuing cyber security guidelines for electronics onboard ships in February 2020. CIRM is a major international NGO for ship's electronical equipment, with over 110 companies in 30 countries around the world, and extensive activities at major international conferences (IMO, ITU, IEC, etc.). The CIRM cyber security guidelines provide information on how vendors build cyber security, reflecting growing interest across the international maritime business community.

- The CIRM Cyber Security Guidelines contains two notable documents:
- CIRM Guideline on Implementing the CIRM Cyber Risk Code of Practice

The CIRM Code of Practice is comprised of six principles for suppliers to build a secure digital maritime environment. The Code enables effective implementation of cost-effective cyber security using best practices taken from the marine and other industries.

Basic Principle	Details
#1 Observance of relevant cyber risk standards, recommendations and guidance	▪ Consider risk mitigation in the way that services and installations are delivered. ▪ Deliver and maintain products and services with a defined level of cyber security and cyber resilience, for example by compliance with standards and recommendations provided by the IMO, ISO, IEC, IACS.
# 2 Default cyber secure	▪ Set products and systems to a configuration, where the necessary cyber security risk mitigations are enabled in their normal operating mode.
# 3 Confidentiality	▪ Treat customer data as confidential when it relates to cyber security and cyber security events. Unless otherwise agreed with the customer.
# 4 Quality as the foundation for cyber risk management	▪ Ensure that products and services are designed, developed and delivered to an accepted industry standard Quality Management System (e.g. ISO 9001)
# 5 Software updates and vulnerability handling	▪ Inform the relevant parties of risks to a product or service's cyber security, as soon as vulnerabilities are identified. ▪ Input vulnerability information when running risk assessments. ▪ Publicize the date deadlines that mark the end of support and updates for products or services. ▪ Share vulnerabilities, threats and cyber incidents to reduce the spread of malware.
# 6 Continuous development	▪ Actively participate in CIRM activities related to the ongoing development of cyber security measures and industry standards/

Vulnerability Analysis and Countermeasures of Wireless Networks

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

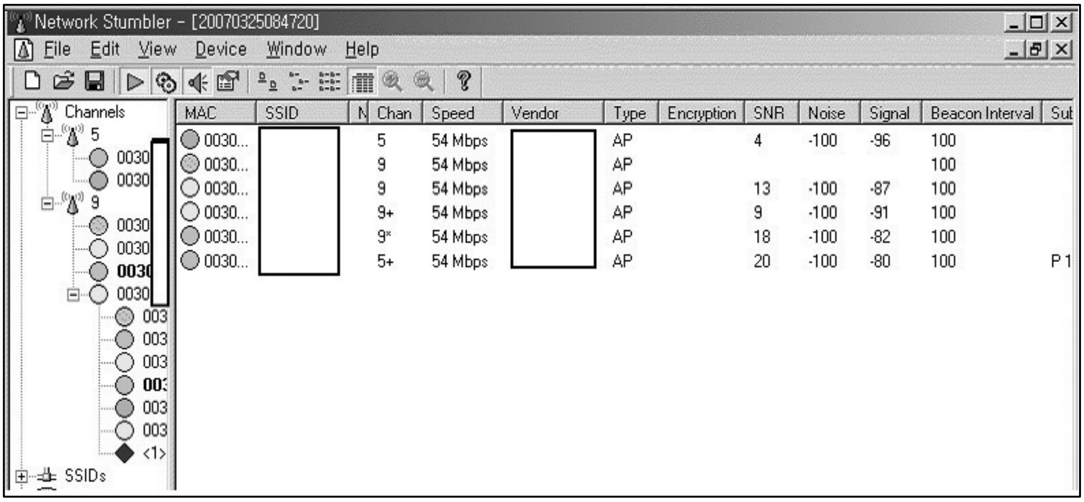
Technical Security Vulnerabilities in Wireless Local Area Networks (WLANs)-1

The security threats facing the WLAN, as defined in the IEEE (Institute of Electrical and Electronics Engineers) 802.11 family of products will be examined. Wireless LANs are widespread thanks to their ease of installation. However, they are vulnerable because they use radio signals to transmit information through the air, which can be intercepted. As a result of the wireless transmission, Wireless LAN is vulnerable to different attack methods than wired LANs. The types of threat are listed below, next to a brief description of the threat.

Type of Threat	Descriptions
Wiretapping	The most fundamental problem of a WLAN is eavesdropping. Wiretapping means an unauthorized person can listen to internet traffic.
Denial of Service (DoS) Attacks	A denial of service attack sends a large volume of wireless packets to wireless AP devices that provide wireless services and can disable wireless LANs.
Rouge AP	An attacker illegally installs a wireless AP to collect data from WLAN users and finding the exact location of an illegal AP is very difficult.
Weak wireless encryption method	WEP (Wired Equivalency Protocol) is an older and more vulnerable wireless data encryption method. The use of short initial vector (IV) value and incomplete RC4 algorithm makes it an ineffective method of encryption.
Unauthorized access	A WLAN can be accessed if there is no authentication procedure. Unauthorized access can involve someone obtaining the Service Set Identifier (SSID) value and setting the acquired SSID value in the wireless terminal.

1. Wiretapping

The most fundamental problem of WLAN is eavesdropping. Radio waves sent from a wireless access point can extend beyond the range they are required, depending on the terrain and signal strength. A client equipped with a wireless LAN card and software for eavesdropping can see and identify the basic configuration of a detected WLAN. An example is software such as 'Net Stumbler' that allows you to check information such as SSID information, WLAN encryption method, WLAN speed and signal sensitivity.



MAC	SSID	N	Chan	Speed	Vendor	Type	Encryption	SNR	Noise	Signal	Beacon Interval	Sul
0030...	[redacted]		5	54 Mbps	[redacted]	AP		4	-100	-96	100	
0030...	[redacted]		9	54 Mbps	[redacted]	AP					100	
0030...	[redacted]		9	54 Mbps	[redacted]	AP		13	-100	-87	100	
0030...	[redacted]		9+	54 Mbps	[redacted]	AP		9	-100	-91	100	
0030...	[redacted]		9*	54 Mbps	[redacted]	AP		18	-100	-82	100	
0030...	[redacted]		5+	54 Mbps	[redacted]	AP		20	-100	-80	100	P 1

Countermeasures to the threat of WIFI Wiretapping

1. Access restriction through the Service Set Identifier (SSID) setting

SSID is the technical term used for a network’s name. A user who wants to access a WLAN service must identify a WLAN service nearby. If the user does not know the SSID, they will not be able to find a WLAN service to connect to. When setting up the SSID, an administrator may choose not to broadcast the SSID (name of network), which will stop potential attackers from being able to eavesdrop. Access by authorized users will just be a case of the administrator disclosing the SSID to the user.

2. Access restriction through Media Access Control (MAC) address authentication

Eavesdropping by attackers can be avoided by restricting MAC address authentication to a wireless AP or router. A MAC address is an exclusive number that is assigned to a computer or router and allows an AP to connect to a network. An administrator can grant access to computers that have an authorized MAC address and it can be applied on the switch or the AP itself. However, this method can increase the load on routers or switches, so there are relatively few examples of it being applied to a router. Attackers may also cause a security breach through MAC Spoofing. Spoofing happens when attackers change their computer’s MAC address to one that has been authorized for another device (identity theft).

출처 : KISA, 무선랜 보안 가이드라인

Understanding Cyber Threats(OWASP Top 10 IoT)

Understanding cyber threats

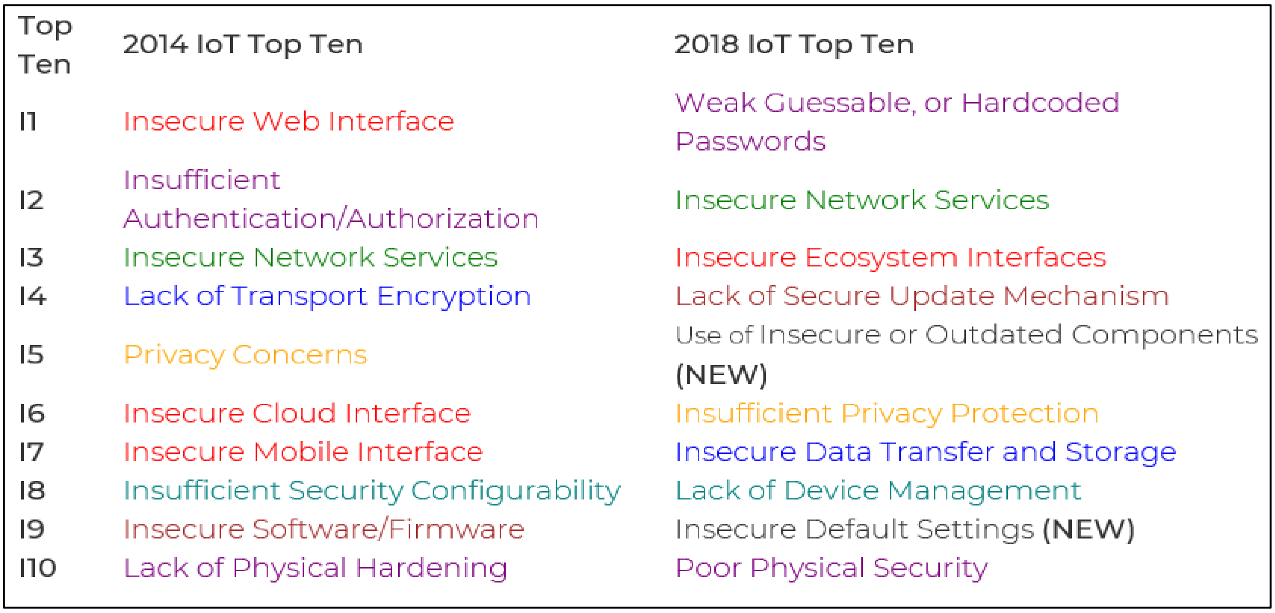
A cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, or the nation state through unauthorized access to an information system, causing destruction,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

Inferred Password Security Vulnerability

The password is the dominant authentication method security tool. If a computer's password is cracked, everything on that computer is available to anyone with that password. Unfortunately, many people use predictable, simple passwords. In 2015, there was a case where an Italian security company 'hacking team' was hacked. The employees were found to be relying on easy-to-guess passwords, such as 'passw0rd' and 'passw@rd'. The company develops and sells spyware for surveillance and eavesdropping. It was also named as one of the top five hacking companies by France's non-governmental organization, Reporters Without Borders

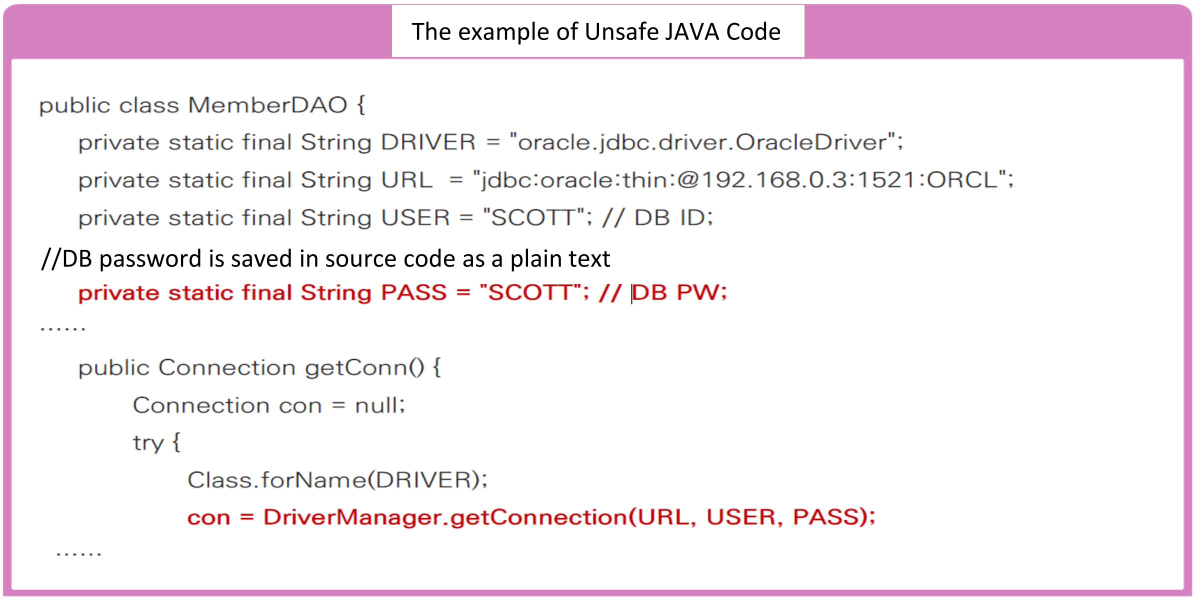
Vulnerability Due to Hardcoded Passwords in Ship Satellite Communication Terminals

A hardcoded password is found within the code of a program used for internal authentication or communication with external components. Hardcoded passwords are dangerous because of the risk that administrator information might be exposed. Satellite communication terminals commonly used in ships, including VSAT, Inmarsat, Iridium, and Thuraya, have well-known security vulnerabilities. The vulnerabilities are the result of hard-coded passwords or sensitive information.

CVE Code	Vulnerability	Description
CVE-2013-6035	Zing protocol	satellite terminals does not require authentication for sessions on TCP port 1827
CVE-2013-6034	hardcoded credentials	satellite terminals has hardcoded credentials, which makes it easier for attackers to obtain unspecified login access via unknown vectors
CVE-2014-0326	hardcoded credentials	Iridium satellite terminals allow remote attackers to read hardcoded credentials via the web interface.
CVE-2014-2964	hardcoded credentials	Cobham Aviator 700D and 700E satellite terminals have hardcoded passwords for the (1) debug, (2) prod, (3) do160, and (4) flrp programs, which allows physically proximate attackers to gain privileges by sending a password over a serial line.
CVE-2014-2941	Hardcoded Credentials	Cobham Sailor 6000 satellite terminals have hardcoded Tbus 2 credentials, which allows remote attackers to obtain access via a TBUS2 command

Countermeasures to the threat of hard coded password

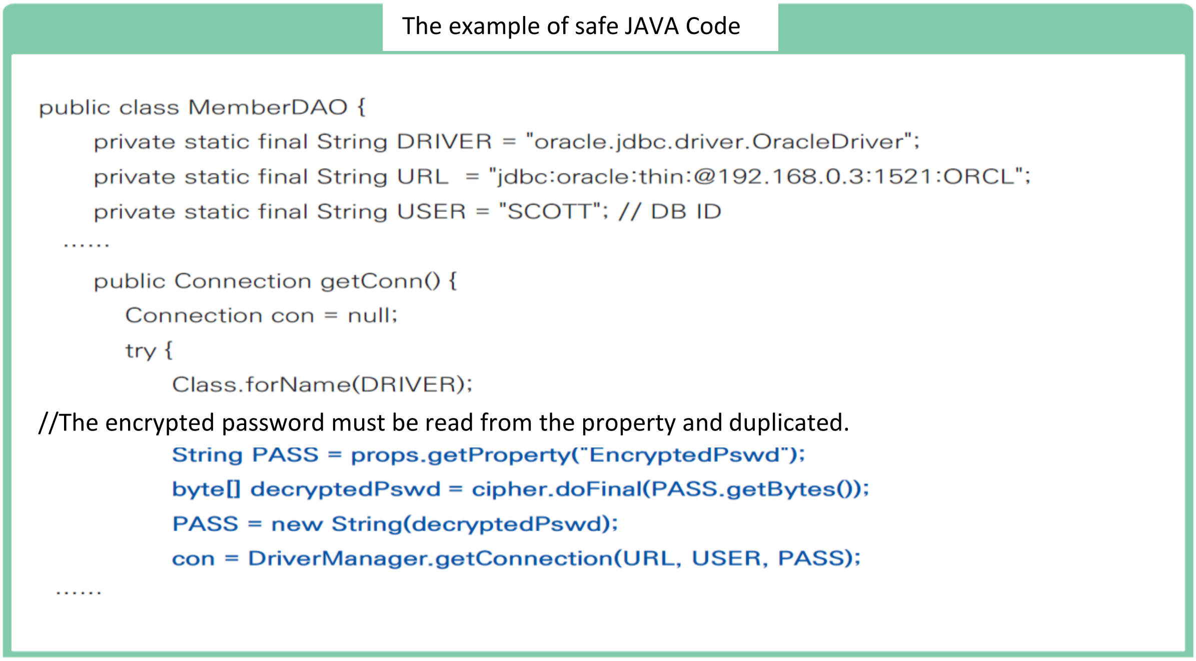
Ideally, a password should be designed to make it easy for users to encrypt the password. The encrypted password or key can improve security, if the user stores it in a separate file and uses the "first-login" mode instead of using the default password and key that were used for software installation. It is dangerous to hard code passwords, especially passwords intended for database connection in constant form inside source code.



The example of Unsafe JAVA Code

```
public class MemberDAO {
    private static final String DRIVER = "oracle.jdbc.driver.OracleDriver";
    private static final String URL  = "jdbc:oracle:thin:@192.168.0.3:1521:ORCL";
    private static final String USER = "SCOTT"; // DB ID;
//DB password is saved in source code as a plain text
    private static final String PASS = "SCOTT"; // DB PW;
……
    public Connection getConn() {
          Connection con = null;
          try {
                Class.forName(DRIVER);
                con = DriverManager.getConnection(URL, USER, PASS);
 ……
```

The password must be encrypted, using a secure encryption method and stored in a separate space (file). In order to use the encrypted password, it must be decrypted.



The example of safe JAVA Code

```
public class MemberDAO {
      private static final String DRIVER = "oracle.jdbc.driver.OracleDriver";
      private static final String URL  = "jdbc:oracle:thin:@192.168.0.3:1521:ORCL";
      private static final String USER = "SCOTT"; // DB ID
  ……
      public Connection getConn() {
         Connection con = null;
         try {
              Class.forName(DRIVER);
//The encrypted password must be read from the property and duplicated.
              String PASS = props.getProperty("EncryptedPswd");
              byte[] decryptedPswd = cipher.doFinal(PASS.getBytes());
              PASS = new String(decryptedPswd);
              con = DriverManager.getConnection(URL, USER, PASS);
 ……
```

Guideline for Type Approval of Maritime Cyber Security

Understanding Guideline for Type Approval of Maritime Cyber Security

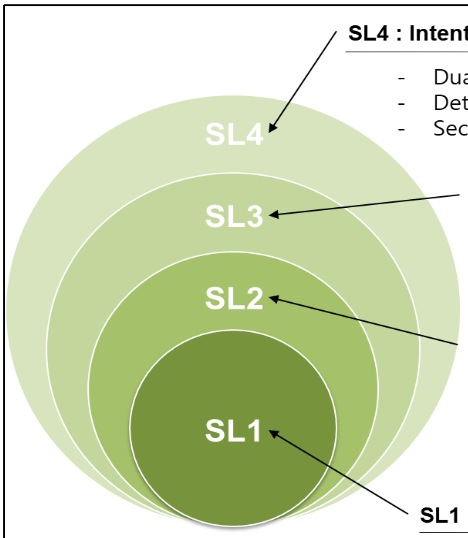
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance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



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 Cyber Security Inspection Items

Host Device Requirements - Support for updates (1104)

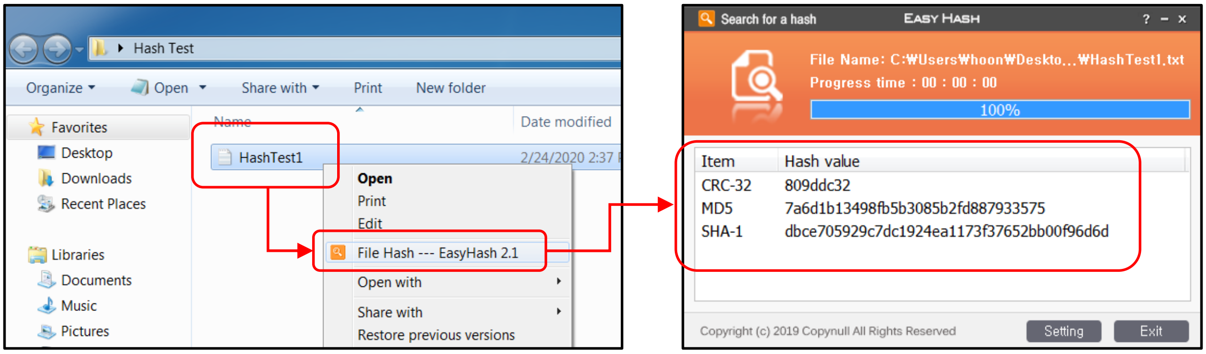
1. Host devices should support the ability to be updated and upgraded.(SL 1)
2. Host devices should validate the authenticity and integrity of any software update or upgrade prior to installation.(SL 2,3,4)

Update File Integrity Check with Hah Value

Some security requirements may need to be applied differently, depending on equipment or type. Cyber security type approval guidelines for these requirements have classified software applications, embedded hardware, host equipment, and network equipment into a total of 54 conditions from Chapter 3 Section 9 to Section 12. This issue concentrates on host device requirement with support for updates.

Host device means a general-purpose device running an operating system (for example, Microsoft Windows, OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers. The typical attributes include file system(s), programmable services, no real-time scheduler and full HMI (Source: IEC 62443 4-2).

Host devices should support the ability to be updated and upgraded. And To meet SL2 requirement, host devices should validate the authenticity and integrity of any software update or upgrade before installation. The concept of integrity is detailed in vol.18 of the newsletter, published in October 2019, so this issue focused on methods and cases study for verifying integrity check function. In case an update file is downloaded from the server and updated from the device, a procedure (service) is required. The procedure should be used to confirm that the file is the original data, sent from the server. In this case, a hash function can work. Simply put, a hash function makes a short and unique value of a file. The hash value of each file can be displayed with simple tools such as EasyHash, HashTab, etc.



File Name: C:₩Users₩hoon₩Deskto...₩HashTest1.txt
Progress time : 00 : 00 : 00
100%

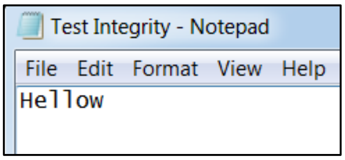
Item	Hash value
CRC-32	809ddc32
MD5	7a6d1b13498fb5b3085b2fd887933575
SHA-1	dbce705929c7dc1924ea1173f37652bb00f96d6d

Copyright (c) 2019 Copynull All Rights Reserved

<Example of Hash Value Check – Used ‘Easy Hash’ Tool>

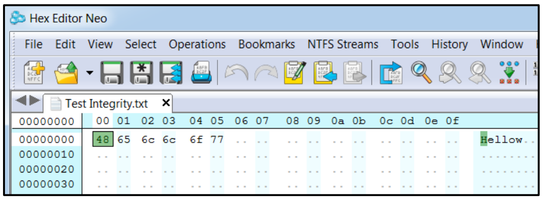
Integrity Check with Hash Value

In case file is tampered hash value can be used to check. Sample text file was created to perform the test and the Hex Editor Neo was used to check the Hex value (the binary code value stored in the PC). The Easy Hash program was used to check the Hash value of the text file for testing.



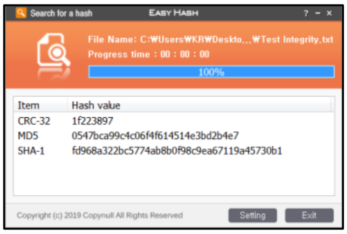
Hellow

<Original File>


Hex Editor Neo
File Edit View Select Operations Bookmarks NTFS Streams Tools History Window
Test Integrity.txt

```
00000000  00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000  48 65 6c 6c 6f 77                                Hellow
00000010
00000020
00000030
```

<Hex Value>

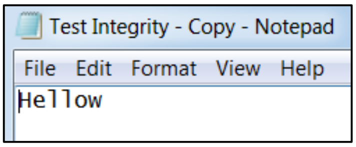


File Name: C:₩Users₩KR₩Deskto...₩Test Integrity.txt
Progress time : 00 : 00 : 00
100%

Item	Hash value
CRC-32	1f223897
MD5	0547bca99c4c06f4f614514e3bd2b4e7
SHA-1	fd968a322bc5774ab8b0f98c9ea67119a45730b1

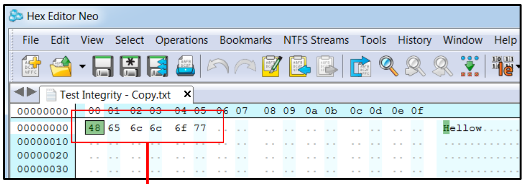
<Hash Value>

Make a copy of original file and compare the Hex/Hash value with the original file. And as you can see in the picitures below, all values are same as original file. (Not Tampered)



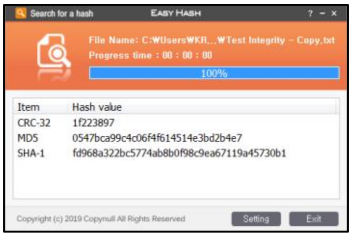
Hellow

<Copied File>


Hex Editor Neo
File Edit View Select Operations Bookmarks NTFS Streams Tools History Window Help
Test Integrity - Copy.txt

```
00000000  00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000000  48 65 6c 6c 6f 77                                Hellow
00000010
00000020
00000030
```

<Hex Value>

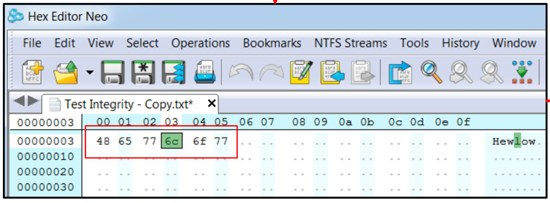


File Name: C:₩Users₩KR...₩Test Integrity – Copy.txt
Progress time : 00 : 00 : 00
100%

Item	Hash value
CRC-32	1f223897
MD5	0547bca99c4c06f4f614514e3bd2b4e7
SHA-1	fd968a322bc5774ab8b0f98c9ea67119a45730b1

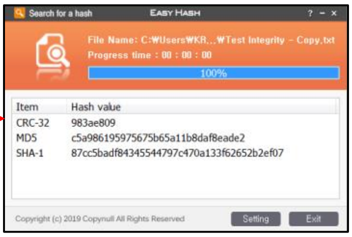
<Hash Value>

48 65 **6c** 6c 6f 77 -> 48 65 **77** 6f 77


Hex Editor Neo
File Edit View Select Operations Bookmarks NTFS Streams Tools History Window
Test Integrity - Copy.txt*

```
00000003  00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
00000003  48 65 77 6c 6f 77                                Hewlow
00000010
00000020
00000030
```

<Hex Value - Tampered>



File Name: C:₩Users₩KR...₩Test Integrity – Copy.txt
Progress time : 00 : 00 : 00
100%

Item	Hash value
CRC-32	983ae809
MD5	c5a986195975675b65a11b8daf8eade2
SHA-1	87cc5badf84345544797c470a133f62652b2ef07

<Hash Value>

Tried tamper to the copied file. Change (modulation/hacking) Hex value and compared if the Hash value is the same as the original value. As you can see, the text file 'Hellow' was changed to 'Hewlow' by forcing a change in the Hex value and that the Hash value was different from the original. These methods are used to provide the ability to compare the hash values of the update files received from the server before the update with the values of the server's original files, indicating that the integrity of the update can be verified before the update.

Explanation of Term

CIRM(Comité International Radio-Maritime)

As a leading international non-governmental organization (NGO) for ship electronics, the company has over 110 companies in 30 countries around the world and has extensive activities at major international conferences (IMO, ITU, IEC, IALA, etc.). have.

SSID(Service Set Identifier)

SSID is a term for WIFI network name. Identifier that indicates the set of services (network) to connect to the IEEE 802.11 wireless networking standard. The SSID is designed with a unique name so that all APs or wireless devices must use the same SSID to access a particular WLAN. No device that knows the unique SSID of a particular BSS can connect to that BSS. Since the SSID is plain text data added on the packet, there is no guarantee on the network because it is likely to be sniffed sufficiently.

Hardcoding

Entering data directly into code Technically, this is a state where data is merged into an executable binary (such as an exe file). When data is entered and stored directly in the program's source code, that is, all 'constants' are hard coding. The initial or default value of a variable is also hard coded. In some cases, the default value itself is read from an external resource file and initialized. However, since the loading of the 'resource' file has a probability of failure, values such as null, 0, and nil are hard-coded until loaded.