KR Maritime Cyber Security

News from KOREAN REGISTER

May 2019

Vol. **013**

Singapore MPA opens maritime cyber security operations centre

● Establishment of MSOC for early detection and response of cyber attack

The Singapore Maritime and Port Authority (MPA) has established a Maritime Cyber Security Operation Center (MSOC) for early detection and quick response to any cyber attacks on Critical Information Infrastructure (CII).

The new MSOC will strengthen Singapore's maritime cyber security position through early discovery, monitoring, analysis and response to potential cyber attacks on maritime CII. It will protect maritime CII and investigate any cyber security threats or incidents. MPA has also established a key data link between the MSOC and the Port Operational Control Center in order to respond more holistically and quickly to cyber incidents.

The Singapore MPA has implemented another plan to enhance cyber security in the maritime sector, with the one day "Marine Cyber Security Training Course" which improves a marine agents knowledge of cyber threat management. This training will be conducted in the first half of next year. The Singapore MPA has begun developing a marine cyber security research program with the Singapore Maritime Research Institute and will further improve the security awareness of port and port cyber security by sharing details of cyber threats and incidents through an information network linked to other port authorities.

Ref. : https://safety4sea.com/mpa-singapore-opens-maritime-cyber-security-centre/

P2P vulnerabilities found on millions of IoT devices

- **Critical security vulnerability found in millions of IoT devices using iLnkP2P**

According to security engineer Paul Marrapese, millions of IoT devices using iLnkP2P have serious security vulnerabilities. iLnkP2P is one of the P2P solutions used by machine builders and allows users to instantly connect to IoT devices on their mobile or computer using a special serial number known as an UID. In this case, there is no need for port forwarding or dynamic DNS to connect, and NAT and firewall scenarios can be overcome.

Marrapese explains that there are two vulnerabilities that can be exploited if they are used simultaneously. (CVE-2019-11220), you do not need to have access rights to equipment, and you can use (CVE-2019-11219) to quickly find many devices.

(CVE-2019-11219) An enumeration vulnerability in iLnkP2P allows attackers to quickly search for devices that are online. The nature of P2P allows an attacker to connect directly to arbitrary devices, bypassing firewall restrictions.

(CVE-2019-11220) An authentication vulnerability in iLnkP2P allows an attacker to intercept connections to devices and perform intermediary attacks. An attacker could use this vulnerability to steal and control the device's password.

- **Countermeasures**

1) Since there are no patches, the recommendation is to buy new equipment from a trusted vendor.
2) Disable P2P functionality by blocking outbound traffic to UDP port 32100

[Image ：LG CNS]

Ref. : https://cyware.com/news/millions-of-iot-devices-affected-by-newly-discovered-p2p-vulnerabilities-d8d92b1c

Cyber pirates and threats to navigation systems

● An analysis of cases of Russian government GPS attacks and methods

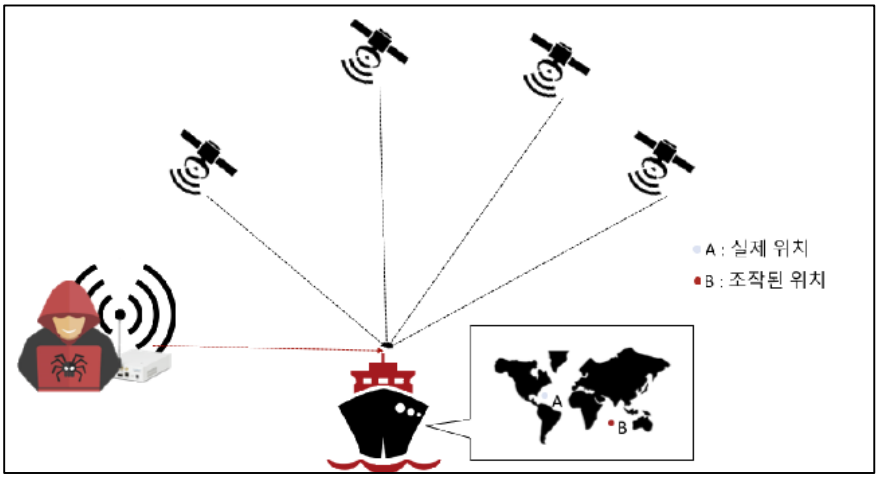
In May 2018, the GPS systems of 24 vessels around the Crimean Peninsula in Russia were found to be operating abnormally, pointing to an actual street and about 65 kilometers away. According to an American research organization, President Putin was near the location, and as a result the Russian government intentionally attacked the GPS.

Currently, the Russian government is targeting satellite systems including GPS, Baidu, Glonass, and Galileo, and is conducting jamming and spoofing attacks at a government and military level. It is reported that about 10,000 vessels have been affected and damaged. As far as we understand, most Russian attacks are around the Crimean Peninsula, the Black Sea, Syria, and around Russia.

It is not difficult to jam and spoof these systems and networks. Hacking equipment can range from cell phone size to briefcase size, and even if it is made in the private sector, it can be available for hundreds or thousands of dollars. A US university in 2017 proved that 65-meter yachts could be hacked for research purposes and fake GPS data could be put into place to cause a ship crash. GPS spoofing is an attack that sends a fake signal stronger than the GPS signal transmitted by GPS satellites, this causes the GPS receiver to pick up the manipulated GPS signal instead of the actual satellite signal. An attacker can manipulate the location and time information of and attack target by sending signals similar to those from a GPS satellite. If the attacker falsely pretends to be a GPS satellite and transmits a position off the normal route, the system will miss the path.

The ship's GPS receiver records position information on dozens of satellites. The hacker replicates the signal of the existing satellite and sends out a manipulated signal to make the ship deviate from its original path. If the signal suddenly moves away from the actual path, the power of the false GPS signal is gradually increased until the ship's GPS receiver transmits the manipulated signal. If the ship's GPS receiver cannot distinguish between the actual true signal and the new signal manipulated by the attacker, the ship systems can be attacked without warning .

Ref. : https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/



NSHC Red Alert Laboratories industrial control system wireless signal attack analysis report

The research team used open source from the GPS-SDR-SIM project to send signals to manipulate location information during the test. They generated a GPS band signal, and transmitted a signal through the SDR equipment to an attack target. The supported SDR devices include HackRF, BladeRF, and USRP. In addition, a TCXO module is required to reduce the noise of the transmitted signal. An attack using these methods, can make a difference of at least 100 meters on all GPS devices, including smartphones, and is virtually undetectable.

Increasingly cyber pirates are emerging, and crime groups are targeting ships and ports. Like cyber security experts, they also study ship systems and structures. At the moment, they are mainly hacking ECDIS and AIS. But by using GPS jamming and spoofing it would be possible to kidnap a ship via cyber attack instead of physically hijacking ship, using the satellite system. To prepare for this, the ship operator cannot rely on their equipment. They must prepare for various attack scenarios by training people to cope with the situation, and by conducting infiltration tests similar to real hacking scenarios instead of using just general penetration testing.

Ref. : https://www.businessinsider.com/gnss-hacking-spoofing-jamming-russians-screwing-with-gps-2019-4

▪ **This article was written by Seung-jun Lee, senior researcher 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 cyber security.

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 **'A4 : 2017 – XML External Entities'**

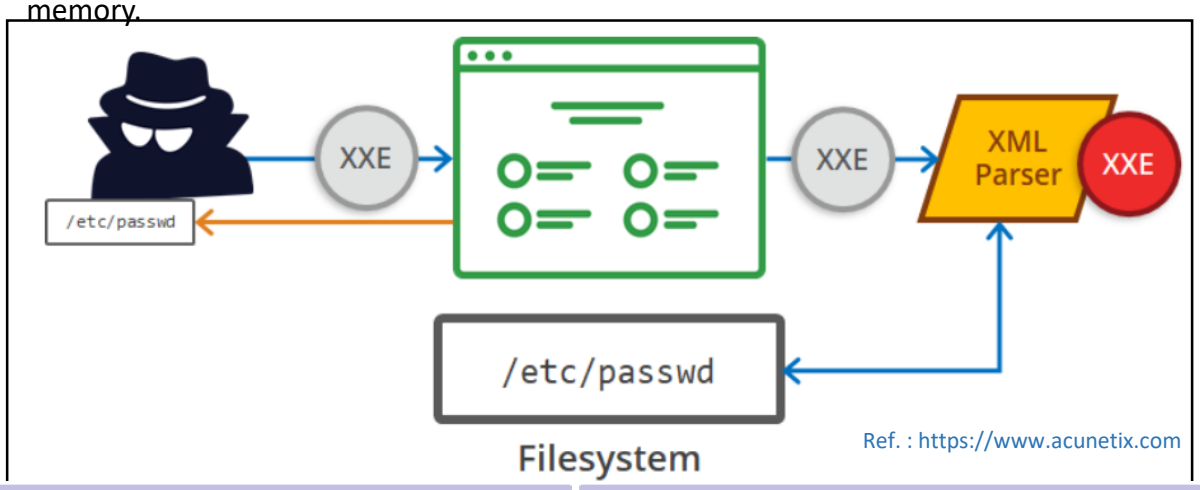
OWASP Top 10 - 2013		OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities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

Ref. : OWASP Top 10 Project

● OWASP Top 10 'A4 : 2017 – XML External Entities'

The XML External Object (XXE) attack is based on Server Side Request Forgery (SSRF). Attackers can use XXE to trigger a Denial of Service (DoS), as well as to access local and remote content and services. Extensible Markup Language (XML) is a very common data format, it is used in everything from web services (XML-RPC, SOAP, REST) to documents (XML, HTML, DOCX) and image files (SVG, EXIF data). To interpret XML data, you need an XML parser (XML parser) in your application.

Attackers can use either an outdated or misconfigured XML parser to achieve major system file access (LFI) and external malicious file referencing (RFI). In addition, it is possible to refer to another Entity continuously in one Entity, which may cause an application load. The code is smaller than 1KB, but the XML Parser needs to process 1 billion (29) strings when processing the referenced Entity, which can make it 3 GB in memory.



Is the Application Vulnerable?

Applications and in particular XML-based web services or downstream integrations might be vulnerable to attack if:

- The application accepts XML directly or XML uploads, especially from untrusted sources, or inserts untrusted data into XML documents, which is then parsed by an XML processor.
- Any of the XML processors in the application or SOAP based web services has document type definitions (DTDs) enabled. As the exact mechanism for disabling DTD processing varies by processor, it is good practice to consult a reference such as the OWASP Cheat Sheet 'XXE Prevention'.
- If your application uses SAML for identity processing within federated security or single sign on (SSO) purposes. SAML uses XML for identity assertions, and may be vulnerable.
- If the application uses SOAP prior to version 1.2, it is likely susceptible to XXE attacks if XML entities are being passed to the SOAP framework.
- Being vulnerable to XXE attacks likely means that the application is vulnerable to denial of service attacks including the Billion Laughs attack.

How to Prevent

Developer training is essential to identify and mitigate XXE. Besides that, preventing XXE requires:

- Whenever possible, use less complex data formats such as JSON, and avoiding serialization of sensitive data.
- Patch or upgrade all XML processors and libraries in use by the application or on the underlying operating system. Use dependency checkers. Update SOAP to SOAP 1.2 or higher.
- Disable XML external entity and DTD processing in all XML parsers in the application, as per the OWASP Cheat Sheet 'XXE Prevention'.
- Implement positive ("whitelisting") server-side input validation, filtering, or sanitization to prevent hostile data within XML documents, headers, or nodes.
- Verify that XML or XSL file upload functionality validates incoming XML using XSD validation or similar.
- SAST tools can help detect XXE in source code, although manual code review is the best alternative in large, complex applications with many integrations.

If these controls are not possible, consider using virtual patching, API security gateways, or Web Application Firewalls (WAFs) to detect, monitor, and block XXE attacks.

Guidelines for establishing system operation security

● Necessity of system operation security

An absence of system operation security policies can lead to serious cybercrime. When an unnecessary or vulnerable service is activated, there is a chance that it will be detected through network scanning, and an unauthorized access or malicious code distribution will be exploited to hack the service. For example, a Server Message Block (SMB) protocol could be used to exploit a vulnerability that could bypass the network traffic to an SMB server or a malicious web site that has been compromised by a hacker. This allows hackers to steal the corresponding login information of Windows PC users. The best security measure against such attacks would be to block the TCP 139 and 445 ports and disable the SMB protocol itself. Web sites such as Shodan are able to find out what services are active and accessible on the Internet by simply inputting search terms such as country, institution, service (port), and IP address for facility-based IT infrastructure such as IoT and ICS.

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

Operating system interface restriction (213.1) : It should be ensured whether unauthorized interfaces, ports, or services exist in the operating system

Change security setting (213.3) : When introducing information assets, the default value should be newly set or changed according to the security policy or change management standard of the company, and the use of the assets should be prohibited before the security setting is changed

Change management (213.4) : Before changing the system, the relevant data should be backed up in case of system failure

Prevent auto-execution (213.6) : All software accessing information assets should be configured not to run automatically

Performing change management (213.7) : When performing change management, pre-test should be conducted and change management records should be kept and managed

● **Procedure for change management (example)**

Raising the need to manage change	→	Apply for change	→	Review security and approve tasks	→	Conduct changes	→	Review Completion

※ Change management procedures should be handled according to internal guidelines (eg IT security guidelines)

● **Change work plan (example)**

Change Work Plan

	Receipt	Server Operation Manager	Server Operation Adminstrator	Security Officer

Registration request number		Reason for request	
Product information	Manufacturer	Product name	Server Name
Scheduled changes			
Work details			
Security review comments			

We would like to make the changes as above.

Explanation of terms

- **CVE (common vulnerabilities and exposures) :** CVE is a dictionary of publicly disclosed cyber security vulnerabilities and exposures that is free to search, use, and incorporate into products and services, as per the terms of use. The CVE List is built by CVE Numbering Authorities (CNAs). Every CVE Entry added to the list is assigned by a CNA.

  (Ex) CVE-2019-0001 : First identified vulnerability in 2019

- **P2P (peer to peer)** : Without the concept of a client or server, peer nodes in the peer-to-peer hierarchy act as clients and servers on the network at the same time. Sharing of arbitrary digital format files such as audio, video, and data is very common. In addition, real-time data such as Internet telephony (VoIP) and the like can be transmitted through P2P technology.

- **SDR (software defined radio)** : Software-based wireless data transmission control technology. An antenna, a radio frequency (RF) processing part, and a battery are configured with only a minimum amount of hardware necessary for wireless communication, and the remaining parts except the hardware are loaded with software according to the frequency, network, and wireless communication method. With this technology, it is possible to enjoy next generation mobile communication services such as WCDMA and GSM in one handset simply by manipulating the software.

- **SSRF (server side request forgery)** : Unlike the Cross Site Request Forgery (CSRF), this is a problem that occurs when the server calls directly. This allows access to the internal network from the outside, scanning and avoiding various security devices. SSRF is mainly a function that receives user input and directly accesses another web or port directly by the server.