IOActive®

SERVICES INDUSTRIES IOACTIVE LABS NEWS ABOUT CONTACT

IOACTIVE LABS Blog Resources Tools Advisories Disclosure Policy

INSIGHTS, NEWS & DISCOVERIES FROM IOACTIVE RESEARCHERS

WEDNESDAY, DECEMBER 9, 2015

Maritime Security: Hacking into a Voyage Data Recorder (VDR)

***by Ruben Santamarta** @reversemode*

In 2014, IOActive disclosed a series of attacks that affect multiple SATCOM devices, some of which are commonly deployed on vessels. Although there is no doubt that maritime assets are valuable targets, we cannot limit the attack surface to those communication devices that vessels, or even large cruise ships, are usually equipped with. In response to this situation, IOActive provides services to evaluate the security posture of the systems and devices that make up the modern integrated bridges and engine rooms found on cargo vessels and cruise ships. [1]

There are multiple facilities, devices, and systems located on ports and vessels and in the maritime domain in general, which are crucial to maintaining safe and secure operations across multiple sectors and nations.

Port security refers to protecting all of these assets from acts of piracy, terrorism, and other unlawful activities, such as smuggling. Recent activity appears to demonstrate that cyberattacks against this sector may have been underestimated. As threats evolve, procedures and policies must improve to take these new attack scenarios into account.
For example, https://www.federalregister.gov/articles/2014/12/18/2014-29658/guidance-on-maritime-cybersecurity-standards
http://www.gao.gov/assets/670/663784.pdf

This blog post describes IOActive's research related to one type of equipment usually present in vessels, Voyage Data Recorders (VDRs). In order to understand a little bit more about these devices, I'll detail some of the internals and vulnerabilities found in one of these devices, the Furuno VR-3000.

SEARCH BLOG

Search

IOACTIVE.COM

ARCHIVE

▼ 2015 (15)
  ▼ December (1)
    Maritime Security: Hacking into a Voyage Data Reco...
  ► November (2)
  ► October (1)
  ► September (3)
  ► August (1)
  ► July (4)
  ► May (1)
  ► March (1)
  ► January (1)
► 2014 (27)
► 2013 (51)
► 2012 (40)
► 2011 (6)
► 2010 (8)
► 2009 (2)
► 2008 (5)

▶ 2007 (10)

What is a Voyage Data Recorder?

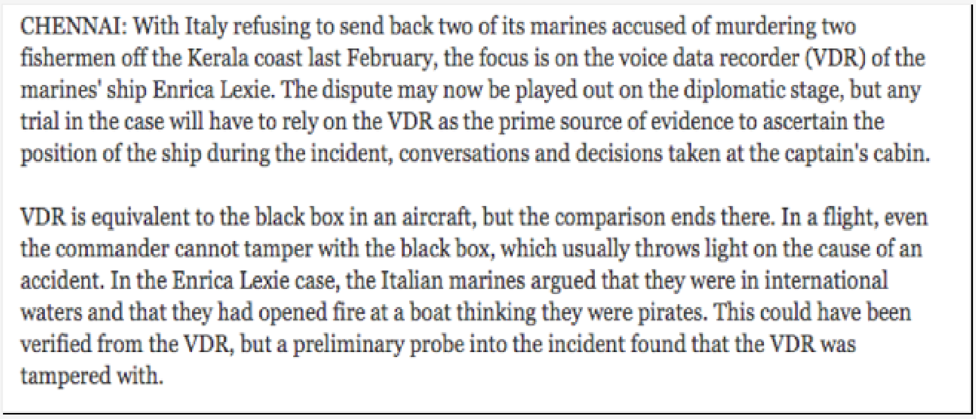
(http://www.imo.org/en/OurWork/Safety/Navigation/Pages/VDR.aspx) A VDR is equivalent to an aircraft's 'BlackBox'. These devices record crucial data, such as radar images, position, speed, audio in the bridge, etc. This data can be used to understand the root cause of an accident.

Real Incidents

Several years ago, piracy acts were on the rise. Multiple cases were reported almost every day. As a result, nation-states along with fishing and shipping companies decided to protect their fleet, either by sending in the military or hiring private physical security companies.

On February 15, 2012, two Indian fishermen were shot by Italian marines onboard the Enrica merchant vessel, who supposedly opened fire thinking they were being attacked by pirates. This incident caused a serious diplomatic conflict between Italy and India, which continues to the present. https://en.wikipedia.org/wiki/Enrica_Lexie_case

'Mysteriously', the data collected from the sensors and voice recordings stored in the VDR during the hours of the incident was corrupted, making it totally unusable for authorities to use during their investigation. As this story, from Indian Times, mentions the VDR could have provided authorities with crucial clues to figure out what really happened.



CHENNAI: With Italy refusing to send back two of its marines accused of murdering two fishermen off the Kerala coast last February, the focus is on the voice data recorder (VDR) of the marines' ship Enrica Lexie. The dispute may now be played out on the diplomatic stage, but any trial in the case will have to rely on the VDR as the prime source of evidence to ascertain the position of the ship during the incident, conversations and decisions taken at the captain's cabin.

VDR is equivalent to the black box in an aircraft, but the comparison ends there. In a flight, even the commander cannot tamper with the black box, which usually throws light on the cause of an accident. In the Enrica Lexie case, the Italian marines argued that they were in international waters and that they had opened fire at a boat thinking they were pirates. This could have been verified from the VDR, but a preliminary probe into the incident found that the VDR was tampered with.

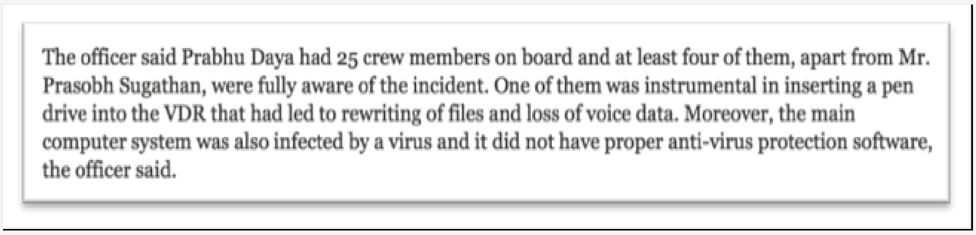
http://timesofindia.indiatimes.com/city/chennai/Lost-voice-data-recorder-may-cost-India-Italian-marines-case/articleshow/18942389.cms

Curiously, Furuno was the manufacturer of the VDR that was corrupted in this incident.

This Kerala High Court's document covers this fact: http://indiankanoon.org/doc/187144571/ However, we cannot say whether the model Enrica Lexie was equipped with was the VR-3000. Just as a side note, the vessel was built in 2008 and the Furuno VR-3000 was apparently released in 2007.

Just a few weeks later, on March 1, 2012, the Singapore-flagged cargo ship MV. Prabhu Daya was involved in a hit-and-run incident off the Kerala Coast. As a result, three fishermen were killed and one more disappeared and was eventually rescued by a fishing vessel in the area. Indian authorities initiated an investigation of the accident that led to the arrest of the MV. Prabhu Daya's captain.

During that process, an interesting detail was reported in several Indian newspapers.



The officer said Prabhu Daya had 25 crew members on board and at least four of them, apart from Mr. Prasobh Sugathan, were fully aware of the incident. One of them was instrumental in inserting a pen drive into the VDR that had led to rewriting of files and loss of voice data. Moreover, the main computer system was also infected by a virus and it did not have proper anti-virus protection software, the officer said.

http://www.thehindu.com/news/national/tamil-nadu/voyage-data-recorder-of-prabhu-daya-may-have-been-tampered-with/article2982183.ece

So, What's Going on Here?

From a security perspective, it seems clear VDRs pose a really interesting target. If you either want to spy on a vessel's activities or destroy sensitive data that may put your crew in a difficult position, VDRs are the key.

Understanding a VDR's internals can provide authorities, or third-parties, with valuable information when performing forensics investigations. However, the ability to precisely alter data can also enable anti-forensics attacks, as described in the real incident previously mentioned.

As usual, I didn't have access to the hardware; but fortunately, I played some tricks and found both firmware and software for the target VDR. The details presented below are exclusively based on static analysis and user-mode QEMU emulation (already explained in a previous blog post). [2]

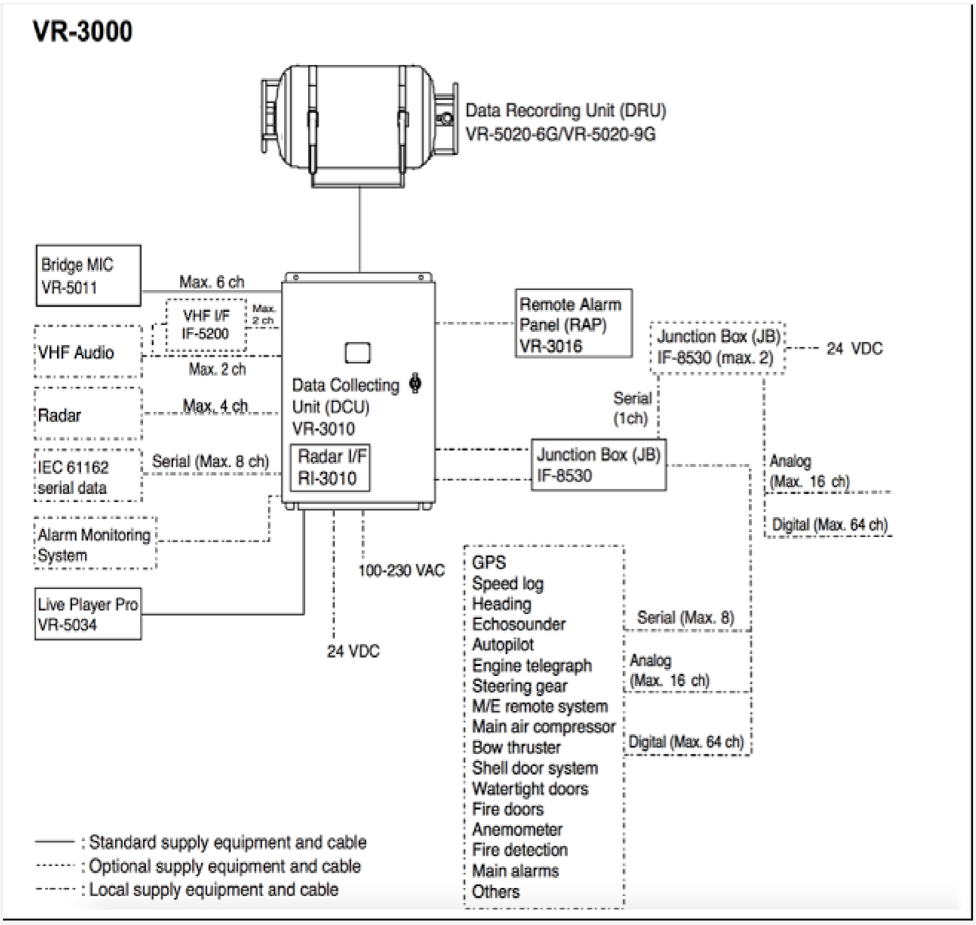


Figure: Typical architecture of a VR-3000

Basically, inside the Data Collecting Unit (DCU) is a Linux machine with multiple communication interfaces, such as USB, IEEE1394, and LAN. Also inside the DCU, is a backup HDD that partially replicates the data stored on the Data Recording Unit (DRU). The DRU is protected against aggressions in order to survive in the case of an accident. It also contains a Flash disk to store data for a 12 hour period. This unit stores all essential navigation and status data such bridge conversations, VHF communications, and radar images.

The International Maritime Organization (IMO) recommends that all VDR and S-VDR systems installed on or after 1 July 2006 be supplied with an accessible means for extracting the stored data from the VDR or S-VDR to a laptop computer. Manufacturers are required to provide software for extracting data, instructions for extracting data, and cables for connecting between a recording device and computer.

The following documents provide more detailed information:

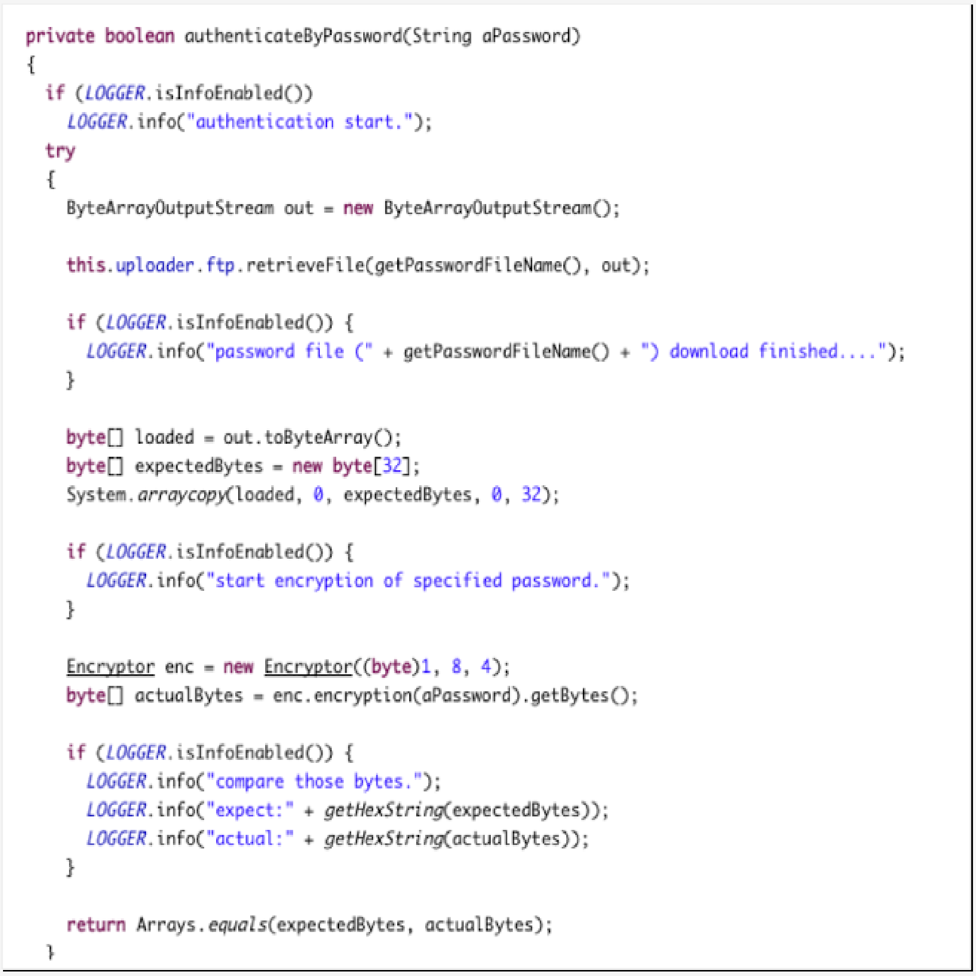
http://www.furunousa.com/ProductDocuments/VR3000%20Data%20Extraction%20Instructions%20for%20version%202.xx.pdf

http://www.furunousa.com/ProductDocuments/VR3000%20LivePlayer%20V4%20Operator's%20Manual%20%20for%20Version%202.xx.pdf

http://www.furuno.fr/Multimedia/VR3000_VR3000S_OME-G1.pdf

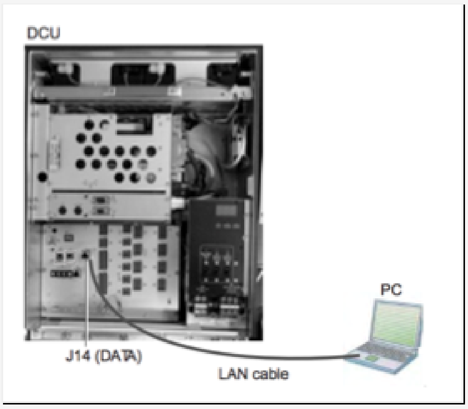
After spending some hours reversing the different binaries, it was clear that security is not one of its main strengths of this equipment. Multiple services are prone to buffer overflows and command injection vulnerabilities. The mechanism to update firmware is flawed. Encryption is weak. Basically, almost the entire design should be considered insecure.

Take this function, extracted from from the Playback software, as an example of how *not* to perform authentication. For those who are wondering what 'Encryptor' is, just a word: Scytale.



```
private boolean authenticateByPassword(String aPassword)
{
  if (LOGGER.isInfoEnabled())
    LOGGER.info("authentication start.");
  try
  {
    ByteArrayOutputStream out = new ByteArrayOutputStream();

    this.uploader.ftp.retrieveFile(getPasswordFileName(), out);

    if (LOGGER.isInfoEnabled()) {
      LOGGER.info("password file (" + getPasswordFileName() + ") download finished....");
    }

    byte[] loaded = out.toByteArray();
    byte[] expectedBytes = new byte[32];
    System.arraycopy(loaded, 0, expectedBytes, 0, 32);

    if (LOGGER.isInfoEnabled()) {
      LOGGER.info("start encryption of specified password.");
    }

    Encryptor enc = new Encryptor((byte)1, 8, 4);
    byte[] actualBytes = enc.encryption(aPassword).getBytes();

    if (LOGGER.isInfoEnabled()) {
      LOGGER.info("compare those bytes.");
      LOGGER.info("expect:" + getHexString(expectedBytes));
      LOGGER.info("actual:" + getHexString(actualBytes));
    }

    return Arrays.equals(expectedBytes, actualBytes);
  }
```

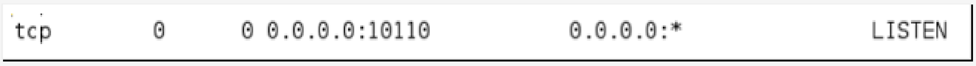
Digging further into the binary services we can find a vulnerability that allows unauthenticated attackers with remote access to the VR-3000 to execute arbitrary commands with root privileges. This can be used to fully compromise the device. As a result, remote attackers are able to access, modify, or erase data stored on the VDR, including voice conversations, radar images, and navigation data.



VR-3000’s firmware can be updated with the help of Windows software known as 'VDR Maintenance Viewer' (client-side), which is proprietary Furuno software.

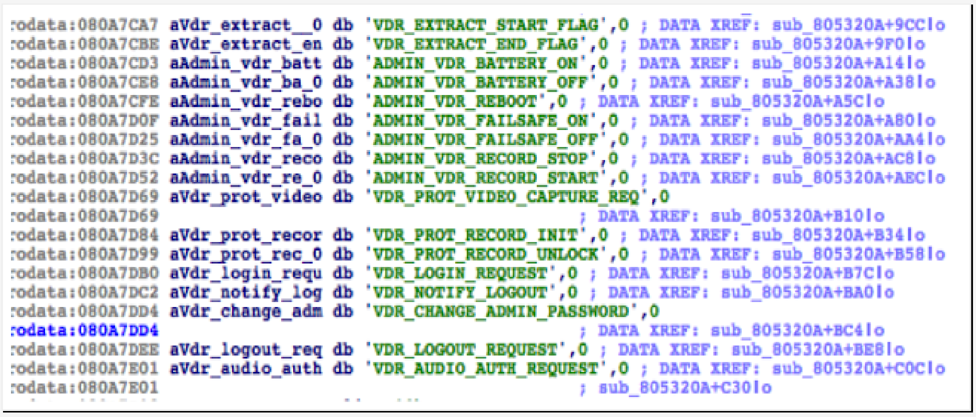
The VR-3000 firmware (server-side) contains a binary that implements part of the firmware update logic: ‘moduleserv’

This service listens on 10110/TCP.



```
tcp        0      0 0.0.0.0:10110           0.0.0.0:*               LISTEN
```

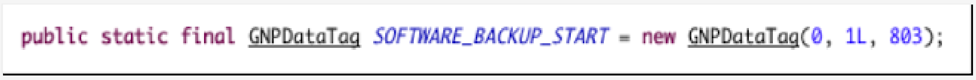
Internally, both server (DCU) and client-side (VDR Maintenance Viewer, LivePlayer, etc.) use a proprietary session-oriented, binary protocol. Basically, each packet may contain a chain of 'data units', which, according to their type, will contain different kinds of data.



```
:odata:080A7CA7 aVdr_extract__0 db 'VDR_EXTRACT_START_FLAG',0 ; DATA XREF: sub_805320A+9CClo
:odata:080A7CBE aVdr_extract_en db 'VDR_EXTRACT_END_FLAG',0 ; DATA XREF: sub_805320A+9F0lo
:odata:080A7CD3 aAdmin_vdr_batt db 'ADMIN_VDR_BATTERY_ON',0 ; DATA XREF: sub_805320A+A14lo
:odata:080A7CE8 aAdmin_vdr_ba_0 db 'ADMIN_VDR_BATTERY_OFF',0 ; DATA XREF: sub_805320A+A38lo
:odata:080A7CFE aAdmin_vdr_rebo db 'ADMIN_VDR_REBOOT',0 ; DATA XREF: sub_805320A+A5Clo
:odata:080A7D0F aAdmin_vdr_fail db 'ADMIN_VDR_FAILSAFE_ON',0 ; DATA XREF: sub_805320A+A80lo
:odata:080A7D25 aAdmin_vdr_fa_0 db 'ADMIN_VDR_FAILSAFE_OFF',0 ; DATA XREF: sub_805320A+AA4lo
:odata:080A7D3C aAdmin_vdr_reco db 'ADMIN_VDR_RECORD_STOP',0 ; DATA XREF: sub_805320A+AC8lo
:odata:080A7D52 aAdmin_vdr_re_0 db 'ADMIN_VDR_RECORD_START',0 ; DATA XREF: sub_805320A+AEClo
:odata:080A7D69 aVdr_prot_video db 'VDR_PROT_VIDEO_CAPTURE_REQ',0
:odata:080A7D69                                        ; DATA XREF: sub_805320A+B10lo
:odata:080A7D84 aVdr_prot_recor db 'VDR_PROT_RECORD_INIT',0 ; DATA XREF: sub_805320A+B34lo
:odata:080A7D99 aVdr_prot_rec_0 db 'VDR_PROT_RECORD_UNLOCK',0 ; DATA XREF: sub_805320A+B58lo
:odata:080A7DB0 aVdr_login_requ db 'VDR_LOGIN_REQUEST',0 ; DATA XREF: sub_805320A+B7Clo
:odata:080A7DC2 aVdr_notify_log db 'VDR_NOTIFY_LOGOUT',0 ; DATA XREF: sub_805320A+BA0lo
:odata:080A7DD4 aVdr_change_adm db 'VDR_CHANGE_ADMIN_PASSWORD',0
:odata:080A7DD4                                        ; DATA XREF: sub_805320A+BC4lo
:odata:080A7DEE aVdr_logout_req db 'VDR_LOGOUT_REQUEST',0 ; DATA XREF: sub_805320A+BE8lo
:odata:080A7E01 aVdr_audio_auth db 'VDR_AUDIO_AUTH_REQUEST',0 ; DATA XREF: sub_805320A+C0Clo
:odata:080A7E01                                        ; sub_805320A+C30lo
```

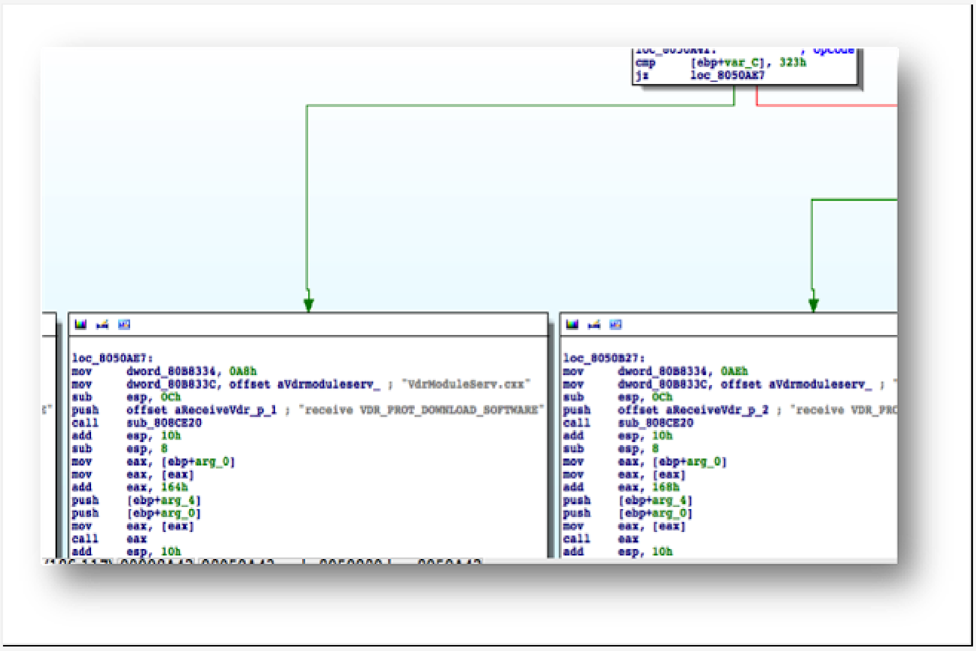
Figure: Some of the supported commands

'moduleserv' several control messages intended to control the firmware upgrade process. Let's analyze how it handles a 'SOFTWARE_BACKUP_START' request:



```
public static final GNPDataTag SOFTWARE_BACKUP_START = new GNPDataTag(0, 1L, 803);
```

An attacker-controlled string is used to build a command that will be executed without being properly sanitized. Therefore, this vulnerability allows remote unauthenticated attackers to execute arbitrary commands with root privileges.

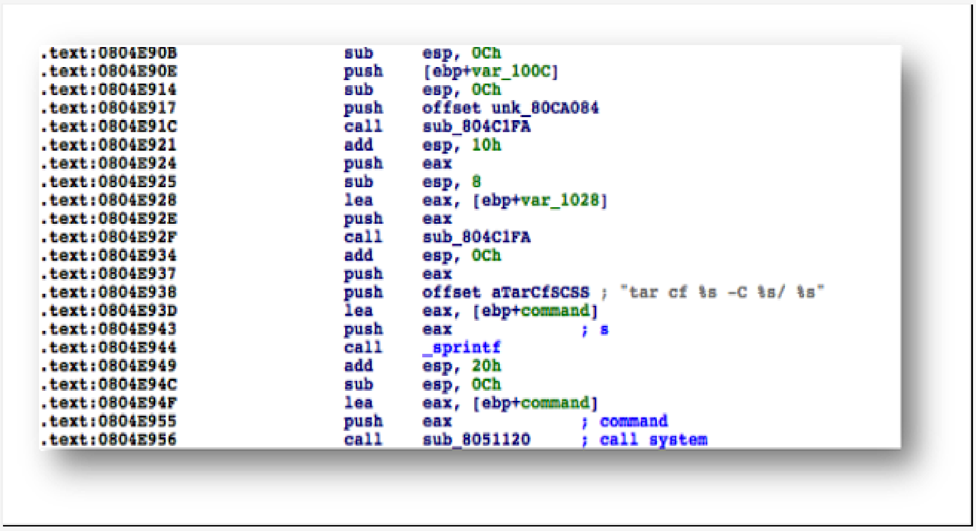


```
cmp     [ebp+var_C], 323h
jz      loc_8050AE7
```

```
loc_8050AE7:
mov     dword_80B8334, 0A8h
mov     dword_80B833C, offset aVdrmoduleserv_ ; "VdrModuleServ.cxx"
sub     esp, 0Ch
push    offset aReceiveVdr_p_1 ; "receive VDR_PROT_DOWNLOAD_SOFTWARE"
call    sub_808CE20
add     esp, 10h
sub     esp, 8
mov     eax, [ebp+arg_0]
mov     eax, [eax]
add     eax, 164h
push    [ebp+arg_4]
push    [ebp+arg_0]
mov     eax, [eax]
call    eax
add     esp, 10h
```

```
loc_8050B27:
mov     dword_80B8334, 0AEh
mov     dword_80B833C, offset aVdrmoduleserv_ ; "
sub     esp, 0Ch
push    offset aReceiveVdr_p_2 ; "receive VDR_PRO
call    sub_808CE20
add     esp, 10h
sub     esp, 8
mov     eax, [ebp+arg_0]
mov     eax, [eax]
add     eax, 168h
push    [ebp+arg_4]
push    [ebp+arg_0]
mov     eax, [eax]
call    eax
add     esp, 10h
```

Figure: ‘Moduleserv’ v2.54 packet processing



```
.text:0804E90B                 sub     esp, 0Ch
.text:0804E90E                 push    [ebp+var_100C]
.text:0804E914                 sub     esp, 0Ch
.text:0804E917                 push    offset unk_80CA084
.text:0804E91C                 call    sub_804C1FA
.text:0804E921                 add     esp, 10h
.text:0804E924                 push    eax
.text:0804E925                 sub     esp, 8
.text:0804E928                 lea     eax, [ebp+var_1028]
.text:0804E92E                 push    eax
.text:0804E92F                 call    sub_804C1FA
.text:0804E934                 add     esp, 0Ch
.text:0804E937                 push    eax
.text:0804E938                 push    offset aTarCfSCSS ; "tar cf %s -C %s/ %s"
.text:0804E93D                 lea     eax, [ebp+command]
.text:0804E943                 push    eax             ; s
.text:0804E944                 call    _sprintf
.text:0804E949                 add     esp, 20h
.text:0804E94C                 sub     esp, 0Ch
.text:0804E94F                 lea     eax, [ebp+command]
.text:0804E955                 push    eax             ; command
.text:0804E956                 call    sub_8051120     ; call system
```

Figure: ‘Moduleserv’ v2.54 unsanitized system call

At this point, attackers could modify arbitrary data stored on the DCU in order to, for example, delete certain conversations from the bridge, delete radar images, or alter speed or position readings. Malicious actors could also use the VDR to spy on a vessel’s crew as VDRs are directly connected to microphones located, at a minimum, in the bridge.

However, compromising the DCU is not enough to cover an attacker’s tracks, as it only contains a backup HDD, which is not designed to survive extreme conditions. The key device in this anti-forensics scenario would be the DRU. The privileged position gained by compromising the DCU would allow attackers to modify/delete data in the DRU too, as this unit is directly connected through an IEEE1394 interface. The image below shows the structure of the DRU.

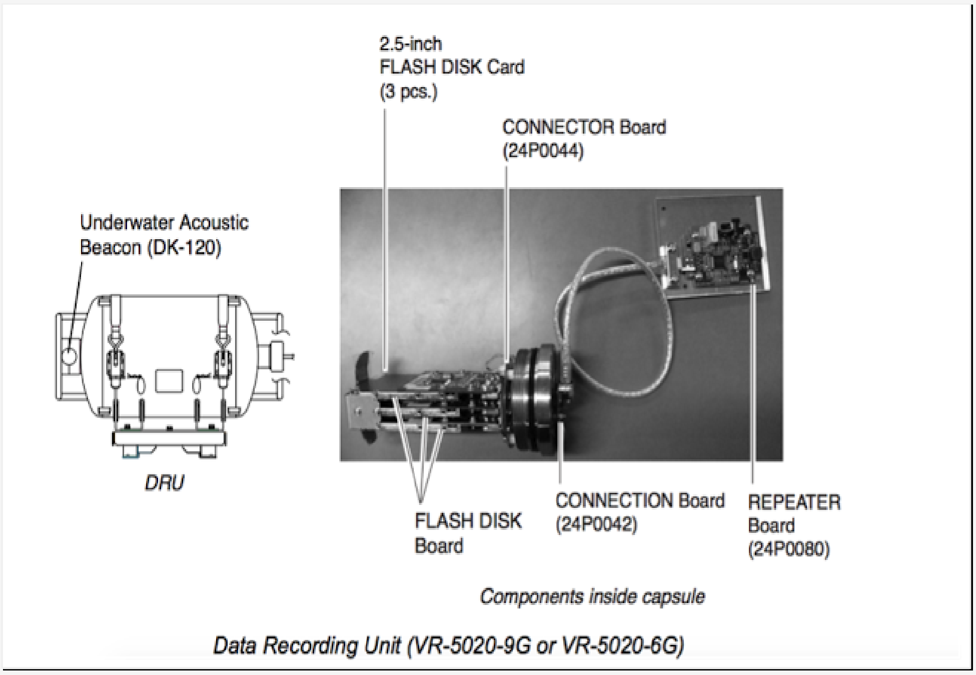

2.5-inch FLASH DISK Card (3 pcs.)
CONNECTOR Board (24P0044)
Underwater Acoustic Beacon (DK-120)
DRU
FLASH DISK Board
CONNECTION Board (24P0042)
REPEATER Board (24P0080)
Components inside capsule
Data Recording Unit (VR-5020-9G or VR-5020-6G)

Figure: Internal structure of the DRU

Before IMO's resolution MSC.233(90) [3], VDRs did not have to comply with security standards to prevent data tampering. Taking into account that we have demonstrated these devices can be successfully attacked, any data collected from them should be carefully evaluated and verified to detect signs of potential tampering.

IOActive, following our responsible disclosure policy, notified the ICS-CERT about this vulnerability in October 2014. The ICS-CERT, working alongside the JPCERT/CC, were in contact with Furuno and were able to reproduce and verify the vulnerability. Furuno committed to providing a patch for their customers "sometime in the year of 2015." IOActive does not have further details on whether a patch has been made available.

References
----

1. http://www.ioactive.com/alerts/maritime-vessel-ship-security-assurance.html
2. http://blog.ioactive.com/2013/09/emulating-binaries-to-discover.html
3. http://www.imo.org/en/KnowledgeCentre/IndexofIMOResolutions/Documents/MSC%20-%20Maritime%20Safety/333(90).pdf

Posted by Cesar at 7:00 AM

G+1 +1 Recommend this on Google

Labels: 0day, cyber attack, Furuno, hacking, maritime, piracy, ruben santamarta, SATCOM, Satellite communication, terrorism, vessels, vulnerabilities

No comments:

Post a Comment

Enter your comment...

Comment as: ggyy (Google)

Sign out

Publish Preview

□ Notify me

Home Older Post

Subscribe to: Post Comments (Atom)

IOActive®

Hardware | Software | Wetware
SECURITY SERVICES

SERVICES
INDUSTRIES
CONTACT

IOACTIVE LABS
Blog
Resources
Tools
Advisories
Disclosure Policy

NEWS
In the News
Press Releases
Events & Speaking

ABOUT
Executive Management
Advisory Board
Philanthropy
Careers