iTrust Webinar II - A Study of Existing Guidelines and Mitigation Measures for Cyber Risks in Shipboard OT Systems

1 Apr 2020

Question and Answer Session

#	*Question*	*Answer*
Questions related to OT systems		
1	Regarding the GPS spoofing, what is the max effective range i.e. what is the max distance the attacker can be from the ship?	It depends on the attacker's capability. There are some incidents occurred at ranges up to 200m.
2	How can GPS jammers be detected?	Spectrum Monitoring enables GPS jammers to be detected and located by mobile direction-finding systems.
3	Is there any alternative for Spectrum analyzer as our vessels are not equip with it?	As of now, our study suggests spectrum analyser for detecting GPS jammers.
4	How to assess ships route have potential threat for GPS and AIS spoofing before we equip them with protecting device?	GPS spoofing threats can be assessed by using techniques like Absolute power monitoring and Spatial processing and AIS spoofing threats can be assessed by using RFeye desktop application.
5	We have lot of incidents of GPS spoofing, did we come to identify any hacker?	Based on the reports, we are not aware of any definite identified hacker.
6	What kind product/firewall to protect GMDSS?	We are unable to recommend any specific brand of products to be used.
7	Will antivirus affect the real-time performance of an ECDIS?	We would expect that anti-virus software running in the background, so it will not affect the actual operation of the shipboard OT systems.
8	Are there any ECDIS systems in the market that has anitivirus installed?	Some ECDIS models are available with installed anti-virus software, however we are unable recommend any specific products to be used.
9	Are modern ECDIS provided with Anti-virus? How are they updated?	Some ECDIS models had integrated security software, such as antivirus and firewalls and those software can be updated through internet.
10	It is difficult to enforce ECDIS or other OT equipment vendor to install anti-virus on the device	In general, the onus is on the users to decide on and purchase safe and secure equipment for operational use.
11	how can we address, equipment ie. ECDIS, Engine Control System, Cargo System - Maker PC without AVS installed, Maker mention AVS cannot be installed	
12	How easy will it be to update anti-virus signature which is almost on daily basis, considering bandwidth issues on the Vessels?	Each vessel should define the update policy, depending on the risks it faces.

13	Many anti-virus software are available in the market. However, too few are capable of detecting ransomwares etc that are newly created. Further, if a vessel is not using Vsat, update is difficult.	Probably we should look for an appropriate anti-virus software that will have capabilities to detect new types of attacks and the existing ones. Notwithstanding updating of virus signatures, zero-day attacks can still present issues. Vessels do use VSAT as it is the way through which they communicate with their offices and other ports when they are far away from land.
14	How can we update our navigational system such as GPS, VDR, AIS?	Navigational systems can be updated through VSAT using internet.
15	What are the common update methods for shipboard update? Via USB, over the air, or via specially built tools?	Most of the updates are done online (VSAT) and USB, depending on the vendor and different equipment(s).
16	Regarding GNSS, only software update is mentioned. Will upgrading equipment such as antenna and receiver reduce chances of jamming and/or spoofing?	Upgrading the equipment may reduce the chance of attacks. Techniques like Absolute power monitoring and Spatial processing for Spoofing and Spectrum monitoring for Jamming are recommended for use.
17	If Engine Control Room does not use Computer with OS and also not controlling with IoT from Bridge and Shore HQ, is it possible for hacker to take over the propulsion system?	It would be more difficult to compromise a computer without OS, but it still depends on the capability of the attacker and what he does.
18	Can the onboard computers networking /LAN effectively reduce cyber security attack?	Onboard computers networking/LAN are vulnerable if proper network segregation is not done. Firewalls, VPN play an important role here.
Other technical questions & general queries		
19	For small tonnage vessel what is the typical cyber incident happening in industry?	From our study we see that the most common cyber incidents in general are on GPS jamming, phishing emails, ransomware, virus intrusion via USB ports and hacking VSAT modems.
20	Could you recommend a usb vaccine? Did this usb vaccine can help to protect electronic onboard against hacking attack?	We haven't come across any known reports that USB vaccine is being used, so there is no assurance if it can totally help protect against cyber attacks.
21	Regarding anti-virus, if this is a zero day vulnerability, how would there be an effective measure when ship's system needs to be in real time operation?	Zero day attacks remain an issue. At the moment, we don't have very effective methods to detect at real time for such kind of attacks.
22	Is there any standard training for seafarers, as they are vulnerable to cause cyber breach?	Yes, there are online training courses available for seafarers on maritime cyber security.
23	Several request for a video to train crews. Can this be looked into.	
24	Due to the COVID-19, suggest a short video training on Cyber security will	

	suffice for onboard training. The rest would be more on the Master's responsibility to ensure such practices on cyber hygiene is constantly practice.	
25	It is difficult for non-IT personnel like seafarers to understand all risks and mitigating measures. Are you planning any training course for seafarers?	At our first step, we will try to make the guideline to be produced being easy to understand and also easy to be enforced and will also be happy to work with the maritime authority to provide the necessary training.
26	With all the cyber security measures implemented, what will be the effect on performance of various systems.? Has this study investigated this issue?	This is one of the issues we need to study and in the next step we will evaluate the impact of each of those risks and then we will give the priority on what kind of the risks need to be addressed first.
27	Dear All, Thank you for your informative presentation. My question: What type of advanced cyber technology (e.g. automated vulnerability risk management, risk management, Intrusion Detection Systems, etc.) that the Owners or Operators of these ships can implement onboard to protect themselves?	We will be discussing on risk assessment and risk management in Webinar 3 (Aug 2021).
28	For Singapore ship owners is there a department where guidance can be provided?	MPA issued a Maritime Cyber Risk Management Shipping Circular no. 15 of 2020 dated 13 August 2020 which is applicable to shipowners, ship managers, operators, and Masters of Singapore registered ships subjected to the ISM Code, and MPA's Recognised Organisations (RO). Hence, guidelines for the implementation of the Maritime Cyber Risk Management may be referred to this Shipping Circular as well as IMO Resolution MSC.428(98) and MSC-FAL.1/Circ.3 which are appended in that Shipping Circular. Shipowners and ship managers may also approach their respective ISM ROs for the guidelines on implementation of the Maritime Cyber Risk Management.
29	Have you received any PSC inspection deficiency reports already concerning cyber security?	Our Administration has not received any PSC deficiency pertaining to the implementation of the Maritime Cyber Risk Management thus far since coming into force on 01 January 2021.
30	Is Singapore going to implement any National standard for Vessel cyber security protection?	The Maritime Cyber Risk Management resides under element 1.2 .2.2 of the ISM Code, thus the implementation at 'National Standard' is not necessary and not required as the Maritime Cyber Risk Management is not an IMO Convention on its own.