2022-11-13

Investigating the Security and Accessibility of Voyage Data Recorder Data using a USB attack

Harish, Avanthika Vineetha

Investigating the Security and Accessibility of Voyage Data Recorder Data using a USB attack

Avanthika Vineetha Harish Kimberly Tam Kevin Jones
Faculty of Science and Engineering
University of Plymouth, Plymouth, United Kingdom
e-mail: {avanthika.vineethaharish, kimberly.tam, kevin.jones}@plymouth.ac.uk

***Abstract*— Voyage Data Recorders (VDR) or 'black boxes' for ships hold critical navigational and sensor data that can be used as evidence in an investigation. These systems have proven extremely useful in determining the cause of several previous shipping accidents. Considering the importance of the VDR and the increasing number of cyber-attacks in the maritime sector, the likelihood of it being attacked is high. This paper examines the security and accessibility of VDR data through a malicious USB device. A USB device is used after a series of tests, detailed in this paper, found it to be a viable way to compromise a VDR system. Intensive penetration testing was performed on a VDR, and this paper presents the four key highlights from the authors' tests. The results show that real-world VDR data might not be secure from an insider threat with little to no cyber knowledge, and future VDRs may open that up to more outsider attackers. For a device like VDR, where confidentiality, integrity and availability of data are critical, a cyber-attack could therefore lead to serious repercussions.**

Keywords- Maritime; Ransomware; USB Rubber Ducky; Voyage Data Recorder.

I. INTRODUCTION

With the maritime industry increasingly dependent on technology, cyber incidents have also been on the rise. The emergence of new technologies has led to the creation of new attack vectors, such as Wi-Fi access, poor network configuration, and unsecure third-party devices, which can cause critical damage to the industry. Maritime industries are targeted in a wide variety of ways, from phishing attacks on shipping company offices to attacks on communications and navigation systems on board ships. In the event of a major incident in the industry, a forensic investigation will be conducted to determine the cause for legal and reporting purposes, which will also help in correcting past mistakes. The study [1] observes that forensic readiness in the maritime sector, though it is not yet developed, can help in assessing cyber risks and mitigating attacks in the future.

A Voyage Data Recorder (VDR), often referred to as 'the black boxes for ships', plays a critical role in forensic investigations on ships. They store sensor data that can be retrieved following an incident, to construct the navigational plan and other factors that lead to the incident. Due to its importance, it is essential that the data stored is secure and tamper-proof, and the International Maritime Organization (IMO) clearly stipulates that VDRs should maintain a store with secure and retrievable information regarding the position, the physical status, and the command and control of the vessel over the period of the accident [2]. Interestingly, in some cases, the forensic investigators were not able to access the VDR or the data recorded. A few incidents have occurred when the VDR data disappeared mysteriously or the VDR status failed to record data at all [3]. There has been some previous research hacking a VDR (documented on a blog [3]) that exclusively used static analysis and Quick Emulator (QEMU) emulation on VDR software. In comparison, this paper builds on this previous understanding. As this study had full access to a VDR, experiments were done on the actual hardware and software of the system, and analyses were primarily dynamic for triggering real digital and physical effects. Our VDR was also connected to other real-world bridge systems, which it collected data from, adding a layer of realism beyond previous studies.

The disappearance of data can either be accidental human error, system malfunction or deliberate tampering. This paper aims to determine how plausible tampering is. With the increase in cyber-attacks in the maritime industry, the possibility of tampering with the VDR data to cover an incident or attacking the VDR itself cannot be eliminated. In addition, we examine if tampering could be simplified, so that even an unskilled insider, could be a significant threat. This is unlike previous work, as it demonstrates how attackers, but also system pen-testers, can more easily penetrate a system using modern-day pen-testing tools (i.e., pre-programmed USB, pre-installed Kali Linux tools, publicly available malware simulators). Moreover, while previous studies [3] examined only Furuno VDR software, which required specific knowledge, the proposed pen-testing USB stick in the paper could be used on any make or model, given there is a USB port.

As a critical part of incident investigations, the disappearance of VDR data can lead to investigation dead ends. As outlined in [30], which looked at incidents from 01/11/2020 to 31/10/2021, there were 275 incidents related to data breach by privilege misuse, and all these incidents

 ISBN: 978-1-61208-996-6

were caused by insiders. It was reported that 78% of the incidents were motivated by financial gain, 9% by grudge, 8% by espionage, and 6% by convenience [30]. A device like VDR, which stores its data for months on board a ship, leaves the possibility of insiders tampering with the evidence [1].

Based on the assumption that the threat actor is an insider, this paper examines the security and accessibility of VDR data with a malicious USB device. [5] shows that USBs are one of the top cyber security threat vectors, with USB threats targeted specifically at industries including shipping growing from 37% in 2021 to 52% in 2022, while the number of threats targeted at Industrial Control Systems (ICS) increased from 30% to 32% over the same period. Most VDRs typically have USB ports for updating the system, and older VDRs can only be updated this way, so leaving them open and accessible to anyone is a risk. Therefore, using the attack path of USB access seemed reasonable when the threat is an insider.

The paper will provide an overview of VDR systems and their importance in Section 2 and then moves on to describe the tools used for testing the VDR in Section 3. In Section 4, the paper will discuss the key results and highlights of the testing, followed by a conclusion with discussions and future work.

II. BACKGROUND

According to [6], the main purpose of a VDR is to collect and provide navigational data to aid in maritime accident investigations and to monitor system performance. A typical VDR system would consist of an electronics unit that gathers data from the sensors and saves it to a storage drive, with interfaces for communication and monitoring like USB, and Ethernet [4]. In addition, it will have an uninterruptible power supply, a hardened capsule, or a floating capsule for storing data and a monitor or console for performing tests [6]. The data collected include but are not limited to GPS data, heading and speed information, Electronic Chart and Display Information System (ECDIS), Automatic Identification System (AIS), data from Radar, voice feeds from bridge and rudder responses [7]. It is important to notice that VDRs currently do not have a mechanism for verifying the integrity of data to confirm if it has been tampered with. As a result, even if any of the data is manipulated, investigators might not be able to detect it.

The IMO requires all passenger ships and other ships except those passenger ships exceeding 3000 gross tonnages that are constructed on or after 1 July 2002, to be equipped with VDRs to comply with the regulations under Safety of Navigation of the International Convention for the Safety of Life at Sea (SOLAS) [2]. The Maritime Safety Committee of the IMO amended SOLAS chapter V regulation 20 in its 79th session to include requirements for VDR on cargo ships [2]. It states that cargo ships engaged in international voyages are required to have a VDR, which can be a simplified version of VDR (S-VDR) [2]. As per MSC Resolution 333.90, all VDRs installed after July 2014 must record continuously and retain data for a period of at least 30 days on the long-term storage medium and at least 48 hours on fixed or floating storage medium [8]. VDRs installed before July 2014 must retain data for a minimum of 12 hours and data will be overwritten at the end of the period. This implies that different ships will have different rules depending on the type of vessel and the date of device installation. Given the long-life span of ships before they are scrapped, there is a possibility that many ships out at sea may still be equipped with outdated VDRs that are prone to cyber-attacks and can compromise forensic investigations.

Investigating authorities like Marine Accident Investigation Board (MAIB) and US National Transportation Safety Board (NTSB) have extensively used and interrogated VDRs as evidence. An iconic investigation was the sinking of El Faro following hurricane Joaquin when NTSB and a few other organizations spent 11 months on 3 expeditions to retrieve the VDR [9]. From 26 hours of audio recordings on the vessel's bridge, a transcript of over 500 pages was produced and it significantly contributed to the discovery of the accident's cause [10]. Another incident was the grounding of Costa Concordia in the Tyrrhenian Sea off the coast of Italy. Italian authorities recovered the hard disk from the concentrator and converted the data to usable formats, generating radar screenshots, National Marine Electronics Association **(**NMEA) strings, and other data logs [4]. The investigators analyzed all this information together to understand key details, such as whether the vessel was being driven by a manual or automatic pilot, rudder instructions given and followed, and the status of watertight doors that controlled the flooding of compartments [4].

III. TOOLS USED

This paper examines whether the VDR data could be accessed or compromised and whether it could lead to unreliable data. Intensive penetration testing was performed to look for vulnerabilities and concerns that could lead to VDR data breaches and manipulation. Penetration testing or Pen-test is the method of attacking the system by authorised personnel, to identify and detect flaws in the system that could be exploited by attackers. Testing is carried out with several dedicated tools and custom scripts and this section will detail each of the tools and devices used to test an off-the-shelf VDR.

A. System Under Test

The System under Test (SuT) is an off-the-shelf VDR manufactured by a global shipping equipment manufacturer that is used by ships around the world. The specific make and model of the SuT are omitted for security purposes. The PC associated with the VDR runs Windows Embedded Standard 7 Operating System (OS). To monitor the system and test for vulnerabilities, an external attack machine that is running on Kali Linux OS is used. Kali Linux is a special OS distribution with pre-configured tools designed for penetration testing purposes. This 64-bit Kali Linux machine with 2048MB base memory is installed on a virtual box to isolate the attacks running from the host machine.

 ISBN: 978-1-61208-996-6

B. USB Rubber Ducky

A $59.99 (around £52.6) malicious device that resembles a USB stick, called USB Rubber ducky was used to execute the attacks [11]. USB Rubber Ducky was created by an information security company, Hak5, and the tool gained popularity in the security community due to its properties, like ease of use and powerful payloads [11]. When physically plugged in, the Rubber Ducky injects keystrokes into the computer it is connected to. Users can specify the keystroke combinations they want using a scripting language called Ducky Script. The script is written in a text file and then transferred to a File Allocation Table (FAT) formatted Secure Digital (SD) card. The SD card used for performing tests, in this case, is of size 128MB. For using this device, users need not have prior complex cyber security knowledge as it automates the keystrokes for the commands and if set up correctly, this could lead to heavily damaging the system. There are Rubber Ducky payloads and resources available as Github repositories, making them publicly accessible [12]. This tool is useful for automating tests, as explained in the following sections.

C. Metasploit Framework

The Metasploit framework is a powerful penetration testing tool with many features [13]. It contains several modules, which are exploits that take advantage of weaknesses in the system to hack it, payloads which are code sets that interact with the system, and auxiliary modules that perform functions, like scanning and sniffing. This framework helps in detecting a vulnerability, exploiting it, creating, and transferring payloads, and executing attacks. Currently, Metasploit has over 2000 exploits for various platforms including Android, Linux, Windows, Java, etc. It also hosts some exploit modules targeting ICS devices and protocols, like Programmable Logic Controllers (PLCs) and Modbus. However, this is limited to generic industrial components and currently, no such framework exists for the maritime industry for evaluating its systems.

D. Shinolocker Ransomware Simulator

Ransomware is a type of malware that, once it infects a system, will encrypt the files and prevent them from being accessed. Users will then be asked by the attacker to pay a ransom to decrypt the files and retrieve them. According to [14], in the year 2021, there was a 151% increase in the number of global ransomware attacks than the previous year and the numbers are predicted to rise in the coming years. For VDRs, where data is crucial and sensitive, a ransomware attack could lead to legal and regulatory issues in the event of an accident. As testing the VDR with real ransomware is dangerous, a ransomware attack on the VDR was carried out by means of a tool called ShinoLocker. ShinoLocker is a ransomware simulator developed by a security researcher, Shota Shinogi, and presented at Black Hat 2016 [16]. It works exactly like real ransomware, except that it does not ask for ransom. Once the payload has been executed, it encrypts all files of the specified type, for example, EXE, PNG, and JPEG, and displays a message, in this case, a transaction id, to retrieve the decryption key for accessing the files [15]. This tool is very useful for training and teaching purposes.

E. Nmap (Network Mapper)

Nmap is a network scanning and auditing tool. It will scan the network, find hosts, open ports and services for each host and its OS [17]. Nmap was used to identify the OS of the VDR PC and its version. It was also used to find open ports on the VDR to create test scenarios.

IV. Highlights From The Testing

After an intensive penetration test on the SuT, four key highlights were derived and presented in this section.

A. Reverse Shell

Reverse shells are interactive shell connections from a target machine to the attacking machine, that allows the attacker to access, transfer, manipulate and delete files. The first test was to determine if the attacker could obtain a reverse shell from the VDR PC to the attacking machine for viewing and manipulating files. Figure 1 shows the attack path and flow of commands. To create a reverse shell session, a reverse TCP shell payload was created using Msfvenom, a payload generator for Metasploit. With Msfvenom, users can specify a shell type, IP address, and port number, as well as a payload type (EXE, ELF, PHP) to target a system of a given architecture [18].

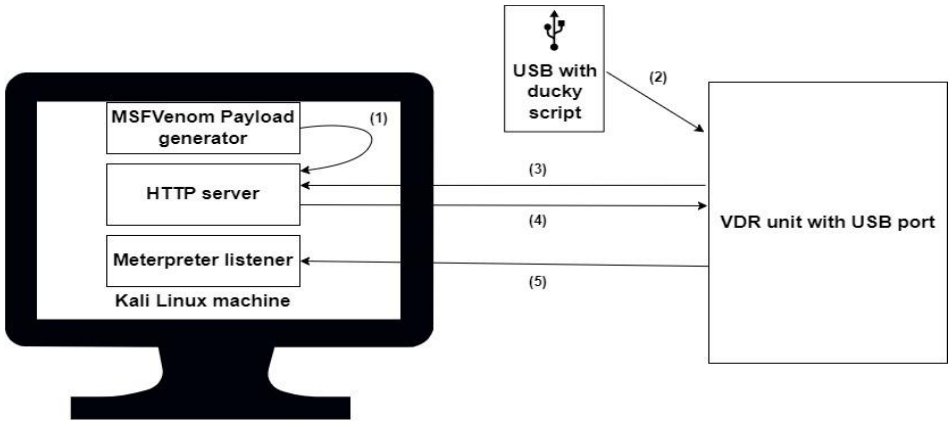

Figure 1. Attack path for creating a reverse shell.

Using Msfvenom, a reverse TCP shell payload was created to target Windows architecture using the local host IP address set as the IP address of the Kali machine. This payload then had to be transferred to the VDR for execution. To transfer the payload to the remote machine, an HTTP server was hosted on the Kali machine, and the payload was uploaded to it (see step (1) of Figure 1). Next, a ducky script was written such that once the USB device is plugged in, the HTTP server would download the payload to the VDR PC from the server. This can be seen in Steps (2) - (4) of Figure 1. Ducky script was written with five-second delays between each command, mimicking the keylogging of a human user in such a way that the VDR would be tricked even if it has a mechanism to flag fast key entries. The script was then encoded and written to an SD card.

During this time, Metasploit was running on the Kali machine with the exploit set as multi/handler; payload as meterpreter/reverse TCP, listening for any connection [19]. When the USB was plugged into Kali, a Meterpreter shell session was opened, i.e., Step (5) of Figure 1.

A complete list of steps for Figure 1 showing the path to the reverse shell:

(1) Payload generated (Msfvenom) and hosted in HTTP server
(2) Ducky Script written with commands to download payload
(3) Once the USB is plugged in, the command to download the payload
(4) Payload downloaded from server to VDR PC and executed
(5) Meterpreter listener receives a connection from VDR, and the session is opened.

Typically, shell sessions only grant local user access to the user. Thus, the privilege was escalated using the 'getsystem' command, which allowed the user to view files and folders. Additionally, other options in the Meterpreter shell were explored, such as viewing and accessing system logs, capturing webcam images, sharing screens, and listing processes. A hash dump of passwords produced 5 New Technology LAN Manager (NTLM) hashes, cracking it produced five passwords, out of which three were blank ones (including that of the 'Administrator' account), and the other two of 'Engineer' and 'Captain' accounts had simple passwords.

In a system like VDR, manipulating files using such a shell could be potentially dangerous and critical. An unauthorised or malicious insider could change the logs or files to create confusion during an accident investigation. Creating and using strong passwords is the first basic step in protecting any device from cyber-attacks. The guidelines on cyber security onboard ships document suggest using Multi-Factor Authentication (MFA) and changing default passwords to protect confidential data on safety critical systems [20]. It also recommends establishing a password policy with guidelines on password creation, updating and securing.

B. Ransomware attack

Ransomware attacks are one of the most common cyber incidents in the maritime industry and according to [22], ransomware is the leading source of cybersecurity threat risk to US ports and terminals. Maritime transport is a billion-dollar industry and ransomware attacks have risen over the past few years to take advantage of this. In the last five years, four major global shipping companies have been negatively affected by ransomware and their operations have been halted for weeks [21]. Recently, a Singapore-based offshore operator - Swift Pacific Offshore has reported a data breach that experts believe to be a ransomware attack [23]. To view the effects of a ransomware attack on the VDR, the ShinoLocker tool was used (see Figure 2). Since it was intended for training and teaching purposes, it appeared to be the most practical option without causing damage to the VDR.

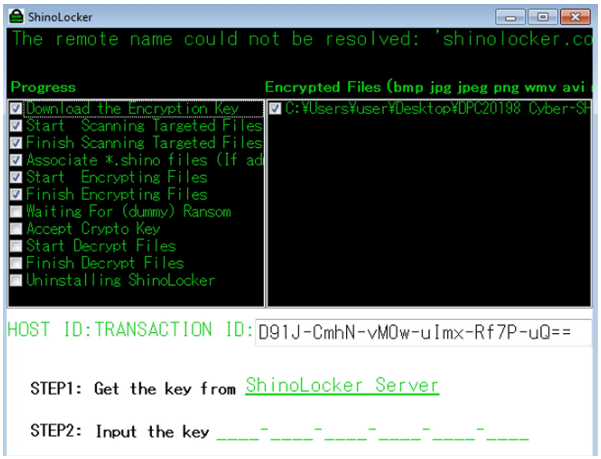

Figure 2. ShinoLocker Message Window.

To encrypt all PNG, JPG, TXT, and EXE files in the VDR, a ShinoLocker payload was created specifying those file types. The payload was transferred to the VDR in the same way as mentioned in the previous section, using an HTTP server hosted on Kali Linux machine. A ducky script was written to download the malware on to the VDR PC and then the script was transferred to the USB Rubber Ducky. As

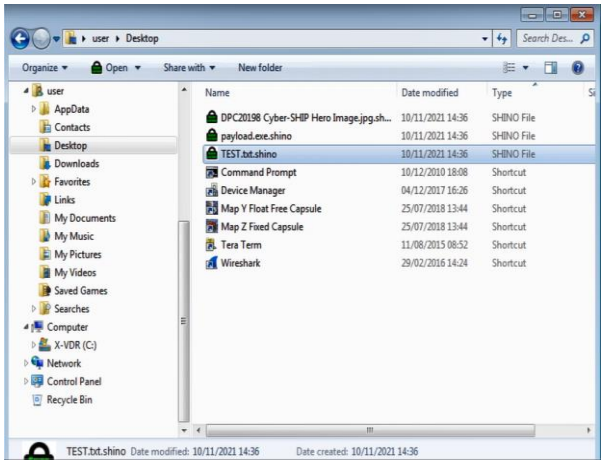

Figure 3. Encrypted Files.

soon as the USB device was plugged in to the VDR system, the malware started encrypting the files of the previously mentioned file types (see Figure 3).

There was a message like a typical ransomware message on the screen, but it did not ask for a ransom. In the message, there was an option to enter the decryption key obtained via the original tool using the transaction ID displayed on the screen after the malware infection (see Figure 4).

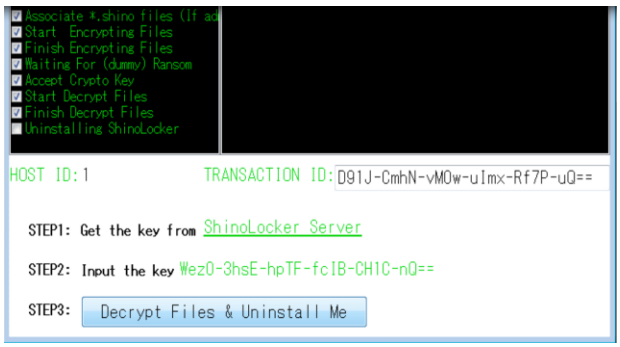

Figure 4. Decrypting Files.

Up until recently, the biggest motivation for ransomware attacks was money, but that is changing slowly. In January 2022, a Belarusian hacktivist group called 'Cyber Partisans' attacked the Belarus Railway systems using ransomware and encrypted the systems. They claim it as an act of protest and demanded the release of fifty 50 high-risk political prisoners in addition to banning Russian soldiers from using Belarusian trains as the ransom [24]. This shows that the definition of ransom in ransomware attacks is changing, and it is interesting to see if cybercriminals are likely to hold VDR data in exchange for ransom in a case where the VDR has critical evidence of a major incident.

C. Hard Drive Erasure

A third scenario involved erasing the disk contents and uninstalling Windows. This test was not performed as it would change the current settings of the machine and may destroy it. However, it could be easily accomplished with a USB Rubber Ducky and a few lines of code. The consequences of such an attack could be catastrophic on an autonomous vessel, where all configurations and settings are controlled by a machine. This is a denial-of-service attack where the system might not be available when it is needed the most or it might not be reliable.

Erasure or tampering of evidence data could lead to serious repercussions in investigations involving legal fines, human life, or geopolitical tensions. Almost a decade ago, on 15th February 2012, two Indian fishermen on a fishing boat 'St.Anthony' were killed off the coast of Kerala, India in a shooting incident mistaking the fishermen as pirates and India detained two Italian mariners on board the ship 'Enrica Lexie', an oil tanker, owned by a Milan-based company [25]. This incident strained the political relationship between the two countries. In this case, the Kerala police seized the VDR hard disk, however, it was alleged that the captain failed to preserve VDR data after the incident and the second officer of 'Enrica Lexie' stated that he did not press the VDR for recording [25].

D. Eternal Blue Vulnerability

While testing, an interesting result was obtained. The VDR PC was running Windows Embedded Standard 7 and a Nmap (Network Mapper) scan discovered that ports 139 and 445 were open. The VDR PC was found to be vulnerable to the Eternal Blue exploit that exploits remote code execution vulnerability in Microsoft SMBv1 Servers with vulnerability entry of CVE-2017-0143 in the Common Vulnerabilities and Exposures (CVE) database [26]. This vulnerability has a Common Vulnerability Scoring System (CVSS) score of 8.1 (HIGH) and the famous WannaCry attack used this exploit to spread its infection [27]. This could not have been found by only emulating parts of VDR firmware.

Even though the exploit module on Metasploit framework for Eternal Blue vulnerability was designed for 64-bit systems, and while the PC had a 32-bit operating system, the exploit module was run to see how the VDR would respond. The session was not opened as expected, however, VDR crashed with a blue screen of death and the machine needed to be manually rebooted. Since the Eternal Blue is a Random Access Memory (RAM) resident implant, once the system has been rebooted, it will function as normal again. As a result, the system may not be available when needed, and if the system is vulnerable to attacks like Eternal Blue, it may cause heavy damage.

V. Future Work and Discussions

Cyber security for maritime equipment is in its infancy, and there is little literature on voyage data recorders with even less research done on their security. Much of the literature available are reports of accidents involving VDRs, published by organisations like MAIB. Other articles analyse the investigation from a digital forensics point of view and suggest ways to improve the security of voyage data recorder data like the paper on the Costa Concordia shipwreck [4]. Data Integrity and Availability are critical properties in the Confidentiality, Integrity, and Availability (CIA) triad for devices, like Voyage Data Recorders. A study by [28] developed an algorithm of hash-based data recording where the time and date of the message are used to generate a key for authentication and a hash function is used to generate a key that combined with the original message can be used to check for message integrity. Research to improve the Remote Alarm Module (RAM) connected to the VDR would be good to alert the crew and people on the bridge if something is wrong in the system [29].

There is a need to improve VDR security from both technical and regulatory perspectives based on the little research conducted in this area. In the coming years, VDRs will become more connected, allowing new attack vectors, such as Wi-Fi access and poor network configuration, widening the attack surface. The encryption of critical data and the deployment of access control methods would help to protect the confidentiality of the evidence to an extent. The use of USB ports must also be restricted in addition to flagging when a USB device is connected to the system.

 ISBN: 978-1-61208-996-6

Using Sheep-dip protocol, where a dedicated computer that is isolated from the ship's network set up onboard, could also protect its systems from USB-based attacks. In this protocol, the removable media is plugged into the dedicated computer for scanning viruses and malware and preventing the spread of infection. This could be particularly useful in maritime systems where systems and charts are updated via USB drives.

The penetration testing of the systems could identify possible threats early on and allow them to be mitigated. At present, most of the testing is done manually by pen-testers who walk into a ship, scan the network, and inspect premises to find potential vulnerabilities. Considering the live networks and systems of critical shipping operations, this can be time-consuming and pose a high risk. In addition, manual penetration testing may miss certain vulnerabilities that are specific to a particular industry or system. An automated USB pen test tool, as demonstrated here, would make this job faster and easier. This is also more realistic than emulating parts of the VDR system [3]. As the paper [31] mentions, the main challenge in securing the maritime industry from cyber-attacks is that the common tools available currently may not be suitable or appropriate for testing due to the bespoke nature of the systems. Therefore, it is necessary to consider automated penetration testing and new vulnerability assessment framework tools that are specific to maritime systems and operations. This paper has done so with the use of the Rubber Ducky and scripts.

VI. CONCLUSION

This paper looked at investigating the security and accessibility of VDR data using an automated USB device. VDRs are safety-critical maritime systems that hold potential evidence in the occurrence of an incident. By performing an intensive penetration test, the authors were able to conclude that the data stored in the VDR is not secure and can be tampered with by a simple USB attack. Four main highlights of the testing were presented and each one discussed the consequences of the exploitation of those vulnerabilities. When VDRs become more networked and connected in future, the cyber-attack surface will expand, creating new attack vectors. Further research is needed to develop and standardize penetration testing methods for the shipping industry that will identify critical assets, uncover vulnerabilities, and report them in a way mariners could understand. It is also necessary to create information security policies and regulations for maritime systems, that will accommodate their industry-specific characteristics, to protect the data contained in these systems.

ACKNOWLEDGEMENT

This research was part of the Cyber SHIP lab project at the University of Plymouth. The authors are grateful to the project funder - Research England and our industry partners who supported our research by providing tools and equipment. The authors would also like to thank Juan Palbar Misas, Wesley Andrews and Rory Hopcraft from the University of Plymouth for their valuable comments and insights.

REFERENCES

[1] K. Tam and K. Jones, "Forensic readiness within the maritime sector," *2019 Int. Conf. Cyber Situational Awareness, Data Anal. Assessment, Cyber SA 2019*, no. June, 2019, doi: 10.1109/CyberSA.2019.8899642.

[2] International Maritime Organization, "Voyage Data Recorders," *Safety of navigation*, 2022. https://www.imo.org/en/OurWork/Safety/Pages/VDR.aspx (accessed 2022.10.21).

[3] R. Santamarta, "Maritime Security: Hacking into a Voyage Data Recorder (VDR)," *IOActive*, 2015. http://blog.ioactive.com/2015/12/maritime-security-hacking-into-voyage.html (accessed 2022.10.21).

[4] M. Piccinelli and P. Gubian, "Modern ships voyage data recorders: A forensics perspective on the Costa Concordia shipwreck," *Proc. Digit. Forensic Res. Conf. DFRWS 2013 USA*, pp. S41–S49, 2013, doi: 10.1016/j.diin.2013.06.005.

[5] Honeywell, "Industrial Usb Threat Report 2021," 2021. Accessed:2022.10.21. [Online]. Available: https://www.honeywellforge.ai/content/dam/forge/en/documents/cybersecurity/Industrial-Cybersecurity-USB-Threat-Report-2022.pdf

[6] N. Bowditch, "American practical navigator: an epitome of navigation and nautical astronomy," vol.1, pp. 72-73, 2019.

[7] IACS, "Recommendations on Voyage Data Recorder," no. 85, pp. 1–7, 2018.

[8] IMO, "Adoption of Revised Performance Standards for Shipborne Voyage Data Recorders Vdrs). IMO Resolution MSC 333(90)," 2012.

[9] N. Degnarain, "Decoding The Black Box: The 2015 US Disaster That Revolutionized Ship Crash Investigations," 2020. https://www.forbes.com/sites/nishandegnarain/2020/10/13/decoding-the-black-box-the-2015-us-disaster-that-revolutionized-ship-crash-investigations/?sh=2d39d9c3712f (accessed 2022.10.21).

[10] National Transportation Safety Board, "Sinking of the US Cargo Vessel El Faro," 2015, [Online]. Available: https://www.ntsb.gov/investigations/AccidentReports/Reports/SPC1801.pdf (accessed 2022.10.21)

[11] Hak5, "USB Rubber Ducky - Hak5," 2022. https://shop.hak5.org/products/usb-rubber-ducky-deluxe (accessed 2022.10.21).

[12] Hak5, "GitHub - hak5/usbrubberducky-payloads: The Official USB Rubber Ducky Payload Repository." 2022. https://github.com/hak5/usbrubberducky-payloads (accessed 2022.10.21).

[13] Rapid7 Inc., "Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit," *Metasploit.Com*, 2019. https://www.metasploit.com/ (accessed 2022.10.21).

[14] Sonicwall, "Mid Year Upadte Sonicwall Cyber Threat Report," 2021, [Online]. Available: https://www.sonicwall.com/2021-cyber-threat-report/ (accessed 2022.10.21).

[15] "ShinoLocker - The Ransomware Simulator-." https://shinolocker.com/ (accessed 2022.10.21).

[16] "ShinoLocker - Malware Wiki." https://malwiki.org/index.php?title=ShinoLocker (accessed 2022.10.21).

[17] nmap.org, "Nmap: the Network Mapper - Free Security Scanner," *Https://Nmap.Org/*, 2021. https://nmap.org/ (accessed 2022.10.21).

[18] Offensive Security, "Msfvenom - Metasploit Unleashed," 2016. https://www.offensive-security.com/metasploit-unleashed/Msfvenom/ (accessed 2022.10.21).

 ISBN: 978-1-61208-996-6

[19] Offensive Security, “About the Metasploit Meterpreter - Metasploit Unleashed,” *Offensive Security*, 2018. https://www.offensive-security.com/metasploit-unleashed/about-meterpreter/ (accessed 2022.10.21).

[20] BIMCO, “The Guidelines on Cyber Security Onboard Ships,” Int. Chambber Shipp. Shipp., vol. 4, pp. 1–53, 2021.

[21] C. Cimpanu, “All four of the world’s largest shipping companies have now been hit by cyber-attacks | ZDNet,” *ZDNet*, 2020. https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/ (accessed 2022.10.21).

[22] J. Walker, “Ports and Terminals Cybersecurity Survey,” 2022.Available:https://sites-communications.joneswalker.com/38/1936/landing-pages/2022-cybersecurity-survey---lp.asp (accessed 2022.10.21).

[23] Maritime Execuritve, “Ransomware Attack on Swire Pacific Offshore Breaches Personnel Data.”2021. https://www.maritime-executive.com/article/ransomware-attack-on-swire-pacific-offshore-breaches-personnel-data (accessed 2022.10.21).

[24] A. Greenberg,“Why the Belarus Railways Hack Marks a First for Ransomware | WIRED ” 2022. https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/ (accessed 2022.10.21).

[25] V. Golitsyn, J.-H. Paik, P. Robinson, F. Francioni, and P. Sreenivasa Rao, “Pca Case No. 2015-28 In The Matter Of An Arbitration-Before-An Arbitral Tribunal Constituted Under Annex Vii To The 1982 United Nations Convention On The Law Of The Sea The Italian Republic-V.-The Republic Of India-Concerning-The ‘Enrica Lexie’ Incident Registry: Permanent Court of Arbitration,” 2020 [Online]. Available: https://pcacases.com/web/sendAttach/16500 (accessed 2022.11.09)

[26] MITRE Corporation, “Cve - Cve-2017-0144,” *Cve*, 2015. https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144 (accessed 2022.10.21).

[27] NIST, “Nvd - Cve-2017-0144,” *National Vulnerability Database*, 2017. https://nvd.nist.gov/vuln/detail/CVE-2017-0144 (accessed 2022.10.21).

[28] K.-T. Seong and G.-H. Kim, “Implementation of voyage data recording device using a digital forensics-based hash algorithm,” *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 9, no. 6, pp. 5412–5419, 2019, doi: 10.11591/ijece.v9i6.pp5412-5419.

[29] J. Kang, B. Youm, D. Cho, H and H. Choe, “Development of Remote Alarm Module with playback functions in Voyage Data Recorder,” 2009, [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5334244 (accessed 2022.10.21).

[30] G. Bassett, D. Hylender, P. Langlois, A. Pinto, and S. Widup, “DBIR Data Breach Investigations Report,” 2022 [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/ (accessed 2022.10.21).

[31] K. Tam, K. Forshaw, and K. Jones, “Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities,” 2019, doi: 10.24868/icmet.oman.2019.005.

 ISBN: 978-1-61208-996-6