

KR Maritime Cyber Security

News from KOREAN REGISTER

Vol. 022

February 2020

KR Cyber Security Activities

- KR awarded cyber security compliance certificate for company to Orange security

Understanding Cyber Threats(OWASP Top 10 Internet of Things)

UK Maritime minister released cyber security guideline for ports

Vulnerability Analysis and Countermeasures of Wireless Networks

Guidelines for Type Approval of Maritime Cyber Security

Explanation of Term



● KR awarded cyber security compliance certificate for company to Orange security

On November 15, 2019, KR awarded the company's Cyber Security Certificate to Orange Security, a cyber security consulting company. The company's cyber security certificate issued by KR to Orange security is the first case issued to a company that is not a maritime business. Orange Security is mainly consulting for cyber security and auditing of information security management system (ISMS) certification and ISO27001 certification for a number of financial institutions and information and telecommunications companies. The company has recently established a subsidiary in Panama to prepare for a leap to become a global maritime cyber security company. Park kaemyoung, general manager of KR cyber certification team, said, "There are many small businesses than large companies in the maritime industry. so I was worried about how to apply control to companies that do not have IT departments or use only clouds, but its experience of auditing to orange security give us the idea"

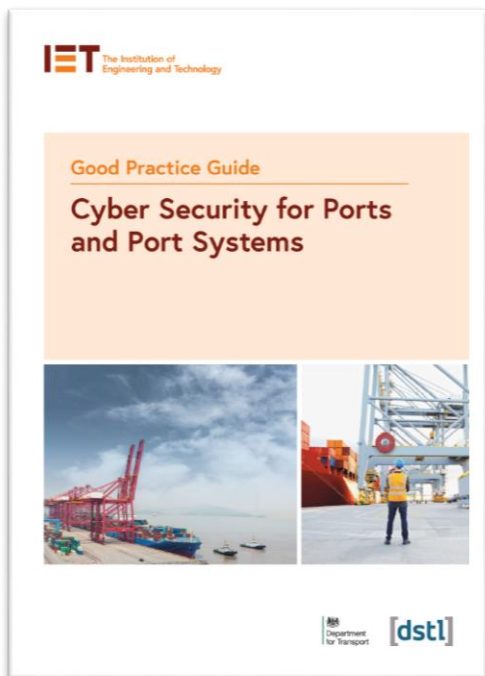
Choi Sung-min, CEO of Orange Security, said, "We have received a lot of help from KR about understanding of the maritime industry while preparing for audit. This is because the security control, which is based on the safety of ships, differs from the control of the land, which is mainly functional. We will continue to monitor the newly established international regulations and be reborn as a maritime cyber risk company representing Korea with KR.





UK, released cyber security guideline for ports

UK Maritime minister released “Good practice guide for ports”



A new UK cyber security good practise guide highlights the very real risk of cyber security breaches and the need for robust prevention strategies to protect financial, security and reputational interests. The ‘Cyber Security for Ports and Port Systems’ guide, published by The Institution of Engineering and Technology, with the UK Department for Transport, aims to help ports highlights what actions need to be taken and by who. “Cyber-attacks on port systems are no longer or simply the stuff of fictional narrative,” said considered hypothetical the guide, which noted how Maersk’s security setup left it open to an attack from the Maersk virus in June 2017.

It stressed that the consequences of failing to address security risks could lead to serious injury or fatality, disruption or damage to port systems, loss of use of buildings, impact upon business operations, reputational damage, loss of revenue, financial penalties or litigation. The guide explained that port facilities are becoming increasingly complex and dependent on the extensive use of information and communications technologies (ICT) at all stages of their lifecycles – for example, in the growth of automated berthing operations. A key aim of the guide is to communicate that cyber security of port systems is managed cost-effectively, as part of mainstream business. The Port of San Diego, Port of Barcelona, Cosco Shipping Lines and APM Terminals are amongst maritime organisations which have suffered cyber attacks. In October 2019, a Cyber Risk Management (CyRiM) project report estimated that losses of up to US\$110bn would occur in an “extreme” cyber-attack scenario involving Asia-Pacific (APAC) ports. According to Nusrat Ghani, UK Minister of Maritime Affairs, observing this guide will help the maritime industry to keep this important transportation hub safe from 21st century style attacks, and will help develop the port's cyber security assessment, Not only can it effectively identify security gaps, it also provides advice on managing cybersecurity attacks.

Source : <https://www.hellenicshippingnews.com/cyber-security-guide-for-ports-released/>



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'

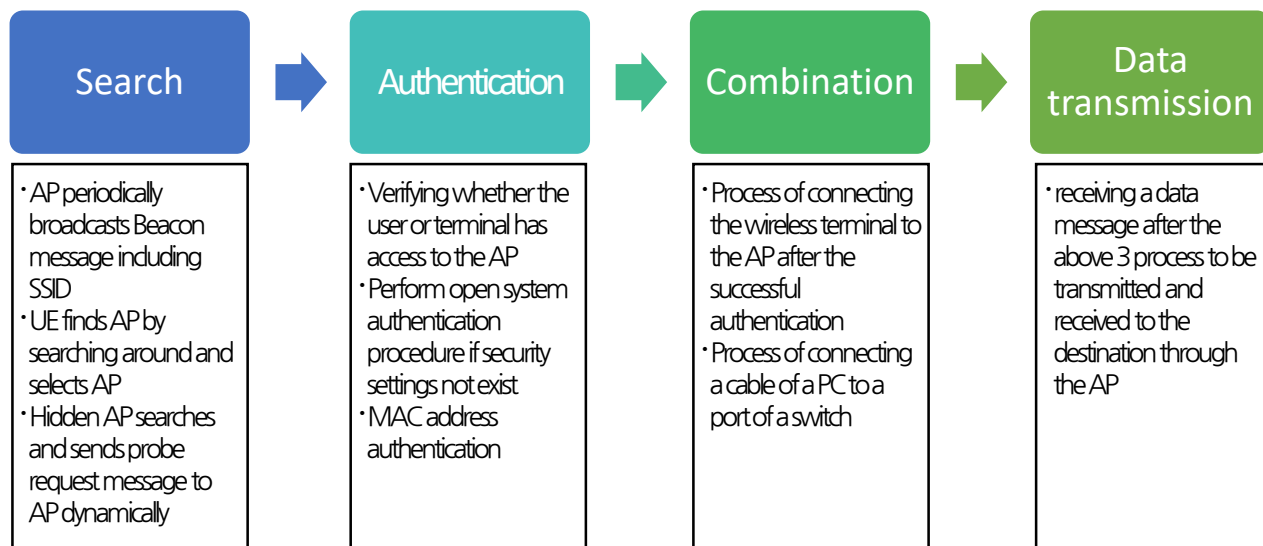
Series news

- 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

Overview of wireless network

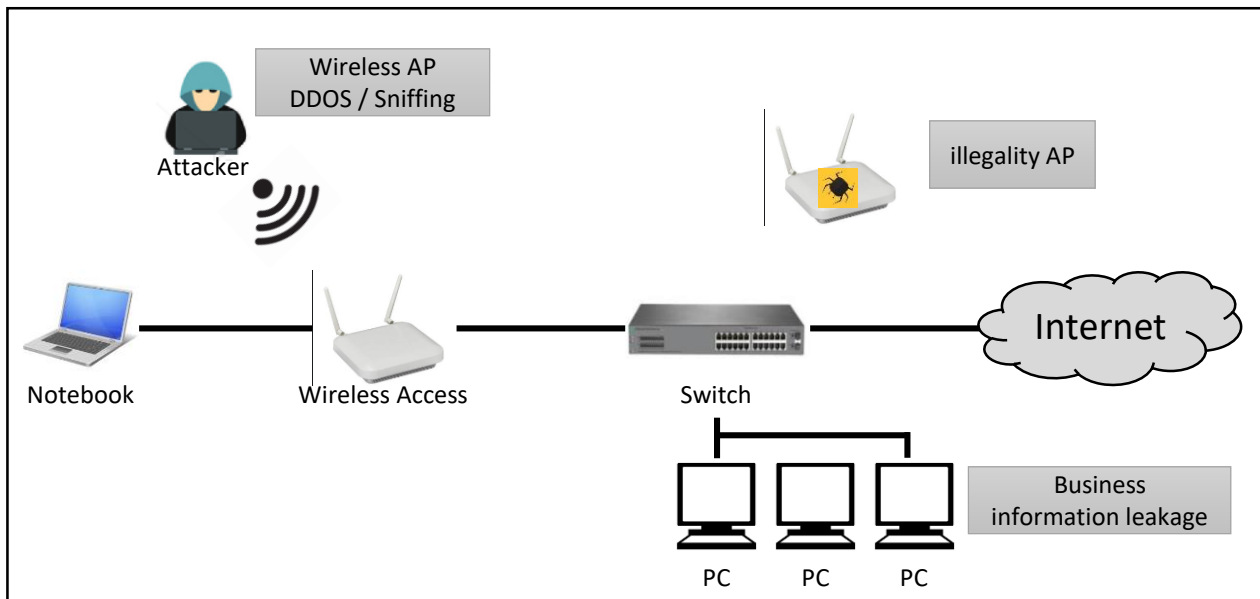
Wireless network refers to a technology that allows a user to access a network and access the Internet without using a network cable. Wireless networks are often replaced with wired cables by many types of wireless network technologies, such as Wi-Fi and Bluetooth, which are widely used in everyday life except cellular communication, as well as Zigbee and Z-Wave, which provide low-power networks with sensors and controls.

Principle of wireless network



● Vulnerability of wireless network

Wireless networks are often used in home or office environments in the existing concept of wired LAN expansion. Most of them are composed of the form of connecting wireless AP to existing wired LANs and installing wireless LAN cards to clients. Therefore, the separation of wired LAN and wireless LAN is not considered at all, and there is a security problem.



Source : Korea Internet & Security Agency Wireless LAN Security Guide

● Wireless LAN(WLAN) encryption method

The vulnerability of WLAN can be classified into problem of the authentication during wireless network access and encryption vulnerability of wireless transmission data. In the first WLAN standard, IEEE802.11, the encryption of the wireless LAN authentication and transmission data was not included, but the first WEP method was introduced at IEEE 802.11b, and now WPA and WPA2 methods are widely used.

	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access2)
Overview	• First WIFI security	• Complement the WEP Method	• IEEE 803.11 compliant
Authentic ation	• use of pre-shared secret keys (64 bits, 128 bits)	• The EAP authentication protocol using the separate certificate server (802.1x) • WPA-PSK(preshared secret key)	• The EAP authentication protocol using the separate certificate server (802.1x) • WPA-PSK(preshared secret key)
Encryption	• The fixed cryptographic key use (a same as the authentication key) • Use RC4 algorithm	• Secret key dynamic change(TKIP) • Use RC4 algorithm	• Secret key dynamic change(CCMP) • Using powerful block encryption algorithms such as AES
Security	• 64-bit WEPkey is exposed in minutes • vulnerable and unused	• WEP method is safe but incomplete RC4 algorithm	• the most powerful security feature



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
11	Insecure Web Interface	Weak Guessable, or Hardcoded Passwords
12	Insufficient Authentication/Authorization	Insecure Network Services
13	Insecure Network Services	Insecure Ecosystem Interfaces
14	Lack of Transport Encryption	Lack of Secure Update Mechanism
15	Privacy Concerns	Use of Insecure or Outdated Components (NEW)
16	Insecure Cloud Interface	Insufficient Privacy Protection
17	Insecure Mobile Interface	Insecure Data Transfer and Storage
18	Insufficient Security Configurability	Lack of Device Management
19	Insecure Software/Firmware	Insecure Default Settings (NEW)
110	Lack of Physical Hardening	Poor Physical Security

● OWASP Internet of Things Top 10(2018)

Vulnerability 1. Easy passwords, inferred passwords or hardcoded passwords

“using public authentication information or unchangeable authentication information that allows firmware or client software to be easily exposed to indiscriminate subpoena attacks, or to grant unauthorized access to distributed systems, including backdoors”

Vulnerability 2. Insecure Network Services

“The unnecessary or unsafe networking service (especially the one exposed to the Internet) that undercuts the confidentiality, integrity/trust or availability of information or allows unauthorized remote control as it runs on the device itself.”

Vulnerability 3. Insecure Ecosystem Interface

“The unsafe web, back-end API, cloud or mobile interface of the device’s external ecosystem that allows for device or related components to be violated. Common problems include the absence of authentication/approval, the absence or weakness of encryption, and the absence of input/output filtering.”

Vulnerability 4. The absence of safe update mechanism

“The absence of a function to safely update your device. This includes a firmware verification member of the device, a member of a secure transmission method (not encrypted during transmission), a member of a rollback prevention mechanism, and a member of security change notification due to updates.”

Vulnerability 5. Use Unsafe or Out-of-Line Components

“Use software components/libraries that cause device infringement that are either unavailable or unsafe. This includes unsafe modifications of operating system platforms, and the use of third-party software or hardware components from the infringed supply chain.”

Vulnerability 6. Insufficient Privacy

“The user’s personal information is stored in the device or ecosystem and used unsafely, inappropriately, or without user permission.”

Vulnerability 7. Insecure Data Transfer and Storage

“The encryption or access control of sensitive data is not performed anywhere in the ecosystem, including storage, transmission or processing.”

Vulnerability 8. Absence of Device Management

“The absence of security support, including asset management, update management, safe disposal, system monitoring and response capabilities for devices deployed in production”

Vulnerability 9. Unsafe default settings




“A device or system shipped in an unsafe default state, or a lack of function to more securely protect the system by restricting configuration modification by an operator.”

Vulnerability 10: The absence of physical protection

“No physical protection means, so potential attackers can acquire sensitive information to use for future remote attacks or take control of the device.”



The infographic features a header with a circular icon containing various IoT symbols and the text "OWASP TOP 10 INTERNET OF THINGS 2018". Below this, ten numbered items are listed, each with a title, a brief description, and a representative icon.

- 1 Weak, Guessable, or Hardcoded Passwords**
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems. 
- 2 Insecure Network Services**
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control... 
- 3 Insecure Ecosystem Interfaces**
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering. 
- 4 Lack of Secure Update Mechanism**
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates. 
- 5 Use of Insecure or Outdated Components**
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain. 
- 6 Insufficient Privacy Protection**
User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission. 
- 7 Insecure Data Transfer and Storage**
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at-rest, in transit, or during processing. 
- 8 Lack of Device Management**
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities. 
- 9 Insecure Default Settings**
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations. 
- 10 Lack of Physical Hardening**
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device. 



Understanding Guideline for Type Approval of Maritime Cyber Security

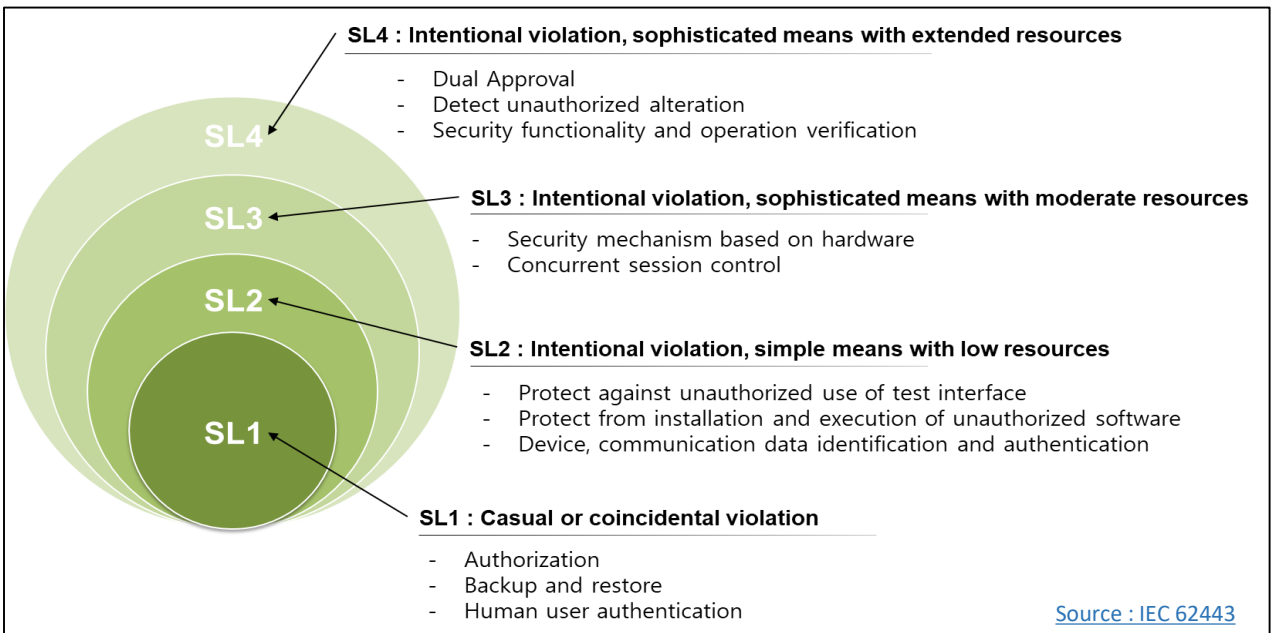
Type approval is to certify for the manufacturers of equipment for marine use that equipment comply with the provisions for the type approved products in the Guidance, where deemed satisfactory by the Society as the results of carrying out the examination, tests and inspection specified in the Guidance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



● KR Type Approval of Maritime Cybersecurity Inspection Items

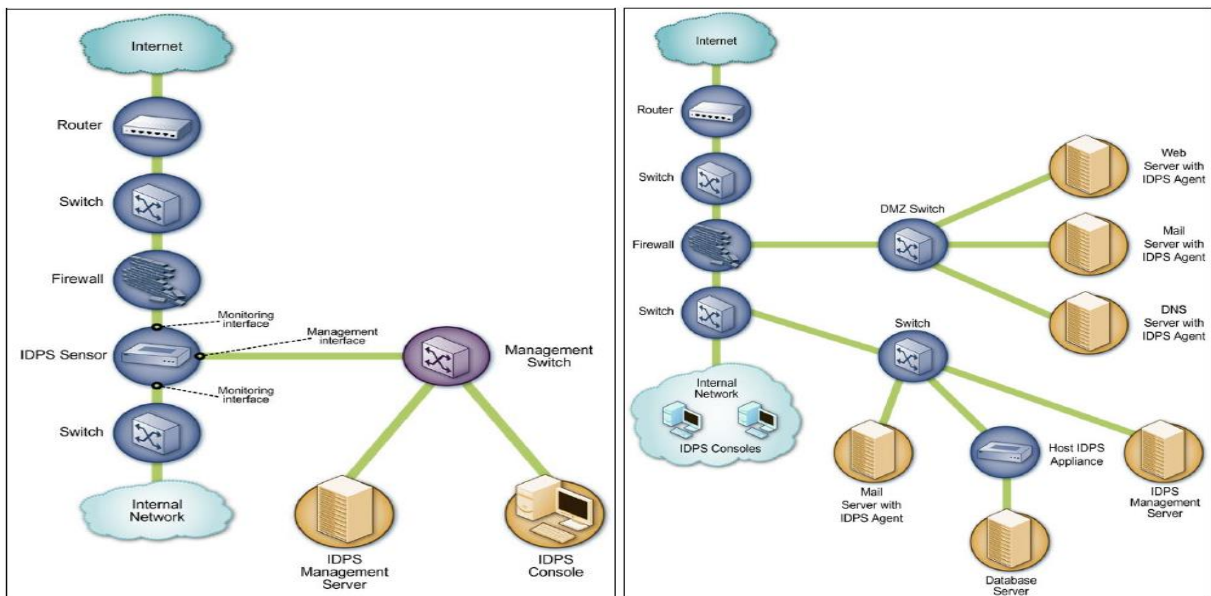
Continuous monitoring (702)

Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner. (SL 2,3,4)

● Guidelines for Data Packet Monitoring

IDS (Intrusion Detection System) is used to monitor security breaches. Definition of IDS is "Software that automates the intrusion detection process" (Source: NIST SP 800-94) and can be used to complement the limitations of firewalls that provide IP address and network port based prevention policy. IDS identifies intrusions and notifies users based on packet analysis for data received even if IP and Ports allowed by the firewall. Similar to IDS, there is an IPS (Intrusion Prevention System) that provides a blocking function instead of notification function.

It is also called IDPS with IDS and IPS together. Applicants want to Security Level 2 or higher have to provide IDS, IPS or equivalent functions to monitor security breaches. Because IDS and IPS detect or block based on data packet analysis, there is a possibility of false positive(detected or blocked normal data packets) and variety of types such as network-based IDS/IPS using network equipment and host-based IDS/IPS using software applications on nodes such as PCs. The applicant should understand types/characteristics of IDS/IPS and provide function for the monitoring of security breaches.



<Network Based IDPS>

<Host Based IDPS>



Explanation of Term



● SSID(Service Set Identifier)

as the unique identifier of 32 byte length added to each header of the packets transmitted through the wireless LAN, when wireless devices access BSS (Basic Service Set), they are used as if they are a password. SSID distinguishes one wireless LAN from another wireless LAN, so all APs or wireless devices to access a specific wireless LAN must match SSID.

● MAC address authentication

Every LAN card on a computer or mobile device has a medium access control (MAC) address. The authentication method using the unique number system enables the use of a wireless network only by a device registered in a wireless AP.

Service	Authentication	Roles	Enforcement	Summary
Type:	MAC Authentication			
Name:				
Description:	MAC-based Authentication Service			
Monitor Mode:	<input type="checkbox"/> Enable to monitor network access without enforcement			
More Options:	<input type="checkbox"/> Authorization <input type="checkbox"/> Audit End-hosts <input type="checkbox"/> Profile Endpoints			
Service Rule				
Matches <input type="radio"/> ANY or <input checked="" type="radio"/> ALL of the following conditions:				
Type	Name	Operator	Value	
1. Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethere	
2. Radius:IETF	Service-Type	BELONGS_TO	Login-U	
3. Connection	Client-Mac-Address	EQUALS	% {Radi	
4. Click to add...				

Source : <https://www.arubanetworks.com/>

● Sniffing

As a cyber hacking technique, sniping means overhearing packet exchanges of other opponents on the network. In short, the process of eavesdropping on network traffic can be called sniping.