

Boarding the VSAT: Real-World Exploits, Testbed Validation, and Policy Gaps in Maritime Connectivity

YongHun No(CYTUR Inc), Seongmin Lee(Handong Univ), Juwon Cho(Yeonsei Univ)

1. Intro - Ship Happens

DEFCON

CYDOME Home About Solutions Maritime Regulations Resources Contact

LAB DOOKHTEGAN CYBER ATTACK ON IRANIAN OIL TANKERS DISRUPTS OPERATIONS

The Iranian anti-government hacktivist group "Lab Dookhtegan" ("sealed lips" in Farsi
March 18th, 2025, that it had successfully disrupted all communications for 116 oil tank
to two Iranian companies that are associated with the government and allegedly ope
international sanctions. The group claims that the attack prevented communications
and ship-to-shore (Satcom).

Communication devices are the bottleneck of maritime vessels. While modern comm
can connect to multiple satellite (and terrestrial, e.g., 4/5G) connectivity services for r
are designed for cyber resilience, and in many cases, cyber protection is even embec
communications devices. This makes the ship's communication device a single point
malicious actor hacks the communication device (VSAT or other), it can take comple
communications of the vessel and even spread out to the IT and OT systems.

The Lab Dookhtegan attack on Irani tankers

https://cydome.io/lab-dookhtegan-cyber-attack-on-iranian-oil-tankers-disrupts-operations/

https://www.iranintl.com/en/202503182119

ایران IRAN INTERNATIONAL Iran Insight Politics Economy Analysis Special Report Opinion Podcast

Cyber group says it disrupted Iranian shipping communications

Mar 18, 2025, 09:01 GMT Updated 9:23 AM Share



File photo of Iranian oil tanker 'Iran Ocean' operated by the National Iranian Tanker Company (NITC)

Method of attack

While Lab Dookhtegan has not publicly disclosed the exact Tactics, Techniques, and Procedures (TTPs) used, open-source reporting indicates the group likely exploited vulnerabilities in the maritime satellite communication systems that these ships rely on.

Vessels use two-way VSAT (Very Small Aperture Terminal) satellite equipment for external connectivity. Communication devices are known to be the common targets for cyber attacks, and vulnerabilities in network equipment are published frequently. A prior study even demonstrated that an attacker with Shodan (a device search engine) could locate ship satellite terminals and remotely compromise them using factory-set passwords, gaining the ability to alter system settings or even upload malicious firmware.

Lab Dookhtegan could have leveraged similar weaknesses. From the information presented by the group, it seems that they were able to take full control of the communications system, with elevated credentials, full access to the ships' networks and ability to remotely execute malicious code:

https://cydome.io/lab-dookhtegan-cyber-attack-on-iranian-oil-tankers-disrupts-operations/

1. Intro - Ship Happens

DEFCON

Method of attack

While Lab Dookhtegan has not publicly disclosed the exact Tactics, Techniques, and Procedures (TTPs)

Vessels use two-way VSAT (Very Small Aperture Terminal) satellite equipment for external connectivity. Communication devices are known to be the common targets for cyber attacks, and vulnerabilities in network equipment are published frequently. A prior study even demonstrated that an attacker with Shodan (a device search engine) could locate ship satellite terminals and remotely compromise them using factory-set passwords, gaining the ability to alter system settings or even upload malicious firmware.

passwords, gaining the ability to alter system settings or even upload malicious firmware.

Lab Dookhtegan could have leveraged similar weaknesses.

nation presented by the

ns system, with elevated credentials, full access to the ships' networks and ability to remotely execute malicious code:

https://cydome.io/lab-dookhtegan-cyber-attack-on-iranian-oil-tankers-disrupts-operations/

1. Intro - INDEX

SLIDO LINK FOR Q&A

https://shorturl.at/y6Xxt

01 Intro

02 About VSAT

03 Firmware Analysis & Rehosting

04 VulnerabilityDiscovery & Exploitation

05 Maritime Testbed & Attack Chain

06 Conclusion & Policy Gaps

MAIN SPEAKER



Yonghun No

- Research Engineer at CYTUR Inc.
- (PL/Mentor) for WHS 3rd at KITRI
- KITRI Best Of the Best 12th
- Research Interests
  - Maritime Cybersecurity,
  - Large Language Models,
  - Adversarial Attacks



Juwon Cho

- M.S. in Yonsei University
- KITRI Best Of the Best 12th
- Research Interests
  - Security of Generative AI Systems
  - Prompt Injection on LLMs
  - Adversarial Prompt Engineering



Seongmin Lee

- Pursuing B.S.E in Handong Univ.
- KITRI Best Of the Best 12th
- Research Interests
  - Maritime Cybersecurity
  - IoT/Baseband Hacking
  - Reverse Engineering

BOB & RESEARCH TEAM

KITRI Korea Information Technology Research Institute

BEST OF THE BEST



Best of the Best 12th

KITRI has trained security talent since 2010 and run the BoB program since 2012.

https://www.kitribob.kr/
https://www.kitri.re.kr/kitri/main

TEAM MEMBER

Mentor

- **Sanghyun Jeon** (CEO, AKDAN Inc.)
- **Kyounggon Kim** (Ph.D, NAUSS)
- **(PL) Jung Jae-wan** (Researcher, DEVICENET Inc.)

Mentee

- **Guckhyeon Jin** (Security Researcher, Stealien Inc.)
- **Jeongho Kim** (Security Researcher, Stealien Inc.)
- **Jeongmin Lee** (Hacker, Sejong Univ.)

THE DEFINITION & PERPOSE OF USING VSAT

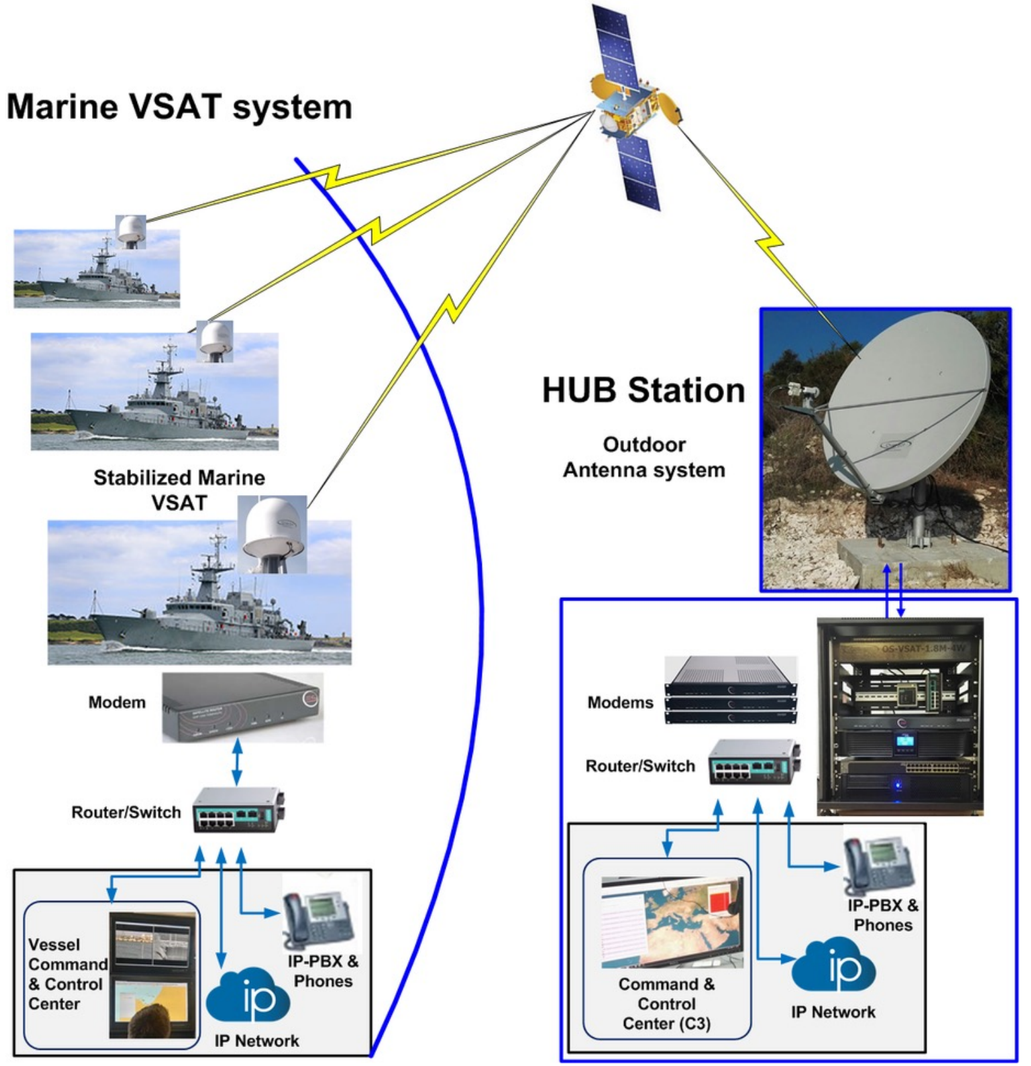
VSAT(Very Small Aperture Terminal)

- VSAT is one of the specific implementation methods of SATCOM.
- Modern vessels are developing various remote support solutions and autonomous navigation technologies
  - This requires complex data communication, making the role of satellite equipment increasingly critical.



https://www.marineeto.we.bs/2020/06/22/vsat-technology-complete-guide/

https://over-sat.com/maritime-vsat/



THE DEFINITION & PERPOSE OF USING VSAT

VSAT(Very Small Aperture Terminal)

Safety & Security

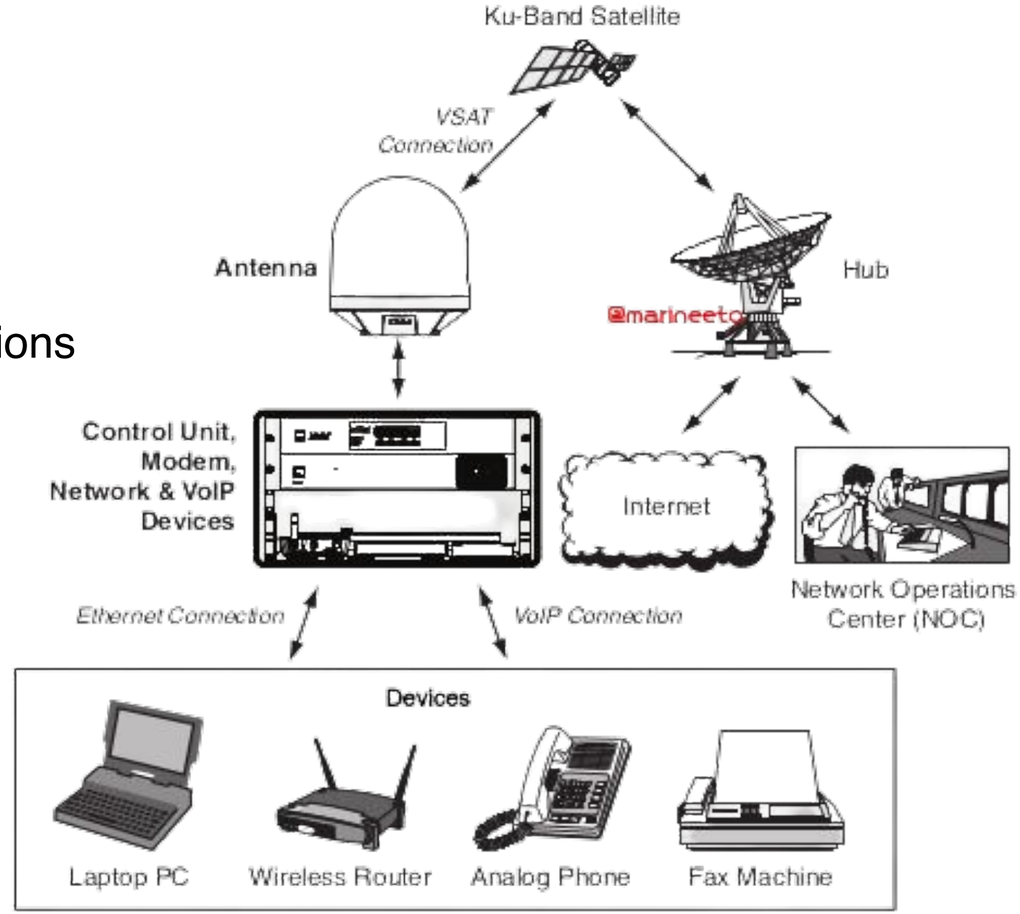
- Real-time weather information and navigation warning reception
- Communication with coastal authorities during emergency situations

Operation Efficiency

- Real-time operational information exchange with headquarters
- Remote diagnostics and technical support

Crew Welfare

- Internet access and entertainment services



https://www.numberanalytics.com/blog/ultimate-guide-satellite-communication-marine-electrical-electronics
https://www.mapfreglobalrisks.com/en/risks-insurance-management/article/satellite-communication-marine-industry/
https://www.rivieramm.com/news-content-hub/news-content-hub/vsat-provides-the-conduit-for-remote-diagnostics-40120
https://www.precisioninfocomm.com/blog/post/the-benefits-of-using-satellite-communications-for-maritime-safety-ensuring-secure-efficient-and-sus

VSAT ARCHITECTURE

Antenna

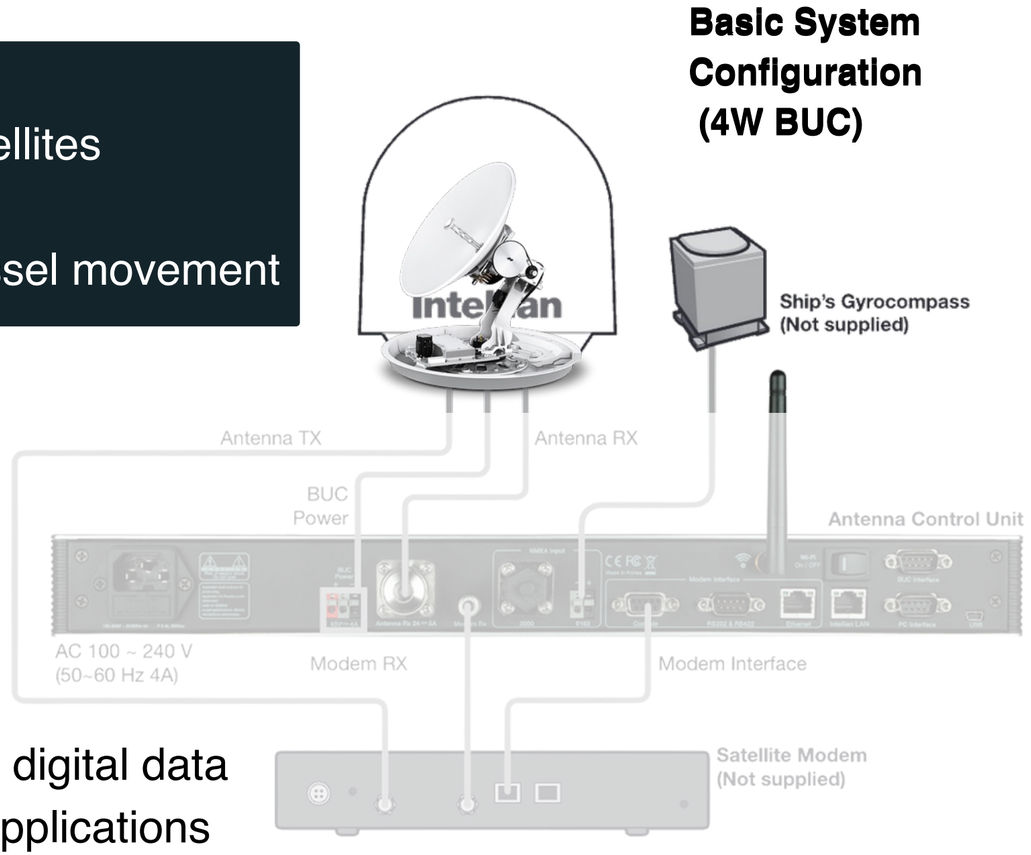
- Equipped with directional antenna for tracking geostationary satellites
- Ku, Ka, and C frequency bands are commonly used
- Automatic tracking capability to maintain satellite lock during vessel movement

ACU (Antenna Control Unit)

- Typically 19-inch rack-mount form factor control device
- Antenna control and monitoring functions
- Web interface provided for remote antenna management

Modem

- Satellite modem that modulates/demodulates RF signals to/from digital data
- Supports various protocols (DVB-S2, DVB-RCS2) for maritime applications
- Integrated with TCP/IP acceleration for optimized satellite link performance



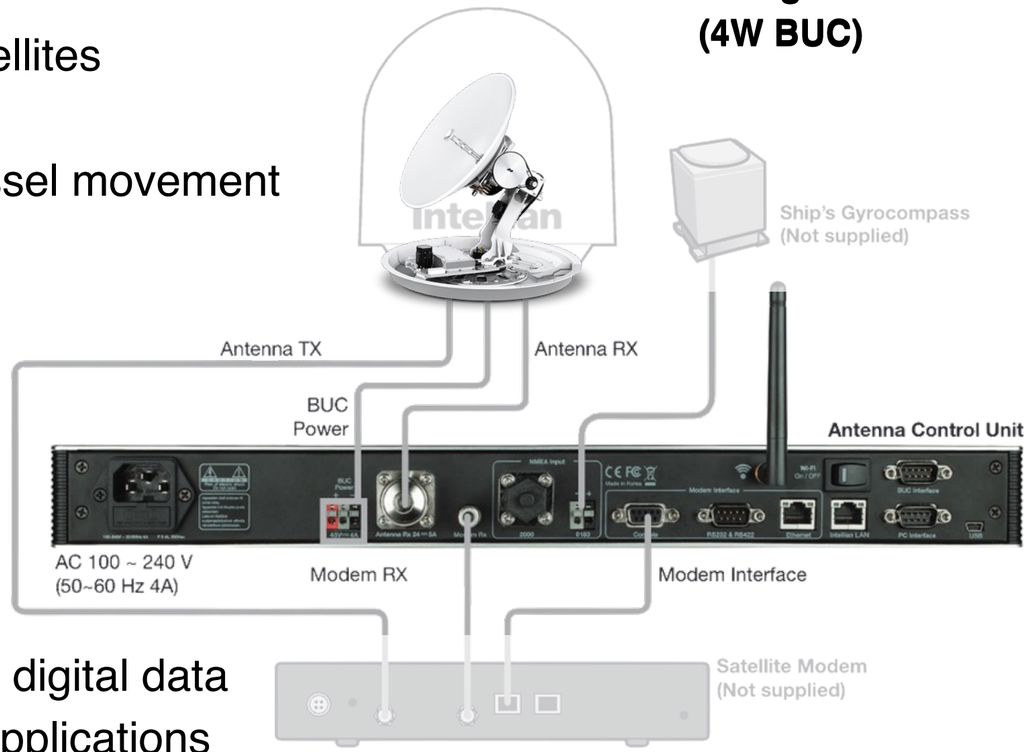
https://bravosatcom.com/2023/03/26/vsat-frequency-bands-c-band-ku-band-and-ka-band/
https://www.rivieramm.com/opinion/opinion/choosing-the-right-bands-38503
https://www.alphatronmarine.com/files/products/357-vsat-intellian-v60-instoper-manual-19-3-2017_1555592251_ed5f3b11.pdf

VSAT ARCHITECTURE

Antenna

- Equipped with directional antenna for tracking geostationary satellites
- Ku, Ka, and C frequency bands are commonly used
- Automatic tracking capability to maintain satellite lock during vessel movement

Basic System Configuration (4W BUC)



ACU (Antenna Control Unit)

- Typically 19-inch rack-mount form factor control device
- Antenna control and monitoring functions
- Web interface provided for remote antenna management

Modem

- Satellite modem that modulates/demodulates RF signals to/from digital data
- Supports various protocols (DVB-S2, DVB-RCS2) for maritime applications
- Integrated with TCP/IP acceleration for optimized satellite link performance

https://bravosatcom.com/2023/03/26/vsat-frequency-bands-c-band-ku-band-and-ka-band/
https://www.rivieramm.com/opinion/opinion/choosing-the-right-bands-38503
https://www.alphatronmarine.com/files/products/357-vsat-intellian-v60-instoper-manual-19-3-2017_1555592251_ed5f3b11.pdf

VSAT ARCHITECTURE

Antenna

- Equipped with directional antenna for tracking geostationary satellites
- Ku, Ka, and C frequency bands are commonly used
- Automatic tracking capability to maintain satellite lock during vessel movement

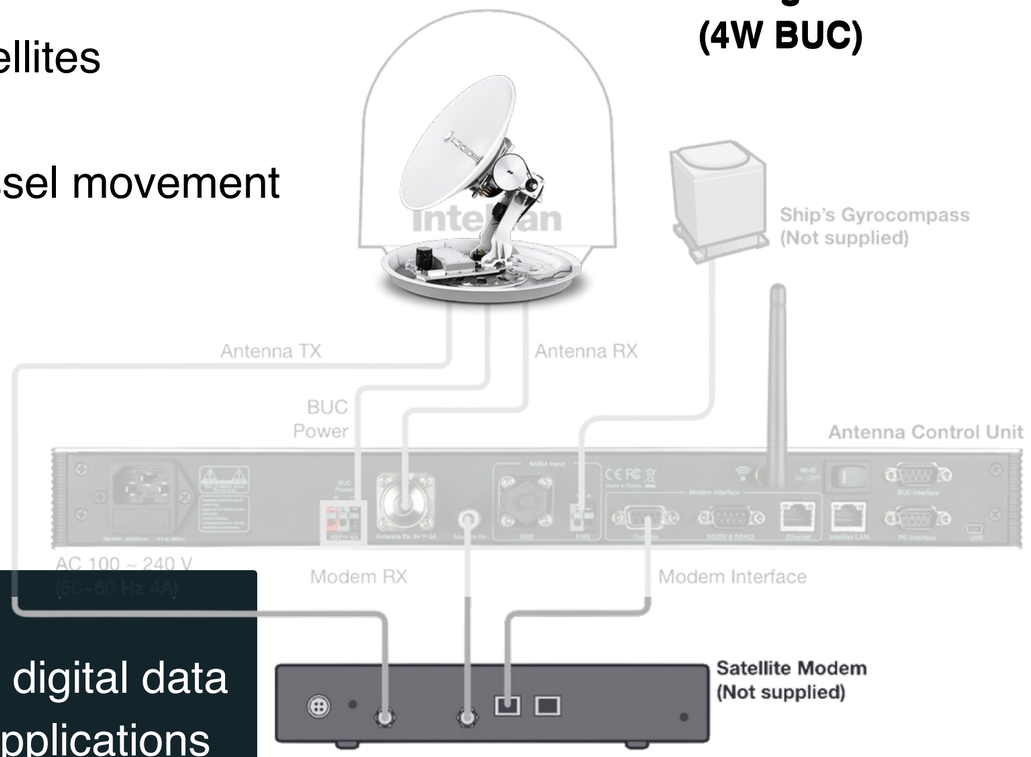
ACU (Antenna Control Unit)

- Typically 19-inch rack-mount form factor control device
- Antenna control and monitoring functions
- Web interface provided for remote antenna management

Modem

- Satellite modem that modulates/demodulates RF signals to/from digital data
- Supports various protocols (DVB-S2, DVB-RCS2) for maritime applications
- Integrated with TCP/IP acceleration for optimized satellite link performance

Basic System Configuration (4W BUC)



https://bravosatcom.com/2023/03/26/vsat-frequency-bands-c-band-ku-band-and-ka-band/
https://www.rivieramm.com/opinion/opinion/choosing-the-right-bands-38503
https://www.alphatronmarine.com/files/products/357-vsat-intellian-v60-instoper-manual-19-3-2017_1555592251_ed5f3b11.pdf

FROM 2018 TO TODAY: THE VSAT SECURITY VOID

2014 BlackHat

- *"A Wake-up Call for SATCOM Security"* IOActive. Comprehensive Information Security
  - Scope of Study: Primarily involved static firmware analysis due to lack of physical access to all devices
  - Scenarios: Spoofing ECDIS chart via satcom, Operational integrity breach
  - Target venders(Maritime sector): Cobham, JRC

2018 BlackHat

- "*Last Call for SATCOM Security"* IOActive. Comprehensive Information Security
  - Scope of Study: Not only maritime sector, they found critical security risks in SATCOM firmware
  - Scenarios: Uncontrolled exposure, Breach High Intensity Radiated Fields (HIRF) regulations
  - Target vender(Maritime sector): Intellian

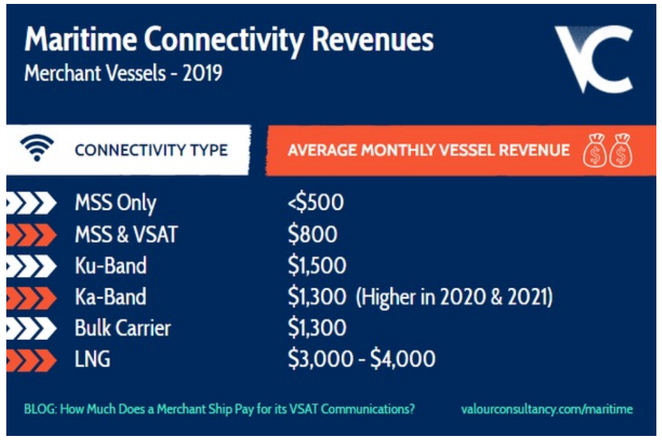
2025

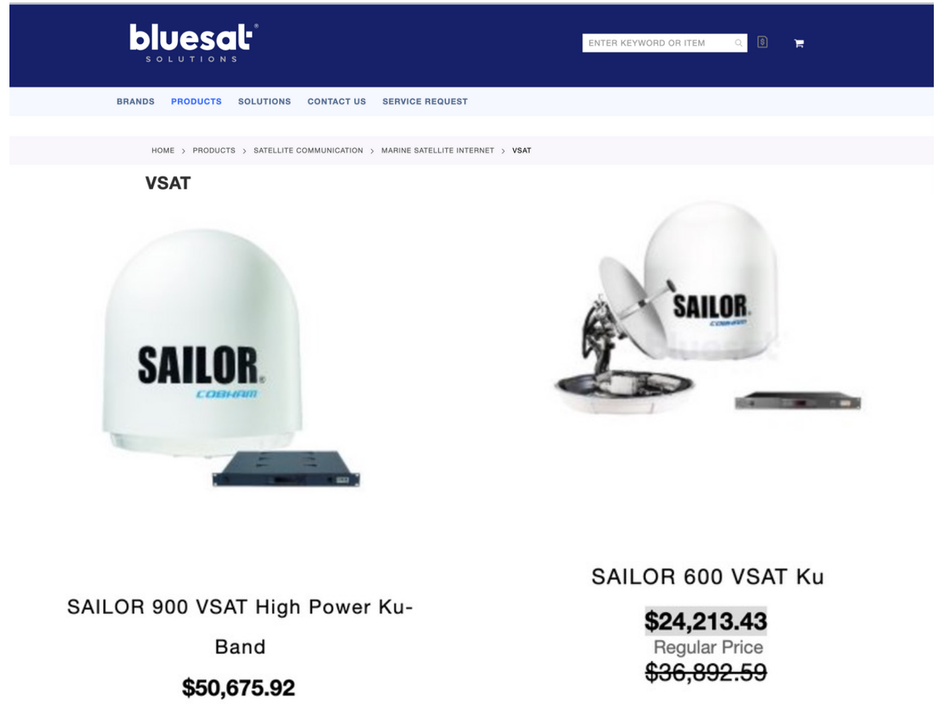
WHAT'S NEXT?

BREAKING: VSAT RESEARCH REQUIRES BREAKING THE BANK?

Common Device Price:

Antenna Size	System Type	Price Range	Usage
60cm	Ku-Band mini-VSAT	$30,000 - $39,995	Small vessels, regional coverage
1m	Ku-Band VSAT	$45,000 - $60,000	Medium vessels
1.8m	Marine VSAT	$90,000	Large vessels
2.4m	C-Band VSAT	$100,000	Large vessels, global coverage



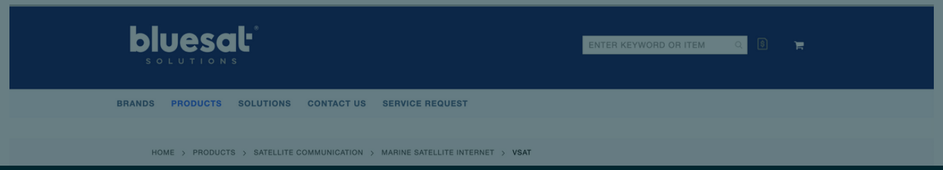


http://www.marinesatellitesystems.com/index.php?page_id=805
https://www.rivieramm.com/news-content-hub/news-content-hub/vsat-size-and-cost-reduced-52364
https://www.made-in-china.com/price/vsat-price.html
https://www.bluesat.com/products/satellite-communication/marine-satellite-internet/vsat.html
https://valourconsultancy.com/how-much-does-a-merchant-ship-pay-for-its-vsat-communications/

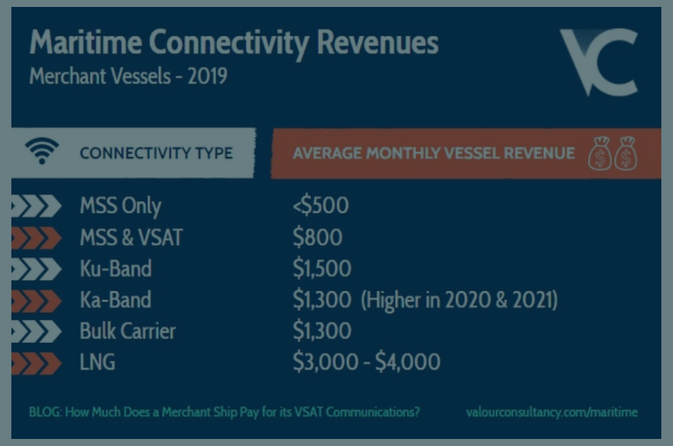
BREAKING: VSAT RESEARCH REQUIRES BREAKING THE BANK?

Common Device Price:

Antenna Size	System Type	Price Range	Usage
60cm	Ku-Band mini-VSAT	$30,000 - $39,995	Small vessels, regional coverage
2.4m	C-Band VSAT	$100,000	Large vessels, global coverage



WE FOUND THE WAY!





SAILOR 900 VSAT High Power Ku-Band

$50,675.92



SAILOR 600 VSAT Ku

$24,213.43

Regular Price

~~$36,892.59~~

http://www.marinesatellitesystems.com/index.php?page_id=805
https://www.rivieramm.com/news-content-hub/news-content-hub/vsat-size-and-cost-reduced-52364
https://www.made-in-china.com/price/vsat-price.html
https://www.bluesat.com/products/satellite-communication/marine-satellite-internet/vsat.html
https://valourconsultancy.com/how-much-does-a-merchant-ship-pay-for-its-vsat-communications/

TARGETS & GETTING THE FIRMWARE

Cobham's firmware download page

SAILOR Ku Software

Date: 26/10/2022
Version: 164B019
Document ID: 60-145900
File name: SAILOR VSAT Ku - Software 164B019
Size: 13 mb
Type: Product Software
Products: SAILOR 900 VSAT Ku Optimised,
SAILOR 900 VSAT Ku Optimised High Power,
SAILOR 800 VSAT Ku High Power,
SAILOR 900 VSAT Ku,
SAILOR 600 VSAT Ku,
SAILOR 900 VSAT Ku,
SAILOR 900 Ku in ST100 radome,
SAILOR 800 VSAT Ku,
SAILOR 900 HP in ST120 radome,
SAILOR 900 VSAT Ku Optimised w Heater,
SAILOR 900 VSAT High Power,
SAILOR 900 HP in ST100 radome,
SAILOR 900 VSAT Ku Optimised High Power w Heater

To ensure that the future improvements and updates reach the possessors of this item, we kin
your contact information in the form below.

Full name* Enter your full name
Email address* Enter your email address
Company Enter your company name

By clicking 'Download', I accept that Cobham SATCOM might contact me in the future with informa
item.

DOWNLOAD

Intellian's firmware download page

[RN-230508-01] C700 Firmware Release Note (V1.1.10)

CATEGORY

Dear All
Intellian is pleased to release new firmware for the C700 terminal. Please apply the firmware update to the models in Table 1.
It is recommended to apply this change at the next service call or visit or visit on board.

Table 1 Firmware Versions

No.	Model Name	Part no.	Previous Version	Release Version
1	C700	C1-70-A00X	1.1.9	1.1.10
2	C700 Winterized	C1-70-A0HR	1.1.9	1.1.10

Table 2 Summary of Changes

Category	Contents	Applied Software	Comments
Improvement	The location service (AptusLX Setup menu) output string now contains the IMEI # of the terminal.	BDU	

Table 3 Software Details

Product	File name	Version	
C700	Certus700_v1.1.10	Firmware	1.1.10
		ADU S/W	1.0.1
		BCX S/W	2.4.5-13243

Our final target for analysis

Cobham:
- Sailor ku software
  - Used 13 devices

Intellian:
- v240MT



SAILOR 900 VSAT Ku Optimised,
SAILOR 900 VSAT Ku Optimised High Power,
SAILOR 800 VSAT Ku High Power,
SAILOR 900 VSAT Ku,
SAILOR 600 VSAT Ku,
SAILOR 900 VSAT Ku,
SAILOR 900 Ku in ST100 radome,
SAILOR 800 VSAT Ku,
SAILOR 900 HP in ST120 radome,
SAILOR 900 VSAT Ku Optimised w Heater,
SAILOR 900 VSAT High Power,
SAILOR 900 HP in ST100 radome,
SAILOR 900 VSAT Ku Optimised High Power w Heater

Unfortunately, we can't analyze encrypted firmwares (Sailor 600 xtr, Sailor 1000 xtr, Intellian C700)

```
Target File:   /binwalk/tt7091_3.08-0011-acu_release.sig.enc.tiif
MD5 Checksum:  1ca5dbbeb5727e43e3e3b27bd4e78b9d
Signatures:    352

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             OpenSSL encryption, salted, salt: 0x300383B17B365C70
```

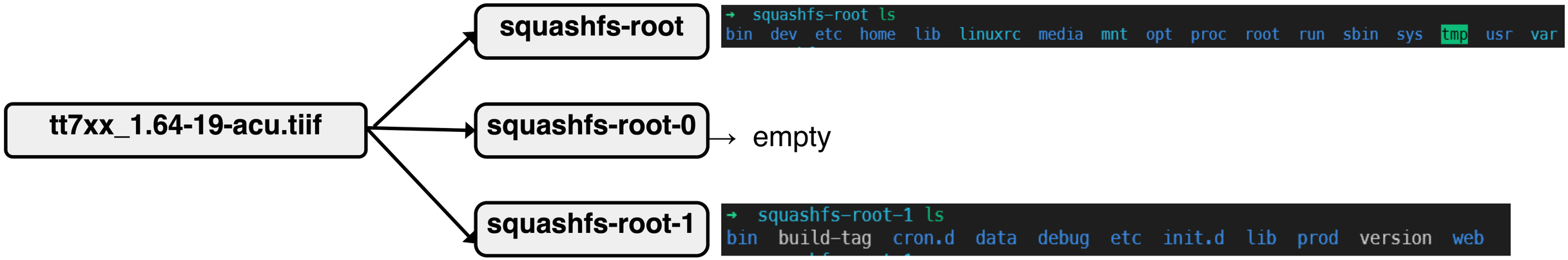
BASIC ANALYSIS & FS EXTRACTION

Boot Loader	uImage
Kernel	Linux kernel ARM zImage
File System	Squashfs filesystem

```
→  sailor-vsat-ku-software-164b019 binwalk tt7xxx_1.64-19-acu.tiif

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
6572          0x19AC          uImage header, header size: 64 bytes, header CRC: 0x8181F123, created: 2014-08-08 07:30:10, image si
0xC0008000, data CRC: 0xA09514B3, OS: Linux, CPU: ARM, image type: OS Kernel Image, compression type: none, image name: "Linux-2.6
6636          0x19EC          Linux kernel ARM boot executable zImage (little-endian)
24564         0x5FF4          gzip compressed data, maximum compression, from Unix, last modified: 2014-08-08 07:30:08
1700848       0x19F3F0        Squashfs filesystem, little endian, version 4.0, compression:gzip, size: 8842487 bytes, 1764 inodes,
10544176      0xA0E430        Squashfs filesystem, little endian, version 4.0, compression:gzip, size: 2953444 bytes, 307 inodes,
```

→ filesystem extraction with binwalk

```
→  _tt7xxx_1.64-19-acu.tiif.extracted ls
19F3F0.squashfs  5FF4  A0E430.squashfs  squashfs-root  squashfs-root-0  squashfs-root-1
```



BASIC ANALYSIS & FS EXTRACTION

squashfs-root/etc/init.d

```
→  init.d ls
S01logging  S10aligntrap  S20urandom  S22passwd  S24hostname  S40network  S41inetd  S50crond  S50sshd  mount-appl.sh  rcK  rcS  rcS-vsat7090-init.sh  suumount.awk
```

/etc/init.d/rcS

- Execute vsat7090-init.sh
- Execute the /tmp/init.d/S* files

```
→  init.d cat rcS
#!/bin/sh

[ "$VERBOSE" != no ] && echo "Init: init.d initializing... "
# Customise our init: mount apps and config, use tmp.
# Easier as oneliner, to merge with upstream buildroot
.  /etc/init.d/rcS-vsat7090-init.sh
# Start all init scripts in /tmp/init.d
# executing them in numerical order.
#
for i in /tmp/init.d/S??*; do

        # Ignore dangling symlinks (if any).
        [ ! -x "$i" ] && continue

        [ "$VERBOSE" != no ] && echo "Init: $i... "

        case "$i" in
        *.dot)
                set start
                . $i
                ;;
        *.sh)
```

rcS-vsat7090-init.sh

```
cp -a -r /tmp/root_fs/tmp/* /tmp/
umount /tmp/root_fs

# Make directories in /var (->/tmp/var)
#mkdir -p /tmp/var /var/lock /var/log /var/run /var/tmp
chmod 1777 /var/tmp
# Used by sshd
if [[ ! -d "/var/empty" ]] ; then
        echo "WARNING: sshd needs a '/var/empty' to run..."
        mkdir -p -v /var/empty
fi

# ------------------------------------------------------
[ "$VERBOSE" != no ] && echo "Mount application file systems... "
# Mount application file systems
. /etc/init.d/mount-appl.sh start

# ------------------------------------------------------
[ "$VERBOSE" != no ] && echo "Creating symlinks to all init.d/S* in /tmp/init.d... "
# Create symlinks to all init.d/S* in /tmp/init.d
# NB! S* files from appl and misc will replace ones linked in earlier
mkdir -p /tmp/init.d
for d in /etc/init.d /mnt/appl/init.d /mnt/misc/init.d; do
        [ -d $d ] && ln -sf $d/S??* /tmp/init.d/
done
# Gah - Get rid of silly link created when dir is non-existent or empty
rm -f '/tmp/init.d/S??*'

# ------------------------------------------------------
```

- Create /tmp/var, /var/lock, /var/log, /var/run, and /var/tmp
- Execute /etc/init.d/mount-appl.sh in /tmp/init.d
- Create symbolic links in /tmp/init.d pointing to the files in /mnt/appl/init.d
- Execute the files in /tmp/init.d

BASIC ANALYSIS & FS EXTRACTION

Boot Process Flow

Kernel Boot

etc/init.d/rcS

rcS-vsat7090-init.sh

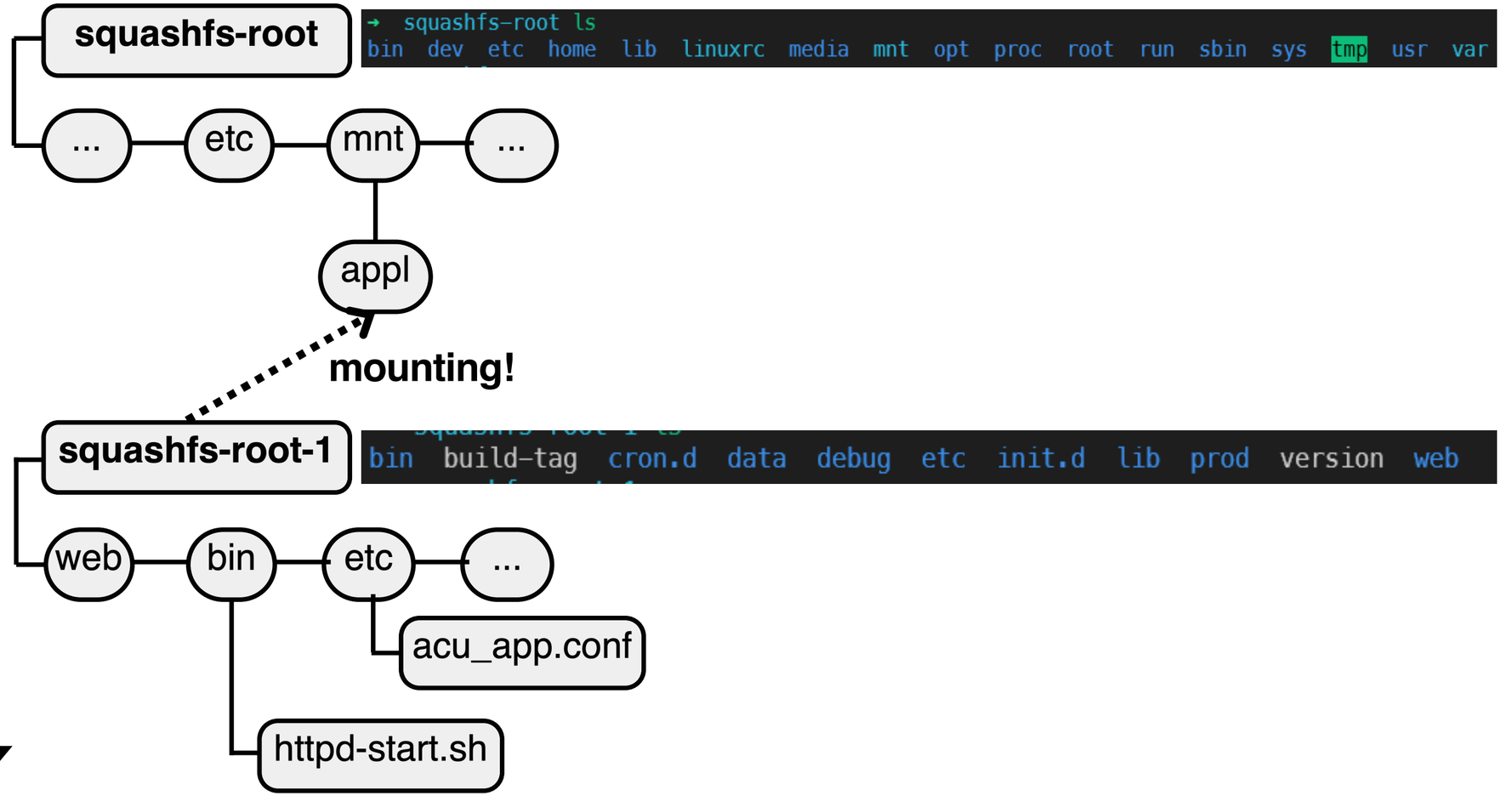
mount-appl.sh

```
# /mnt points to /tmp/mnt
mkdir -p /tmp/mnt

# Mount flash partitions
if [ "$SUUSET" != "SAFESET" ]; then
        do_mount /dev/mtdblock6  /mnt/config jffs2
        do_mount /dev/mtdblock15 /mnt/log    jffs2
        do_mount /dev/mtdblock17 /mnt/misc   jffs2
fi;

# Mount active SUU partitions
mkdir /mnt/appl
/etc/init.d/suumount.awk
```

suumount.awk

```
BEGIN {
    x = ENVIRON["SUUMNT"]
    split(x, s, ";")
    for (i in s) {
        if (s[i] == "") break
        split(s[i], r, ",")
        mountstr = "mount -t " r[3] " /dev/" r[1] " " r[2]
        print "Executing: " mountstr
        es = system(mountstr)
        if (es != 0)
            print "WARNING: Execution failed"
    }
```

FileSystem mounting flow



BASIC ANALYSIS & FS EXTRACTION

Boot Process Flow

Kernel Boot

etc/init.d/rcS

rcS-vsat7090-init.sh

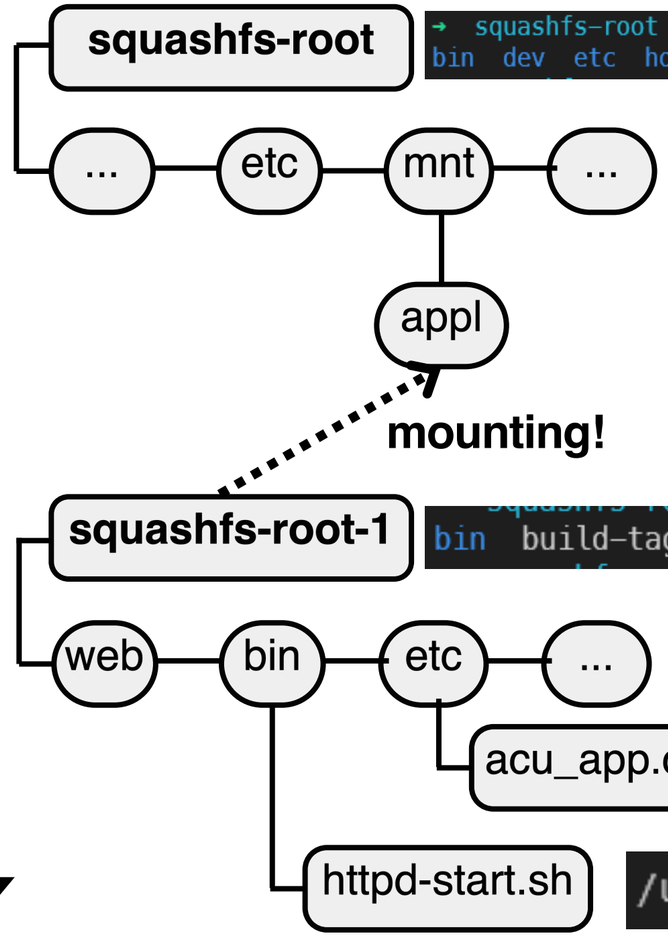
mount-appl.sh

```
# /mnt points to /tmp/mnt
mkdir -p /tmp/mnt

# Mount flash partitions
if [ "$SUUSET" != "SAFESET" ]; then
        do_mount /dev/mtdblock6  /mnt/config jffs2
        do_mount /dev/mtdblock15 /mnt/log    jffs2
        do_mount /dev/mtdblock17 /mnt/misc   jffs2
fi;

# Mount active SUU partitions
mkdir /mnt/appl
/etc/init.d/suumount.awk
```

suumount.awk

```
BEGIN {
    x = ENVIRON["SUUMNT"]
    split(x, s, ";")
    for (i in s) {
        if (s[i] == "") break
        split(s[i], r, ",")
        mountstr = "mount -t " r[3] " /dev/" r[1] " " r[2]
        print "Executing: " mountstr
        es = system(mountstr)
        if (es != 0)
            print "WARNING: Execution failed"
    }
```

FileSystem mounting flow




```
➜  squashfs-root ls
bin  dev  etc  home  lib  linuxrc  media  mnt  opt  proc  root  run  sbin  sys  tmp  usr  var
```

```
bin  build-tag  cron
```

Ready for rehosting?

```
# base application
appl base
proc base /mnt/appl/bin/cbus_server
proc base /mnt/appl/bin/acu_config
proc base /mnt/appl/bin/acu_event
```

```
# web application
appl web base net
proc web /mnt/appl/bin/acu_web nice=4
#
# Web server
appl httpd net
oproc httpd /mnt/appl/bin/httpd-start.sh nice=15
```

```
/usr/sbin/lighttpd -D -f /mnt/appl/etc/httpd.conf
```

NO BUDGET, NO PROBLEM : FIRMWARE REHOSTING FTW!

Build ARM QEMU

```
→  qe cat run.sh
qemu-system-arm \
-net nic -net user,hostfwd=tcp::2022-:22,hostfwd=tcp::2080-:80 \
-M vexpress-a9 \
-kernel ./vmlinuz-3.2.0-4-vexpress \
-initrd ./initrd.img-3.2.0-4-vexpress \
-drive if=sd,file=./debian_wheezy_armhf_standard.qcow2 \
-append "root=/dev/mmcblk0p2" \
--nographic
#-redir tcp:2022::22
```

Run QEMU

```
guest@debian-armhf:~$ uname -a
Linux debian-armhf 3.2.0-4-vexpress #1 SMP Debian 3.2.51-1 armv7l GNU/Linux
```

Mounting squashfs-root-1 manually

```
lsest@debian-armhf:~/_tt7xxx_1.64-19-acu.tiif.extracted/squashfs-root/mnt/appl$
bin  build-tag  cron.d  data  debug  etc  init.d  lib  prod  version  web
```

NO BUDGET, NO PROBLEM : FIRMWARE REHOSTING FTW!

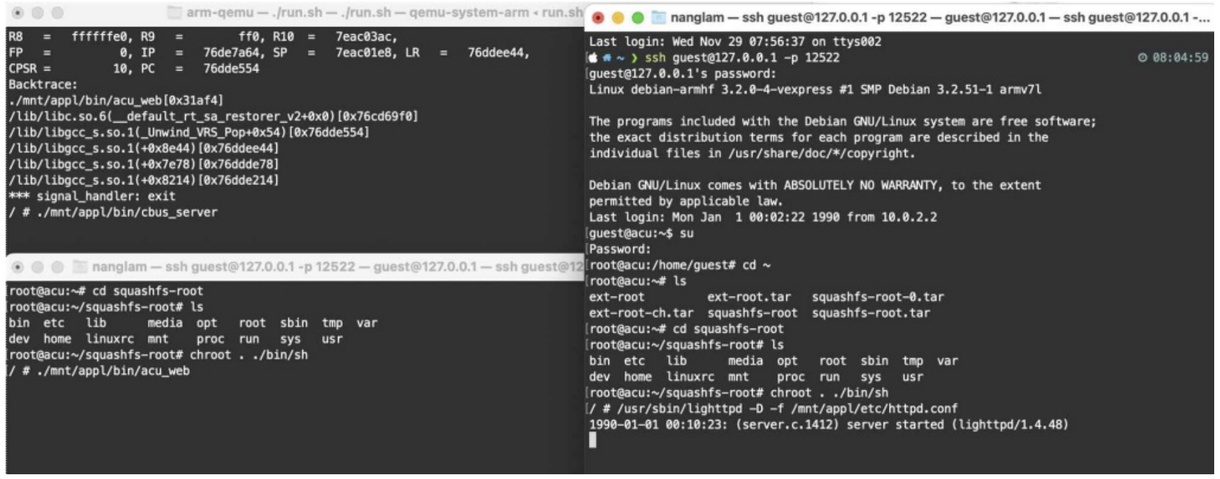
Change root with ‘chroot’ command

```
root@debian-armhf:~/squashfs-root# chroot . ./bin/sh
/ # ls
bin       home      media     proc      sbin      usr
dev       lib       mnt       root      sys       var
etc       linuxrc   opt       run       tmp
/ # pwd
/
```

Execute /etc/init.d/rcS

```
Init: /tmp/init.d/S82-ucli.sh...
Init: /tmp/init.d/S97-after_factory.sh...
Init: /tmp/init.d/S98-sleep.sh...
/etc/init.d/rcS: let: line 7: arithmetic syntax error
sh: bad number
Init: /tmp/init.d/S99-lvsat_block.sh...
Init: init.d completed...
```

/mnt/appl/bin/acu_web
/mnt/appl/bin/cbus_server
Run lighttpd



NO BUDGET, NO PROBLEM : FIRMWARE REHOSTING FTW!



REPORTED VULNERABILITIES

Attack Target	CVE ID	Description	CVSS Version 3.x
ACU	CVE-2023-44852	XSS in ACU web Diagnostics Report settings	8.2 HIGH
ACU	CVE-2023-44853	XSS in ACU web Statistics Report settings	4.8 MEDIUM
ACU	CVE-2023-44854	XSS in ACU web Remote Syslog settings	6.1 MEDIUM
ACU	CVE-2023-44855	XSS in ACU web SNMP Traps settings	6.5 MEDIUM
ACU	CVE-2023-44856	ACU Diagnostics Report: OS Command Injection	6.1 MEDIUM
ACU	CVE-2023-44857	ACU Statistics Report: OS Command Injection	8.1 HIGH

UNSANITIZED SYSTEM CALLS

CVE-2023-44853 – Command Injection Vulnerability in the Report Page

```
sub_219c4:
   0 @ 000219d4  char command[0x200]
   1 @ 000219d4  command[0] = 0
   2 @ 000219dc  void** r0 = cJSON_GetObjectItem(arg1, &data_39b54)
   3 @ 000219e4  if (r0 != 0)
```

```
   4 @ 000219ec  void** r0_1 = cJSON_GetObjectString(r0, "sender")
   5 @ 000219fc  void** r0_3 = cJSON_GetObjectItem(r0, "recipients")
   6 @ 00021a08  if (r0_1 != 0 && r0_3 != 0)
```

```
   7 @ 00021a44  char var_110[0x100]
   8 @ 00021a44  __snprintf_chk(&var_110, 0x100, 1, 0x100, "--immediate_mode --recipients %s…", r0_3[4], r0_1[4])
   9 @ 00021a80  __snprintf_chk(&command, 0x200, 1, 0x200, "%s %s %s %s", "/mnt/appl/bin/mail-report.sh -n …",
   9 @ 00021a80      &var_110, "-c /mnt/appl/bin/diag.sh", "-f `hostname`_diag_`date +%Y%m%d…")
  10 @ 00021a90  __strcat_chk(&command, " &", 0x200)
  11 @ 00021a98  system(&command)
  12 @ 00021a9c  return 1
```

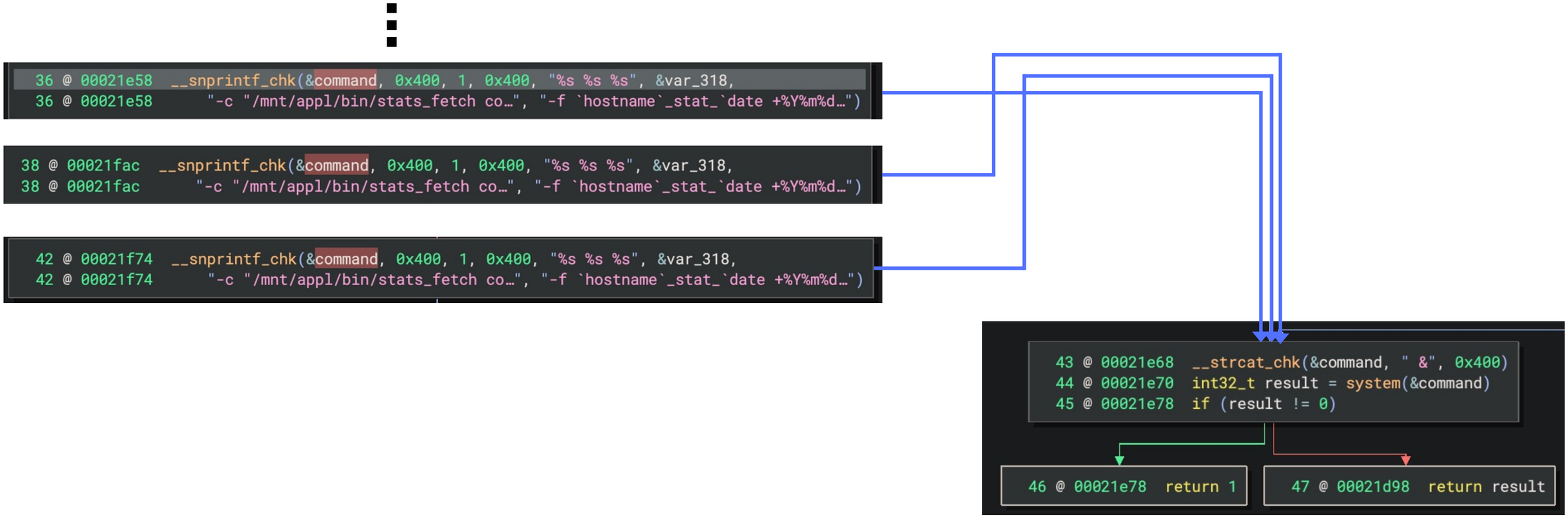
UNSANITIZED SYSTEM CALLS

CVE-2023-44857 – Command Injection Vulnerability in the Diagnostics report Page



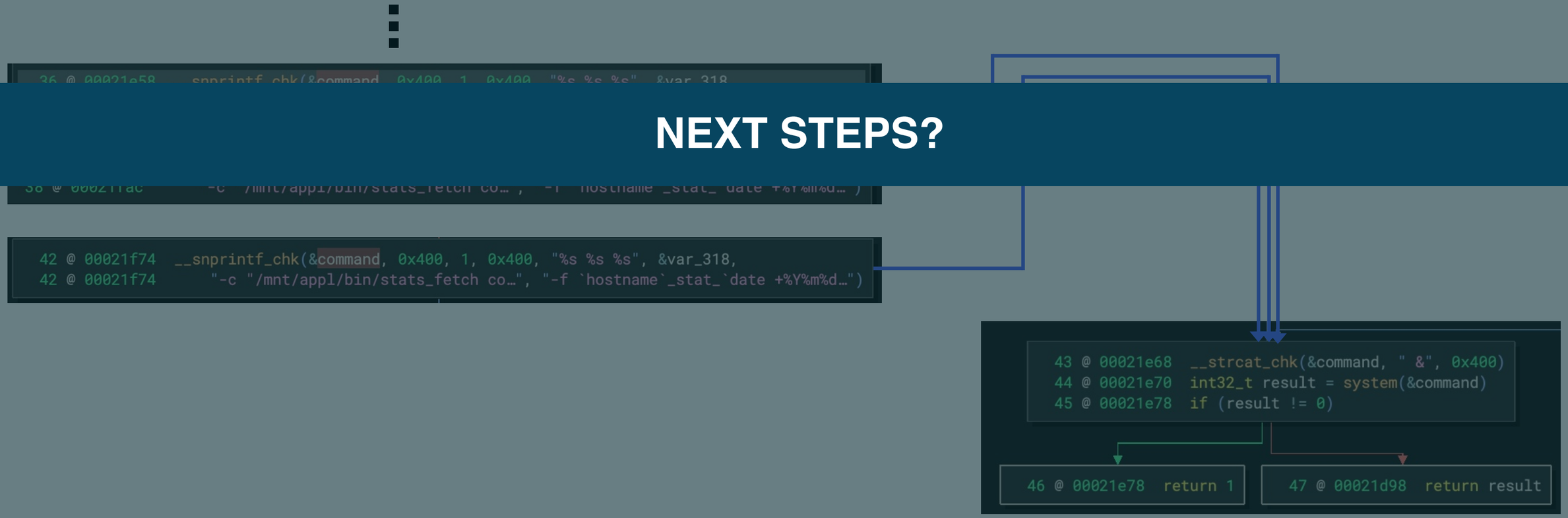
UNSANITIZED SYSTEM CALLS

CVE-2023-44857 – Command Injection Vulnerability in the Diagnostics report Page



UNSANITIZED SYSTEM CALLS

CVE-2023-44857 – Command Injection Vulnerability in the Diagnostics report Page



NEXT STEPS?

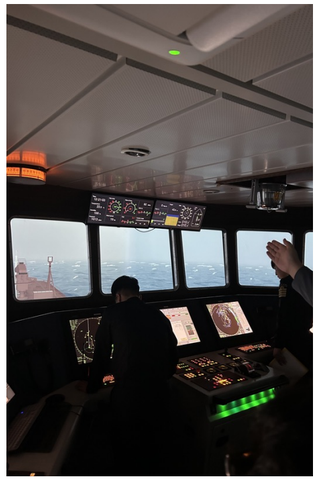
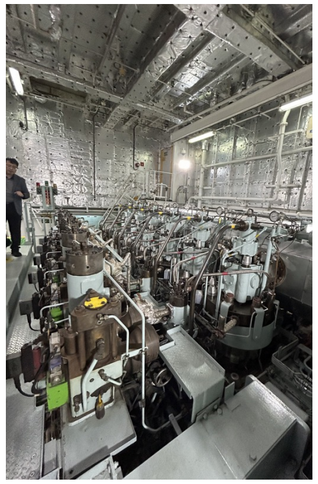
MODERN VESSELS: WHAT HAS BEEN CHANGED?

Characteristics of Autonomous Navigation Ships

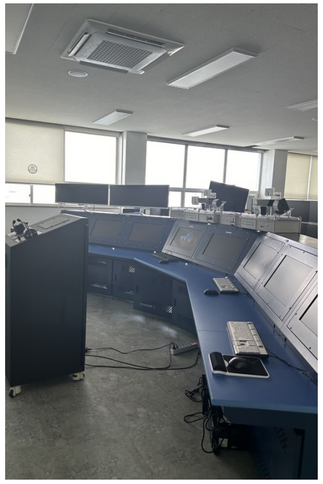
- Blurred network separation → OT infrastructure is being connected to networks
- Increased use of satellite communication → Various sensor information and control communication from LIDAR, vision cameras, etc. are conducted through satellite communication
- Increased use of Ethernet → Existing control protocols like NMEA, CAN, etc. can be replaced by Ethernet

Field Trip

- Advisory from Korea Maritime and Ocean University
  - Visit to Bridge, Engine Room, and Autonomous Ship Research Laboratory

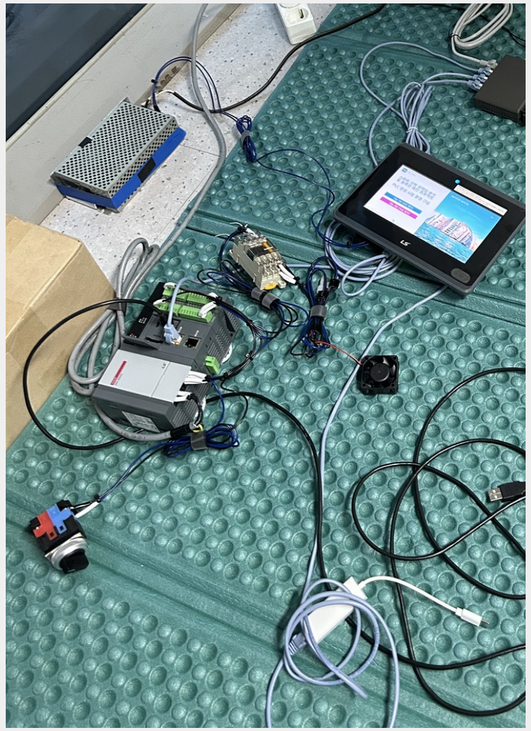





SET UP THE EXPERIMENTAL ENVIRONMENT

Development Goals

- Access satellite communication terminals to verify the possibility of accessing ship's OT infrastructure and remote attacks





Raspberry Pi 4

- Running Cobham Sailor VSAT firmware
- Point of vulnerability occurrence

N Company Layer-2 Switch

- A standard network switch handling MAC-based switching
- Point of Vulnerability

MOXA Industrial Hub

- Widely used on vessels
- Unmanaged switching hub

Raspberry Pi 3

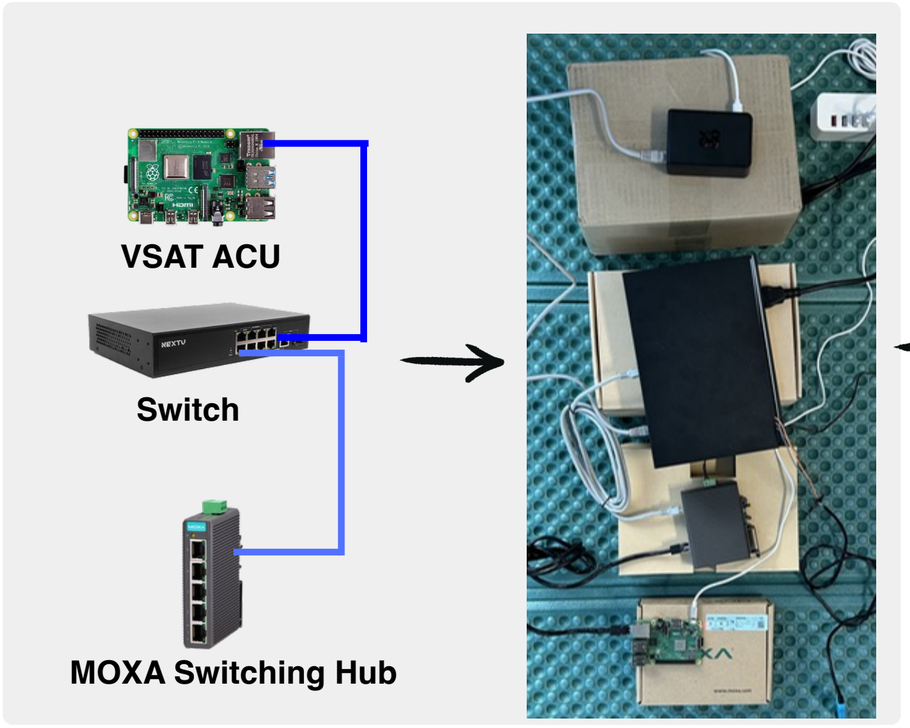
- OT environment downstream of the industrial hub
- Capable of running an HMI (Human–Machine Interface)

OT system implementation

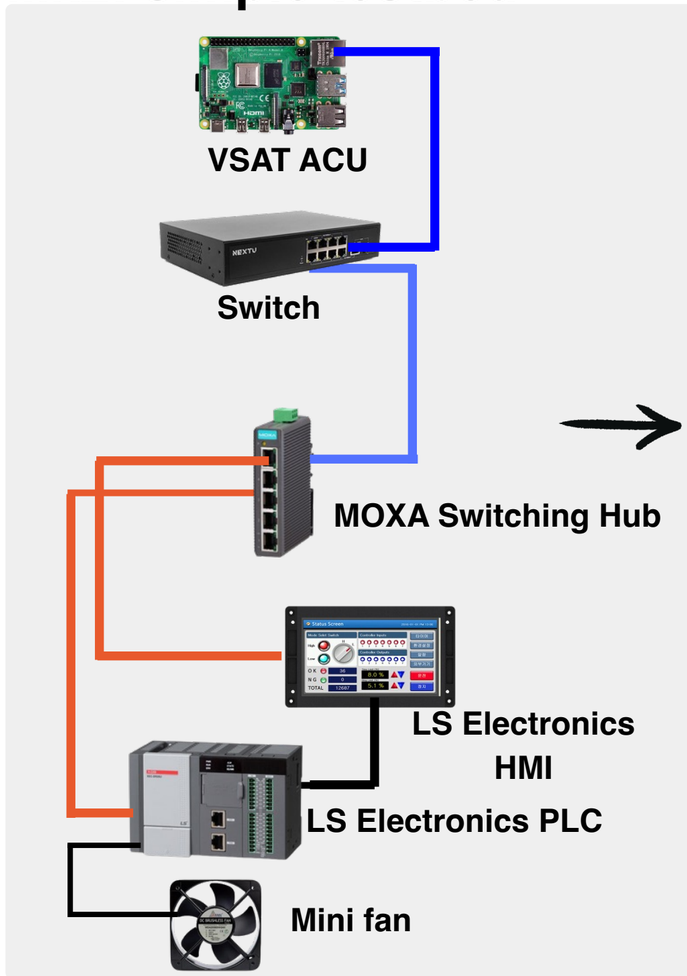
- Deployment of the OT system at the vessel's lowest level
- Simple ship propeller control implemented using an LS Electric PLC

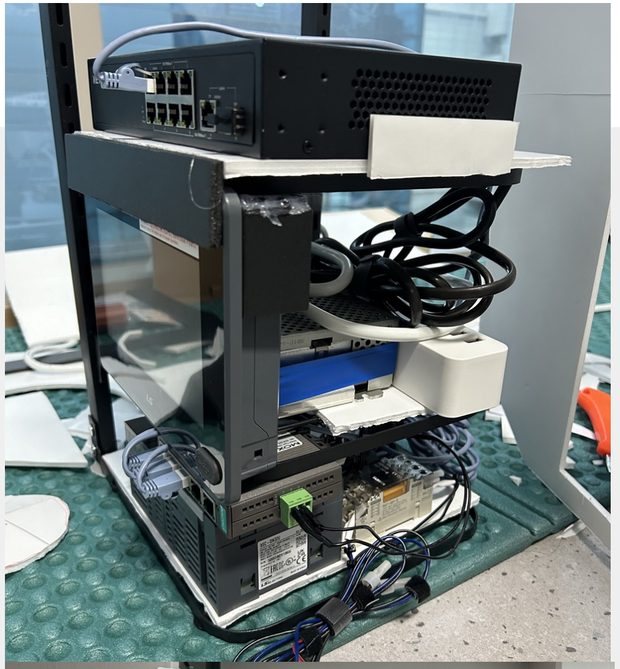
SET UP THE EXPERIMENTAL ENVIRONMENT

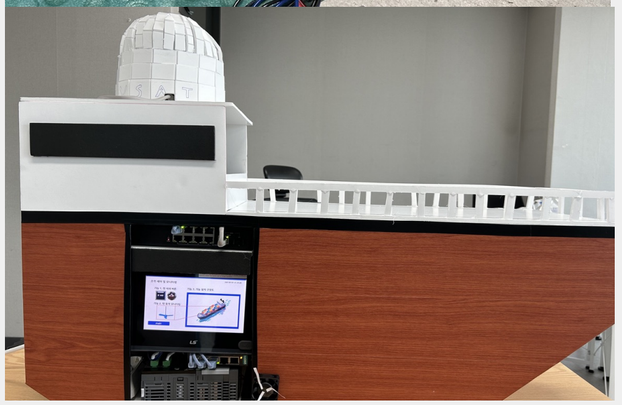
Mk1: function test



Mk2: simple testbed







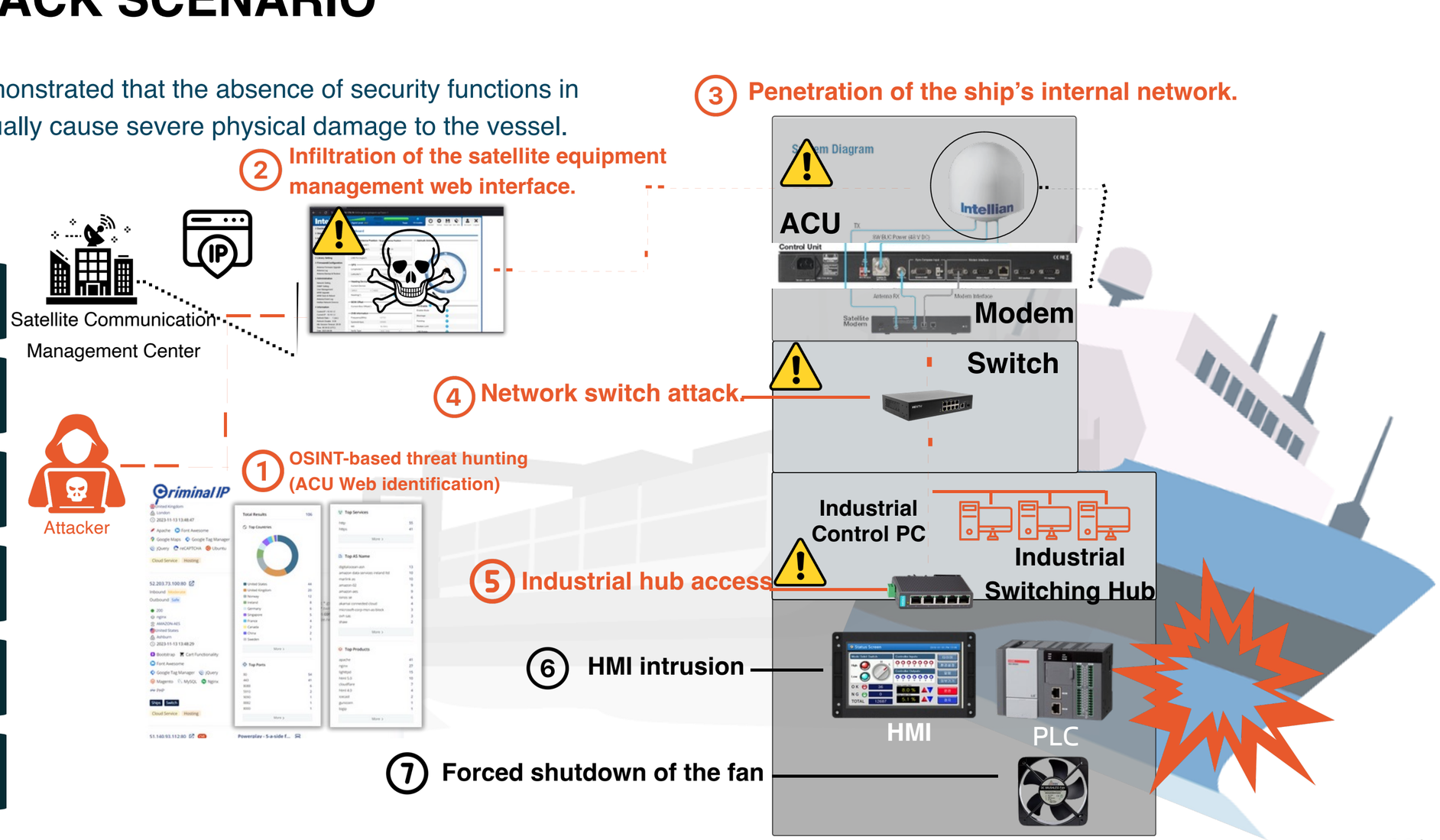
SET UP THE ATTACK SCENARIO

Overview

- Through experiments, we demonstrated that the absence of security functions in shipboard equipment can actually cause severe physical damage to the vessel.

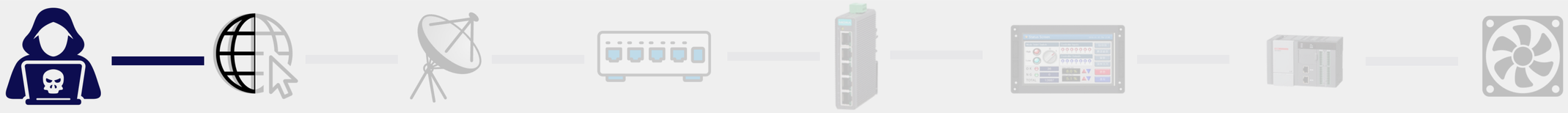
STEPS:

- (1) OSINT threat hunting
- (2) Infiltration through ACU web
- (3) Ship network penetration
- (4) Attack network devices
- (5) HMI intrusion
- (6) Overwriting PLC project



5. Maritime Testbed & Attack Chain

OSINT Exposure Status of Shipboard Equipment

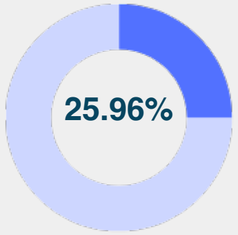


STEPS:

- **(1) OSINT threat hunting**
- (2) Infiltration through ACU web
- (3) Ship network penetration
- (4) Attack network devices
- (5) HMI intrusion
- (6) Overwriting PLC project

*For the year 2023

Cobham



- Identified 104 items
- Identified 54 HTTP pages

< Vulnerable Page Ratio

Intellian

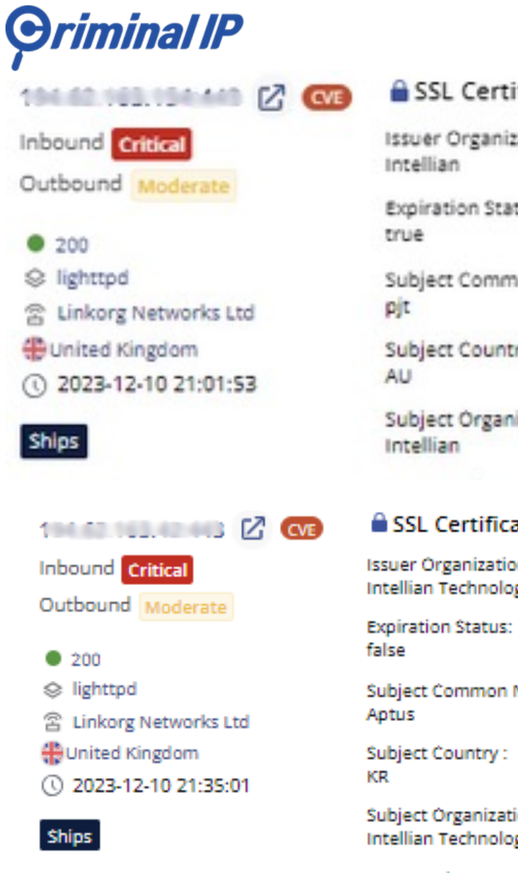


- Identified 14 instances (via favicon search)
- Identified 11 actual vessels

< Vulnerable Page Ratio

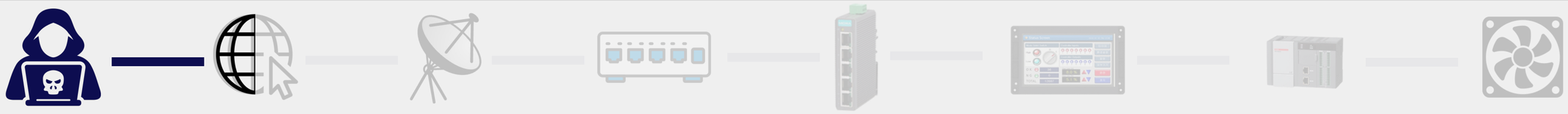
Vulnerable VSAT web interface IPs

```
cobham

192.2[redacted]
70.23[redacted]
70.232.[redacted]:443
70.232.[redacted]:443
70.232.[redacted]8
70.232.[redacted]
http://[redacted]:8882/ [sea tell]
213.234.[redacted] [sea tell]
213.234.[redacted] [sea tell]
http://8[redacted]:10000/
http://7[redacted]3:8088/c?pageId=service
http://1[redacted]15:2003/ [sea tell]
http://14[redacted]13:5910/index.lua?pageID=Tracking&langID=english[ se
http://192.[redacted]:8088/c?pageId=service [master]
http://192.[redacted] 8088/ [slave]
http://12[redacted]003/ [sea tell]
http://21[redacted] 8083/ [sea tell]
http://14[redacted]6:5910/ [sailor 500]
http://5.[redacted]003/Login.html [sea tel]
http://14[redacted]:5910/ [chinese sea tell]
https://80[redacted]/
http://212.[redacted]:4004/ [sea tell]
http://213.[redacted]8082/Login.html [sea tell]
http://213.[redacted]8083/ [sea tell]
http://102.[redacted]:2003/ [sea tell]
```



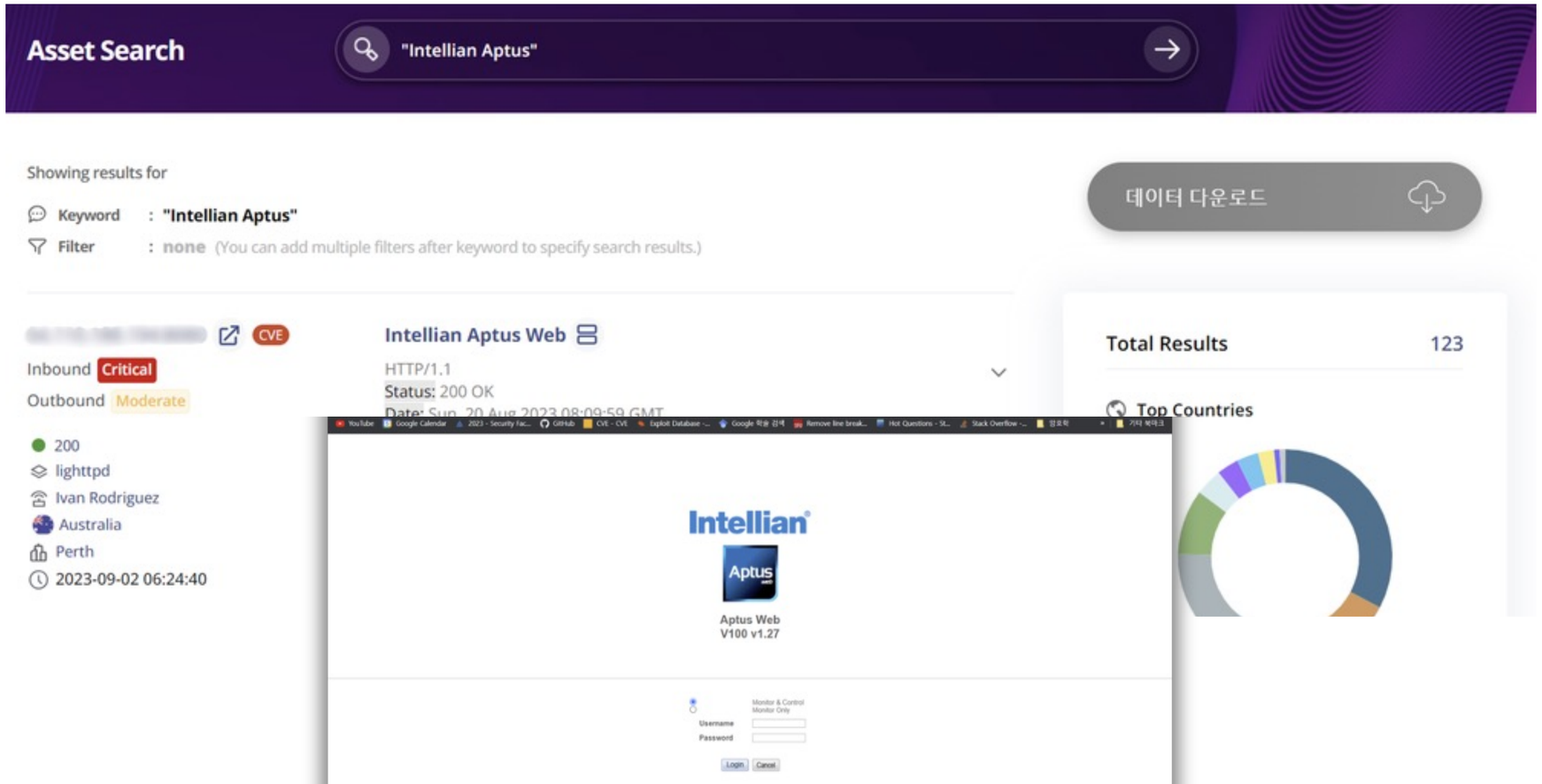
5. Maritime Testbed & Attack Chain

OSINT Exposure Status of Shipboard Equipment



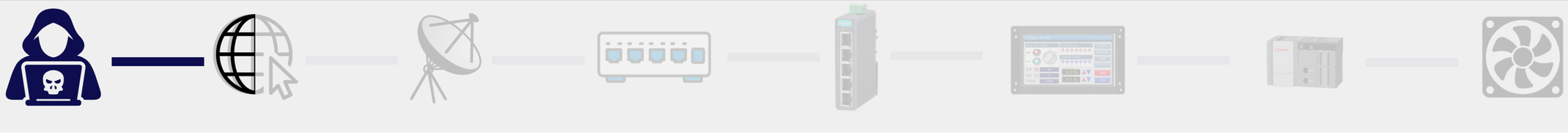
STEPS:

- **(1) OSINT threat hunting**
- (2) Infiltration through ACU web
- (3) Ship network penetration
- (4) Attack network devices
- (5) HMI intrusion
- (6) Overwriting PLC project



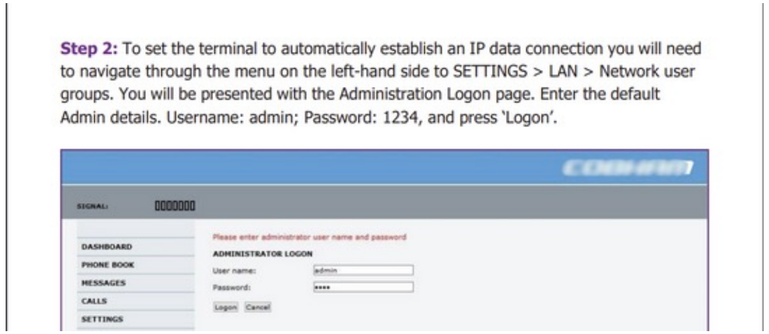
5. Maritime Testbed & Attack Chain

OSINT Exposure Status of Shipboard Equipment

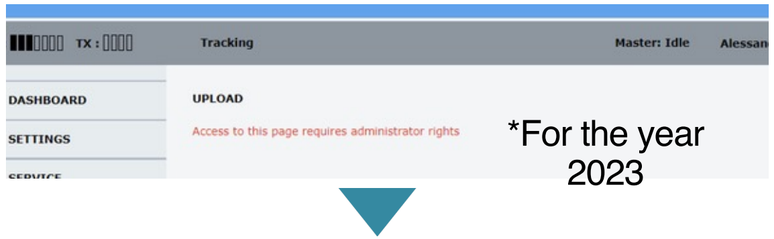


STEPS:

- **(1) OSINT threat hunting**
- **(2) Infiltration through ACU web**
- **(3) Ship network penetration**
- **(4) Attack network devices**
- **(5) HMI intrusion**
- **(6) Overwriting PLC project**



In the default account state, certain functions are hidden.



*For the year 2023

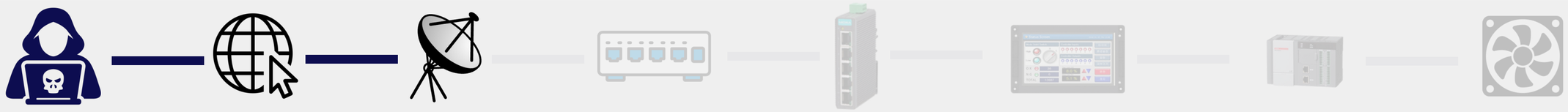


ACU Web interface

- Default administrator account information listed on the satellite equipment manual page. (admin, 1234)
- Confirmed that hidden functions become active under admin privileges.
  - Allows viewing of the satellite in use and vessel location information.
  - Network configuration functions and various communication interface details can be accessed.
  - NMEA network device settings (GPS, gyro sensor, etc.) can be modified.
  - Satellite information and configuration logs can be viewed.

5. Maritime Testbed & Attack Chain

Attack on the Ship's Satellite Antenna Control Unit (ACU)



CVE-2023-44856 – Command Injection Vulnerability in the Report Page

STEPS:

- (1) OSINT threat hunting
- (2) Infiltration through ACU web
- (3) Ship network penetration
- (4) Attack network devices
- (5) HMI intrusion
- (6) Overwriting PLC project

The sub_219C4 function does not validate the `sender` and `recipient` fields when it receives an object keyed by `cmd`

```
v16[0] = 0;
Obj_Item_cmd = cJSON_GetObjectItem(a1, "cmd");
v5 = Obj_Item_cmd;
if ( Obj_Item_cmd )
{
  Obj_Item_sender = cJSON_GetObjectString(Obj_Item_cmd, "sender", v3, v4);
  Obj_Item_recipients = cJSON_GetObjectItem(v5, "recipients");
  v8 = Obj_Item_sender == 0;
  if ( Obj_Item_sender )
    v8 = Obj_Item_recipients == 0;
  if ( v8 )
```

Expected behavior

- Malicious control of the satellite antenna
- Disabling the satellite equipment
- Tampering with GPS and gyro sensor configuration settings
- Theft and malicious modification of account credentials

Unvalidated values are inserted into a string and executed via a system call, allowing execution of any command on the system.

```
_snprintf_chk(
  v17,
  256,
  1,
  256,
  "--immediate_mode --recipients %s --sender %s",
  *(const char **)(Obj_Item_recipients + 16),
  *(const char **)(Obj_Item_sender + 16));
_snprintf_chk(
  v16,
  512,
  1,
  512,
  "%s %s %s %s",
  "/mnt/appl/bin/mail-report.sh -n rdiag -s \"Diagnostics report `hostname` `date +%Y%m%d-%H%M%S`\" -p \"ram.rdiag.status\"",
  v17,
  "-c /mnt/appl/bin/diag.sh",
  "-f `hostname`_diag_`date +%Y%m%d%H%M%S`.txt");
_strcat_chk(v16, " &", 512);
system(v16);
```

Impact

- Causing interruption of ship-to-shore communications
- Loss of the ship's location tracking functionality
- Malware injection

5. Maritime Testbed & Attack Chain

Attack on the Ship's Network device



Demonstration of penetration testing on the ship's internal network: https://youtu.be/4amgwaMx74s

Vulnerability Overview:

- A packet replay attack allows an attacker to change the administrator password without authorization. By forcibly modifying the account credentials, the attacker can exfiltrate the switch's internal configuration. This can be used as an additional attack vector or to cause abnormal behavior or complete failure of the switch.

Impact:

- If the switch's internal settings are leaked, the attacker gains critical information about devices connected to the switch and the ship's internal network, enabling further, more targeted attacks.

STEPS:

(1) OSINT threat hunting

(2) Infiltration through ACU web

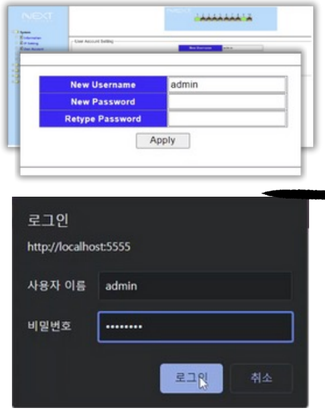
(3) Ship network penetration

(4) Attack network devices

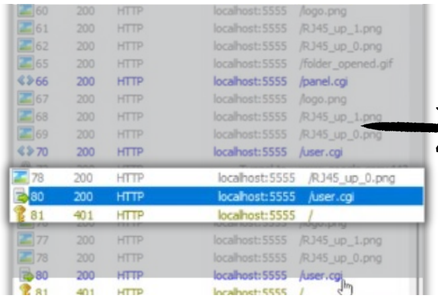
(5) HMI intrusion

(6) Overwriting PLC project

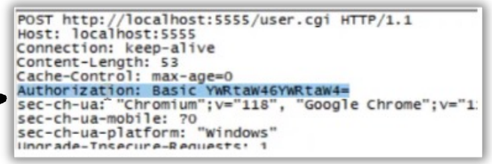
Access the management page and attempt to log in.



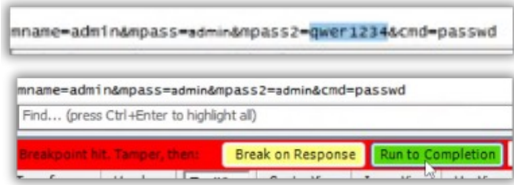
Capture the modification request's POST packet in Fiddler.



In the captured packet, modify the values of mname, mpass, and mpass2 in the packet body to the desired values, then send the packet.



The POST request does not verify authorization.



5. Maritime Testbed & Attack Chain

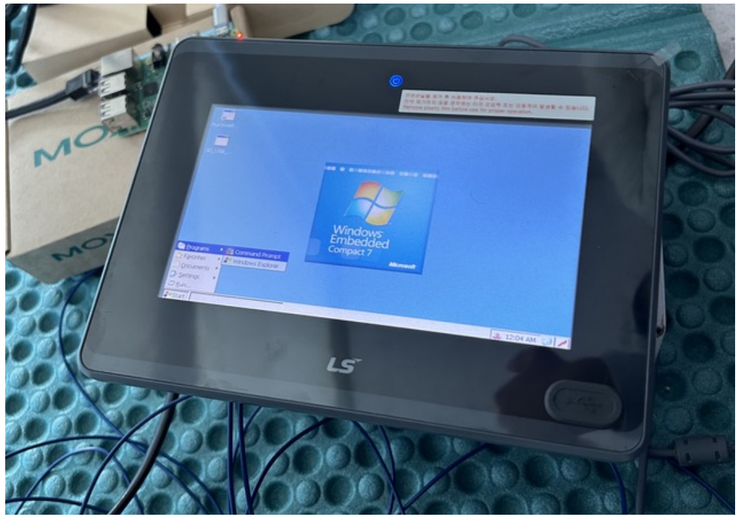
Intrusion into the ship’s HMI and forced shutdown of internal devices.



STEPS:

- **(1) OSINT threat hunting**
- **(2) Infiltration through ACU web**
- **(3) Ship network penetration**
- **(4) Attack network devices**
- **(5) HMI intrusion**
- **(6) Overwriting PLC project**

The HMI was confirmed to be based on Windows CE.
When accessed remotely via the VSAT ACU web interface, the HMI device connected beneath the MOXA industrial hub was reachable.
An attacker could remotely modify or overwrite the HMI project file.
They could also inject ransomware disguised as a PDF or similar document.
In our test, we rendered the control screen unusable by remotely overwriting the project file.





HMI Attack Demo: https://youtu.be/R8MxV70MvIw

PENTEST

DEMO

SHIPS NEED RED TEAMS, NOT JUST COMPLIANCE

The Maritime Attack Surface is MASSIVE

- Modern ships carry 400-700 various devices - impossible to audit everything, but security awareness enables priority setting
- Many still exposed through OSINT, requiring immediate action
- Single-point failures can cascade into total system compromise

Compliance != Minimum Security

- IACS UR E27 focuses on individual device hardening
- Real APTs chain vulnerabilities across multiple systems

WHY MARITIME PENETRATION TESTING WORKS

- Discovers unknown attack paths - Compliance testing misses creative exploitation chains
- Reveals realistic impact - Shows how VSAT compromise leads to navigation system takeover
- Provides actionable intelligence - Real attack scenarios > theoretical risk assessments

WHAT WE'VE PROVEN & NEXT TAKEAWAYS

Demonstrated VSAT → internal network pivot

Mapped attack flows through maritime system architectures

Built scalable testbed methodology for continued research

The Real Challenge Ahead

- We intentionally tested in simplified conditions (no firewall, single PLC, no VSAT redundancy) to prove the concept.
- The next phase requires partnership with actual shipping companies to build realistic testbeds mirroring production environments.

Call to Action

- Maritime industry: IACS UR E26/E27 is a great start - now let's add red team testing to validate those controls
- Hacker community: The ocean is calling - these systems need your skills
- Regulators: Start requiring red team assessments, not just vendor certifications

Thank you!

Slido link for Q&A



https://shorturl.at/y6Xxt