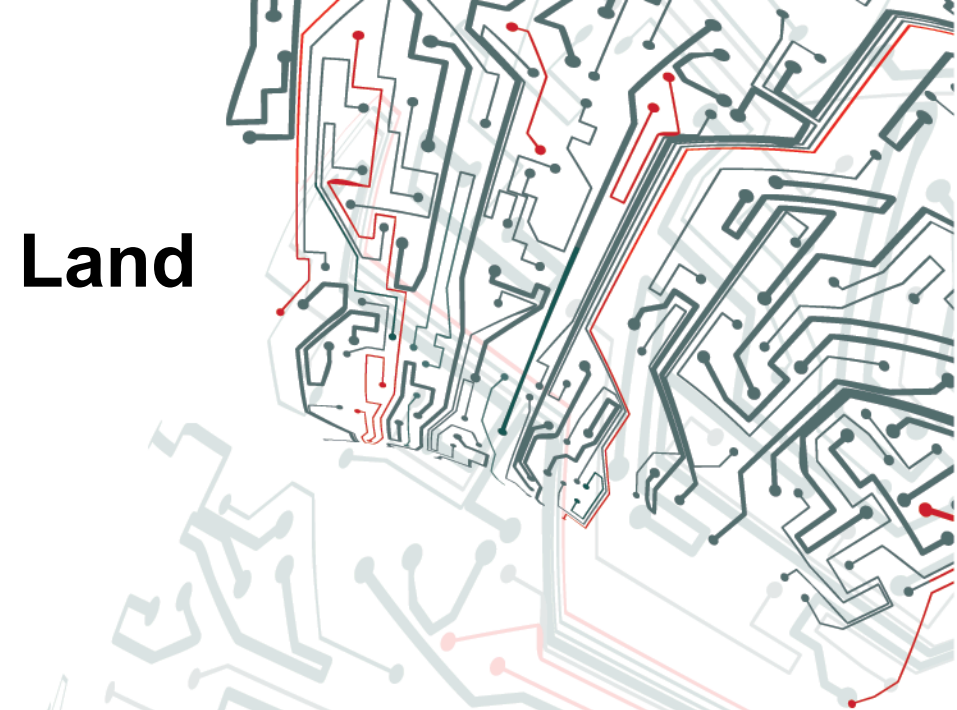
SATCOM Terminals Hacking by Air, Sea, and Land

Ruben Santamarta
Principal Security Consultant



IOActive
Hardware | Software | Wetware
SECURITY SERVICES

Agenda

- Introductions
- Methodology
- Vulnerabilities
- Demos
- Vendor responses

IOActive™

Who Am I?

- Ruben Santamarta
- IOActive Principal Security Consultant
- Reverse engineering, research, embedded, software, ICS, smart meters…
- rubens@ioactive.com

IOActive™

Satellite Communications

IOActive™

Maritime

Industrial

Military

Aerospace

Emergencies

Media

IOActive™

Space Segment

Ground Segment

+

IOActive™

Affected Vendors

IOActive

Methodology

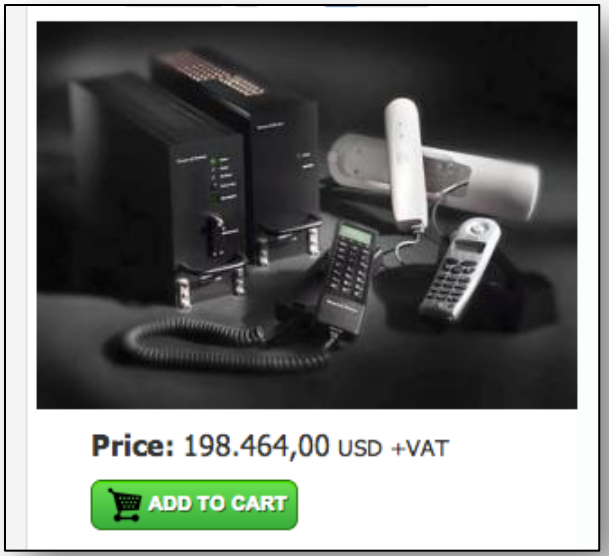
IOActive™

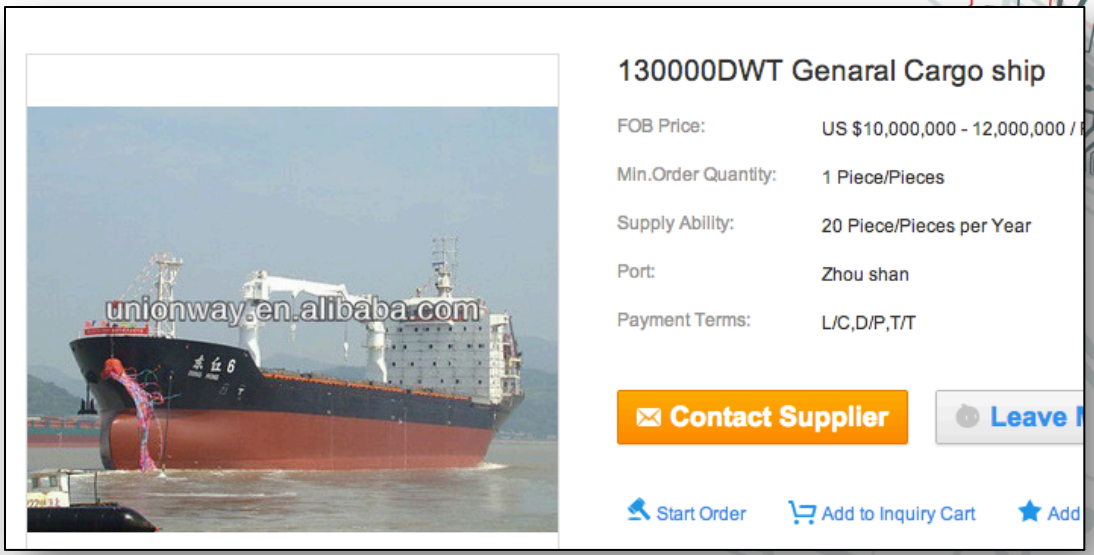
Ideal Research Environment



IOActive™

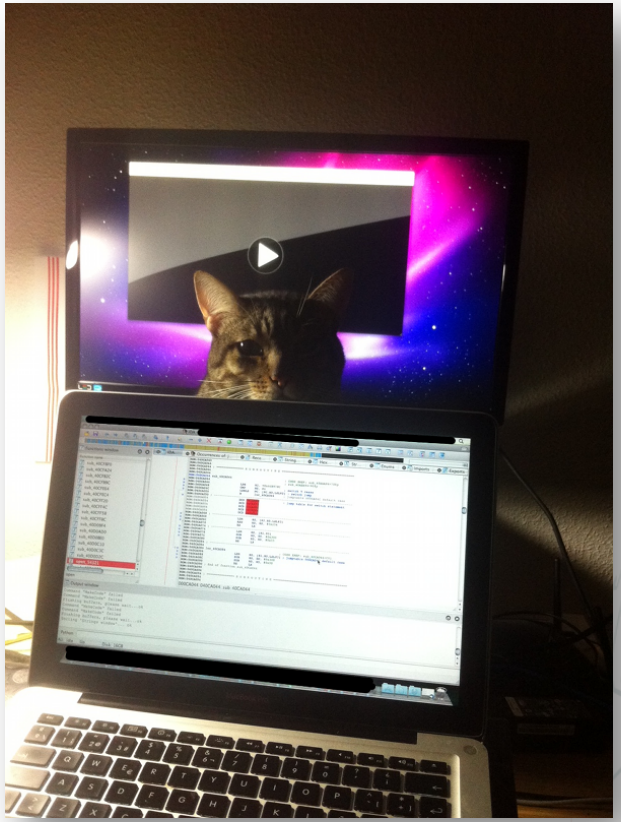
Reality





IOActive™

Actual Research Environment



IOActive™

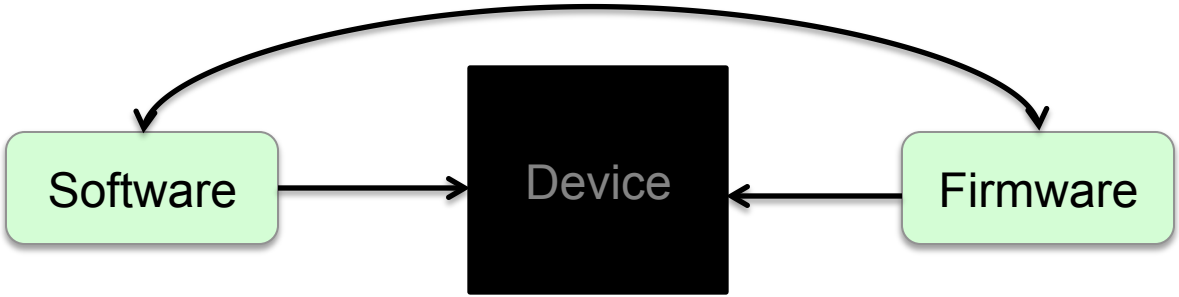
Static Analysis

- **Information gathering**
  - Datasheets
  - Multimedia material: videos, presentations, pictures …
  - Success cases
  - Manuals
  - Press releases
- **Reverse engineering**
  - Mapping features into code

IOActive™

Reverse Engineering

- Software
  - Configuration, management, upgraders, setup...
- Firmware



IOActive™

Vulnerabilities

IOActive™

It’s not a bug. It’s a feature.

- Hard-coded Credentials
- Backdoors
- Insecure Protocols
- Undocumented Protocols

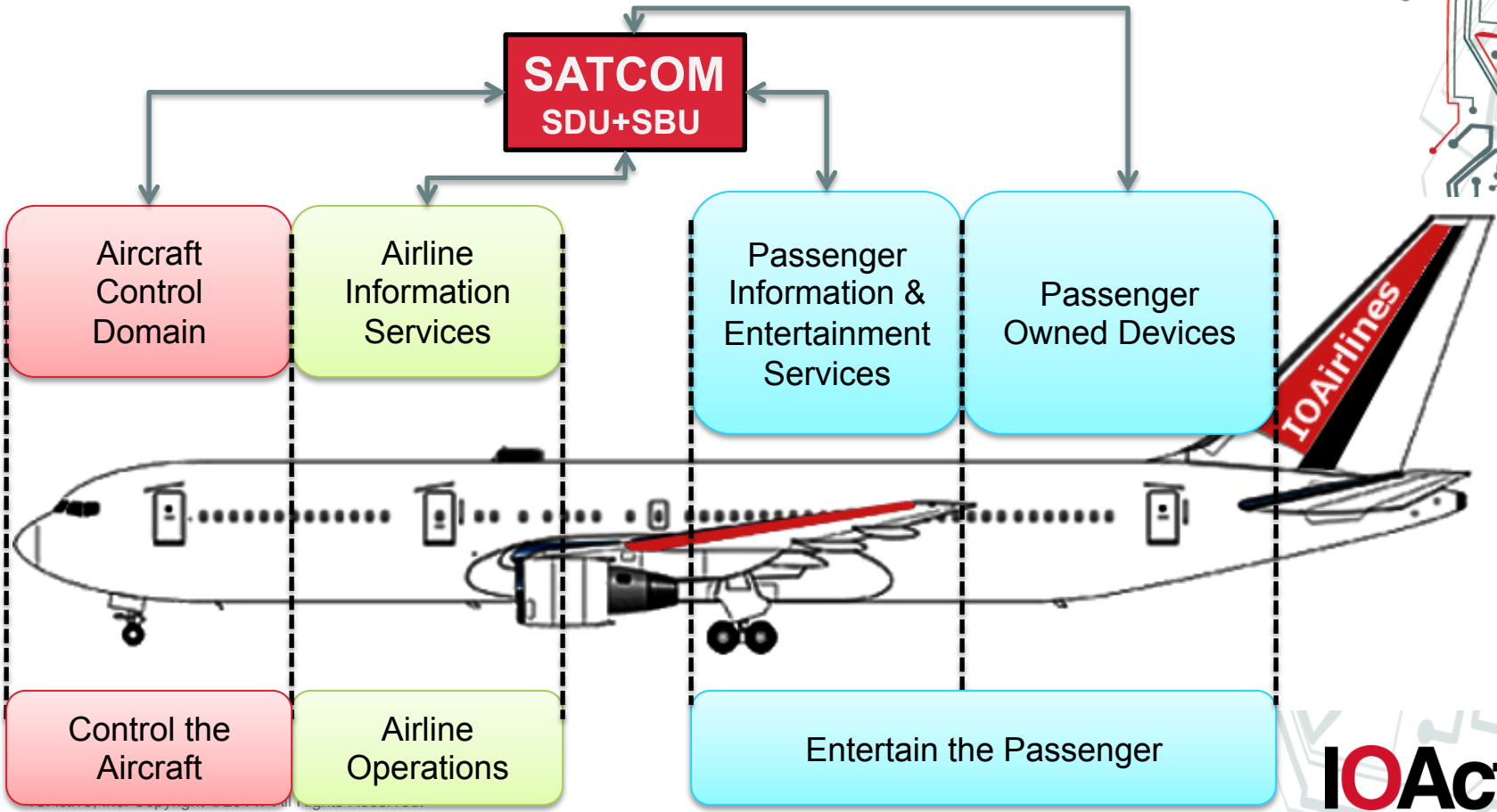
No patches

IOActive™

AIR

IOActive™

Aircraft Data Networks Domain Model



IOActive

FAA Special Conditions

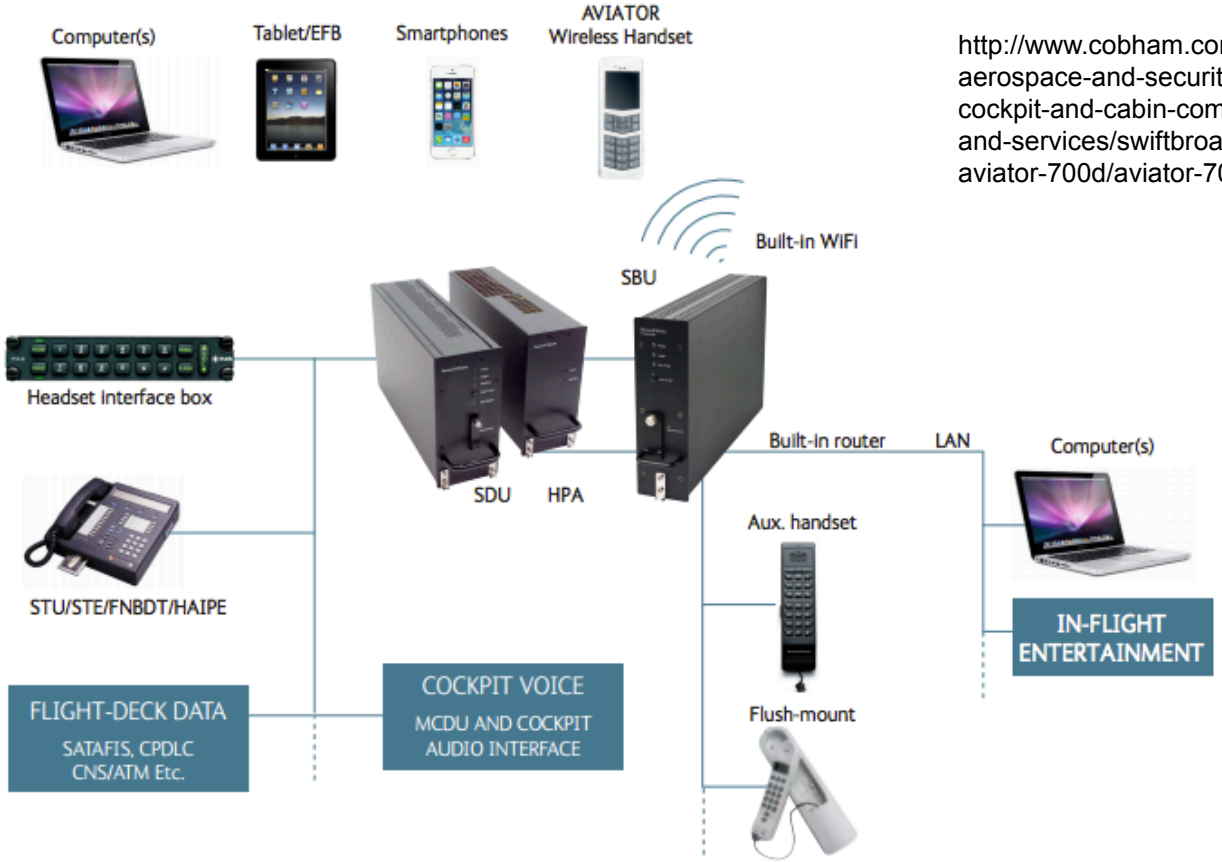
Boeing Model 787-8 Airplane; Systems and Data Networks Security—Isolation or Protection From Unauthorized Passenger Domain Systems Access

> AIRBUS Comment (b): Airbus stated that in the sentence ``The design shall prevent all inadvertent or malicious changes to, and all adverse impacts * * *'', the wording ``shall prevent ALL'' can be interpreted as a zero allowance. According to the commenter, demonstration of compliance with such a requirement during the entire life cycle of the aircraft is quite impossible because security threats evolve very rapidly. The only possible solution to such a requirement would be to physically segregate the Passenger Information and Entertainment Domain from the other domains. This would mean, for example, no shared resources like SATCOM (satellite communications), and no network connections. Airbus maintained that such a solution is not technically and operationally viable, saying that a minimum of communications is always necessary. Airbus preferred a less categorical

http://www.gpo.gov/fdsys/pkg/FR-2008-01-02/html/E7-25467.htm

IOActive™

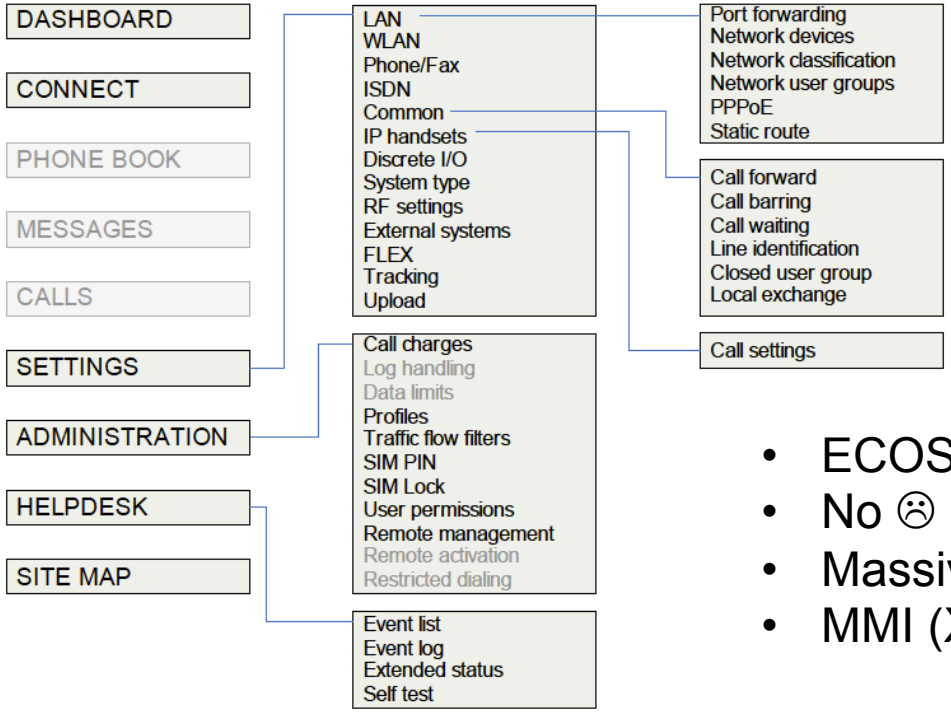
Cobham – AVIATOR 700D



http://www.cobham.com/about-cobham/aerospace-and-security/about-us/satcom/cockpit-and-cabin-communication/products-and-services/swiftbroadband-systems/aviator-700d/aviator-700d-product-sheet.aspx

IOActive™

AVIATOR Satellite SwiftBroadBand Unit (SBU)



- ECOS + T&T Layer (MIPS)
- No ☹ but many traces ☺
- Massive attack surface
- MMI (Xavante Lua Web Server)

IOActive™

Cobham – AVIATOR 700D Install Manual

Use the built-in web interface of the SBU to access the SBU configuration settings in the CM of the SBU. A subset of the configuration settings are stored in a write-protected area of the CM. This subset contains the physical settings for the antenna, cabling and other external input.

Important To setup or change the settings of the write-protected area you must connect a PC to the connector marked **Maintenance** on the SBU front plate. You can view all SBU settings from any LAN or WLAN interface.

The CM also contains the SIM card for accessing the SwiftBroadband service. The settings that can only be changed when connected to the SBU maintenance connector are:

- **Discrete I/O** settings
- **System type**
- Cable loss data in **Settings, RF settings,**
- Input from navigational systems in **Settings, External systems**
- Enabling options (Router, WLAN) in **Settings, Flex**.

IOActive™

MMI Security Clarifications

- Cobham claims it is impossible to attack the SBU through WiFi, since physical access (a maintenance port) is required.
- AVIATOR's MMI uses 'lua_is_aero_cm_write_protected as an authentication mechanism. This function verifies if the maintenance port is connected but can be easily bypassed. Also, its documentation states that any LAN/WLAN interface can access the MMI.
- AVIATOR protects part of the Flash Storage (FS) in the Configuration Module (CM). Write access is triggered through GPIO hardware when the maintenance port is connected. Firmware files are located in a separate FS.
- AVIATOR's SBU firmware checks the CM's write protection status only when updating certain settings. It does not check it when updating firmware files and other settings, such as during administrator password resets. As a result, the SBU can be attacked through WiFi.

IOActive™

MMI Security

Secure MMI by adding a disabled HTML attribute to inputs or buttons when:

- The user is not properly authenticated, or
- The functionality requires a connection to the maintenance port and the user is not connected

Firmware upload authentication:

```
-- check access permission
error_msg_2 =""
disabled_string = ''
allowed = true
if admin_status < 0 then
    allowed = msg_if.lua_get_user_permissions("upload_firmware")
    if not allowed then
        disabled_string = ' disabled '
        error_msg_2 = dict("admin_locked")
    end
end
```

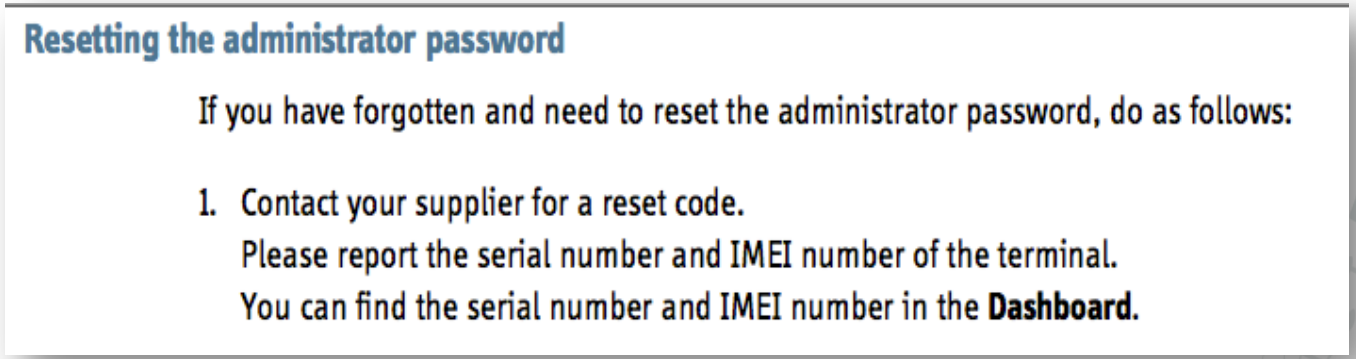
```
-- check write protection
allowed = true
if aero_if.lua_is_aero_cm_write_protected() then
    allowed = false
    disabled_string = ' disabled '
    if error_msg == "" then
        -- don't overwrite message from submit
        error_msg = dict("write protected page")
    end
```

```
put('      <th align="left"  colspan="2"><hr><p class="menutext">' .. dict("upload software to terminal")
put('    </tr><tr>\n')
put('    <td>\n')
put('      <form method="post" action="/upload_image" enctype="multipart/form-data">')
put('        <p><input ' .. disabled_string .. ' name="file" type="file"> </p></td><td><p><input ' ..
put('      </form>\n')
```


IOActive™

MMI Security

Predictable Admin Reset Code CVE-2013-7810 – SAILOR/AVIATOR/Explorer



Resetting the administrator password

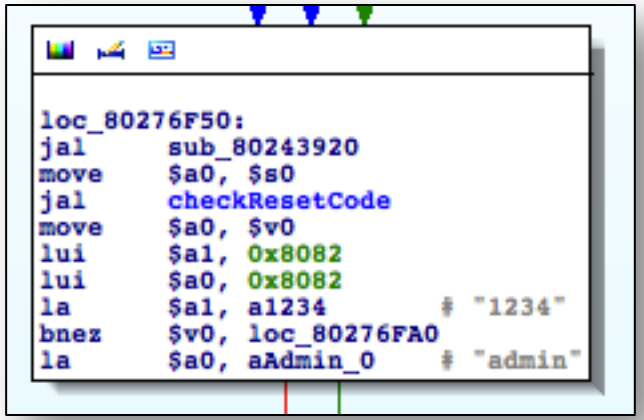
If you have forgotten and need to reset the administrator password, do as follows:

1. Contact your supplier for a reset code.
   Please report the serial number and IMEI number of the terminal.
   You can find the serial number and IMEI number in the **Dashboard**.

IOActive™

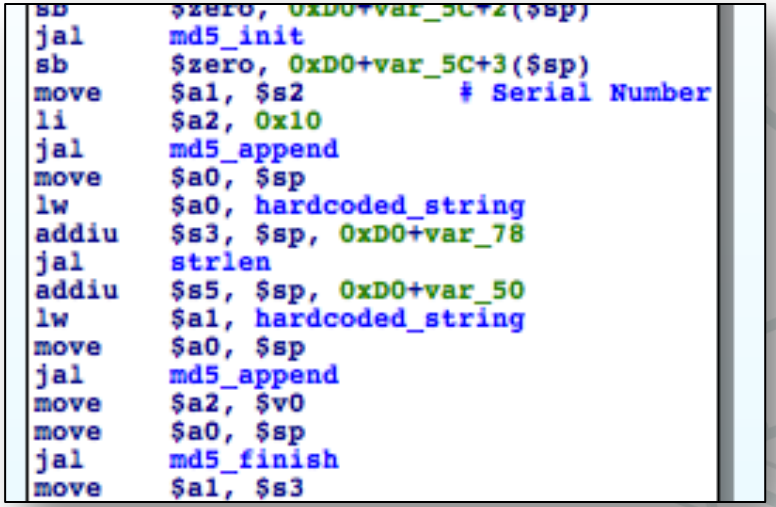
MMI Security

lua_reset_admin



```
loc_80276F50:
jal     sub_80243920
move    $a0, $s0
jal     checkResetCode
move    $a0, $v0
lui     $a1, 0x8082
lui     $a0, 0x8082
la      $a1, a1234          # "1234"
bnez    $v0, loc_80276FA0
la      $a0, aAdmin_0       # "admin"
```

CheckResetCode



```
jal     md5_init
sb      $zero, 0xD0+var_5C+3($sp)
move    $a1, $s2            # Serial Number
li      $a2, 0x10
jal     md5_append
move    $a0, $sp
lw      $a0, hardcoded_string
addiu   $s3, $sp, 0xD0+var_78
jal     strlen
addiu   $s5, $sp, 0xD0+var_50
lw      $a1, hardcoded_string
move    $a0, $sp
jal     md5_append
move    $a2, $v0
move    $a0, $sp
jal     md5_finish
move    $a1, $s3
```


IOActive™

MMI Security

- Device serial number: Hex, 16-bytes, padded with zeros
- Redacted hard-coded string: “kd04rafIOACTIVE”, 16-bytes

```
import md5
m = md5.new()
m.update("\x12\x34\x56\x78"+"\x00"*12)
m.update("kdf04rafIOACTIVE")
m.hexdigest()
```


IOActive™

Firmware Update through the SBU's MMI

```
local simplerules = {
    {match = "/upload_image",     with = upload_image,
    {match = "/reboot_terminal", with = reboot_terminal,
    {match = "/import_config",    with = import_config,
    {match = "/config.dat",       with = export_config,
    {match = "/call_log.txt",     with = export_call_log,
    {match = "/debug_info",       with = debug_info,
```

/lua/lib/xavante/config.lua

POST /upload_image process:

1. dl.init
2. dl.feed
3. dl.finish
4. dl.reboot

```
local ctx = dl.init()

repeat
    if content_len_remaining < MAX_READ_SIZE then
        read_size = content_len_remaining
    else
        read_size = MAX_READ_SIZE
    end

    data, err = req.socket:receive (read_size)
    if err then
        trace(0, 1, string.format("socket:receive error %s", err))
        break
    end

    if not data then
        err = "ran out of data"
        break
    end

    len = len + string.len(data)
    err = dl.feed(ctx, data)
    content_len_remaining = content_len_remaining - read_size
until content_len_remaining == 0 or err
trace(0, 1, string.format("uploaded %d bytes", len))

err = dl.finish(ctx, err)
```

/lua/lib/upload_image.lua

IOActive™

Firmware Update Implementation

```
.word aInit_14          # DATA XREF: init_lua_library+101c
                        # "init"
.word dl_init
.word aFeed             # "feed"
.word dl_feed
.word aFinish           # "finish"
.word dl_finish
.word aReboot           # "reboot"
.word dl_reboot
.byte    0
```

```
186   0x5f06311e ./lua/bin/xavante-start.lua
187   0x4a27c422 ./lua/bin/compat-5.1.lua
188   0x2d85b23c ./eq_fpga.img
189   0x0a7e7c1c ./MAIN_CPU
190   0x7527e7f7 ./I2C_AVR.hex
191   0x97f6becb ./tt305xd-hpa.dl
192   0xc833b436 ./welcome_msg.amb
```

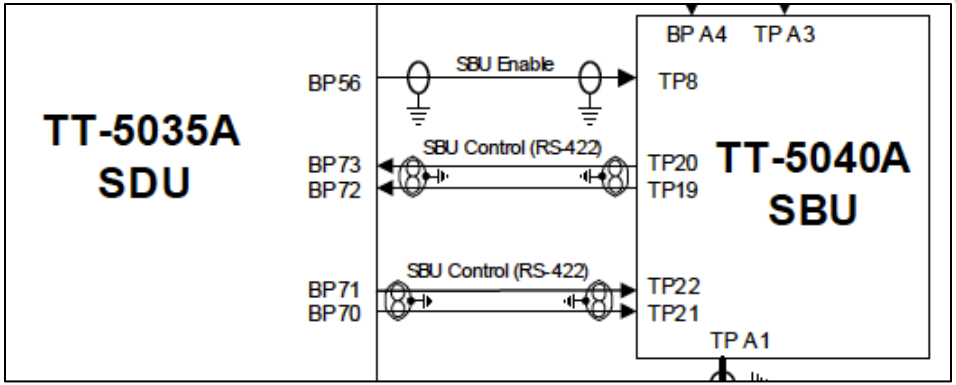
manifest

1. dl_init initializes the /dl directory to hold the files.
2. dl_feed writes and handles the firmware TAR file received in the POST request. The TAR file contains a manifest file in the format “0xchecksum filepath”.
3. dl_finish verifies checksums for the MAIN_CPU file, which contains the SBU firmware, and verifies the MAIN_CPU file is for the right platform. If everything is ok, the current version is moved to MAIN_CPU.old and the new one is copied to /MAIN_CPU.
4. dl_reboot reboots the terminal to complete the operation.

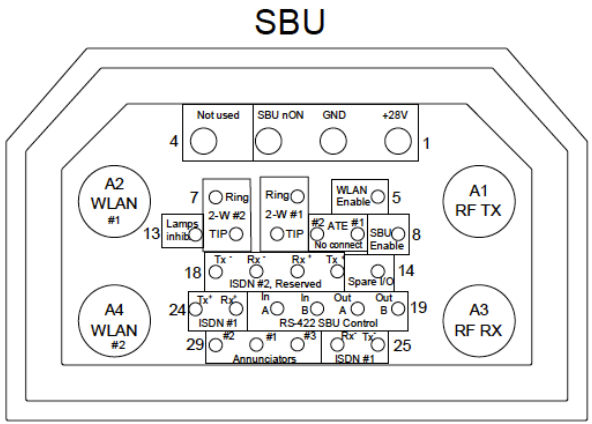
IOActive™

Exploring Attack Vectors

Physical Connection SBU-SDU



SDU pin	SBU pin	Description with reference to SDU
BP56	TP8	SBU Enable
BP73	TP20	Data bus input from SBU; Input A, RS422
BP72	TP19	Data bus input from SBU; Input B, RS422
BP71	TP22	Data bus output to SBU; Output A, RS422
BP70	TP21	Data bus output to SBU; Output B, RS422



ARINC-404a

IOActive™

LLH Protocol

Internal Communication between Boards/Threads(Message Queues)

- Dozens of OpCodes
- Boards: HSU, H+, SBU, HPA, HSD
- SDU <-> HSU, H+, SBU, HPA, HSD
- SBU <-> SDU
  - OPLLH_SBU_SATELLITE_LOGOFF_RSP
  - OPLLH_SBU_SATELLITE_LOGOFF_IND
  - OPLLH_SBU_SATELLITE_REPORT
  - OPLLH_SBU_START_REJ
  - OPLLH_SBU_START_ACK
  - OPLLH_SBU_POWER_REQ (EIRP Allocation)
  - OPLLH_SBU_START_REQ
  - OPLLH_SBU_READ_POWER_LEVEL
  - OPLLH_SBU_START_CAL
  - OPLLH_SBU_POWER_MEASUREMENT

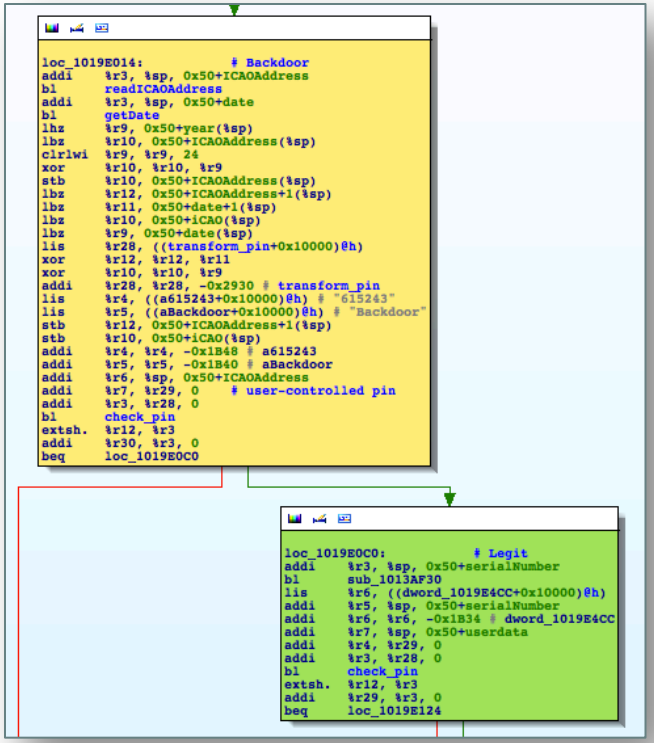
IOActive

AVIATOR 700D – SDU Backdoor

- PowerPC. No symbols. Quite a few traces. ☺
- The SDU can be configured through the MCDU or a full-feature handset.
- Some functions are restricted, so a PIN is required.
- According to the documentation, three levels exist:
  - Normal user
  - Super user
  - Service provider
- According to the firmware, a backdoor exists.

IOActive™

AVIATOR 700D – SDU Backdoor



```
loc_1019E014:           # Backdoor
addi    %r3, %sp, 0x50+ICAOAddress
bl      readICAOAddress
addi    %r3, %sp, 0x50+date
bl      getDate
lhz     %r9, 0x50+year(%sp)
lbz     %r10, 0x50+ICAOAddress(%sp)
clrlwi  %r9, %r9, 24
xor     %r10, %r10, %r9
stb     %r10, 0x50+ICAOAddress(%sp)
lbz     %r12, 0x50+ICAOAddress+1(%sp)
lbz     %r11, 0x50+date+1(%sp)
lbz     %r10, 0x50+iCAO(%sp)
lbz     %r9, 0x50+date(%sp)
lis     %r28, ((transform_pin+0x10000)@h)
xor     %r12, %r12, %r11
xor     %r10, %r10, %r9
addi    %r28, %r28, -0x2930 # transform_pin
lis     %r4, ((a615243+0x10000)@h) # "615243"
lis     %r5, ((aBackdoor+0x10000)@h) # "Backdoor"
stb     %r12, 0x50+ICAOAddress+1(%sp)
stb     %r10, 0x50+iCAO(%sp)
addi    %r4, %r4, -0x1B48 # a615243
addi    %r5, %r5, -0x1B40 # aBackdoor
addi    %r6, %sp, 0x50+ICAOAddress
addi    %r7, %r29, 0    # user-controlled pin
addi    %r3, %r28, 0
bl      check_pin
extsh.  %r12, %r3
addi    %r30, %r3, 0
beq     loc_1019E0C0
```

```
loc_1019E0C0:           # Legit
addi    %r3, %sp, 0x50+serialNumber
bl      sub_1013AF30
lis     %r6, ((dword_1019E4CC+0x10000)@h)
addi    %r5, %sp, 0x50+serialNumber
addi    %r6, %r6, -0x1B34 # dword_1019E4CC
addi    %r7, %sp, 0x50+userdata
addi    %r4, %r29, 0
addi    %r3, %r28, 0
bl      check_pin
extsh.  %r12, %r3
addi    %r29, %r3, 0
beq     loc_1019E124
```

- Backdoor Authentication
- Legit Authentication

IOActive™

Backdoor Generation

Legitimate authentication:

- Each PIN is locally stored after it is “transformed” through a series of logical operations. The transformation process uses the SDU’s serial number to obtain different values for a single PIN, and a fixed 24-bit value.
- When a user enters a PIN, it goes through the same algorithm. It then goes through a comparison.

IOActive™

Backdoor Generation

Backdoor authentication:

- For backdoor authentication, an opposite approach is used:
  - The PIN is always “615243”.
  - The serial number is “Backdoor”.
- To prevent backdoor PIN reuse, these values are used:
  - ICAO 24-bit address. Each registered aircraft has a different address.
  - Current date (year-month-day). The hard-coded PIN is transformed using this algorithm and then compared against the PIN the user entered.

IOActive™

SEA

IOActive™

ThraneLINK Insecure Protocol CVE-2013-0328

"ThraneLINK is a sophisticated communication protocol that connects the SAILOR products in a network, offering important new opportunities to vessels. It provides facility for remote diagnostics and enables access to all the SAILOR products from a single point for service. This results in optimized maintenance and lower cost of ownership because less time is needed for troubleshooting and service. Installation is made easier as ThraneLINK automatically identifies new products in the system. The uniform protocol is an open standard which provides a future proof solution for all vessels " - Cobham

IOActive™

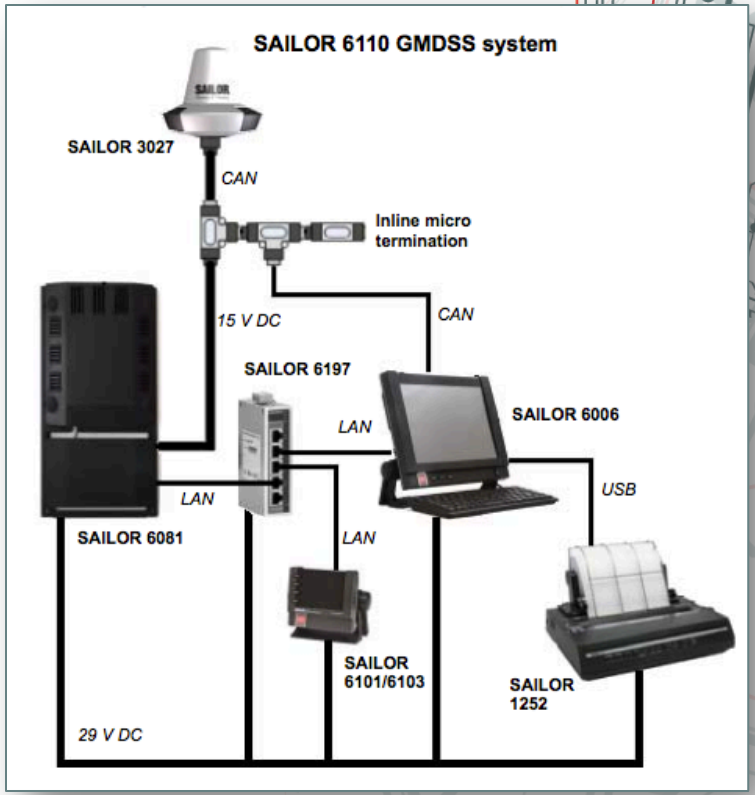
ThraneLink

- Discovery (SLP)

S	.rdata:005…	0000000E	C	device-vendor
S	.rdata:005…	0000000D	C	device-model
S	.rdata:005…	00000011	C	device-serial-no
S	.rdata:005…	00000012	C	device-sw-version
S	.rdata:005…	0000000F	C	device-product
S	.rdata:005…	00000010	C	device-sw-build
S	.rdata:005…	0000000D	C	device-alias

- Management (SNMP)
  1. System configuration
  2. Software download
  3. Diagnostics report
  4. Logging

thrane_tt3739_all_SMIv2_v1.mib
thrane_tt3748_all_SMIv2_v1.mib
thrane_tt3771_all_SMIv2_v1.mib
thrane_tt6004_all_SMIv2_v1.mib
thrane_tt6004a_all_SMIv2_v1.mib
thrane_tt6006_all_SMIv2_v1.mib
thrane_tt6006_c_all_SMIv2_v1.mib
thrane_tt6006_r_all_SMIv2_v1.mib
thrane_tt6081_all_SMIv2_v1.mib
thrane_tt6101_all_SMIv2_v1.mib
thrane_tt6103_all_SMIv2_v1.mib



IOActive

ThraneLINK – Spoof devices

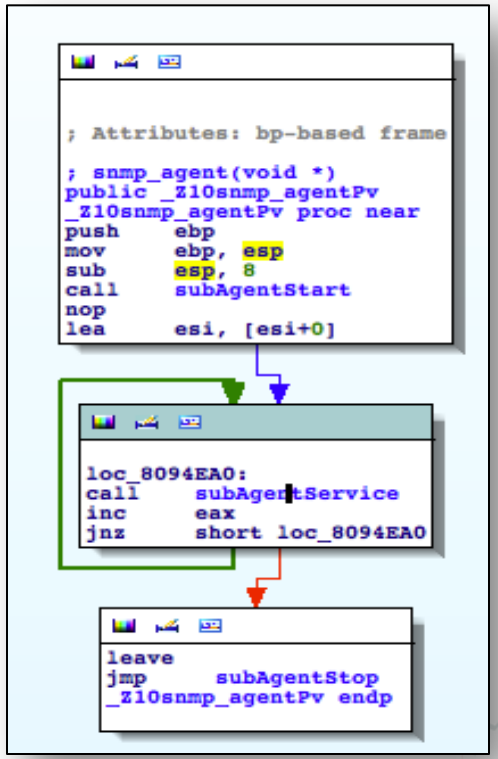
```
---6006_C.reg---
service:device.thrane://192.168.1.7,en,65535
device-vendor=Thrane & Thrane
device-model=6006_C
device-serial-no=123467890
device-sw-version=1.00
device-product=SAILOR 6006 Message Terminal
Inmarsat-C
device-sw-build=666
---6006_C.reg----
$ slpd -r 6006_C.reg
```


IOActive™

ThraneLINK - SNMP

SubAgent Schema

```
; Attributes: bp-based frame

; start_snmp_agent(void)
_ZL16start_snmp_agentv proc near
push    ebp
mov     ebp, esp
sub     esp, 10h
push    0                   ; char
push    0                   ; int
push    offset _Z10snmp_agentPv ; int
push    0                   ; stacksize
push    0                   ; int
push    offset aSnmpAgentx ; "snmp/agentX"
call    tt_task_create
xor     eax, eax
leave
retn
_ZL16start_snmp_agentv endp
```



IOActive™

ThraneLink Software Download

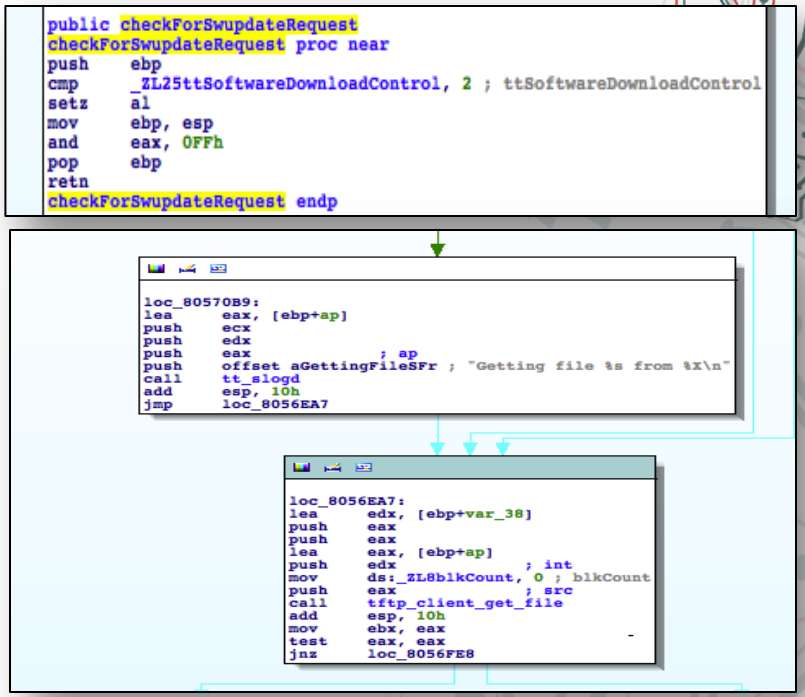
oid_ttSoftwareDownloadProtocol	oid_ttSoftwareDownloadControl
oid_ttSoftwareDownloadIpAddress	oid_ttSoftwareDownloadStatus
oid_ttSoftwareDownloadPortNumber	oid_ttSoftwareDownloadErrorDescription
oid_ttSoftwareDownloadFileName	oid_ttSoftwareDownloadProgress

```
loc_8056270:
push    eax
push    0Bh
push    offset _ZL31oid_ttSoftwareDownloadIpAddress ; oid_ttSoftwareDownloadIpAddress
push    0
push    offset write_ttSoftwareDownloadIpAddress
push    offset read_ttSoftwareDownloadIpAddress
push    5
push    offset aTtsoftwaredo_0 ; "ttSoftwareDownloadIpAddress"
call    ttSnmpScalarCreate
add     esp, 20h
test    eax, eax
jz      short loc_80562A0
```


IOActive™

ThraneLink Firmware Update

1. Create malicious firmware.
2. Set up a TFTP server.
3. Send SLP requests to discover a device.
3. Send SNMP requests to:
    - Set the TFTP server IP
    - Set the file name
    - Set the DownloadControl variable
4. Have fun. ☺



IOActive™

TIIF – Cobham's SAILOR Firmware File Format

- MAGIC
- STREAM 0
- …
- STREAM n

```
0000000  46 49 49 54 54 49 49 46 80 6D 70 AC 01 00 10 00 80 CD 01 05 4F 25 09 F4  FIITTIIF.mp.........O%..
0000018  03 FE 03 65 01 00 4C 00 18 00 00 00 74 74 3A 52 65 6C 65 61 73 65 48 65  ...e..L.....tt:ReleaseHe
0000030  61 64 65 00 93 A9 2A 9C 01 05 03 00 D8 62 B0 52 74 74 36 30 30 36 63 2D  ade...*......b.Rtt6006c-
0000048  33 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  3.......................
0000060  00 00 00 00 70 72 6F 64 75 63 74 73 3D 36 30 30 36 2C 36 30 30 36 5F 43  ....products=6006,6006_C
0000078  0A 00 00 00 05 4A 20 4C 04 00 40 00 00 EC 57 04 72 6F 6F 74 2E 63 70 69  .....J L..@...W.root.cpi
0000090  6F 00 00 00 00 00 00 00 91 31 06 43 01 1B 00 00 30 32 37 00 00 00 00 00  o........1.C....027.....
00000A8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 30 37 30 37  ....................0707
```

Hdr CRC	ClassID: 1	Hdr Size	Body Size	Name	
	Body CRC	Version	Timestamp	ID	Data

Hdr CRC	ClassID: 4	Hdr Size	Body Size	Name
	Body CRC	Version	ID	Data

IOActive™

Demo

SAILOR 6006

Two ways to update firmware:

- Physical: USB
- Remote: ThraneLink

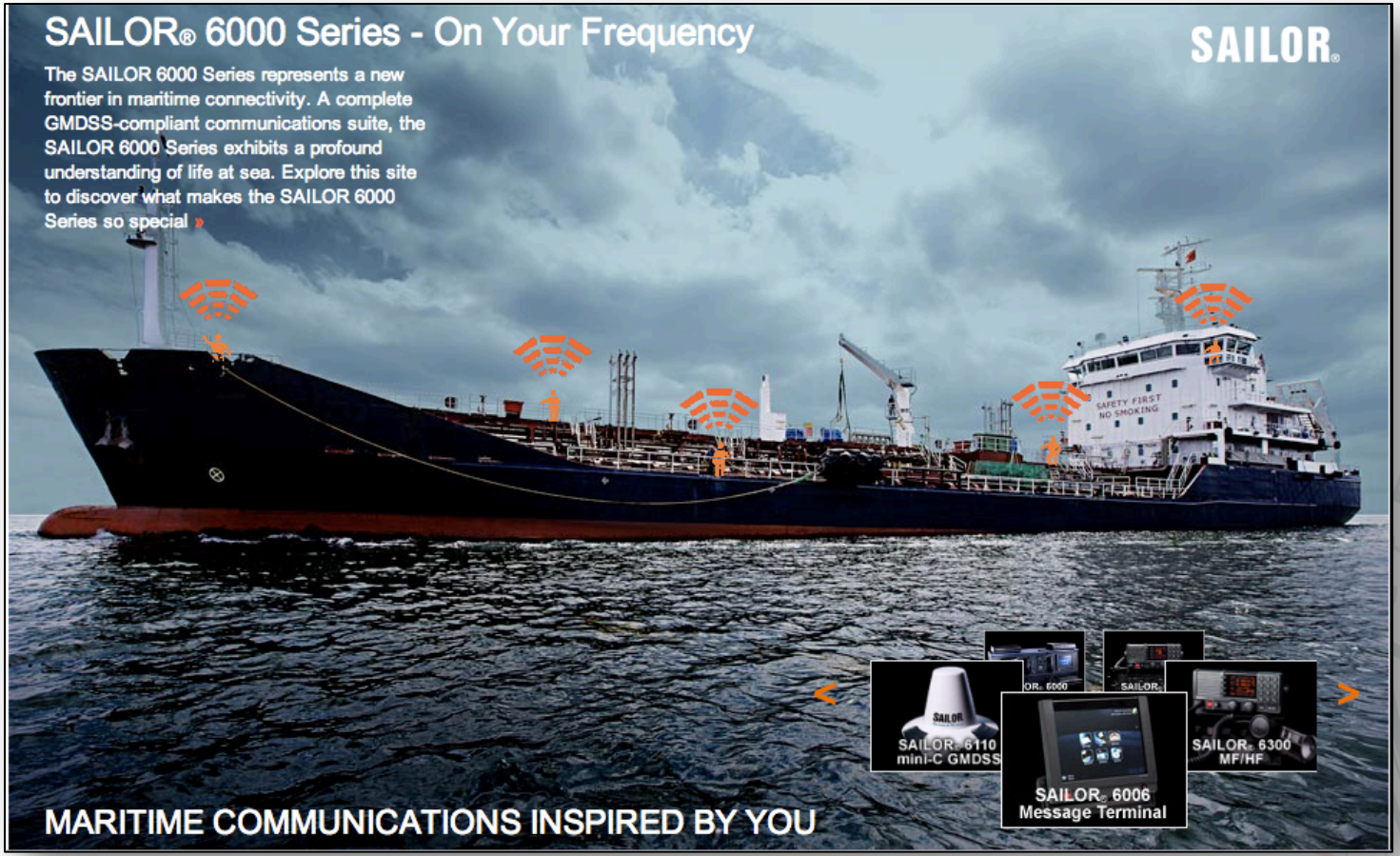
Winner

Three firmware streams:

- root.cpio
- var.cpio
- app.tar.gz

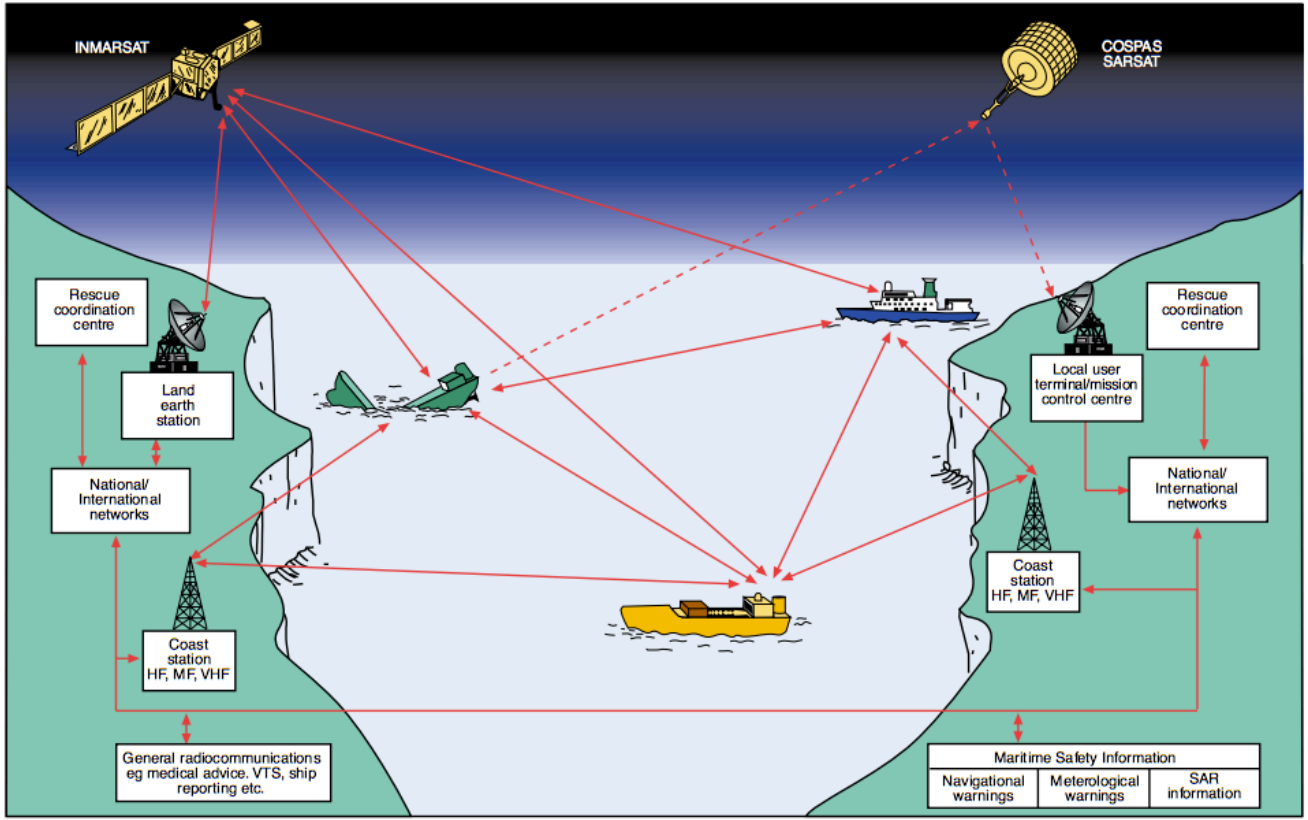
IOActive™

Demo



IOActive™

Global Maritime Distress and Safety System



http://www.amsa.gov.au/forms-and-publications/publications/gmdss-handbook-2013.pdf

IOActive™

Demo

Cobham SAILOR GMDSS Console

Operational Requirements of Integrated Radio Communication System (A.811/2.4)

The IRCS shall:

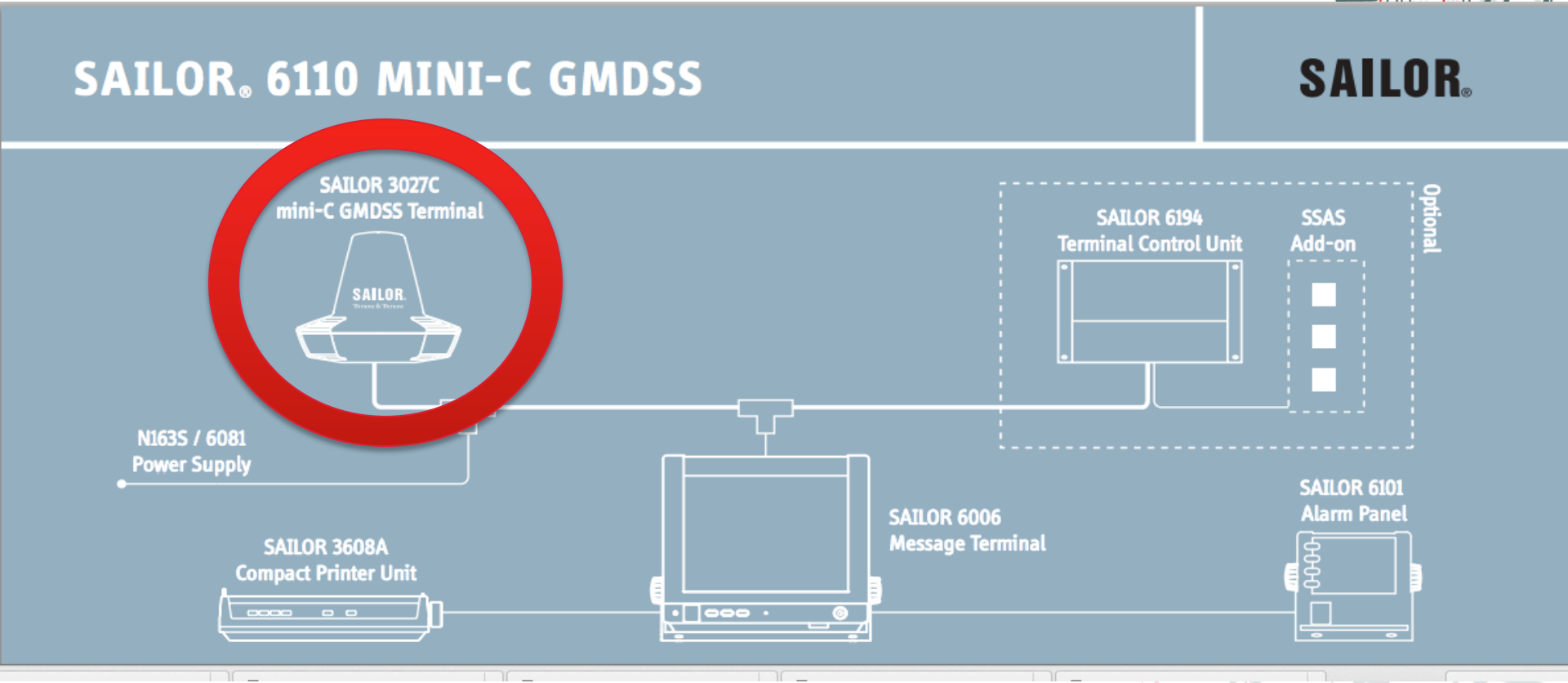
1. Comprise at least two GMDSS workstations each connected to each GMDSS radio-communication sensor over a network or connecting system…

6. Be protected against the effects of computer viruses. (November 1995)

http://www.imo.org/blast/blastDataHelper.asp?data_id=23894&filename=811(19).pdf

IOActive™

SAILOR Mini-C Backdoor - CVE-2014-2941



IOActive™

SAILOR Mini-C Backdoor - CVE-2014-2941

When the transceiver receives a data message of less than 2 kbytes it is checked whether this message has the format of a TBus 2 message. A TBus 2 message is not stored on the transceiver as a normal message; instead the transceiver handles the commands in the message.

The commands are handled in the order they are placed in the message. After successfully completing a command the next command is handled until all commands are handled or the handling of a command fails. The transceiver aborts the handling of the command sequence if one command fails.

As with the shell interface not all commands are allowed for all users there is 4 authority levels: Normal, super, sysadm and distb. On the remote TBus 2 interface all commands except for one needs at least super authority. Only the commands, which set the authority, can be handled at normal authority. The transceiver always handles the first command within a new command sequence received on the remote TBus 2 interface, with normal authority. Which means that the first command always has to be the 'set authority' command. The password for a given authority level is the same as in the shell interface. It is not possible to use a default password on the remote interface, the password has to be changed for a given authority level before it is possible to use that authority level for the remote TBus 2 interface.

http://www.gmpcs-us.com/multimedia/gmpcs/pdfs/GMPCS%20-%20SAILOR%206110%20Mini%20-%20C%20GMDSS%20Terminal.pdf

IOActive

Actually, There are Six Levels…

maincpu-omap_minic.linux-gnu-gcc.arm.elf'

```
.rodata:00109CF0 ; UserTab
.rodata:00109CF0 _ZL7UserTab     DCD aNormal_0          ; DATA XREF: GetCurrentUser(void)+4↓o
.rodata:00109CF0                                        ; .text:off_A6FA8↓o ...
.rodata:00109CF0                                        ; "normal"
.rodata:00109CF4                 DCD 0
.rodata:00109CF8                 DCD aSuper             ; "super"
.rodata:00109CFC                 DCD 0
.rodata:00109D00                 DCD aSysadm            ; "sysadm"
.rodata:00109D04                 DCD 0
.rodata:00109D08                 DCD aDistb             ; "distb"
.rodata:00109D0C                 DCD 0
.rodata:00109D10                 DCD aProd              ; "prod"
.rodata:00109D14                 DCD 1
.rodata:00109D18                 DCD aDevl              ; "devl"
.rodata:00109D1C                 DCD 1
```

Documented

- normal
- super
- sysadm
- distb

Undocumented

- prod:joakim
- dev1:caribien32

Configuration:
RestoreFacDefPswData(TPswData *)

```
BL      memcpy
LDR     R0, [R4]
MOV     R5, #5
ADD     R0, R0, #0x2240
MOV     R2, R5          ; n
LDR     R1, =aProd      ; "prod"
ADD     R0, R0, #0x39   ; dest
BL      memcpy
LDR     R0, [R4]
MOV     R2, R7          ; n
ADD     R0, R0, #0x2280
LDR     R1, =aJoakim    ; "joakim"
ADD     R0, R0, #2      ; dest
BL      memcpy
LDR     R0, [R4]
MOV     R2, R5          ; n
ADD     R0, R0, #0x2280
LDR     R1, =aDevl      ; "devl"
ADD     R0, R0, #0x12   ; dest
BL      memcpy
LDR     R0, [R4]
LDR     R1, =aCaribien32 ; "caribien32"
ADD     R0, R0, #0x2280
ADD     R0, R0, #0x1B
MOV     R2, #0xB
ADD     SP, SP, #4
LDMFD   SP!, {R4-R7,LR}
B       memcpy
; End of function Configuration::RestoreFacDefPswData(TPswData *)
```


IOActive™

Thrane &Thrane Over-the-Air Command (T&T OTAC)

Detect OTAC Message

“,\TTOTAC\”

```
; DecodeRemoteConfigCmd(unsigned char *, unsigned short)
EXPORT _Z21DecodeRemoteConfigCmdPht
_Z21DecodeRemoteConfigCmdPht

var_sE=  0xE

STMFD   SP!, {R4-R7,LR}
SUB     SP, SP, #0x14
ADD     R7, SP, #2
LDR     R6, =AppTrGroup
MOV     R2, #0xA        ; n
MOV     R4, R0
MOV     R5, R1
MOV     R0, R7          ; dest
LDR     R1, =aITtotac   ; ",\\TTOTAC\\"
BL      memcpy
LDR     R2, [R6]
LDR     R3, [R2]
CMP     R3, #0
BEQ     loc_6818C
```

OTACParse_LESID(uchar **,LESstruct *)	.text	00067408	00000134
OTACParse_ItemEndTag(uchar **)	.text	00067550	000000C4
OTACParse_LESList(uchar **,LESstruct *,uchar *)	.text	00067624	00000104
OTACParse_UserID(uchar **,uchar *)	.text	00067738	000000C8
OTACParse_LESLock(uchar **,LESstruct *,uchar *)	.text	00067810	000001BC
OTACParse_String(uchar **,char *,int)	.text	000679E0	000001E4
OTACParse_Password(uchar **,char *,int)	.text	00067BE4	000000D4
OTACParse_Cmd(uchar **,uchar *)	.text	00067CC8	00000454
DecodeRemoteConfigCmd(uchar *,ushort)	.text	00068148	000001B8

IOActive™

T&T OTAC Authentication

1.Documented accounts:

- Check passwords in clear text

```
; CheckPasswordForAuthorityLevel(unsigned char, char *)
EXPORT _Z30CheckPasswordForAuthorityLevelhPc
_Z30CheckPasswordForAuthorityLevelhPc

var_16C= -0x16C
var_70= -0x70

STMFD   SP!, {R4-R8,R10,LR}
SUB     SP, SP, #0x154
ADD     R5, SP, #0x170+var_16C
SUB     R5, R5, #1
MOV     R6, R0
MOV     R0, R5
MOV     R7, R1
BL      _Z12ReadPassWordP8TPswData ; ReadPassWord(TPswData *)
LDR     R3, =_ZL7UserTab ; UserTab
MOV     R10, R6,LSL#3
LDRB    R2, [R3,#4]
CMP     R2, #0
```

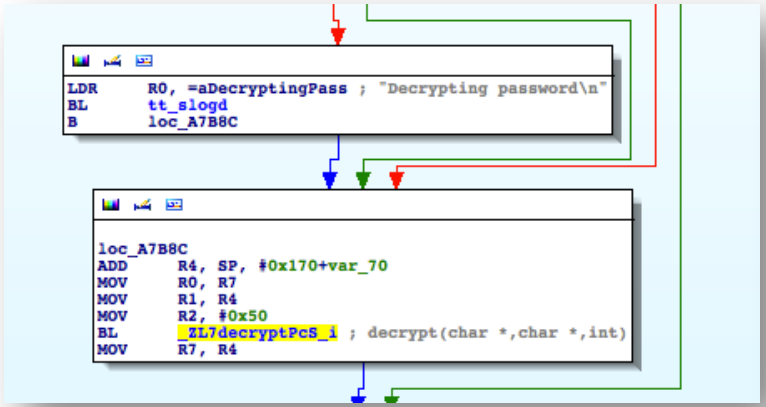
```
loc_A7BA4
MOV     R1, R6,LSL#5
RSB     R1, R10, R1
ADD     R1, R1, R6
ADD     R1, R5, R1
MOV     R0, R7          ; s1
ADD     R1, R1, #9      ; s2
BL      strcmp
```

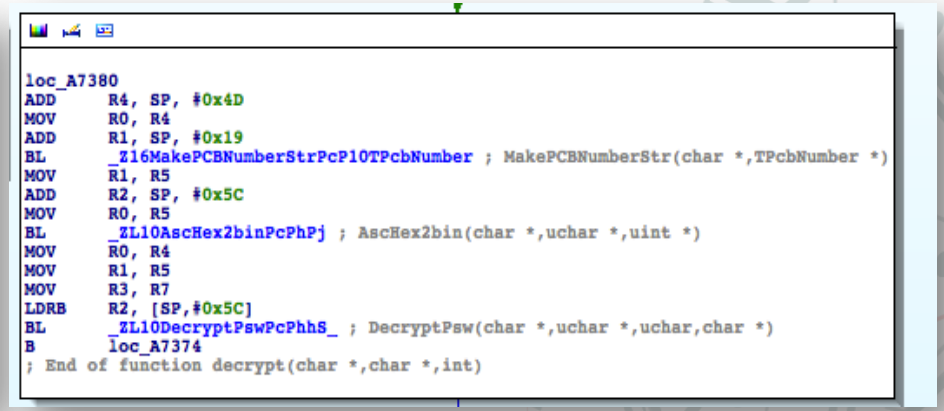

IOActive™

T&T OTAC Authentication

2. Undocumented accounts:

- Use a hard-coded password that is encrypted
- Encryption/decryption routines are based on the terminal's PCB number, which is unique per terminal.





IOActive™

OTA Commands

- 48 commands exist.
- Each command belongs to one of 46 Shell command categories, including Setup, SSAS, Tx/Rx, EGC, and Distress/Alerts.
- Each Shell command category needs an authorization level (four documented and two undocumented).
- Undocumented accounts have the highest privileges.
- Some commands require a privilege level that is only granted by undocumented accounts.

IOActive™

Attacking Inmarsat-C

- ThraneLINK remote firmware upgrade
- Repurpose binaries to generate malformed frames

IOActive™

LAND

IOActive™

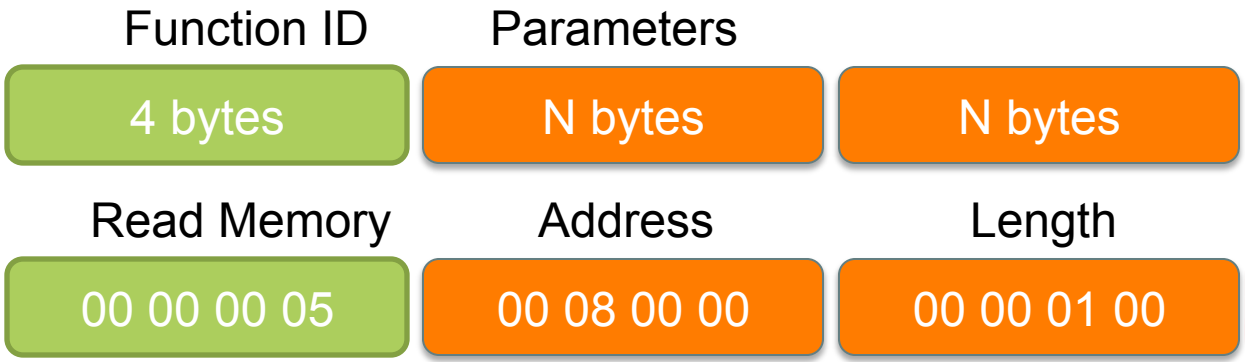
Inmarsat BGAN Terminals - Hughes

- VxWorks
- USB, Ethernet, WiFi…
- BGAN Stack
  - GateHouse: www.gatehouse.dk
- Hughes firmware
  - Deployed with symbols
  - CRC
  - Updated through FTP
  - Debug, test, in-house functionalities
- Different vendors
  - Harris
  - JRC FB
  - …

IOActive™

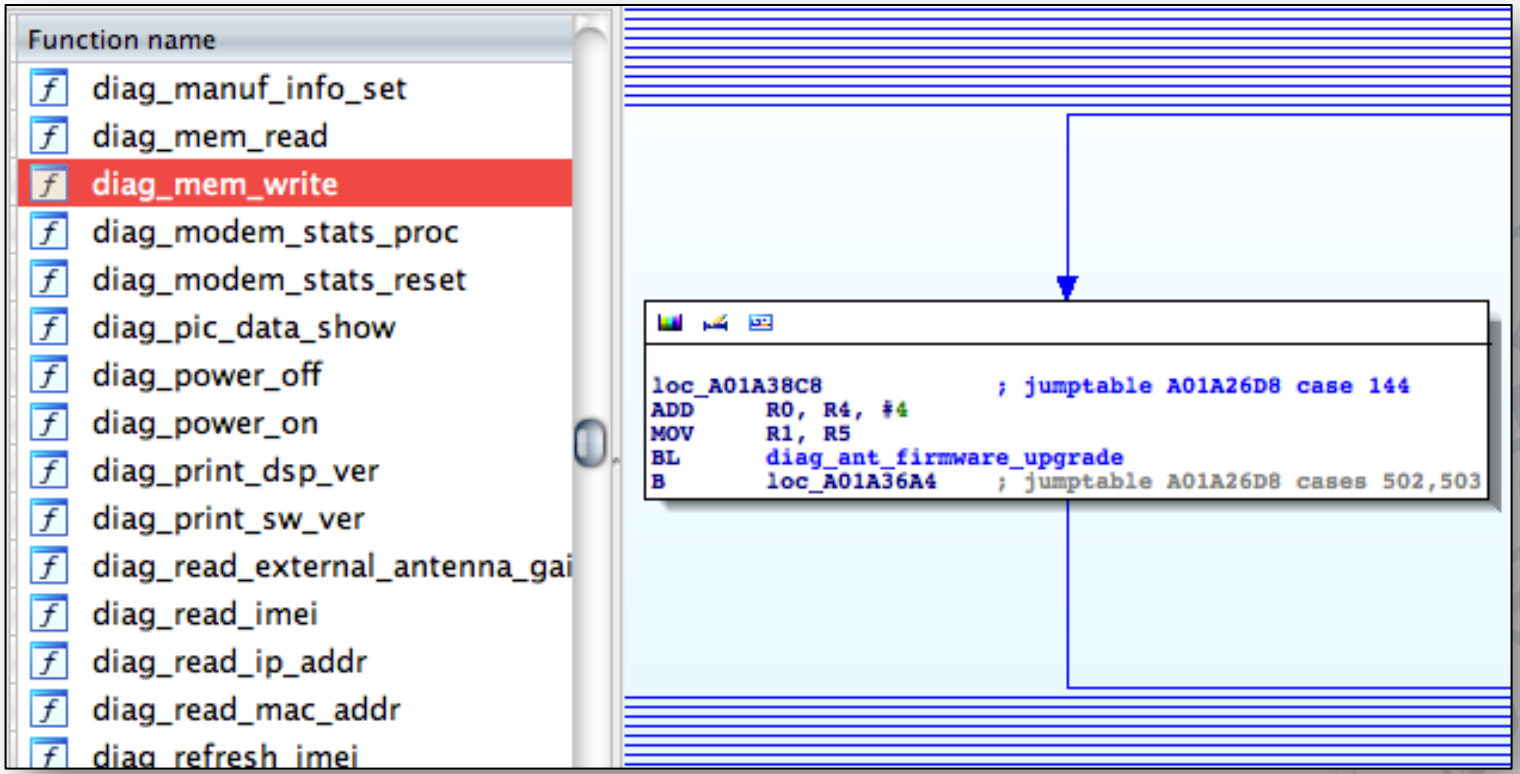
Zing Protocol - CVE-2013-6035

- Undocumented binary protocol
- Inmarsat BGAN (Harris, Hughes, JRC FB) terminals and Thuraya IP
- 1827/TCP
- Dozens of functions: antenna, GPS/DSP/FPGA, memory, communications
- Complete terminal control



IOActive™

Zing Protocol - CVE-2013-6035



IOActive™

Hard-coded Credentials - CVE-2013-6034

- FTP/Shell access:

```
ROM:A002449C                    LDR     R0, =aLogininit ; "*** loginInit() ***\n"
ROM:A00244A0                    BL      printf
ROM:A00244A4                    BL      loginInit
ROM:A00244A8                    LDR     R1, =aSr9cqrqqcc ; "SR9cQRQQcc"
ROM:A00244AC                    LDR     R0, =aBganx     ; "bganx"
ROM:A00244B0                    BL      loginUserAdd
ROM:A00244B4 ; ---------------------------------------------------------------------------
ROM:A00244B4                    LDR     R1, =aCqbszcsrrd ; "cQbSzcSRRd"
ROM:A00244B8                    LDR     R0, =aBganuser  ; "bganuser"
ROM:A00244BC                    BL      loginUserAdd
ROM:A00244C0 ; ---------------------------------------------------------------------------
```

Username	Password (Hashed)	Cleartext
target	RcQbRbzRyc	password
bganx	SR9cQRQQcc	satellite
bganuser	cQbSzcSRR	broadband

IOActive™

Hard-coded Credentials - CVE-2014-0326

- Thuraya IP
- FTP/Shell access


```
ROM:A002DC14                LDR     R0, =aDslp      ; "dslp"
ROM:A002DC18                LDR     R1, =aSybcbcrczz ; "SybcbcRczz"
ROM:A002DC1C                BL      loginUserAdd
ROM:A002DC20                LDR     R2, =0xA064C458
ROM:A002DC24                LDR     R3, [R2]
ROM:A002DC28                ANDS    R4, R3, #0x20
ROM:A002DC2C                BNE     loc_A002DC44
ROM:A002DC30                LDR     R0, =aDslTargetShell ; "DSL+ Target Shell [BSP 2C]\n\nUsername: "
ROM:A002DC34                BL      loginStringSet
ROM:A002DC38                MOV     R1, R4
ROM:A002DC3C                LDR     R0, =loginPrompt2
ROM:A002DC40                BL      shellLoginInstall
```

Username	Password (Hashed)	Cleartext
target	RcQbRbzRyc	password
dslp	SybcbcRczz	dslpuser

IOActive™

Hughes Admin Code Backdoor

Hughes 9502 BGAN M2M External Antenna Terminal

The world's most cost-effective, all-IP BGAN machine-to-machine satellite terminal with exceptionally low power consumption

The Hughes 9502 IP satellite terminal provides reliable connectivity over the Inmarsat Broadband Global Area Network (BGAN) for IP SCADA and machine-to-machine (M2M) applications. The Hughes terminal delivers affordable, global, end-to-end IP data connectivity enabling applications in industry sectors such as environmental monitoring, SmartGrid, pipeline monitoring, compressor monitoring, well site automation, video surveillance, and out-of-band management to primary site communications.

IOActive™

Hughes Admin Code Backdoor

5 Local and Remote Control

There are a number of message channels that can be used to connect the terminal with its configuring equipment.

- Using the Ethernet connection on the UT (Local)
- Using the USB connection on the UT (Local)
- Using the BGAN network (Remote)

The Ethernet connection may be used to:

- Connect a PC to access the WebUI to configure the terminal
- Connect a third party equipment that communicates using AT commands, which could be user equipment e.g. intelligent SCADA RTUs

The USB port may only be used to connect a PC to access the WebUI to configure the terminal

The BGAN network may be used to support remote terminal management both using SMS exchanges and using WebUI. AT messages can also be used indirectly over the BGAN connection if there is intelligent user equipment connected to the UT that is accessible remotely by virtue of its PDP context. The user equipment can then be remotely commanded to issue AT commands across its local Ethernet connection to the UT.

IOActive™

Hughes Admin Code Backdoor

The security passwords page includes the following functions:

- Personalization Key to lock the UT to a particular USIM (SIM to Phone lock)
- Administration password – off by default. Default password is ***admin***
- SMS Remote Control – off by default. On/Off radio button
- SMS Remote Password – default is ***remote***
- List of phone numbers allowed to send remote control SMS

IOActive™

WebUI Authentication

Admin login handled by:

mmi_wms__handle_security_admin_entry
mmi_wms__handle_security_admin_change

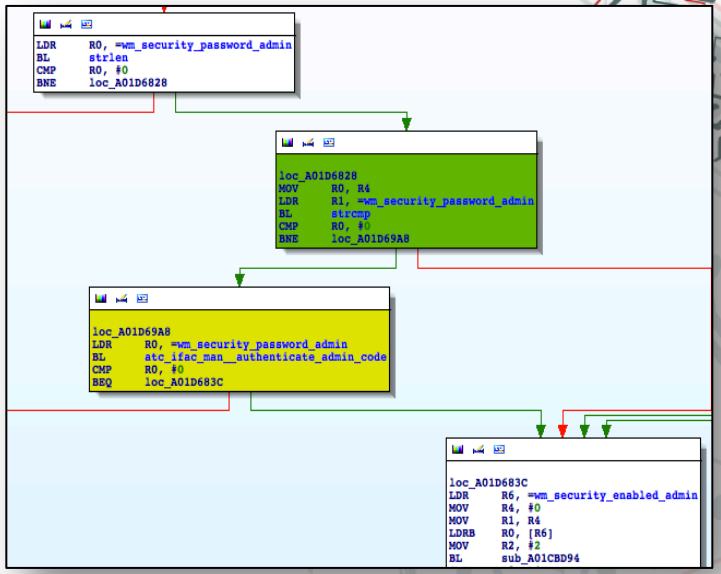
Two ways to authenticate:

Legit Password

Backdoor Password

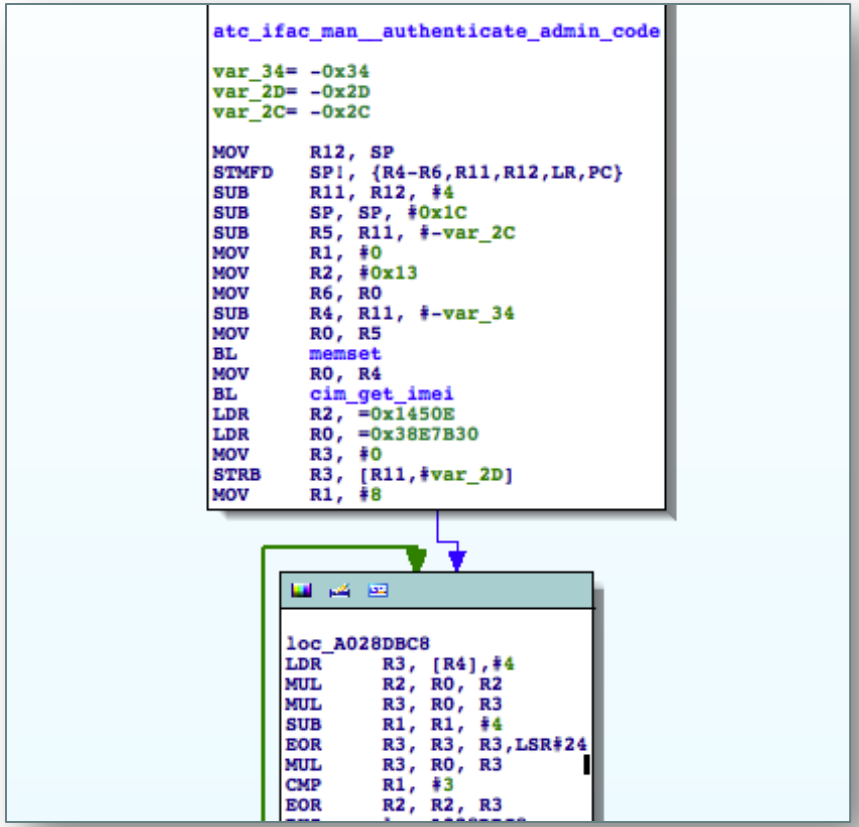
Backdoor:

atc_ifac_man_authenticated_admin_code



IOActive™

Admin Code Backdoor Derived from UT's IMEI

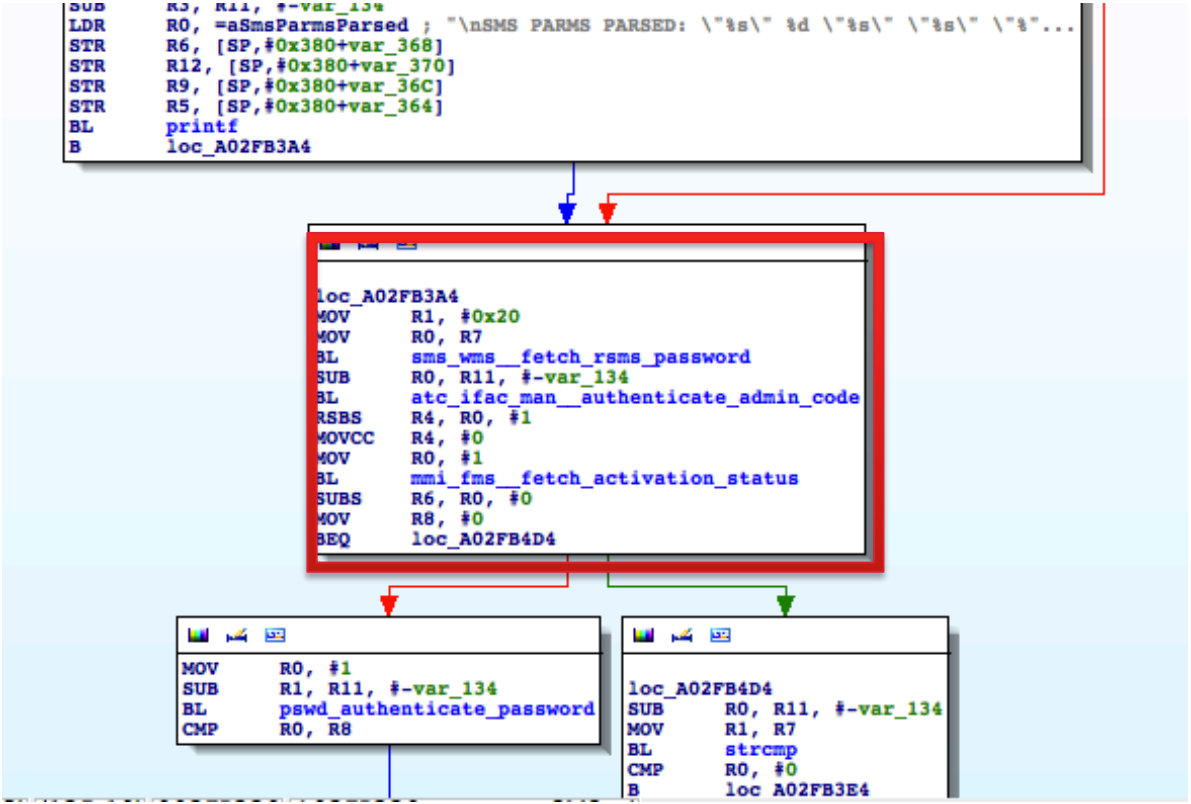


```
atc_ifac_man__authenticate_admin_code

var_34= -0x34
var_2D= -0x2D
var_2C= -0x2C

MOV     R12, SP
STMFD   SP!, {R4-R6,R11,R12,LR,PC}
SUB     R11, R12, #4
SUB     SP, SP, #0x1C
SUB     R5, R11, #-var_2C
MOV     R1, #0
MOV     R2, #0x13
MOV     R6, R0
SUB     R4, R11, #-var_34
MOV     R0, R5
BL      memset
MOV     R0, R4
BL      cim_get_imei
LDR     R2, =0x1450E
LDR     R0, =0x38E7B30
MOV     R3, #0
STRB    R3, [R11,#var_2D]
MOV     R1, #8
```

```
loc_A028DBC8
LDR     R3, [R4],#4
MUL     R2, R0, R2
MUL     R3, R0, R3
SUB     R1, R1, #4
EOR     R3, R3, R3,LSR#24
MUL     R3, R0, R3
CMP     R1, #3
EOR     R2, R2, R3
```


IOActive™

SMS Authentication



IOActive™

SMS Authentication

8 SMS commands

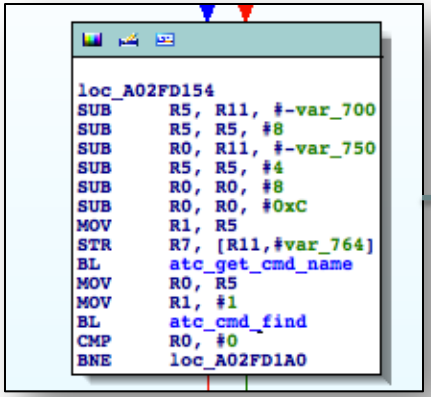
The UT may also be configured by SMS commands and these commands may vary between manufacturers. The SMS commands supported by the Hughes BGAN M2M UT are shown in the table below. Note that the last command in the list, ATCO, enables the integrator to encapsulate specific AT commands into a SMS messages.

ACTIVATE	-	Activates a PDP context for the device(s) connected to the UT
DEACTIVATE	-	Deactivates some or all the PDP contexts for devices connected to the UT
CLEAR	-	Deletes SMS messages on the UT SIM card
GETINFO	-	Retrieves current information from the UT. This can be GPS fix information and/or communications information such as IMEI and carrier beam strength.
RESTART	-	Restarts the UT
WATCHDOG	-	Requests or modifies the current Watchdog settings
ATCO	-	Issues AT commands to the UT AT command handler which returns the response in an SMS. Not all AT commands are supported. See the Hughes 9502 SMS Remote Control Feature User Guide (RD.3) for the full list of supported ACTO AT commands..

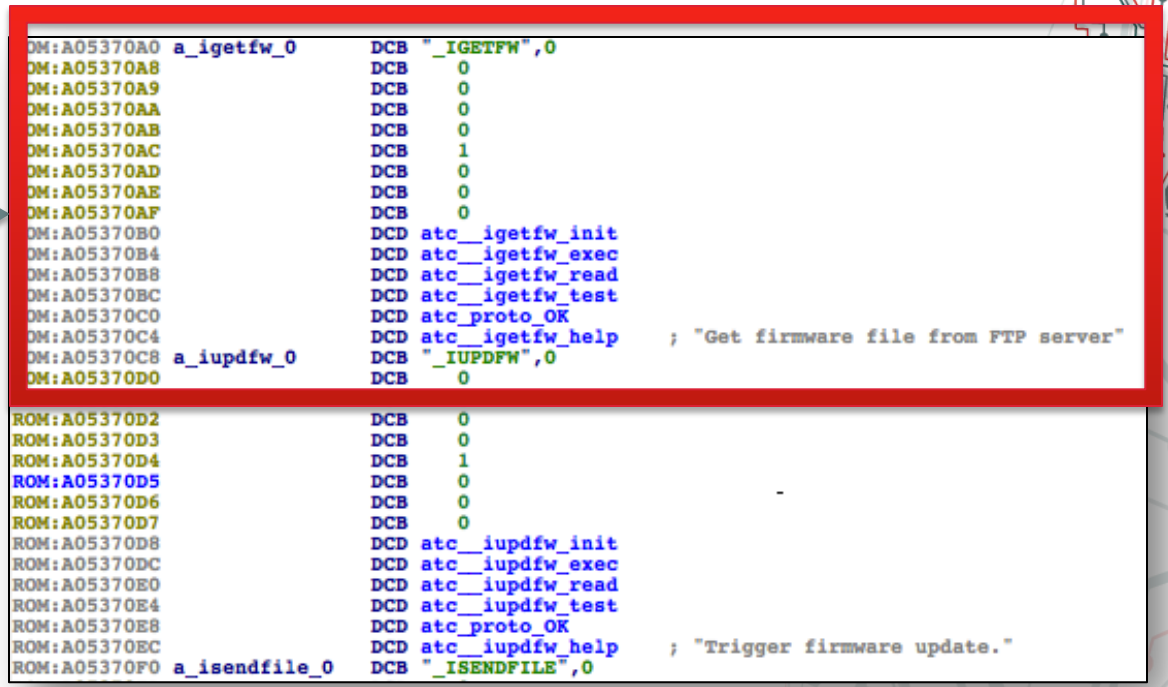
https://s3.amazonaws.com/gwx_hughes/uploads/b2c09f10-9f11-0130-febf-4040a5068ef5/Hughes_9502_BGAN_M2M_System%20Integrators%20Guide%20Version%201.5%20100512.pdf

IOActive™

ATCO: AT-supported Commands



```
loc_A02FD154
SUB     R5, R11, #-var_700
SUB     R5, R5, #8
SUB     R0, R11, #-var_750
SUB     R5, R5, #4
SUB     R0, R0, #8
SUB     R0, R0, #0xC
MOV     R1, R5
STR     R7, [R11,#var_764]
BL      atc_get_cmd_name
MOV     R0, R5
MOV     R1, #1
BL      atc_cmd_find
CMP     R0, #0
BNE     loc_A02FD1A0
```



```
OM:A05370A0 a_igetfw_0      DCB "_IGETFW",0
OM:A05370A8                 DCB   0
OM:A05370A9                 DCB   0
OM:A05370AA                 DCB   0
OM:A05370AB                 DCB   0
OM:A05370AC                 DCB   1
OM:A05370AD                 DCB   0
OM:A05370AE                 DCB   0
OM:A05370AF                 DCB   0
OM:A05370B0                 DCD atc__igetfw_init
OM:A05370B4                 DCD atc__igetfw_exec
OM:A05370B8                 DCD atc__igetfw_read
OM:A05370BC                 DCD atc__igetfw_test
OM:A05370C0                 DCD atc_proto_OK
OM:A05370C4                 DCD atc__igetfw_help    ; "Get firmware file from FTP server"
OM:A05370C8 a_iupdfw_0      DCB "_IUPDFW",0
OM:A05370D0                 DCB   0
ROM:A05370D2                DCB   0
ROM:A05370D3                DCB   0
ROM:A05370D4                DCB   1
ROM:A05370D5                DCB   0
ROM:A05370D6                DCB   0
ROM:A05370D7                DCB   0
ROM:A05370D8                DCD atc__iupdfw_init
ROM:A05370DC                DCD atc__iupdfw_exec
ROM:A05370E0                DCD atc__iupdfw_read
ROM:A05370E4                DCD atc__iupdfw_test
ROM:A05370E8                DCD atc_proto_OK
ROM:A05370EC                DCD atc__iupdfw_help    ; "Trigger firmware update."
ROM:A05370F0 a_isendfile_0  DCB "_ISENDFILE",0
```

- …
- _IGETFW
- _IUPDFW
- ..

http://www.hughes.com/AT_Command_Reference.html

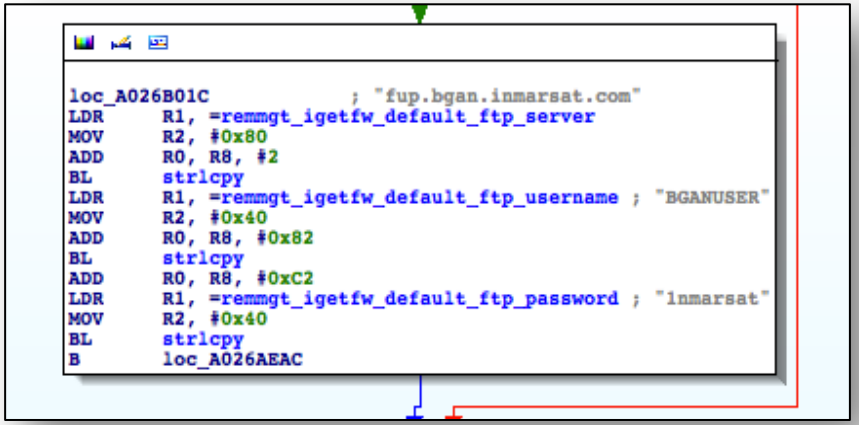
IOActive™

ATCO: AT-supported Commands

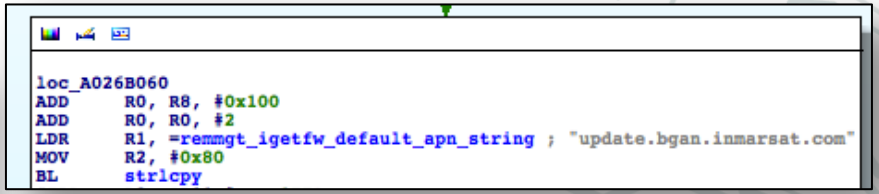
"Future firmware releases would be uncommon, meanwhile any such modem update will qualify for no charge over-the-air (OTA) upgrades saving customers time and money."

http://www.hughes.com/technologies/mobilesat-systems/mobile-satellite-terminals/hughes-9502-bgan-m2m

atc__igetfw_exec



```
loc_A026B01C            ; "fup.bgan.inmarsat.com"
LDR     R1, =remmgt_igetfw_default_ftp_server
MOV     R2, #0x80
ADD     R0, R8, #2
BL      strlcpy
LDR     R1, =remmgt_igetfw_default_ftp_username ; "BGANUSER"
MOV     R2, #0x40
ADD     R0, R8, #0x82
BL      strlcpy
ADD     R0, R8, #0xC2
LDR     R1, =remmgt_igetfw_default_ftp_password ; "inmarsat"
MOV     R2, #0x40
BL      strlcpy
B       loc_A026AEAC
```



```
loc_A026B060
ADD     R0, R8, #0x100
ADD     R0, R0, #2
LDR     R1, =remmgt_igetfw_default_apn_string ; "update.bgan.inmarsat.com"
MOV     R2, #0x80
BL      strlcpy
```

- FTP: fup.bgan.inmarsat.com
- Username: BGANUSER
- Password: 1nmarsat
- APN: update.bgan.inmarsat.com

IOActive

Enhanced Security Mode

Features

You can enable special features from this page. Before features can be used you must obtain the feature activation code from your service provider and activate the feature by entering the UT specific code in the **Feature Activation Code** field. You will need to provide the unit IMEI to the Service Provider. This can be found on the Properties Page.

SMS Remote Management allows the unit to receive and act on special remote control SMS messages. To use the feature you must next enable it on the **Remote Settings** SMS page.

Enhanced Security allows you to lock the UT so that it can only be accessed locally after entering a password. Refer to the **Security Management** section below. When this feature is active, the remote SMS password will be stored encrypted and will not be visible on the **Remote Settings** SMS page.

Hughes Control Pad - Feature Management

C/N0

BEAM REGIONAL 13

BATT

MAINS WLAN: Off

- PROPERTIES
- SETUP
- STATISTICS
- PDP CONTEXTS
- WLAN

Feature Name	Feature Status	Activate
SMS Remote Management	Active	
Enhanced Security	Active	

Feature Activation Code:

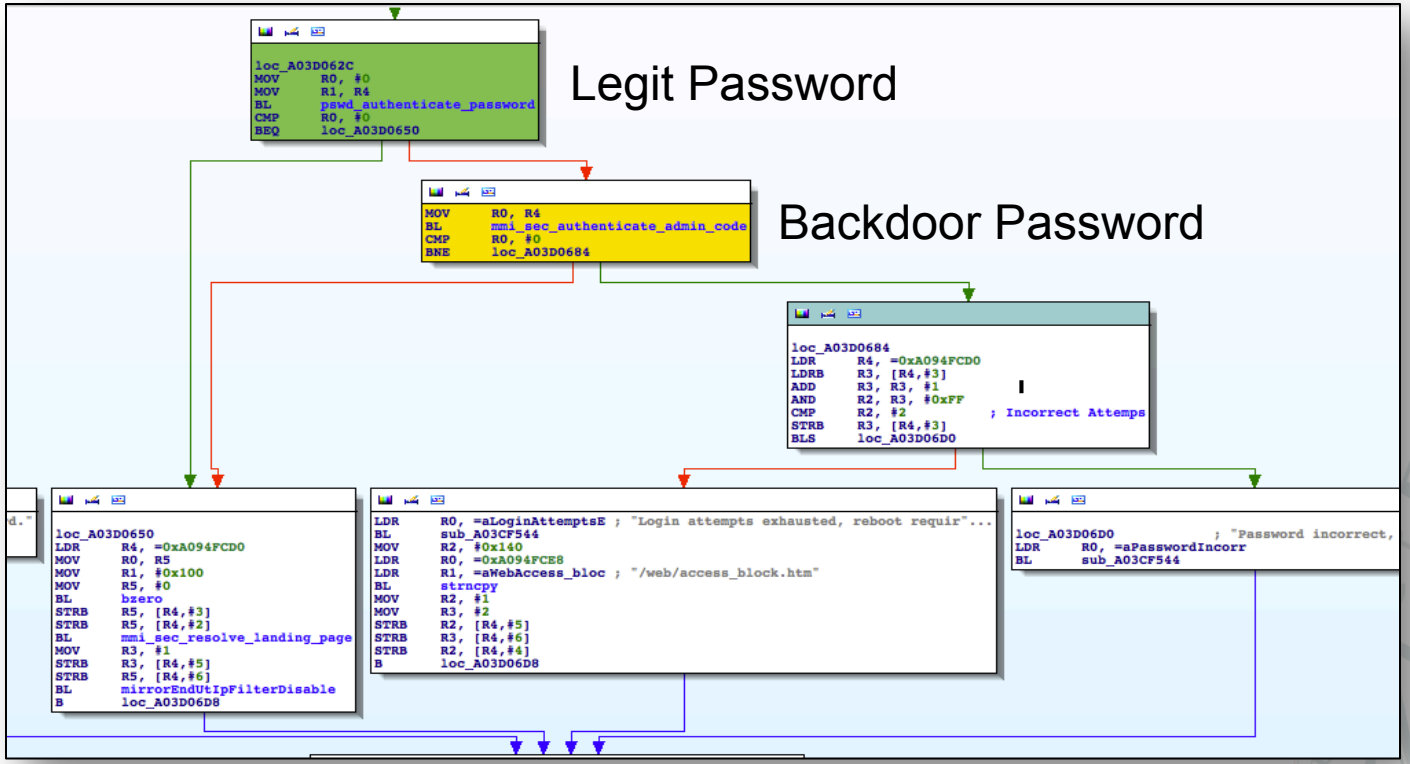
Apply Cancel

9201

9502

IOActive

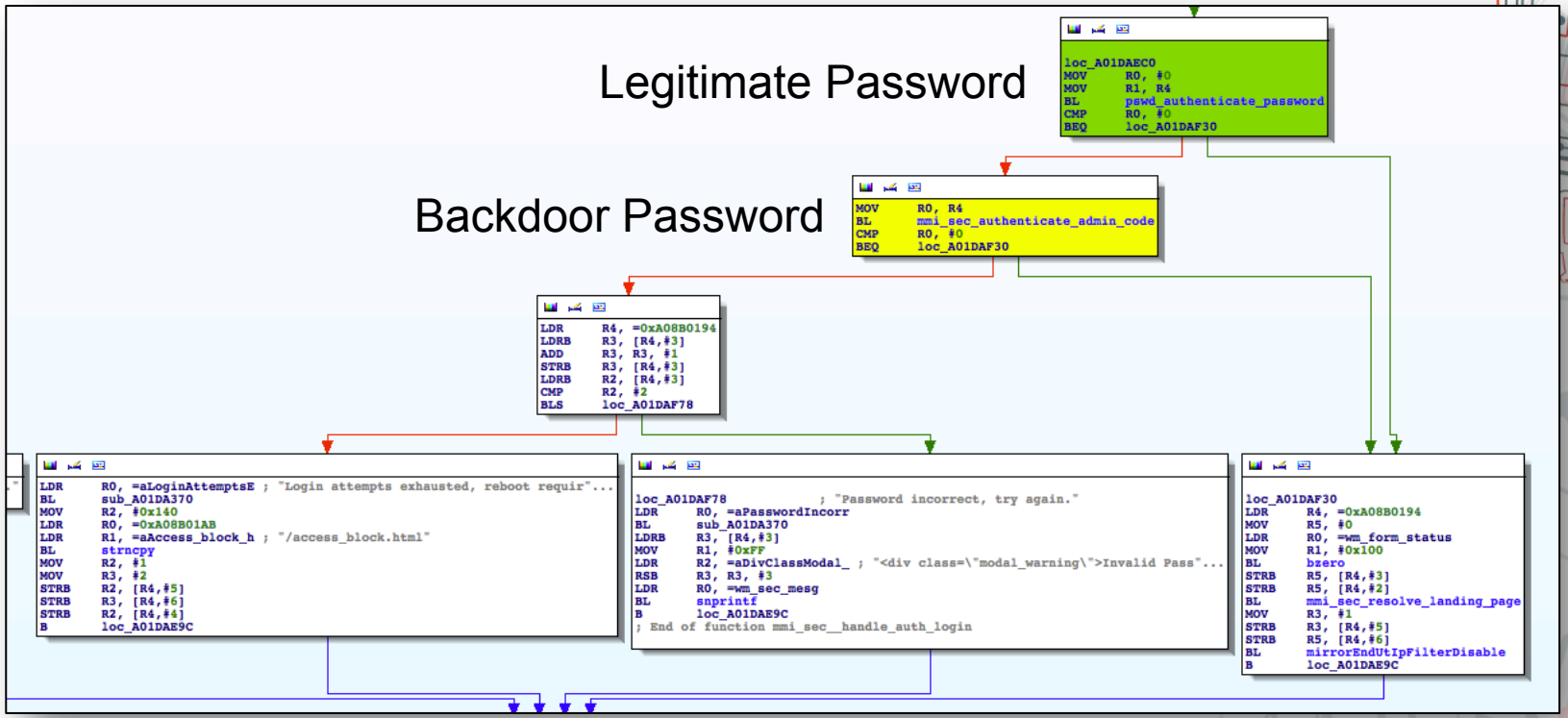
9201



Backdoor: mmi_sec_authenticate_admin_code

IOActive™

9502



Backdoor: mmi_sec_authenticate_admin_code

IOActive™

Backdoor: mmi_sec_authenticate_admin_code

```
mmi_sec_authenticate_admin_code
STMFD    SP!, {R4,R5,LR}
SUB      SP, SP, #0x14
MOV      R4, SP
MOV      R1, #0
MOV      R2, #0x13
MOV      R5, R0
MOV      R0, R4
BL       memset
MOV      R0, R4
BL       derive_backdoor_from_imei ; not the original symbol :)
MOV      R0, R4
MOV      R1, R5
BL       strcmp
CMP      R0, #0
MOVNE    R0, 0xFFFFFFFF
MOVEQ    R0, #0
ADD      SP, SP, #0x14
LDMFD    SP!, {R4,R5,PC}
; End of function mmi_sec_authenticate_admin_code
```

```
; not the original symbol :)

derive_backdoor_from_imei
STMFD    SP!, {R4,LR}
MOV      R4, R0
LDR      R0, =0x1450E
BL       derive_from_imei
LDR      R3, =0x51EB851F
LDR      R12, =0xBC614E
LDR      R1, =0xA03CF6C0 ;  %d
UMULL    LR, R2, R3, R0
MOV      R0, R4
ADD      R2, R12, R2,LSR#4
LDMFD    SP!, {R4,LR}
B        sprintf
; End of function derive_backdoor_from_imei
```


IOActive™

Demo

BBC’s journalists using Hughes 9201 during Ukrainian conflict

https://twitter.com/pmarsupia/status/438084883643396096/photo/1

IOActive™

Cobham Vendor Responses

- *"[…] From a network security perspective, Cobham devices can therefore only be subject to attacks if the attacker has either physical access to the device or segment or the network has been installed incorrectly"*
- *"All Over-The-Air (OTA) commands require user authentication based on specific passwords to the specific terminal. No hard-coded credentials can be used in any case. User authentication is required for each individual command set so there is no possibility to exploit another user's credentials".*

IOActive™

Iridium Vendor Response

“We won’t fix that.”

IOActive™

Hughes Vendor Response

Hughes: It is correct to say that hard coded credentials are used in the Modem. These credentials are required when initiating local ftp and telnet sessions. The primary reason for these credentials is to deter unskilled users from accessing the flash file system and operating system shell within the Modem. However, the credentials are readily made available to field technicians and other skilled personnel who need them. They are also embedded in certain applications like software upgraders that utilize the ftp facility in the Modem. As such, these credentials are not intended to be a terminal security mechanism. In most UNIX and Linux based machines, ftp and telnet exist without even this level of deterrence. Access to ftp and telnet into the Modem does not pose a security risk.

Hughes Vendor Response

Hughes: It is correct to say that the Modem contains backdoors to facilitate the recovery of the terminal when passwords are lost or forgotten. This is common practice in commercial electronic products that support user selected password protections for configuration settings. The backdoor is based upon a hash function that takes the unit's IMEI (electronic serial number) and yields a unit specific backdoor password. The primary use of the backdoor password is to unlock Admin password protected terminals. The Admin password's function is to avoid less skilled end users from modifying their IT department's selected configuration parameters for the Modem. Many terminals are deployed without the Admin password being enabled at all by their owners. There is no known threat to security as a result of this backdoor mechanism's existence; it only protects the Modem's configuration.

Conclusions

- If someone can remotely or physically reach your SATCOM devices, it's over.
- Backdoors are insecure.
- Hardcoded data is insecure.
- Avoid using insecure protocols
- Digital signatures are great!
- We are just scratching the surface and have a long way to go.

IOActive™

Thank you for coming!

IOActive™