SATCOM Terminals
Hacking by Air, Sea, and Land

Ruben Santamarta
Principle Security Consultant

IOActive™
Hardware | Software | Wetware
SECURITY SERVICES

Agenda

- Introduction
- Methodology
- Attack surface
- Vulnerabilities
- Real world Attacks
- Demo

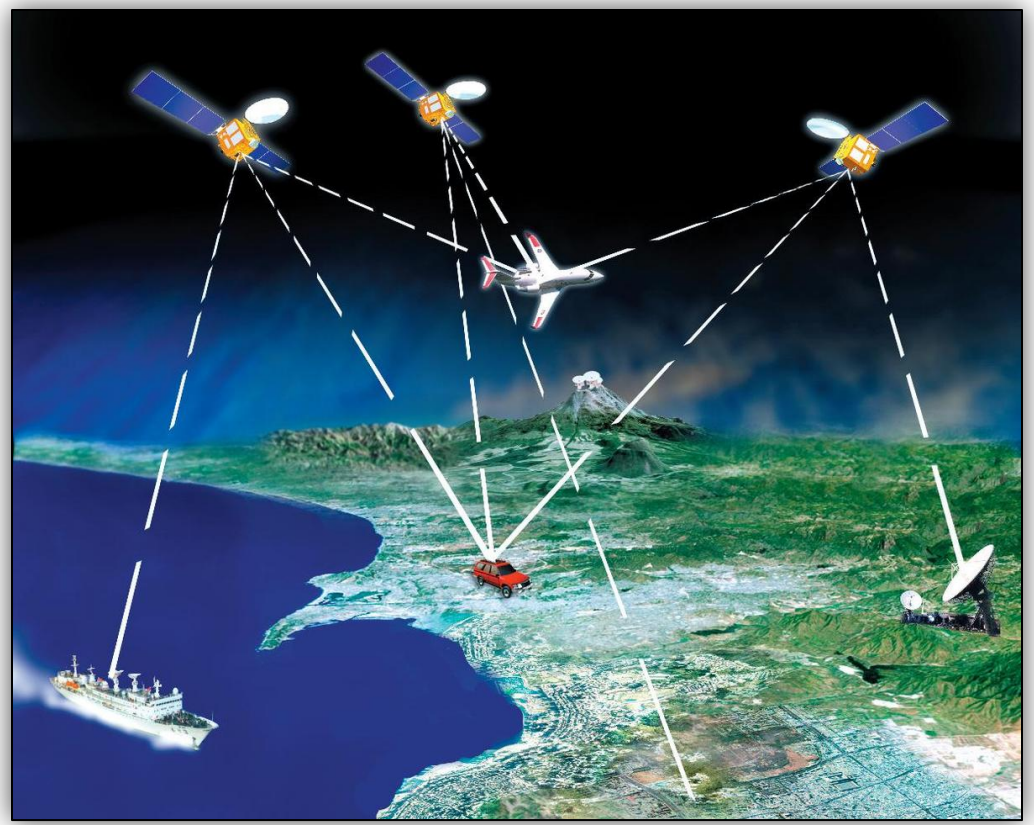
IOActive™

Who Am I?

- Ruben Santamarta
- Principal Security Consultant at IOActive
- Reverse Engineering,
  Research, Embedded, Software, ICS
- rubens[at]ioactive[dot]com

IOActive™

SATELLITE COMMUNICATIONS



IOActive™

Maritime

Industrial

Military

Aerospace

Emergencies

Media

SPACE SEGMENT

GROUND SEGMENT

IOActive™

Vendors Affected

IOActive™

SATCOM Terminals





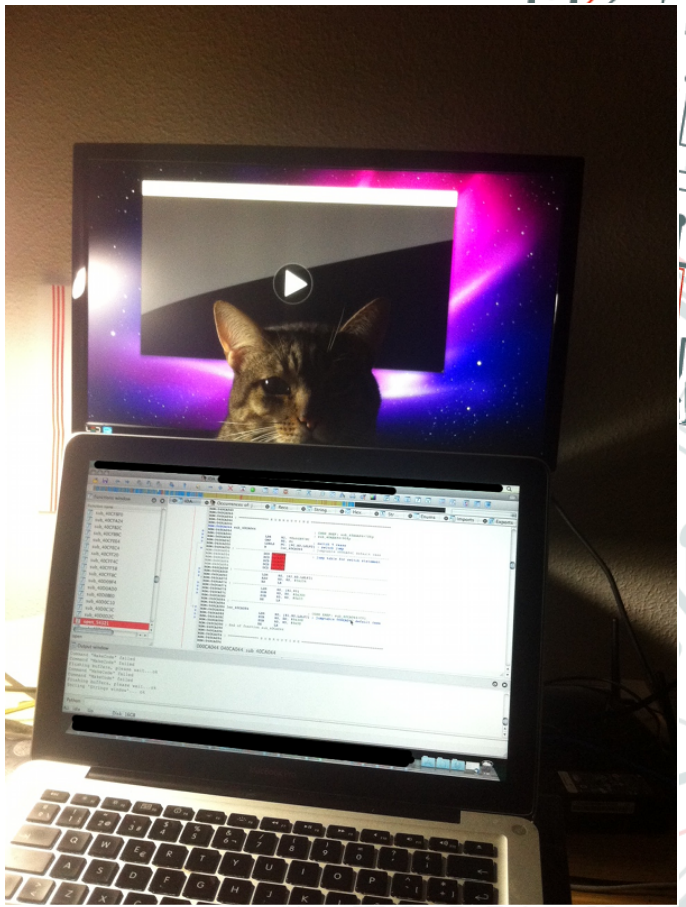


IOActive™

Ideal Research Environment

IOActive™

Actual Research Environment



IOActive™

Methodology

Static Analysis

- Information gathering
- Reverse engineering

Information Gathering

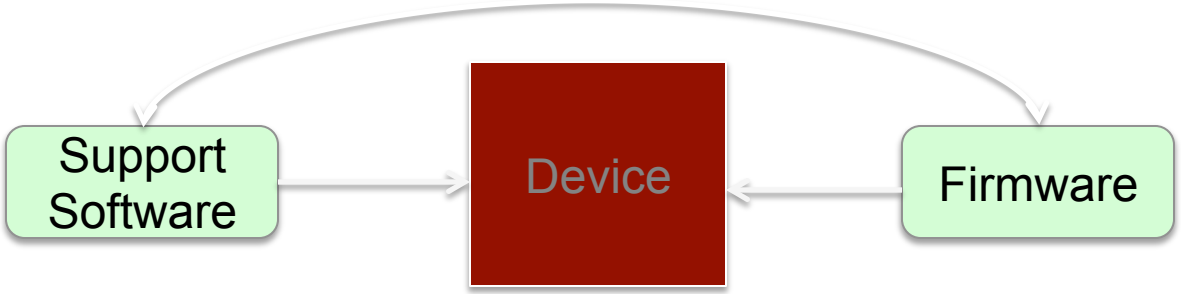
- Datasheets
- Implementation and support guides
- Success cases
- Manuals
- Public information
- Press releases
- Multimedia material: videos, presentations, pictures …

Information Gathering

- How was the system designed?
- How is it typically deployed in real world situations?
- What are its components?
- What are its main features?

Reverse Engineering

- Support software
  - Configuration, setup
  - Firmware



Vulnerabilities

IOActive™

It's Not a Bug, It's a Feature

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

- 13 CVEs
- No patches

IOActive™

Inmarsat BGAN Terminals

- BGAN Stack
  - GateHouse – www.gatehoude.dk
- Customization/firmware
  - Hughes
- Different Vendors
  - Harris, JRC, Hughes …

Inmarsat BGAN Terminals

- VxWorks
- USB, Ethernet, …
- Firmweare
  - Contains symbols
  - CRC
  - Upgrade via FTP
  - Debug/test/in house functionalities

IOActive™

Zing Protocol – CVE-2013-6035

- Undocumented binary protocol
- Inmarsat BGAN/FB terminals and Thuraya IP
- 1827/TCP
- Dozens of functions – GPS/DSP/FGPA, Memory, Comms
- Complete control over the terminal

4 bytes	N bytes	N bytes
Read Memory	Address	Length
00 00 00 05	00 08 00 00	00 00 01 00

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™

Demo

Hard-coded Credentials ThurayaIP - CVE-2014-0326

- VxQWorks
- 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™

```
; Attributes: bp-based frame

dbg_wms__init
MOV     R12, SP
STMFD   SP!, {R4-R7,R11,R12,LR,PC}
LDR     R7, =aDbg_wms__init ; "dbg_wms__init"
LDR     R5, =aSupport_grp ; "support_grp"
LDR     R6, =aJazi_grp  ; "jazi_grp"
SUB     R11, R12, #4
LDR     R4, =aEverywhere ; "Everywhere"
MOV     R2, R7
MOV     R0, #2
LDR     R1, =aBegin     ; "BEGIN"
BL      mmi_trace_message
LDR     R1, =aSupport   ; "support"
LDR     R2, =aHnsupport ; "hnsupport"
MOV     R0, R5
BL      httpPwdConfAdd
LDR     R1, =aJaziuser  ; "jaziuser"
LDR     R2, =aJZ1       ; "j@z1"
MOV     R0, R6
BL      httpPwdConfAdd
MOV     R1, R5
MOV     R2, R4
LDR     R0, =aFsEnHtmlDebug_ ; "/fs/en/html/debug.htm"
BL      httpCtrlConfAdd
MOV     R1, R6
MOV     R2, R4
LDR     R0, =aFsEnHtmlJazi_h ; "/fs/en/html/jazi.htm"
BL      httpCtrlConfAdd
MOV     R1, R5
MOV     R2, R4
LDR     R0, =aFsEnHtmlSyslog ; "/fs/en/html/syslog.htm"
BL      httpCtrlConfAdd
MOV     R1, R5
MOV     R2, R4
LDR     R0, =aFsEnHtmlPhysta ; "/fs/en/html/phystat_collector.htm"
BL      httpCtrlConfAdd
MOV     R1, R5
MOV     R2, R4
LDR     R0, =aFsEnHtmlMstat_ ; "/fs/en/html/mstat_collector.htm"
BL      httpCtrlConfAdd
LDR     R1, =(aLle_suspend+8)
MOV     R2, R7
MOV     R0, #2
LDMFD   SP, {R4-R7,R11,SP,LR}
B       mmi_trace_message
; End of function dbg_wms__init
```

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™

Introduction

The ThraneLINK Management Application (TMA) is a Windows program that provides easy monitoring, remote operation and software update of connected Thrane & Thrane devices with ThraneLINK support.

All Thrane & Thrane devices with ThraneLINK support must be on the same LAN.

IOActive™

ThraneLINK – Discovery Phase (Client Side)

- Service Locater Protocol (SLP) – OpenSLP

```
.text:00476188    push    offset sub_475CE0
.text:0047618D    push    0
.text:0047618F    push    0
.text:00476191    push    edi
.text:00476192    push    ecx
.text:00476193    mov     [ebx], esi
.text:00476195    call    ds:SLPFindSrvs
```

- Attributes

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

IOActive™

ThraneLINK – Discovery Phase (Client Side)

```
call    _strncpy
push    ebx
lea     ebx, [ebp+var_A0]
push    offset format    ; "service:device.thrane://%s"
push    32h              ; maxlen
push    ebx              ; s
call    _snprintf
add     esp, 1Ch
lea     esi, [ebp+var_E6]
push    offset aSailor6006Mess ; "SAILOR 6006 Message Terminal Inmarsat-C"...
push    46h              ; maxlen
push    esi              ; s
call    _snprintf
mov     dword ptr [esp], 0Ah ; pri
push    esi
push    4
push    1
mov     eax, [ebp+arg_0]
lea     esi, [ebp+var_212]
add     eax, 0A9h
push    eax
push    offset a6006_c   ; "6006_C"
push    offset aDeviceVendorTh ; "(device-vendor=Thrane & Thrane),(device"...
push    12Ch             ; maxlen
push    esi              ; s
call    _snprintf
add     esp, 30h
mov     edx, [ebp+src]
push    edx
push    offset AppSLPRegReport
push    1
push    esi
push    0
push    0FFFFh
push    ebx
mov     eax, [ebp+arg_0]
mov     eax, [eax+270h]
push    eax
call    _SLPReg
mov     edx, [ebp+arg_0]
```


IOActive™

ThraneLINK Remote Management (Server Side)

- Features
  - Firmware update
  - Diagnostic
  - Reboot
  - Forwarded Syslog
    - Custom configuration settings
- Implementation
  - SNMP
    1. System config
    2. Software download
    3. Diagnostics report
    4. Logging

IOActive™

Demo

Predictable Admin Reset Code – CVE-2013-7810

- COBHAM
- Explorer/Sailor/Aviator/VSAT

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™

2. Click the link **Forgot administrator password?** at the bottom of the **ADMINISTRATOR LOGON** page (see the previous section).

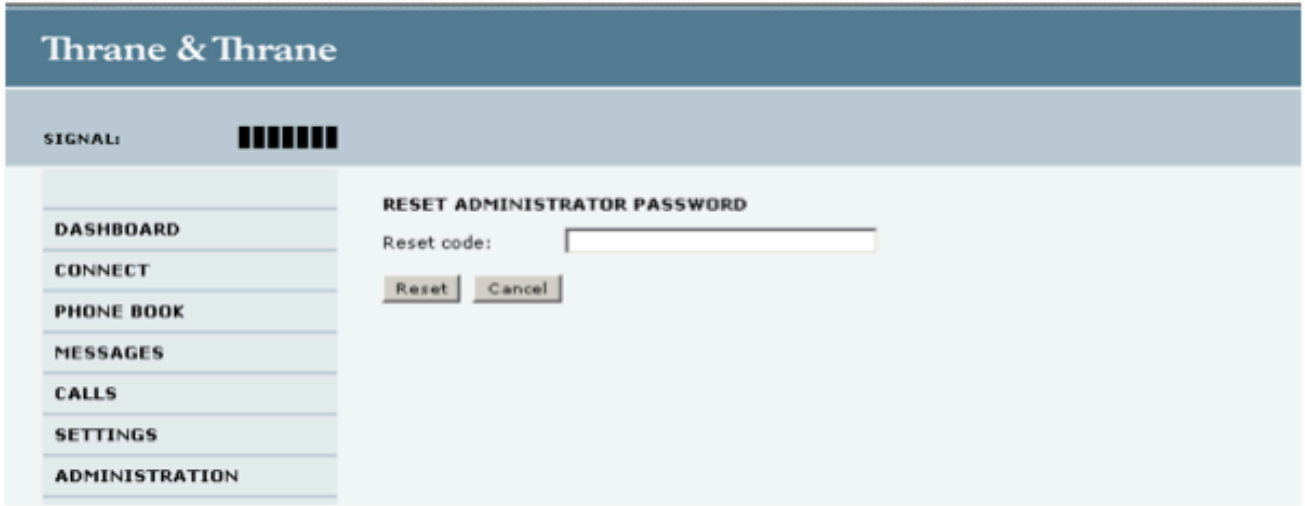


Figure 6-52: Web interface: Administration, Reset administrator password

3. Type in the reset code obtained from your supplier and click **Reset**.
4. Type in the user name **Admin** and the default password **1234**.

Predictable Admin Reset Code – CVE-2013-7810

- Device serial number
  - Hex. 16 bytes, padded with zeros
- Hard coded string (redacted)
  - “kd04rafIOACTIVE” (16 bytes)

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


IOActive™

Aviator 700D

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.**

Who Am I?

- Ruben Santamarta
- Principal Security Consultant at IOActive
- Reverse Engineering,
  Research, Embedded, Software,ICS

IOActive™

Demo

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™

Demo

AVIATOR SDU Shell Hardcoded Credentials – CVE-2014-2964

```
bl      sub_10248C48     # Branch
lis     %r3, ((aDebug+0x10000)@h) # "debug"
addi    %r3, %r3, -0x7448 # aDebug # Add Immediate
lis     %r4, debug@h     # Load Immediate Shifted
addi    %r4, %r4, debug@l # Add Immediate
li      %r5, 0           # Load Immediate
bl      sub_10248C48     # Branch
lis     %r3, ((aProd+0x10000)@h) # "prod"
addi    %r3, %r3, -0x7440 # aProd # Add Immediate
lis     %r4, prod@h      # Load Immediate Shifted
addi    %r4, %r4, prod@l # Add Immediate
li      %r5, 1           # Load Immediate
bl      sub_10248C48     # Branch
lis     %r3, ((aDo160+0x10000)@h) # "do160"
addi    %r3, %r3, -0x7438 # aDo160 # Add Immediate
lis     %r4, do160@h     # Load Immediate Shifted
addi    %r4, %r4, do160@l # Add Immediate
li      %r5, 0           # Load Immediate
bl      sub_10248C48     # Branch
lis     %r3, ((aFrlp+0x10000)@h) # "frlp"
addi    %r3, %r3, -0x7430 # aFrlp # Add Immediate
lis     %r4, frlp@h      # Load Immediate Shifted
addi    %r4, %r4, frlp@l # Add Immediate
li      %r5, 1           # Load Immediate
bl      sub_10248C48     # Branch
```


IOActive™

Cobham TBus2 Hardcoded Credentials – 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.

IOActive™

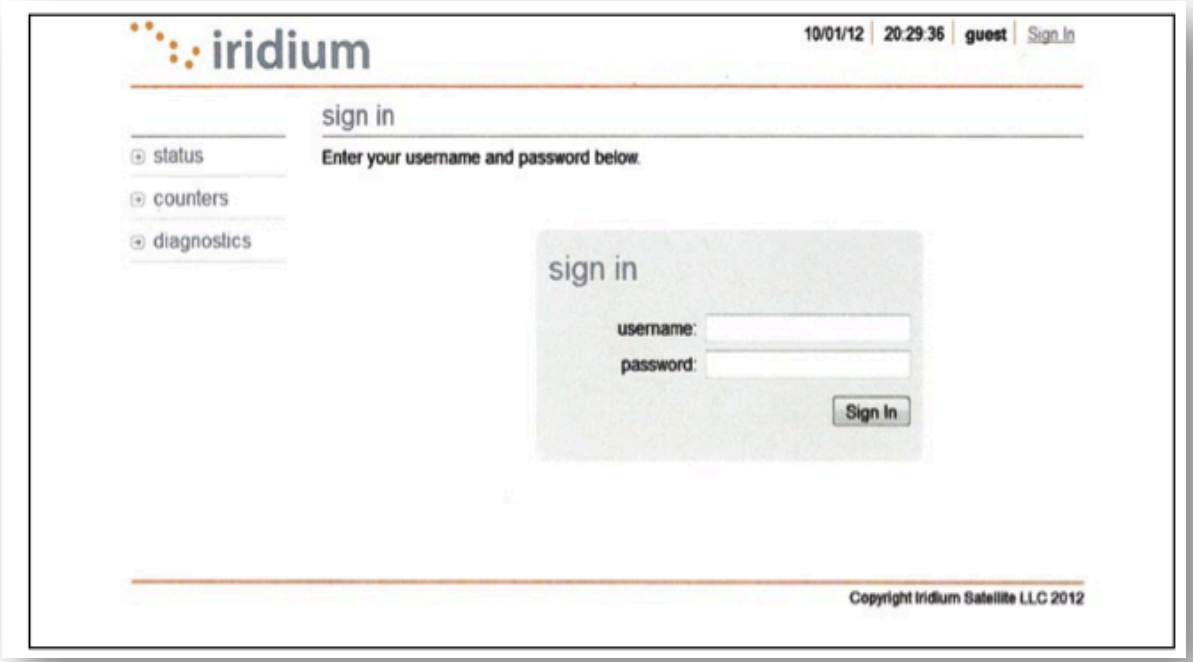
Cobham TBus2 Hardcoded Credentials – CVE-2014-2941

```
.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
```


IOActive™

Demo

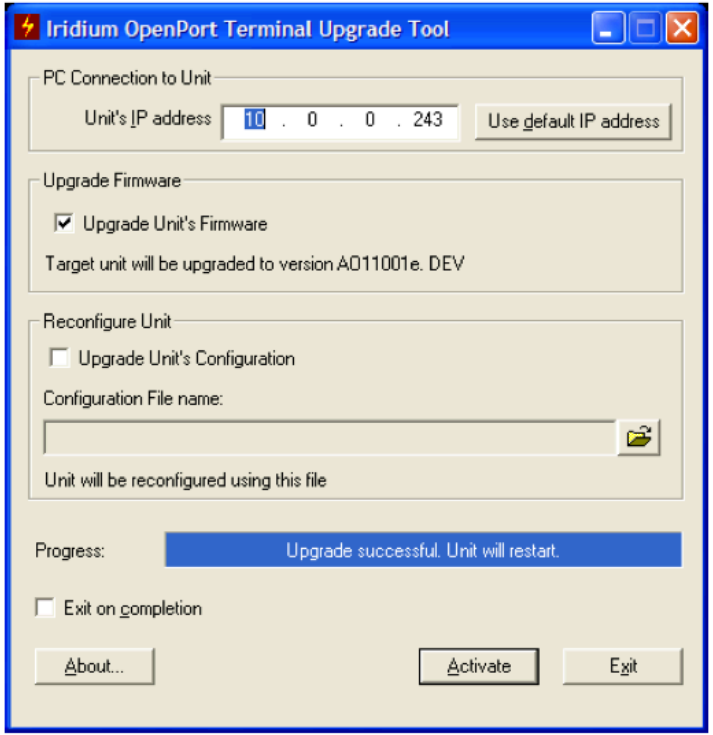
IRIDIUM – Pilot Hard Coded Account



IOActive™

Demo

IRIDIUM Pilot Unauthenticated Firmware Upload



Demo

Real World Attacks

Maritime

Aerospace

Military

IOActive™

Demo

Vendor Responses

- TBD