KR Maritime Cyber Security

News from KOREAN REGISTER

Mar 2019

Vol. 011

KR Cyber Security Activities

● Cyber security and ICT equipment joint development MOU signing with Hanwha Systems

On March 14, the executive vice president of Korean Register(KR) R&D Center, Tae-bum Ha and the executive vice president of the Hanwha Systems Business Division, Seok-hong Jeong signed a memorandum of understanding (MOU) for joint development on cyber security and ICT equipment for naval ships.

Under the agreement, the two companies jointly study cyber security rules applicable to naval ships based on the capabilities of KR advanced cyber security certification process and the integration capabilities and the experience of developing security solutions for military networks of Hanwha systems. In addition, they will develop new business opportunities by developing security solutions tailored to maritime affairs, and work together in areas such as training of professional personnel, and utilization of ICT equipment and materials.

Hanwha System is a comprehensive defense electronics that successfully supplied combat systems to more than 80 naval vessels and submarines for more than 30 years contributing to the strengthening of the power of Korean navy. In addition, the company is developing unmanned vessels and submarines that demonstrate capability of 4th Industrial Revolution technology.

Application cases in OT System Penetration Test

● The Necessity of OT System Penetration Test for the Maritime Industry

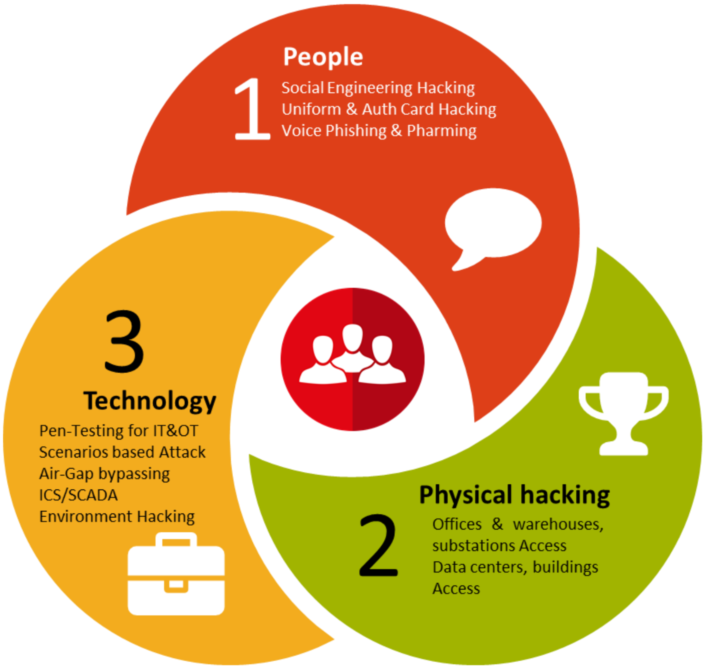
According to the 'Guidelines on Cyber Security onboard Ships' (Rev.3) published by the international shipping industry, ships are experiencing the same types of cyber security problems as other IT systems. This document includes rules and guidelines for the security of the ship's IT system, and gives examples of what happens when the ship does not follow the correct procedures. This case is a cyber security incident in ships and harbor in the past and has not been publicly revealed until now. Especially, the threat range extends from the physical factors of pirates, cargo loss/deprivation and stowage, which were frequently mentioned in existing physical security, to IoT, embedded systems, and hacking for various cyber assets that are recently being reviewed.

In response to these changes, many companies and organizations are increasingly trying to prevent and respond to these threat of control systems of vessels and offshore industrial facilities in advance through Penetration test.

● The Necessity of OT System Diagnosis and Red Teaming Project

Based on an understanding of the site and related industry, there is a Red Teaming project in which security checks are carried out in the Operation Zone with such a security diagnosis of ports and vessels. The Red Teaming assessment focuses on providing the company's security teams with real experience in dealing with cyberattacks in the OZ area, not just IT, while avoiding attacks that damage the company's actual operating system or business, and using existing and intelligent attackers Tactics, Techniques and Procedures (TTPs) to develop security targets in a variety of ways.

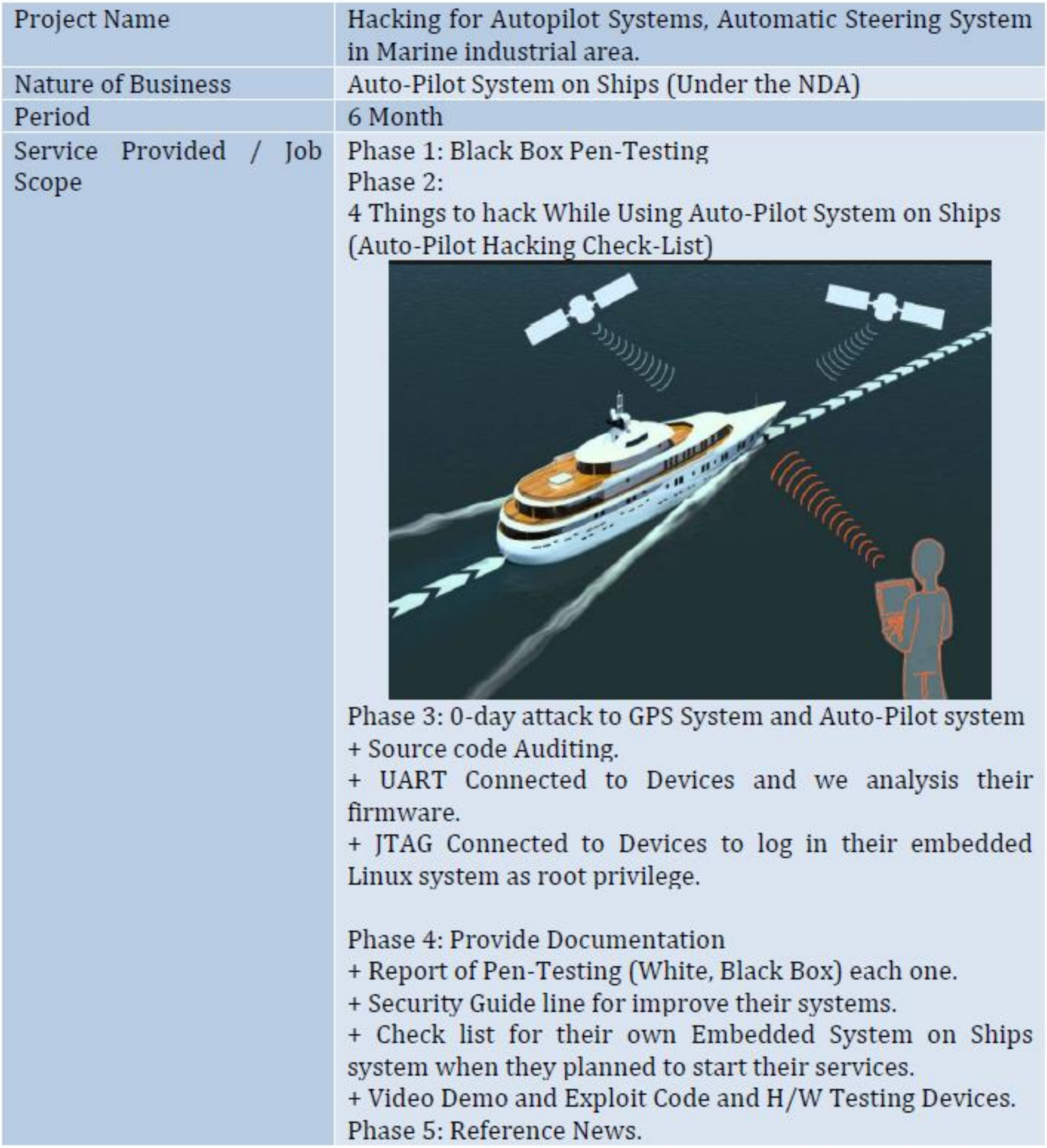
As shown in the figure below, physical penetration is carried out through understanding the actual operating environment by transcending security checks on existing technology areas, and attacks on internal staff (including ship officers) who work on land and sea using social engineering Hacking etc.


People
1
Social Engineering Hacking
Uniform & Auth Card Hacking
Voice Phishing & Pharming
2
Physical hacking
Offices & warehouses, substations Access
Data centers, buildings Access
3
Technology
Pen-Testing for IT&OT
Scenarios based Attack
Air-Gap bypassing
ICS/SCADA
Environment Hacking

- **Ship Security Checklist**

Category	Contents
Unauthorized use	Normally, only authentic users can be connected to client's service & asset. However, Client can be used as a platform for launching a cyber-attack. This can be done by bypassing the authorization and connect to the internet as an anonymous user.
Sniffing user data and modify network packet	Attacker can sniff or modify packet, and steal other user data (id, password)
Malware infection	Attacker can redirect normal users to a malware page, and install malware to the phones that are connected. This can be done using zeroday vulnerability. After malware has been successfully installed into victim's phone, attacker can easily sniff their call or messages.
Service disruption	Attacker can exploit Embedded System on Ships vulnerability via the network, and cause disruption to services. It may cause catastrophic damages if client is used for deploying IoT services in the future.
Connect the OT system from external network	For the above scenario, an attacker do not necessary have to connect to the their important system directly. This can be done by connect to OT Zone via external network using only IP address.
Connect the OT Network	Through 7 kinds of surface. We can access their system over the airgap. We're going to test to connect their system through wireless, Bluetooth, RF and etc..
Attack to GPS Signaling system	We're going to test their auto-pilot system on ship. We're going to test GPS Spoofing and jamming and others for their GPS systems.

- **Scenario of Autopilot Systems Penetration Test**



Project Name	Hacking for Autopilot Systems, Automatic Steering System in Marine industrial area.
Nature of Business	Auto-Pilot System on Ships (Under the NDA)
Period	6 Month
Service Provided / Job Scope	Phase 1: Black Box Pen-Testing Phase 2: 4 Things to hack While Using Auto-Pilot System on Ships (Auto-Pilot Hacking Check-List) Phase 3: 0-day attack to GPS System and Auto-Pilot system + Source code Auditing. + UART Connected to Devices and we analysis their firmware. + JTAG Connected to Devices to log in their embedded Linux system as root privilege. Phase 4: Provide Documentation + Report of Pen-Testing (White, Black Box) each one. + Security Guide line for improve their systems. + Check list for their own Embedded System on Ships system when they planned to start their services. + Video Demo and Exploit Code and H/W Testing Devices. Phase 5: Reference News.

- **This article was written by Louis Hur, CEO at NSHC & Shield Consulting co., Ltd.**

NSHC SECURITY, the only cyber security company in Domestic and Asian that can carry out penetration testing of ICS/SCADA(OT), is conducting malicious code analysis such as ransomware and APT attacks, penetration testing of industrial devices and source code diagnosis. SHIELD CONSULTING is providing consulting on physical security(CCTV, control of outsider's access, control of electronic devices and locks) required in cybersecurity.

Understanding of Cyber Threat(OWASP Top 10)

● Understanding of cyber threat

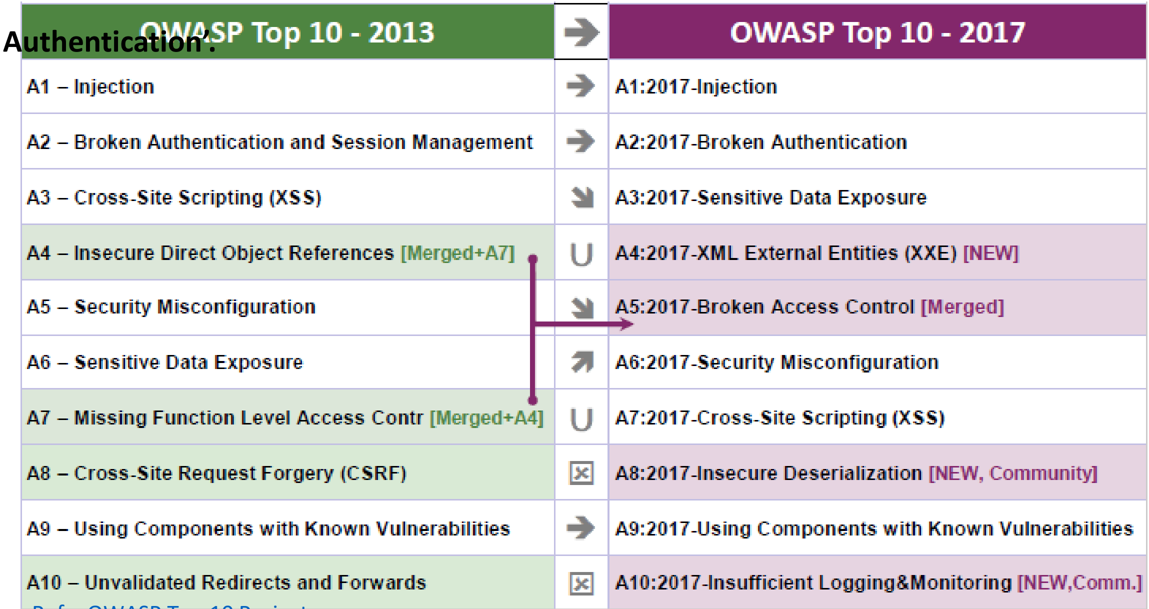
A Cyber threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, 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 '**A2 : 2017 – Broken Authentication'.**

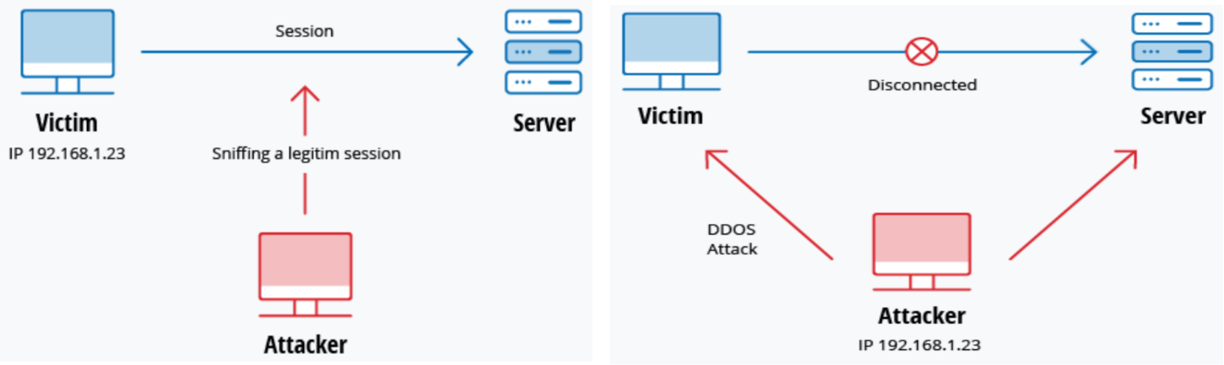


OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	∪	A4:2017-XML External Entities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

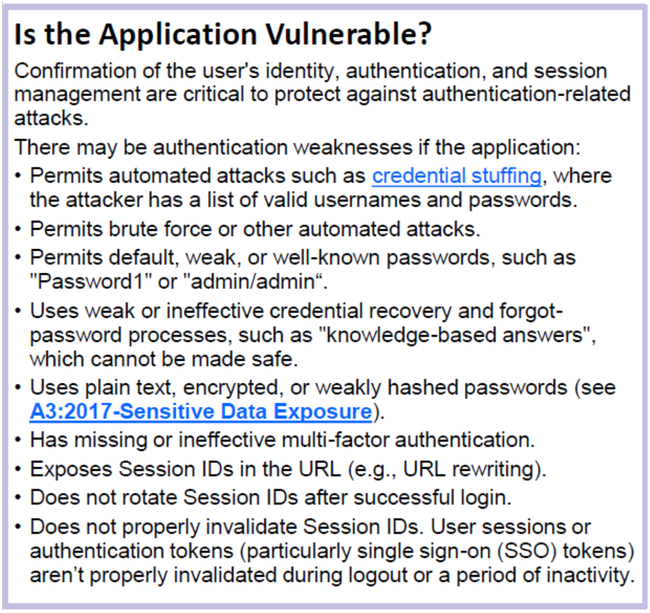
In a Web application, the user who logs in goes through an authentication process that verifies that the user who is registered on the site is correct using an ID and password. Once verified as a user through this authentication process, the user receives certain permissions from the website. In addtition, when moving the page after authentication, the login state is maintained, and a session is created to initialize the connection at a predetermined time. However, if a defect occurs during the authentication process, the user's account information is exposed and the attacker can log in with the account information exposed through the brute-force attack. In addition, if session management is poor, the attacker may obtain the user's privilege by taking the session ID.



1. A client connects to a server
2 Attackers sniffing a legitim session

3. Attacker`s computer gains control of the client and disconnects the client from the server
4. Attacker`s computer replaces the client`s IP
5. Spoof the client`s sequence numbers
6. Server believes it is still communicating with the client

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

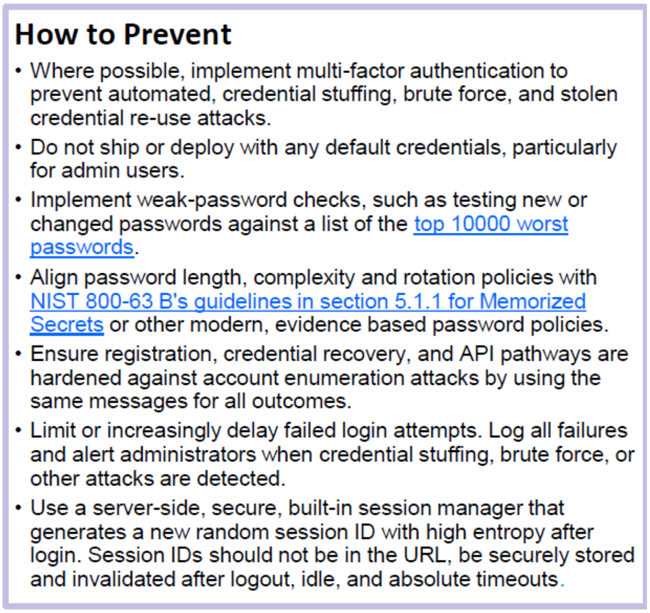


Is the Application Vulnerable?

Confirmation of the user's identity, authentication, and session management are critical to protect against authentication-related attacks.

There may be authentication weaknesses if the application:

- Permits automated attacks such as credential stuffing, where the attacker has a list of valid usernames and passwords.
- Permits brute force or other automated attacks.
- Permits default, weak, or well-known passwords, such as "Password1" or "admin/admin“.
- Uses weak or ineffective credential recovery and forgot-password processes, such as "knowledge-based answers", which cannot be made safe.
- Uses plain text, encrypted, or weakly hashed passwords (see **A3:2017-Sensitive Data Exposure**).
- Has missing or ineffective multi-factor authentication.
- Exposes Session IDs in the URL (e.g., URL rewriting).
- Does not rotate Session IDs after successful login.
- Does not properly invalidate Session IDs. User sessions or authentication tokens (particularly single sign-on (SSO) tokens) aren’t properly invalidated during logout or a period of inactivity.



How to Prevent

- Where possible, implement multi-factor authentication to prevent automated, credential stuffing, brute force, and stolen credential re-use attacks.
- Do not ship or deploy with any default credentials, particularly for admin users.
- Implement weak-password checks, such as testing new or changed passwords against a list of the top 10000 worst passwords.
- Align password length, complexity and rotation policies with NIST 800-63 B's guidelines in section 5.1.1 for Memorized Secrets or other modern, evidence based password policies.
- Ensure registration, credential recovery, and API pathways are hardened against account enumeration attacks by using the same messages for all outcomes.
- Limit or increasingly delay failed login attempts. Log all failures and alert administrators when credential stuffing, brute force, or other attacks are detected.
- Use a server-side, secure, built-in session manager that generates a new random session ID with high entropy after login. Session IDs should not be in the URL, be securely stored and invalidated after logout, idle, and absolute timeouts.

Guidelines of Establishing Mobile Security Policy

● Necessity of establishing mobile security policy

Mobile devices such as smart phones are highly utilized by individuals and corporations and are constantly exposed to new security threats due to their portability and connectivity to the Internet. In particular, public wireless LAN and private wireless LAN access environment using Wi-Fi and Bluetooth function is very easy to infiltrate malicious code or attack hacking. Therefore, mobile security policy is needed to prevent leakage of corporate information as well as personal damage.

The use of mobile equipment, physical protection, access control (including VPN), encryption, virus policy, internal network and connection security policy should be managed, and security training for users of mobile equipment should be conducted regularly. In addition, security policies and procedures should be established during remote work, and proper identification, authentication, and access control measures should be established when accessing the internal network via the public network, and recovery and management of access rights and equipment should be completed.

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

Mobile security policy(215.1) : The company must establish security policies to control the use of corporate mobile devices and employee owned mobile devices.

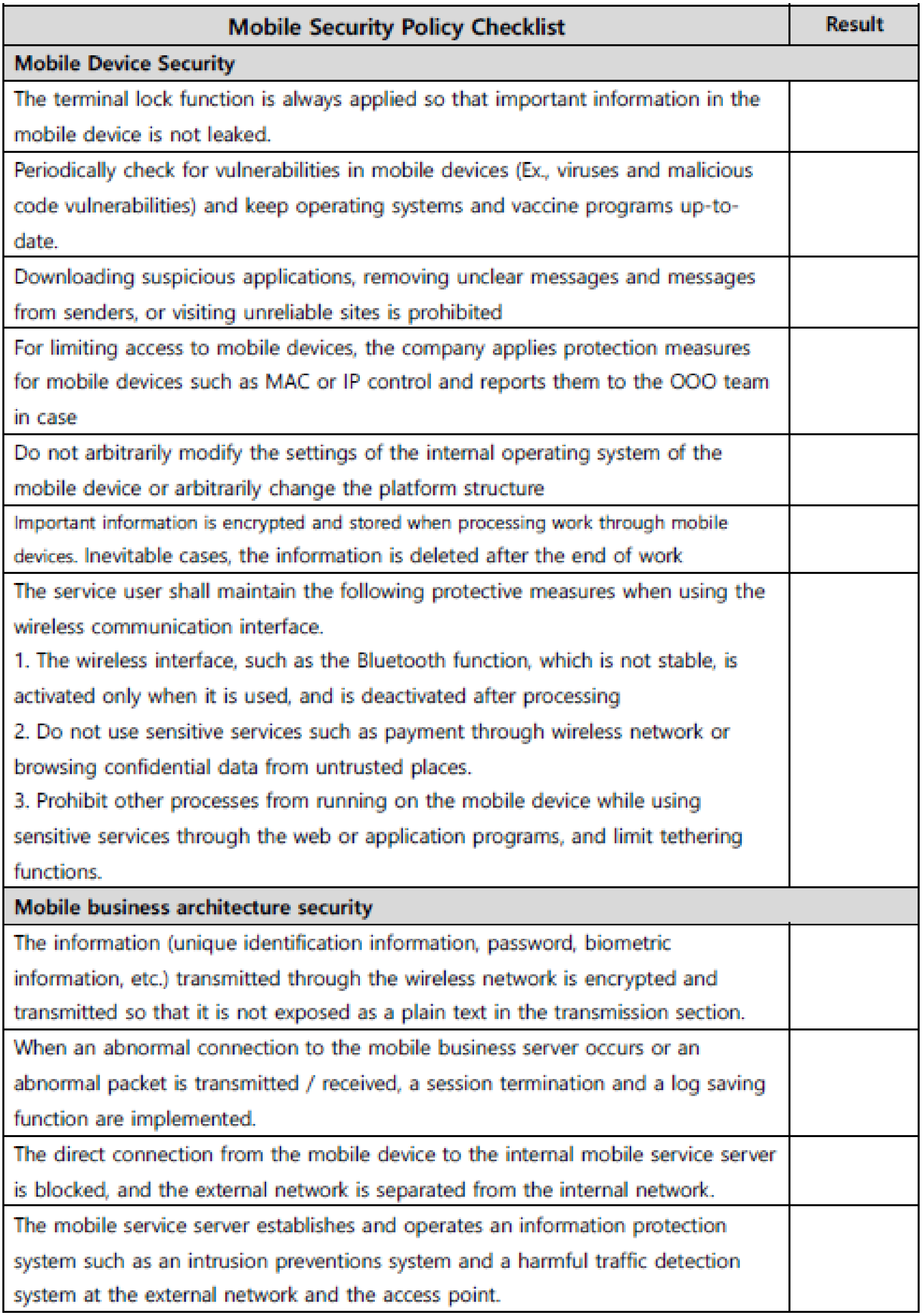
Mobile device management(215.2) : The company must define the mobile devices and functions available in the company and identify the devices in use.

Prevent unauthorized access points (215.4) : The company should prevent mobile devices used by employees from accessing unauthorized access points(Rogue Access Points) that are exploited for malicious code infections or hacking.

● Smartphone User Rules

1. Do not download suspicious applications, do not visit untrusted sites
2. Delete unclear or suspicious messages and messages from senders
3. Use the password setting function and change password on a regular basis
4. Always update operating systems and anti-virus programs to the latest version

- **Mobile Security Policy Checklist (Example)**



Mobile Security Policy Checklist	Result
Mobile Device Security	
The terminal lock function is always applied so that important information in the mobile device is not leaked.	
Periodically check for vulnerabilities in mobile devices (Ex., viruses and malicious code vulnerabilities) and keep operating systems and vaccine programs up-to-date.	
Downloading suspicious applications, removing unclear messages and messages from senders, or visiting unreliable sites is prohibited	
For limiting access to mobile devices, the company applies protection measures for mobile devices such as MAC or IP control and reports them to the OOO team in case	
Do not arbitrarily modify the settings of the internal operating system of the mobile device or arbitrarily change the platform structure	
Important information is encrypted and stored when processing work through mobile devices. Inevitable cases, the information is deleted after the end of work	
The service user shall maintain the following protective measures when using the wireless communication interface. 1. The wireless interface, such as the Bluetooth function, which is not stable, is activated only when it is used, and is deactivated after processing 2. Do not use sensitive services such as payment through wireless network or browsing confidential data from untrusted places. 3. Prohibit other processes from running on the mobile device while using sensitive services through the web or application programs, and limit tethering functions.	
Mobile business architecture security	
The information (unique identification information, password, biometric information, etc.) transmitted through the wireless network is encrypted and transmitted so that it is not exposed as a plain text in the transmission section.	
When an abnormal connection to the mobile business server occurs or an abnormal packet is transmitted / received, a session termination and a log saving function are implemented.	
The direct connection from the mobile device to the internal mobile service server is blocked, and the external network is separated from the internal network.	
The mobile service server establishes and operates an information protection system such as an intrusion preventions system and a harmful traffic detection system at the external network and the access point.	

Explanation of Term

- **OT(Operating Technology)** : Refers to hardware and software that detects or causes a change in physical processes through direct monitoring or control of physical devices such as valves, pumps, and etc. OT systems on-board ships include propulsion, power generation and distribution, steering, navigation, communications, and cargo operations systems.
- **Zero-day threat :** This is a technical security threat that exploits vulnerabilities in computer software. It is an attack that occurs when a patch for the vulnerability is not developed yet. A 1-day vulnerability is an attack that occurs when a patch has been released but has not been applied due to validation and various reasons.
- **Brute Force Attack** : In order to acquire account for a user, it tries all the character combinations of usernames and passwords by repetitive manner until the user's account are matched to obtain account information. If a password has a certain pattern, such as a user password, the range of values to be assigned can be greatly reduced. In this case, a dictionary attack is used in which dictionary words are combined and assigned. Therefore, it is important to make password patterns irregular and not to be linked to personal information.
- **Session Hijacking** : It is an attack that intercepts the connection state of the attacked object already connected to the system and accesses the system and uses resources or data without knowing the ID and password .
- **Rogue AP** : Rogue access point is a wireless access point installed in a secure network without the explicit permission of the local network administrator. In a corporate wireless LAN environment, proper regulation is needed because an external user or an illegal intruder can access all resources with the same qualification as an internal employee through a wireless AP.