



Federal Communications Commission
Washington, D.C. 20554

February 26, 2016

Marlene H. Dortch
Secretary
Federal Communications Commission
445 12th Street, S.W.
Washington, DC 20554

Re: Use of Spectrum Bands Above 24 GHz for Mobile Radio Services *et al.*, GN Docket No. 14-177; IB Docket Nos. 15-256 and 97-95; RM-11664; WT Docket No. 10-112

Dear Ms. Dortch:

This letter supplements information filed on February 19, 2016 by EchoStar Satellite Operating Corporation, Hughes Network System, LLC and Alta Wireless, Inc. (collectively "EchoStar") regarding an *ex parte* meeting between EchoStar and FCC staff members discussing the above-captioned proceeding, which took place on February 18, 2016.¹

In addition to covering the issues summarized in EchoStar's *Ex Parte* Letter,² the meeting included a discussion of security issues associated with the proceeding. In the course of the discussion, the FCC staff raised questions about certain statements made in EchoStar's filed comments indicating that "although FSS systems have been operating for decades, there is no indication that security issues have been a problem or are likely to become one ... [EchoStar] submits that there is no concern with respect to the FSS operations that needs to be addressed."³

Specifically FCC staff provided EchoStar an IOActive presentation,⁴ which describes a number of critical security vulnerabilities affecting Satellite Communications (SATCOM) Terminals.

¹ See Letter from Jennifer A. Manner, Vice Pres. Regulatory Affairs, EchoStar Satellite Operating Corporation, to Marlene H. Dortch, Secretary, FCC, GN Docket No. 14-177, IB Docket Nos. 15-250 and 97-95, RM-11664; WT Docket No. 10-112 (filed Feb. 19, 2016) (EchoStar's *Ex Parte* Letter).

² *Id.*

³ EchoStar, *Comments of EchoStar Satellite Operating Corporation, Hughes Network Systems, LLC, and Alta Wireless, Inc.*, GN Docket No. 14-177, IB Docket No. 15-256, RM-11664, WT Docket No. 10-112, IB Docket No. 97-95, at 41 (filed Jan. 28, 2016).

⁴ Ruben Santamarta, Principal Consultant, IOActive, *SATCOM Terminals, Hacking by Air, Sea, and Land*, presented at the Black Hat Conference, Aug. 6-7, 2014, Las Vegas, NV. IOActive, http://www.ioactive.com/pdfs/IOActive_SATCOM_Presentation_Black_Hat_2014.pdf (last visited Feb. 26, 2016).

The presentation summarizes an IOActive research paper on the same topic.⁵ The FCC staff highlighted the major security vulnerability findings of the study during the meeting, which include:

1. Backdoors,
2. Hard Coded Credentials,
3. Insecure Protocols, and
4. Weak Password Resets.

EchoStar stated that it was familiar with the IOActive research paper but indicated that it contained some inaccuracies, without elaborating.⁶ We append the IOActive material to this letter in order to provide additional context.

Sincerely,

_____/s/_____
Gregory F. Intoccia
Special Counsel
Cybersecurity & Communications Reliability Division
Public Safety & Homeland Security Bureau
Federal Communications Commission
(202) 418-1470.
gregory.intoccia@fcc.gov

cc: Participants

Attachments

1. Ruben Santamarta, Principal Consultant, IOActive, *SATCOM Terminals, Hacking by Air, Sea, and Land*, presented at the Black Hat Conference, Aug. 6-7, 2014, Las Vegas, NV.
2. Ruben Santamarta, *SATCOM Terminals: Hacking by Air, Sea, and Land*, White Paper (2014).
3. Vulnerability Note, VU#250358.

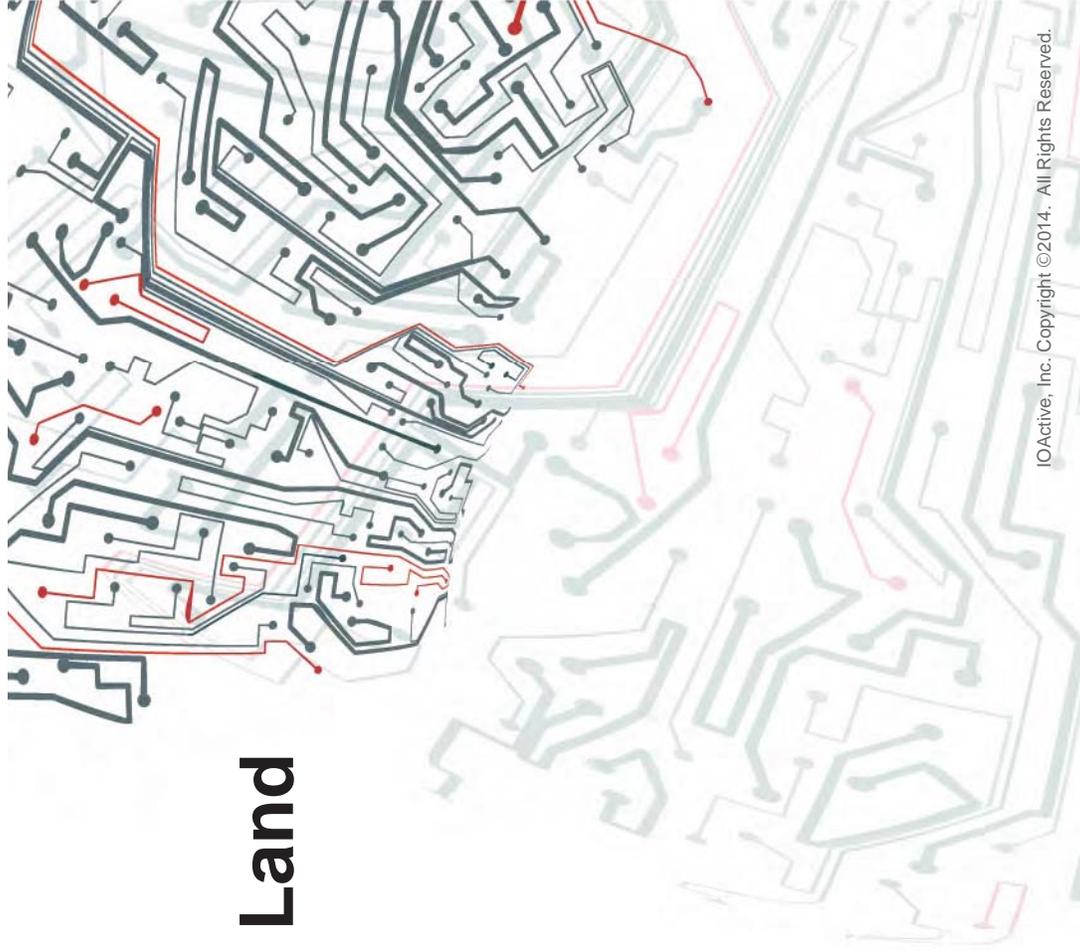
⁵ Ruben Santamarta, *SATCOM Terminals: Hacking by Air, Sea, and Land*, White Paper (2014), Black Hat, <https://www.blackhat.com/docs/us-14/materials/us-14-Santamarta-SATCOM-Terminals-Hacking-By-Air-Sea-And-Land-WP.pdf>. (last visited Feb. 26, 2016). See also Vulnerability Note, VU#250358, for additional details on Cert Software Institute, <http://www.kb.cert.org/vuls/id/250358> (last visited Feb. 26, 2016).

⁶ FCC Staff is not aware of any inaccuracies associated with this research.

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



Who Am I?

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



SATELLITE COMMUNICATIONS



IOActive, Inc. Copyright ©2014. All Rights Reserved.



Maritime



Industrial



Military



Aerospace



Emergencies

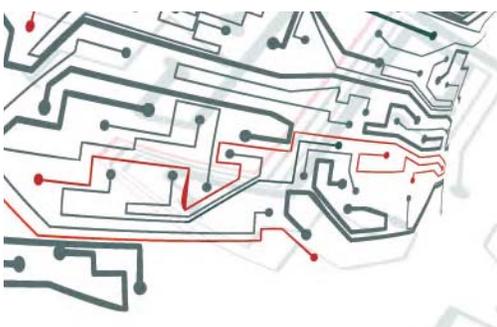


Media





SPACE SEGMENT



GROUND SEGMENT

IOActive[™]



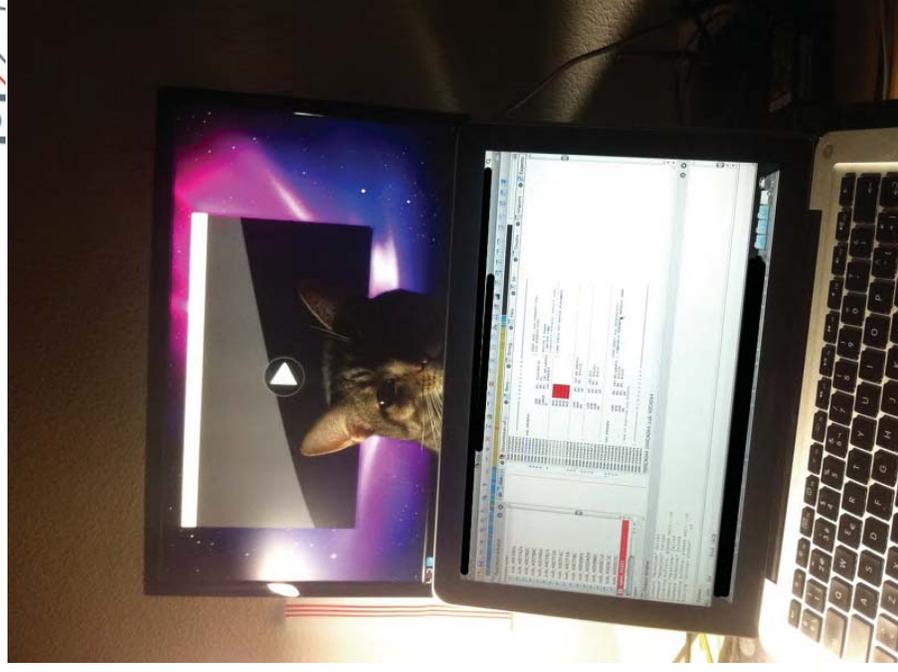
Vendors Affected



Ideal Research Environment



Actual Research Environment



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, Inc. Copyright ©2014. All Rights Reserved.



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

Hard coded
Credentials

Backdoors

Insecure Protocols

Undocumented
Protocols

- 13 CVEs
- No patches



Inmarsat BGAN Terminals

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



Inmarsat BGAN Terminals

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



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



Hard Coded Credentials - CVE-2013-6034

- FTP/Shell access

```
ROM:A002449C
ROM:A00244A0
ROM:A00244A4
ROM:A00244A8
ROM:A00244AC
ROM:A00244B0
ROM:A00244B4
ROM:A00244B8
ROM:A00244BC
ROM:A00244C0

LDR R0, =aLoginInit ; "### loginInit() ###\n"
BL printf
BL loginInit
LDR R1, =aSr9cqrqqcc ; "SR9cQRQQcc"
R0, =aBganx ; "bganx"
BL loginUserAdd

LDR R1, =aCqbszcarrd ; "cQbSzcSRRd"
LDR R0, =aBganuser ; "bganuser"
BL loginUserAdd
```

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



Demo



Hard-coded Credentials ThurayaIP - CVE-2014-0326

- VxQWorks
- FTP/Shell access

```
ROM:A002DC14      LDR    R0, =adslp
ROM:A002DC18      LDR    R1, =aSybcrczz ; "Sybcrczz"
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 [ASP 3C]\n\nuseramet"
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	SybcrcRczz	dslpuser



```

; Attributes: bp-based frame
dbg_wms_init
MOV R12, SP
STMFD SP!, {R4-R7, R11, R12, LR, PC}
LDR R7, =dbg_wms_init ; dbg_wms_init"
LDR R5, =asupport_grp ; "support_grp"
LDR R6, =ajazi_grp ; "ajazi_grp"
SUB R11, R12, #8
LDR R4, =everywhere ; "Everywhere"
MOV R2, R7
MOV R0, #2
LDR R1, =aBegin ; "BEGIN"
mmi_trace_message
LDR R1, =asupport ; "support"
LDR R2, =ahnsupport ; "hnsupport"
MOV R0, R5
LDR R1, =ajaziuser ; "ajaziuser"
LDR R2, =ajz1 ; "ajz1"
MOV R0, R6
LDR R1, =httpPwdConfAdd
LDR R2, =httpPwdConfAdd
MOV R1, R5
MOV R0, R4
LDR R1, =afsnHtmIdebug ; "/fs/en/html/debug.htm"
LDR R2, =httpCtrlConfAdd
MOV R1, R6
MOV R0, R4
LDR R1, =afsnHtmIjazi_h ; "/fs/en/html/jazi.htm"
LDR R2, =httpCtrlConfAdd
MOV R1, R5
MOV R0, R4
LDR R1, =afsnHtmISyslog ; "/fs/en/html/syslog.htm"
LDR R2, =httpCtrlConfAdd
MOV R1, R5
MOV R0, R4
LDR R1, =afsnHtmIphysta ; "/fs/en/html/phystat_collector.htm"
LDR R2, =httpCtrlConfAdd
MOV R1, R5
MOV R0, R4
LDR R1, =afsnHtmIMstat ; "/fs/en/html/mstat_collector.htm"
LDR R2, =httpCtrlConfAdd
LDR R1, =(allie_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*

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.



ThraneLINK – Discovery Phase (Client Side)

- Service Locator Protocol (SLP) – OpenSLP

```
.text:00476188          push    ebx
.text:0047618B          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:SLPFAndSrvs
```

- 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



ThraneLINK – Discovery Phase (Client Side)

```
call _strncpy
push ebx, [ebp+var_A0]
lea offset format ; "service:device.thrane://%g"
push 32h ; maxlen
push ebx ; s
call _sprintf
add esp, 1Ch
lea esi, [ebp+var_E6]
push offset aSailor6006Mess ; "SAILOR 6006 Message Terminal Inmarsat-C"...
push 46h ; maxlen
push esi ; s
call _sprintf
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 _sprintf
add esp, 30h
mov edx, [ebp+strc]
push edx
push offset AppSLPRegReport
push 1
push 0
push 0FFFFh
push ebx, [ebp+arg_0]
mov eax, [eax+270b]
push eax
call _SLPReg
mov edx, [ebp+arg_01]
```

IOActive, Inc. Copyright ©2014. All Rights Reserved.

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

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**.



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



The screenshot shows a web interface for Thrane & Thrane. At the top, there is a dark blue header with the text "Thrane & Thrane". Below the header, there is a navigation menu with the following items: SIGNAL, DASHBOARD, CONNECT, PHONE BOOK, MESSAGES, CALLS, SETTINGS, and ADMINISTRATION. The "ADMINISTRATION" item is highlighted. To the right of the navigation menu, there is a "RESET ADMINISTRATOR PASSWORD" form. The form has a label "Reset code:" followed by a text input field. Below the input field, there are two buttons: "Reset" and "Cancel".

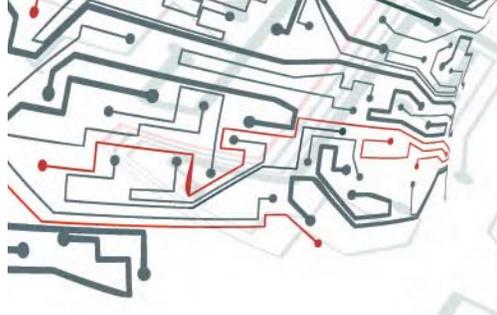
Figure 6-52: Web interface: Administration, Reset administrator password

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)
 - “kd04raf**IOACTIVE**” (16 bytes)

```
import md5
m = md5.new()
m.update( "\x12\x34\x56\x78" + "\x00" * 12 )
m.update( "kd04rafIOACTIVE" )
m.hexdigest()
```



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



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.



Demo



IOActive, Inc. Copyright ©2014. All Rights Reserved.



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, ((aDol160+0x10000)@h) # "dol160"
addi #r3, #r3, -0x7438 # aDol160 # Add Immediate
lis #r4, dol160@h # Load Immediate Shifted
addi #r4, #r4, dol160@l # Add Immediate
li #r5, 0 # Load Immediate
bl sub_10248C48 # Branch
lis #r3, ((aFrip+0x10000)@h) # "frip"
addi #r3, #r3, -0x7430 # aFrip # Add Immediate
lis #r4, frip@h # Load Immediate Shifted
addi #r4, #r4, frip@l # Add Immediate
li #r5, 1 # Load Immediate
bl sub_10248C48 # Branch
```

IOActive, Inc. Copyright ©2014. All Rights Reserved.



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.



Cobham TBus2 Hardcoded Credentials – CVE-2014-2941

```
.rodats:00109CF0 ; UserTab  
.rodats:00109CF0 _3L7UserTab DCD aNormal_0  
.rodats:00109CF0  
.rodats:00109CF0  
.rodats:00109CF4  
.rodats:00109CF8  
.rodats:00109CFC  
.rodats:00109D00  
.rodats:00109D04  
.rodats:00109D08  
.rodats:00109D0C  
.rodats:00109D10  
.rodats:00109D14  
.rodats:00109D18  
.rodats:00109D1C  
DCD 0  
DCD aSuper  
DCD 0  
DCD aSysadm  
DCD 0  
DCD aDistb  
DCD 0  
DCD aProd  
DCD 1  
DCD aDev1  
DCD 1
```

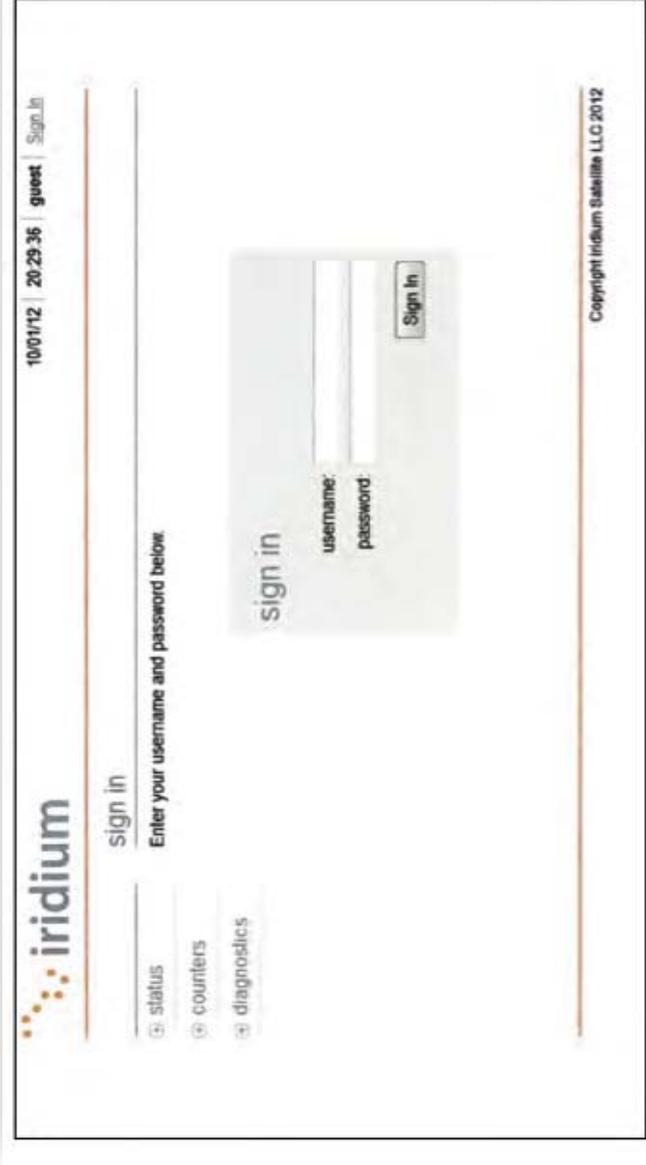
```
; DATA XKEY, GetCurrentUser(void)+tlo  
; .Text:off_A6FAB10 ...  
; "normal"  
; "super"  
; "sysadm"  
; "distb"  
; "prod"  
; "dev1"
```



Demo



IRIDIUM – Pilot Hard Coded Account



The screenshot shows the Iridium website's sign-in interface. At the top left is the Iridium logo. Below it are navigation links for 'status', 'counters', and 'diagnostics'. The main heading is 'sign in' with the instruction 'Enter your username and password below'. A secondary 'sign in' box contains 'username:' and 'password:' labels with input fields and a 'Sign In' button. The top right corner shows the date '10/01/12', time '20:29:36', and user status 'guest' with a 'Sign In' link. The footer contains the copyright notice 'Copyright Iridium Satellite LLC 2012'.

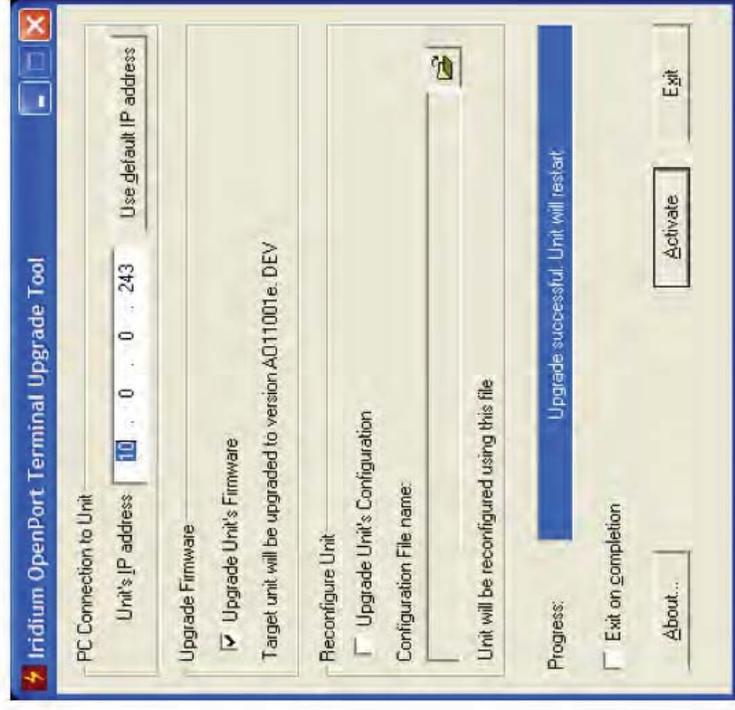
IOActive, Inc. Copyright ©2014. All Rights Reserved.



Demo



IRIDIUM Pilot Unauthenticated Firmware Upload



IOActive, Inc. Copyright ©2014. All Rights Reserved.

IOActive[™]



Demo



Real World Attacks

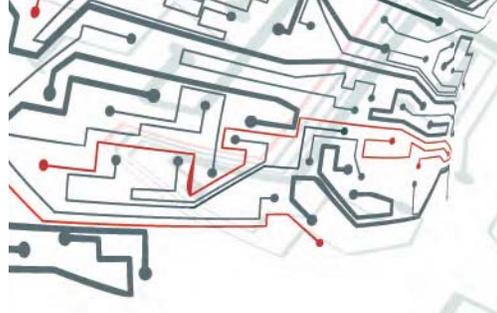
Maritime



Aerospace



Military



Demo



Vendor Responses

- TBD



SATCOM Terminals: Hacking by Air, Sea, and Land

Ruben Santamarta
Principal Security Consultant

Abstract

Satellite Communications (SATCOM) plays a vital role in the global telecommunications system. IOActive evaluated the security posture of the most widely deployed Inmarsat, Iridium, and Thuraya SATCOM terminals.

IOActive analyzed the firmware of these devices and found that malicious actors could abuse all of the devices within the scope of this study. The vulnerabilities included what would appear to be backdoors, hardcoded credentials, undocumented, and/or insecure protocols.

These vulnerabilities have the potential to allow a malicious actor to intercept, manipulate, or block communications, and in some cases, to remotely take control of the physical device.

IOActive
Hardware | Software | Wetware
SECURITY SERVICES

Contents

INTRODUCTION	3
TYPES OF SATCOM INFRASTRUCTURE	3
<i>Inmarsat-C</i>	3
<i>VSAT</i>	4
<i>BGAN</i>	4
<i>BGAN M2M</i>	4
<i>FB</i>	4
<i>SwiftBroadband</i>	4
<i>Classic Aero Service</i>	4
SCOPE OF STUDY	5
METHODOLOGY	6
IMPACT.....	9
VULNERABILITY CLASSES	9
<i>Backdoors</i>	9
<i>Hardcoded Credentials</i>	9
<i>Insecure Protocols</i>	9
<i>Undocumented Protocols</i>	9
<i>Weak Password Reset</i>	9
ATTACK SCENARIOS AGAINST HARRIS BGAN TERMINALS.....	10
ATTACK SCENARIOS AGAINST HUGHES BGAN M2M TERMINALS.....	13
<i>Scenario One</i>	14
<i>Scenario Two</i>	14
ATTACK SCENARIOS AGAINST COBHAM BGAN TERMINALS	15
<i>Scenario: Personal Communications for the Military as Attack Vector</i>	16
ATTACK SCENARIOS AGAINST MARINE VSAT AND FB TERMINALS	17
<i>Scenario One: Navigation Charts</i>	18
<i>Scenario Two: Operational Integrity</i>	18
ATTACK SCENARIOS AGAINST COBHAM AVIATOR.....	19
<i>Level A–Catastrophic</i>	19
<i>Level B–Hazardous</i>	19
<i>Level C–Major</i>	19
<i>Level D–Minor</i>	20
<i>Level E–No Effect</i>	20
ATTACK SCENARIOS AGAINST COBHAM GMDSS TERMINALS.....	22
CONCLUSION	25
ACKNOWLEDGEMENTS	26
REFERENCES.....	26

Introduction

Satellite Communications (SATCOM) plays a vital role in the global telecommunications system. We live in a world where an ever-increasing stream of digital data is flowing between continents. It is clear that those who control communications traffic have an upper hand. The ability to disrupt, inspect, modify, or reroute traffic provides an invaluable opportunity to carry perform surveillance or conduct cyber-attacks.

Terrestrial network infrastructures are subject to physical limitations and simply cannot meet the needs of certain activities. To fill this gap and provide improved performance, there are multiple satellite constellations orbiting the Earth. These networks are responsible for, among other things, allowing people in remote locations to access the Internet, helping vessels and aircrafts operate safely, and providing the military and emergency services with critical communication links during armed conflicts or natural disasters.

Sectors that commonly rely on satellite networks include:

- Aerospace
- Maritime
- Military and governments
- Emergency services
- Industrial (oil rigs, gas, electricity)
- Media

Types of SATCOM Infrastructure

SATCOM infrastructure can be divided into two major segments, space and ground. Space includes those elements needed to deploy, maintain, track, and control a satellite. Ground includes the infrastructure required to access a satellite repeater from Earth station terminals.

Earth station terminals encompass the equipment located both on the ground and on airplanes and ships meaning that this segment includes air and sea. This specific portion of the ground segment was the focus of our research.

IOActive conducted the initial phase of an internal SATCOM research project. This phase focused on analyzing and reverse engineering the freely and publicly available firmware updates for popular SATCOM technologies manufactured and/or marketed by Harris, Hughes, Cobham, Thuraya, JRC, and Iridium.

IOActive's goal was to provide an initial evaluation of the security posture of the most widely deployed Inmarsat and Iridium SATCOM terminals. We analyzed devices used to access these services:

Inmarsat-C

This maritime communication system provides ship-to-shore, shore-to-ship, and ship-to-ship services. Its store-and-forward capabilities make possible to use it for telex, fax, data, or email. It is a key part of the Global Maritime Distress and Safety

System (GMDSS), an internationally agreed-upon set of procedures, types of equipment, and communication protocols intended to increase safety and ensure a rapid and automated response from authorities and emergency services in the event of a marine distress. The international convention for Safety of Life at Sea (SOLAS) makes GMDSS-compliant equipment mandatory on all merchant vessels with more than 300 Gross Tonnage (GRT).

VSAT

Very Small Aperture Terminal (VSAT) systems use satellite transponders, usually operating at C-band and Ku-band, to transmit data, video, or voice.

BGAN

Broadband Global Area Network (BGAN) is a global Satellite Internet and voice network. Built-in security options make this service suitable for military operations.

BGAN M2M

This global, two-way IP data service is designed for long-term machine-to-machine (M2M) management of fixed assets. It is popular in the Industrial Control Systems (ICS) sector as well as for SCADA applications.

FB

FleetBroadband (FB) is an IP-based, broadband data and voice maritime satellite system used for operational and crew communications. Modern navigation systems installed on ships, such as Electronic Chart Display and Information System (ECDIS), may rely on the data connection provided by this service to operate properly. An ECDIS is a computer-based navigation information system that complies with [International Maritime Organization](#) (IMO) regulations and can be used as an alternative to paper [nautical charts](#).

SwiftBroadband

This is an IP-based broadband data and voice aeronautical satellite system. It is approved by the International Civil Aviation Organization (ICAO) for aircraft safety services, playing an important role within the Future Air Navigation Systems (FANS).

Classic Aero Service

This is an aeronautical satellite communication system intended for voice, fax, and data. It includes these services:

- **Aero H** Multi-channel voice, 10.5kbps fax and data, delivered via a high-gain antenna within the satellites' global beams. ICAO approved for safety services.
 - **Aero H+** Multi-channel voice, 10.5kbps fax and data, delivered via a high-gain antenna within the spot beams of the Inmarsat-3 satellites and the full footprint of the Inmarsat-4 Atlantic Ocean Region (AOR) satellite, at a lower cost per connection. ICAO approved for safety services.
 - **Aero I** Multi-channel voice, 4.8kbps circuit-mode data and fax, delivered via an intermediate-gain antenna. Also supports low-speed packet data.
-

Available in the spot beams of the Inmarsat-3 satellites and the full footprint of the Inmarsat-4 AOR satellite. ICAO approved for safety services.

- **Mini M Aero** Single-channel voice, fax or 2400bps data, for general aviation and smaller corporate aircraft.

Study Scope

Due to multiple constraints of our initial research scope, it was not feasible to acquire each target device. In most cases, IOActive conducted this research without physical access to the actual equipment. Instead, we performed static firmware analysis by reverse engineering all of the devices. Our research was not intended to stress the software in search of common memory corruptions, but rather to understand the devices' native security strengths and weaknesses.

IOActive found that a malicious actor could abuse all devices within the scope of this research. We uncovered vulnerabilities that appear to be multiple backdoors, hardcoded credentials, undocumented and/or insecure protocols, and weak encryption algorithms. These vulnerabilities allow remote, unauthenticated attackers to compromise the affected products. In certain cases, no user interaction is required to exploit the vulnerability; just sending a simple SMS or specially crafted message from one ship to another ship would be successful for some of the SATCOM systems.

In addition to design flaws, IOActive also uncovered deliberately introduced features in the devices that clearly pose security risks.

This document explains how attackers could leverage these vulnerabilities to perform different kinds of attacks. Every scenario is based on vendor-provided documentation as well as real-world deployments.

Methodology

The approach was focused on two critical key areas:

- Information gathering
- Reverse engineering

Information Gathering

The best way to find a way to compromise the security of a system is by understanding how it works. As a result, information gathering is a fundamental piece. During this phase, we collected as much information as possible about the target through Open Source Intelligence.

IOActive looks for information that can be used to build a model of the equipment. Some of the contents we look for are:

- Datasheets
- Implementation and support guides
- Success cases
- Manuals
- Public procurements
- Press releases
- Multimedia material (videos, presentations, pictures..)
- Software/firmware

Everything is carefully analyzed and evaluated. The information extracted from this phase should allow the researcher to respond a series of four basic questions:

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

At this point, we are able to accurately estimate the attack surface and build a map of features. Having a detailed list of functionalities provides an invaluable help for the reverse engineering phase.

Reverse Engineering

We are facing a scenario where the main target, the physical device, may be inaccessible. Thus, we have to compensate this disadvantage by enforcing the analysis of two fundamental components:

- Configuration software
 - Firmware
-

Configuration Software

Vendors usually provide customers with client-side software to configure and control the equipment. By reverse engineering these programs we can understand how the target expects to communicate with the outside world and the kind of protocols and/or proprietary mechanisms involved in this process.

IOActive often develops a simulated device to trick the configuration software into thinking it is actually connected to a real device. We leverage this environment to collect the set of inputs that a device supposedly accepts, as well as the outputs the configuration software expects. This data is later on leveraged to analyze the firmware.

Firmware

While the configuration software is usually built for three main platforms: Windows, Mac, or Linux, the firmware is more heterogeneous. There are many components: Multiple Real Time Operating Systems (RTOS), processors, boards, chips, peripherals, interfaces, and so on.

This makes the analysis of the firmware a time consuming task, which requires very specific knowledge. The basic approach involves reconstructing symbols, string references, and memory maps. Then, the firmware is reverse engineered in order to

- Map functionalities to code.
- Discover undocumented functionalities
- Discover how the different components talk to each other
- Identify entry points

In certain cases, it is possible to emulate specific pieces of code present in the firmware, so even without access to the physical device, we can detail how some features are actually implemented.

At that point, we have achieved a solid understanding on the internals of the firmware so it is possible to look for security issues and elaborate attack vectors.

This methodology for static analysis of embedded devices has been successfully used many times. As a result, IOActive has uncovered serious vulnerabilities in equipment used in industrial control systems, satellite communications or advanced metering infrastructures.

Table 1: Summary of Vulnerabilities

Vendor	Product	Vulnerability Class	Service	Severity
Harris	 RF-7800-VU024 RF-7800-DU024	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	 9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	 ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	 EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical
Cobham	 SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	 AVIATOR 700 (E/D)	Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Cobham	 SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobham	 SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	 JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Iridium	 Pilot/OpenPort	Hardcoded Credentials Undocumented Protocols	Iridium	Critical

Impact

Table 1 summarizes the types of vulnerabilities IOActive uncovered during this research phase. The threats posed by these vulnerabilities deserve calm, measured analysis. That said, from a technical perspective, it is not wise for commercial entities to downplay the severity of the risks to businesses dependent upon the integrity and secrecy of such communications. As explained in the introduction, some of the services these products access are critical from a safety perspective.

Vulnerability Classes

Backdoors

Mechanisms used to access undocumented features or interfaces not intended for end users.

Hardcoded Credentials

Undocumented credentials that can be used to authenticate in documented interfaces expected to be available for user interaction.

Insecure Protocols

Documented protocols that pose a security risk.

Undocumented Protocols

Undocumented protocols, or protocols not intended for end users, that pose a security risk.

Weak Password Reset

Mechanism that allows resetting other's passwords.

Attack Scenarios Against Harris BGAN Terminals



Figure 1: Land Portable and Land Mobile Harris BGAN Terminals

Both land portable and land mobile Harris BGAN terminals are intended for use by the military. The main purpose of these terminals, such as the RF-7800B, is to provide enhanced tactical radio network capabilities. They are used in conjunction with software-defined radios (SDRs), such as the FALCON III® AN/PRC-117G SDR shown in Figure 2.



Figure 2: AN/PRC-117G SDR

When the RF-7800B BGAN terminal is combined with the AN/PRC-117G SDR, the terminal operates simultaneously with the ANW2 waveform, providing beyond-line-of-sight (BLOS) communications. The system provides range extension of ANW2 networked data.

Harris' documentation contains a practical example:

For example, consider an attack on a convoy in the mountains. Such an event requires an immediate reaction from many different units. Previously, this response was pieced together through fragmented systems.

By leveraging a network of AN/PRC-117G radios, commanders would be able to launch and coordinate an immediate response using some or all of the following applications:

- Streaming video: Commanders would be able to analyze reconnaissance feeds from cameras, both on the ground and in their air, to plan their response.
 - Legacy interoperability: Quick Reaction Force teams would be able to call for close-air support for a counter attack.
 - Text messaging: Convoy personnel would be able to send details via text messaging, limiting confusion and removing traffic from voice networks.
-

- Satellite communications: The radio will support reach-back capability through satellite communications to connect warfighters to brigade headquarters."

This example matches Harris' tactical schema, shown in Figure 3.

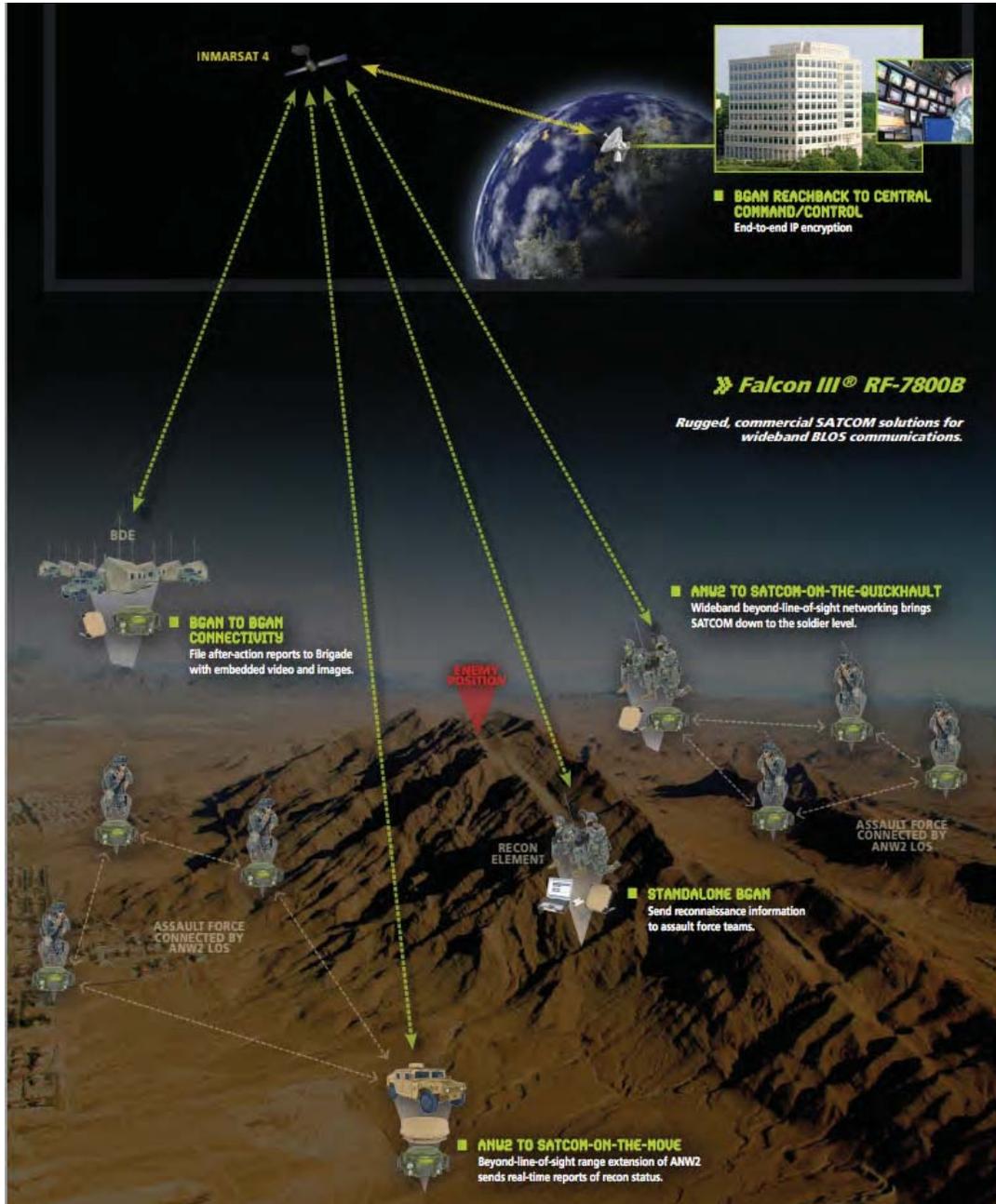


Figure 3: Harris' Tactical Schema

The vulnerabilities IOActive found in the RF-7800B terminal allow an attacker to install malicious firmware or execute arbitrary code. A potential real-world attack could occur as follows:

1. By exploiting the vulnerabilities listed in Table 1, an attacker injects malicious code into the terminal. Malware running on an infected laptop connected to the terminal, as shown in Figure 4, could deploy this payload.



Figure 4: System Components, Including Laptop

2. The malicious code uses the built-in GPS to obtain the coordinates where the system is located. This would allow the attacker to compare the system's position with a fixed area (target zone) where an attack from enemy forces is planned.
3. If a Packet Data Protocol (PDP) context is detected or the system enters the target zone, the malicious code disables communications or even damages the terminal.
4. The ability of the victims to communicate vital data or ask for support to perform a counter-attack is limited or even cut off. In the worst-case scenario, loss of lives is possible.

This kind of equipment is common within the forces of the North Atlantic Treaty Organization (NATO).

Attack Scenarios Against Hughes BGAN M2M Terminals



Figure 5: Hughes 9502 BGAN M2M Antenna and Indoor Unit

According to [Hughes' BGAN M2M Operational Scenarios document](#), the satellite user terminal (UT) can be controlled remotely via SMS messages or AT commands as shown in Figure 6 and Figure 7.

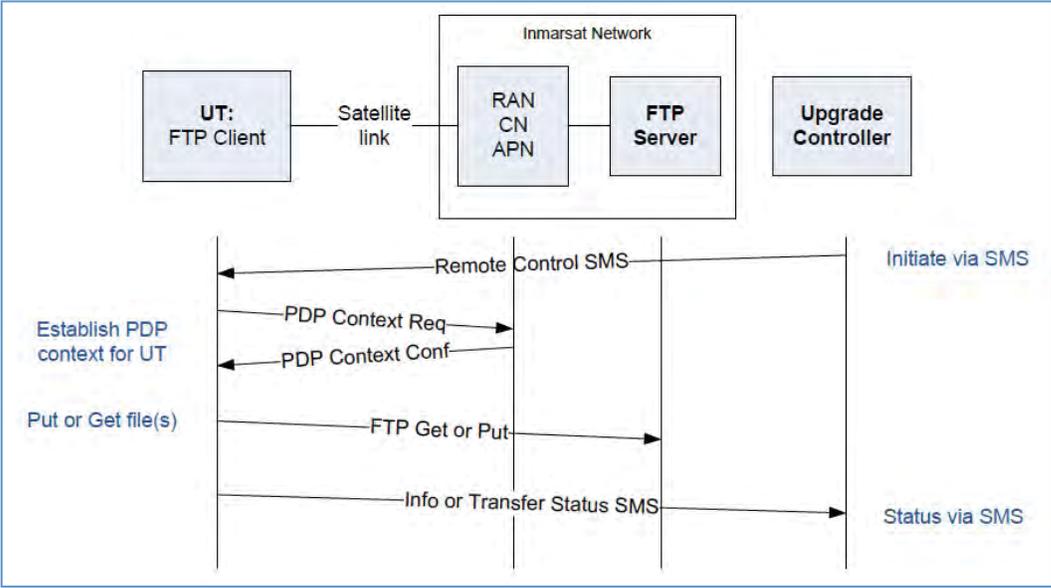


Figure 6: Remote Control of the Hughes BGAN M2M UT via SMS

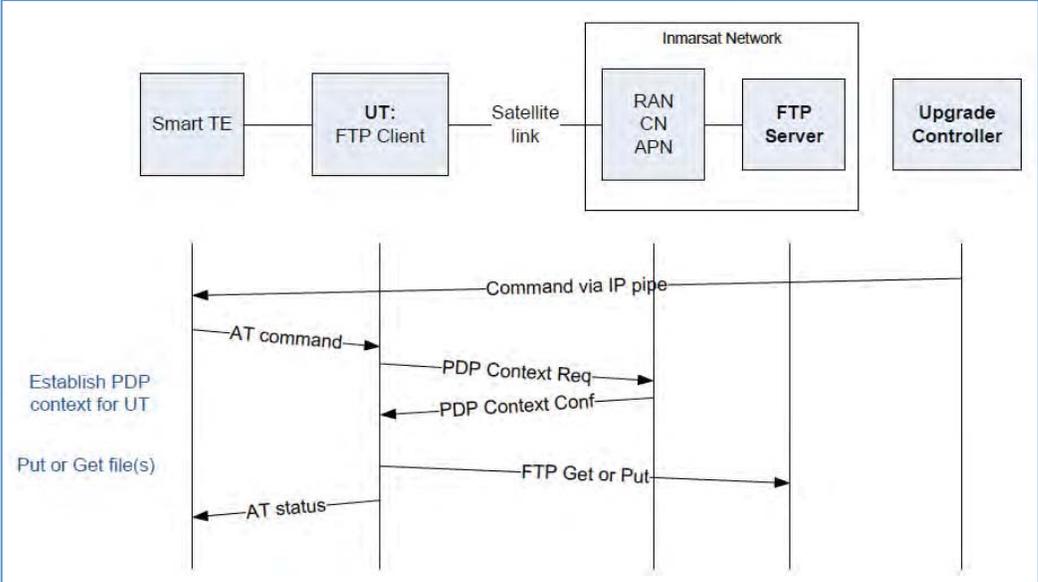


Figure 7: Remote Control of the HUGHES BGAN M2M UT via AT Commands

As Figure 7 illustrates, AT commands can be sent using Smart Terminal Equipment (TE) controlled via the IP pipe over the PDP context.

The following two scenarios describe how an attacker could compromise the UT by exploiting the vulnerabilities listed in Table 1.

Scenario One

An attacker with access to the Smart TE, either directly or via malware, could exploit the ‘admin code’ backdoor when ‘Enhanced Security’ is activated. The attacker could also leverage the undocumented ‘Zing’ protocol.

Scenario Two

An attacker already knows the Mobile Subscriber Integrated Services Digital Network-Number (MSISDN) and International Mobile Station Equipment Identity (IMEI) of the UT. By generating the backdoor ‘admin code’, an attacker can send an SMS containing an encapsulated AT command to install malicious firmware.

According [Inmarsat’s Channel Sales presentation](#), the Hughes 9502 BGAN M2M is deployed in six target markets, shown in Figure 8.

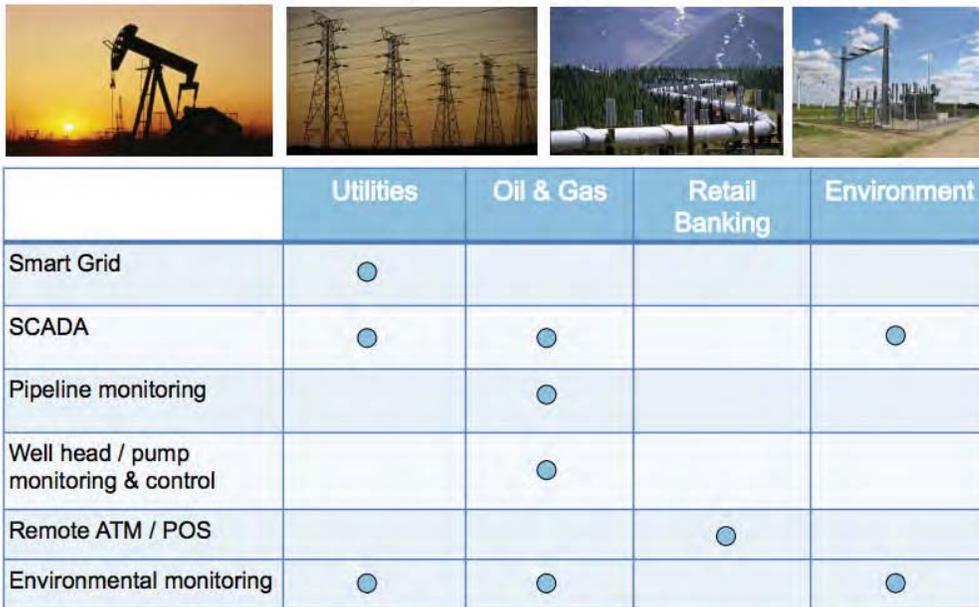


Figure 8: Hughes BGAN M2M Target Market Overview

A successful attack against Hughes BGAN M2M terminals can have these impacts:

- Fraud
- Denial of service
- Physical damage
- Data spoofing

Attack Scenarios Against Cobham BGAN Terminals

More than two-thirds of the Inmarsat satellite terminals currently in use belong to the Explorer family, manufactured by Cobham (formerly Thrane & Thrane). An attacker can take complete control of these devices by exploiting a weakness in their authentication mechanism using either direct access or scripted attacks (malware).

Cobham Explorer terminals are deployed in multiple sectors. Attacks against these communication devices would have different impacts depending on the specific application. The following images below come from the documentation that vendors and integrators provide to illustrate case studies.



Figure 9: Military Use



Figure 10: Emergency Services and Field Operations



Figure 11: Life Saving Equipment



Figure 12: Personal Communications for the Military

Scenario: Personal Communications for the Military as Attack Vector

Historically, tracking the position of military units has provided the adversary with vital information about the units' objectives and tactical approach. If a member of a unit was targeted with a client-side exploit while browsing the Internet during personal communications time, an attacker would be able to install malicious firmware in the terminal. The attacker's code could then take advantage of the terminals' built-in GPS receiver to leak its position in real-time.

There have been significant examples of this kind of exposure:

- [US Army: Geotagged Facebook posts put soldiers' at risk](#)
- [The Israeli military cancelled a planned raid on a Palestinian village after one of its soldiers posted details of the operation on Facebook](#)

Attack Scenarios Against Marine VSAT and FB Terminals



Figure 13: Cobham SAILOR 900 VSAT and JRC JUE-250 FB Terminals

The Cobham SAILOR 900 VSAT, Cobham Sailor FB and JRC JUE-250/500 FB terminals are both deployed on ships as part of a satellite communication system or an Inmarsat FB system, as shown in Figure 14.

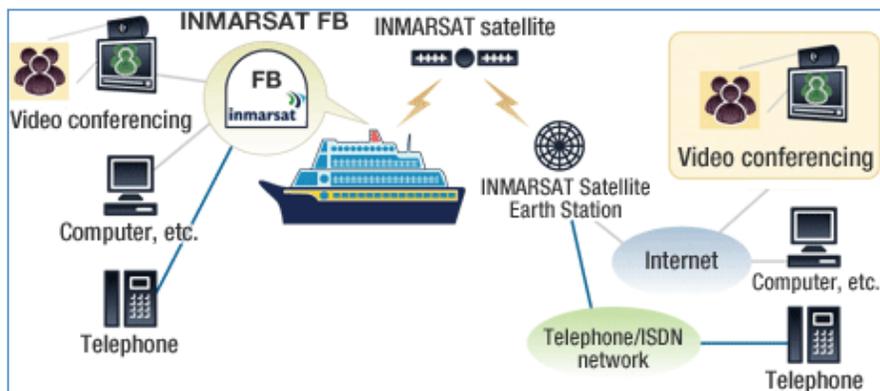


Figure 14: Inmarsat FB System

Numerous services use the satellite link:

- Telephone, ISDN, SMS, and VoIP
- Broadband Internet
- Email and file transfer
- Multi-voice
- Video conferencing
- Safety 505 and red button
- Notice to mariners
- Maritime/port regulations
- ECDIS
- Vessel routing
- Cargo management
- Planned/Predictive maintenance
- Radio over IP (RoIP) via walkie talkie

-
- VHF/UHF radio integration
 - Crew welfare
 - Telemedicine
 - Tele-training/certification
 - Weather forecasts

Compromising one of these terminals would give an attacker full control over all of the communications that pass through the satellite link.

Scenario One: Navigation Charts

The vulnerabilities in these terminals make attacks that disrupt or spoof information consumed by the on-board navigations systems, such as ECDIS, technically possible, since navigation charts can be updated in real time via satellite.

Scenario Two: Operational Integrity

The ability to control the satellite link of a vessel can be used to put the operational integrity of cargo vessels at risk. SATCOM links are often used to track the status and condition of container ships while in transit. This is especially important when transporting sensitive goods such as munitions or hazardous chemical products. The operational information enables the cargo's owner to take proper action and address any potential situation.

Attack Scenarios Against Cobham AVIATOR

The Cobham AVIATOR family is designed to meet the satellite communications needs of aircraft, including those related to safety operations. Figure 15 illustrates a [US military aircraft](#) equipped with this product.



Figure 15: US Air Force C-130J Super Hercules

Aircraft safety is highly dependent on the redundancy and accuracy of on-board systems. When it comes to aircraft, software security is not an added value but a mandatory requirement. International certification authorities provide a series of standards that represent the industry consensus opinion on the best way to ensure safe software, such as the Radio Technical Commission for Aeronautics (RTCA) specification DO-178B or the European Organization for Civil Aviation Equipment (EUROCAE) ED-12B

These regulatory standards define five levels of failure conditions, categorized by their effects on the aircraft, crew, and passengers:

Level A–Catastrophic

Failure may cause multiple fatalities, usually with loss of the airplane.

Level B–Hazardous

Failure has a large negative impact on safety or performance, reduces the ability of the crew to operate the aircraft due to physical distress or a higher workload, or causes serious or fatal injuries among the passengers.

Level C–Major

Failure significantly reduces the safety margin or significantly increases crew workload. May result in passenger discomfort (or even minor injuries).

Level D–Minor

Failure slightly reduces the safety margin or slightly increases crew workload. Examples might include causing passenger inconvenience or a routine flight plan change.

Level E–No Effect

Failure has no impact on safety, aircraft operation, or crew workload.

Software approved to levels A, B, or C requires strong certification involving formal processes for verification and traceability. Software approved to levels D or E is subject to a more ‘relaxed’ control.

Although the failure condition levels are intended to cover not only the software as a standalone entity, but also as part of a more complex system, some claim that there is room for improvement. The main concerns seem to be related to interactions between equipment at different levels.

IOActive was able to demonstrate that it is possible to compromise a system certified for level D that interacts with devices certified for level A, potentially putting the level A devices’ integrity at risk.

The AVIATOR 700 system is available in two versions:

- AVIATOR 700 approved to RTCA specification DO-178B level E and DO-254 level E
- AVIATOR 700D approved to RTCA specification DO-178B level D and DO-254 level D

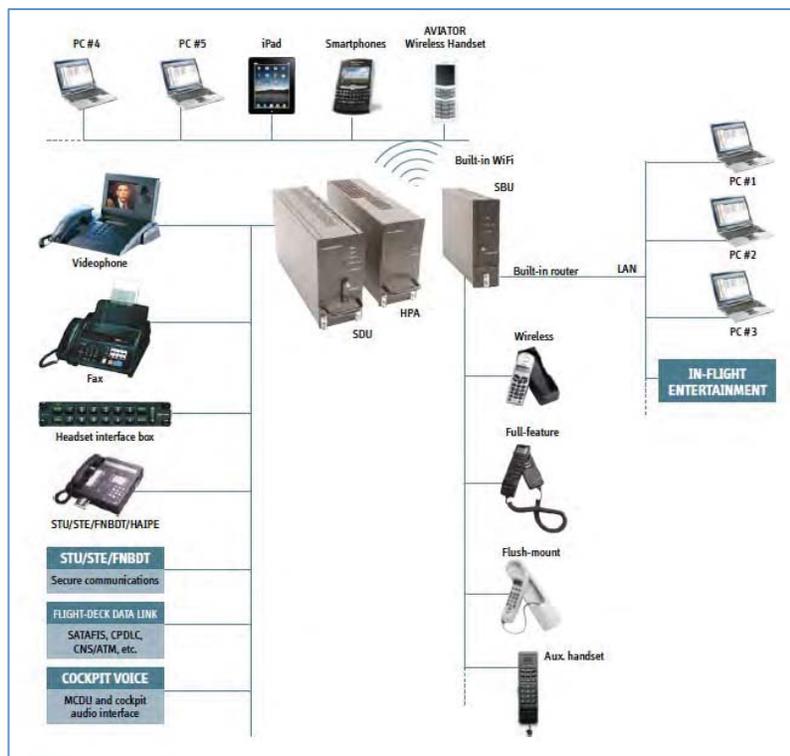


Figure 16: AVIATOR 700 System Interactions

Both versions of the AVIATOR 700 operate in complex systems with multiple interfaces to other systems on board; however, only the AVIATOR 700D level D is approved for safety purposes.

The vulnerabilities listed in Table 1 could allow an attacker to take control of both the SwiftBroadband Unit (SBU) and the Satellite Data Unit (SDU), which provides Aero-H+ and Swift64 services. IOActive found vulnerabilities an attacker could use to bypass authorization mechanisms in order to access interfaces that may allow control of the SBU and SDU. Any of the systems connected to these elements, such as the Multifunction Control Display Unit (MCDU), could be impacted by a successful attack. More specifically, a successful attack could compromise control of the satellite link channel used by the Future Air Navigation System (FANS), Controller Pilot Data Link Communications (CPDLC) or Aircraft Communications Addressing and Reporting System (ACARS). A malfunction of these subsystems could pose a safety threat for the entire aircraft.



Figure 17: The SDU (Level D) Interacts with the MCDU (Level A Component Present in the Cockpit)

Attack Scenarios Against Cobham GMDSS Terminals

GMDSS was briefly discussed in the description of Inmarsat-C services. The complete GMDSS regulation is defined in Chapter IV of the SOLAS convention. Under this international agreement, every GMDSS-equipped ship, while at sea, must be capable of:

- Transmitting ship-to-shore distress alerts by at least two separate and independent means, each using a different radio communication service
- Receiving shore-to-ship distress alerts
- Transmitting and receiving ship-to-ship distress alerts
- Transmitting and receiving search and rescue coordinating communications
- Transmitting and receiving on-scene communications
- Transmitting and, as required by regulation V/19.2.3.2, receiving signals for locating
- Transmitting and receiving maritime safety information
- Transmitting and receiving general radio communications to and from shore-based radio systems or networks subject to regulation 15.8
- Transmitting and receiving bridge-to-bridge communications

SOLAS establishes the type of radio communications systems that a ship needs, in order to be GMDSS compliant. This requirement depends on the ship's area of operation as illustrated in Figure 18.

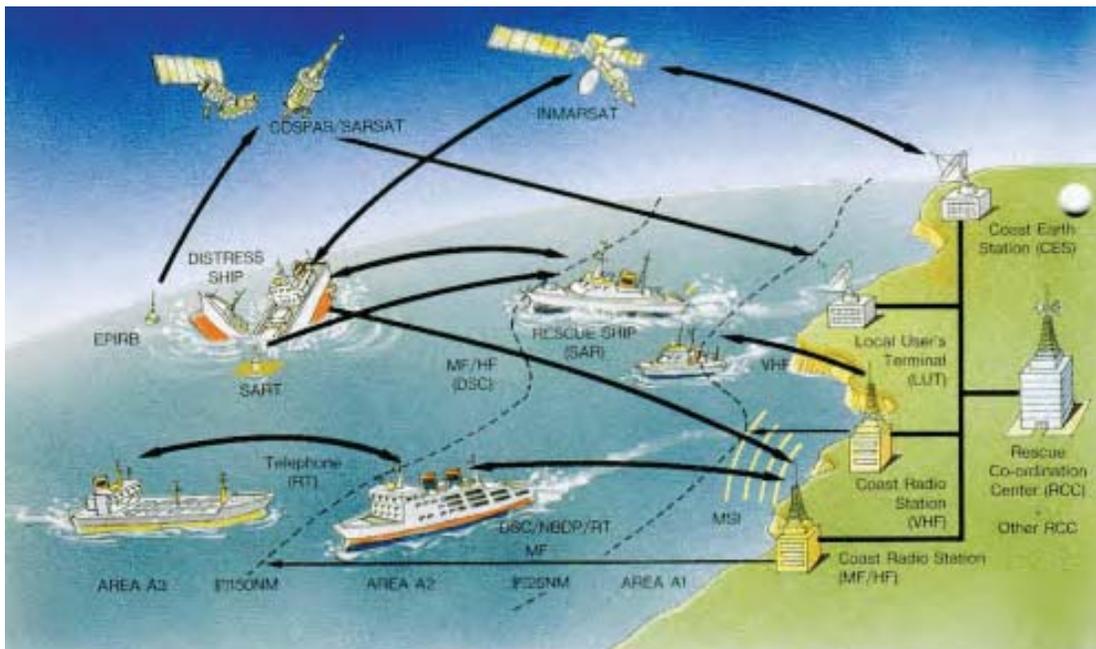


Figure 18: Sea Areas for GMDSS Communication Systems

There are four sea areas:

- **A1** An area within the radio telephone coverage of at least one VHF coast station in which continuous DSC alerting is available (20–30 nautical miles)
- **A2** An area, excluding the previous one, within the radio telephone coverage of at least one MF coast station in which continuous DSC alerting is available (approximately 100/150 nautical miles).
- **A3** An area, excluding A1 and A2, within the coverage of an Inmarsat geostationary satellite in which continuous alerting is available.
- **A4** An area outside sea areas A1, A2, and A3.

Cobham SAILOR 6000 is a GMDSS-compliant communications suite which provides the equipment specified by SOLAS.

The basic equipment includes:

- A VHF radio
- One SART if under 500 GRT, 2 SARTs if over 500 GRT
- Two portable VHF transceivers for use in survival craft if under 500 GRT, three if over 500 GRT
- A NAVTEX receiver, if the ship is engaged on voyages in any area where a NAVTEX service is provided
- An Inmarsat Enhanced Group Call (EGC) receiver, if the ship is engaged on voyages in any area of Inmarsat coverage where Marine Safety Information (MSI) services are not provided by NAVTEX or HF NBDP
- A 406 MHz Emergency Position-Indicating Radio Beacon (EPIRB)

Additional equipment includes:

 <p>SAILOR A2 solution</p>	<ul style="list-style-type: none">1 SAILOR 630x MF/HF Control Unit1 SAILOR 62xx VHF Radio
 <p>SAILOR A3 solution</p>	<ul style="list-style-type: none">1 SAILOR 630x MF/HF Control Unit1 SAILOR 62xx VHF Radio1 SAILOR H1252B USB/Parallel Printer1 SAILOR 6006 Message Terminal
 <p>SAILOR A4 solution</p>	<ul style="list-style-type: none">1 SAILOR 630x MF/HF Control Unit1 SAILOR 62xx VHF Radio2 SAILOR H1252B USB/Parallel Printer2 SAILOR 6006 Message Terminal
 <p>SAILOR A4 solution</p>	<ul style="list-style-type: none">2 SAILOR 630x MF/HF Control Unit3 SAILOR H1252B USB/Parallel Printer3 SAILOR 6006 Message Terminal

IOActive found that the insecure 'thraeLINK' protocol could be leveraged to compromise the entire SAILOR 6000 communications suite, posing a critical threat to the ship's safety. An attacker can install malicious firmware in order to control devices, spoof data, or disrupt communications.

The Ship Security Alert System (SSAS) is also impacted by the vulnerabilities IOActive discovered in the Inmarsat Mini-C terminal.

The SSAS is part of the International Ship and Port Facility Security (ISPS) code and contributes to the IMO's efforts to strengthen maritime security and suppress acts of terrorism and piracy. In case of attempted piracy or terrorism, the ship's SSAS beacon can be activated and appropriate law-enforcement or military forces will be dispatched. Once a SSAS alert has been triggered, the following protocol is applied:



- Rescue Coordination Centers or SAR Points of Contact for the country code the beacon is transmitting are discreetly notified.
- National authorities dispatch appropriate forces to deal with the terrorist or pirate threat.

As a result of the security flaws listed in Table 1, an attacker can remotely disable the SSAS by sending a series of specially crafted messages to the target ship. No user interaction is required.

An attacker successfully exploiting any of the SSAS and GMDSS vulnerabilities may be able to:

- Provide false information to trick crew into altering routes
 - Spoof or delete incoming communications such as Distress calls from other ships, weather warnings, or any other EGC message
 - Render devices unusable, effectively disrupting communications and leaving a vessel without the ability to interact with the outside world
 - Remotely disable safety systems before attacking a ship
 - In the worst-case scenario, loss of lives is possible.
-

Conclusion

Considering the sectors where these products are deployed and the affected vendors, the specific nature of the vulnerabilities IOActive uncovered is of great concern.

The current status of the products IOActive analyzed makes it almost impossible to guarantee the integrity of thousands of SATCOM devices. Appropriate action to mitigate these vulnerabilities should be taken. Owners and providers should evaluate the network exposure of these devices, implement secure policies, enforce network segmentation, and apply restrictive traffic flow templates (TFT) when possible. Until patches are available, we encourage vendors to provide official workarounds in addition to recommended configurations in order to minimize the risk these vulnerabilities pose.

If one of these affected devices can be compromised, the entire SATCOM infrastructure could be at risk. Ships, aircraft, military personnel, emergency services, media services, and industrial facilities (oil rigs, gas pipelines, water treatment plants, wind turbines, substations, etc.) could all be impacted by these vulnerabilities.

Acknowledgements

1. IOActive, Inc.
2. CERT Coordination Center <http://cert.org/>

References

Related CERT Coordination Center advisory <http://www.kb.cert.org/vuls/id/250358>

All images copyright their respective owners, as indicated

1. Figures 1–4: <http://rf.harris.com>
2. Figures 5–8: <http://www.hughes.com/>
3. Figures 9–12: Cobham/Thrane&Thrane
4. Figures 14: <http://www.kddi.com>
5. Figure 17: Cobham/Thrane&Thrane

About IOActive

IOActive is a comprehensive, high-end information security services firm with a long and established pedigree in delivering elite security services to its customers. Our world-renowned consulting and research teams deliver a portfolio of specialist security services ranging from penetration testing and application code assessment through to semiconductor reverse engineering. Global 500 companies across every industry continue to trust IOActive with their most critical and sensitive security issues. Founded in 1998, IOActive is headquartered in Seattle, USA, with global operations through the Americas, EMEA and Asia Pac regions. Visit www.ioactive.com for more information. Read the IOActive Labs Research Blog: <http://blog.ioactive.com/>. Follow IOActive on Twitter: <http://twitter.com/ioactive>.

Vulnerability Note VU#250358

Hughes Network Systems Broadband Global Area Network (BGAN) satellite terminal firmware contains multiple vulnerabilities

Original Release date: 31 Jan 2014 | Last revised: 14 Aug 2014

Overview

Firmware developed by Hughes Network Systems used in a number of BGAN satellite terminals contains undocumented hardcoded login credentials (CWE-798). Additionally, the firmware contains an insecure proprietary communications protocol, likely a debugging service, that allows unauthenticated local network users to perform privileged operations on the device (CWE-306).

Description

CWE-798: Use of Hard-coded Credentials - CVE-2013-6034

Firmware developed by Hughes Network Systems and used in numerous broadband satellite terminals contain hardcoded login credentials. Most of these devices are utilized for broadband connectivity through the Inmarsat satellite telecommunications network.

CWE-306: Missing Authentication for Critical Function - CVE-2013-6035

Additionally, these devices accept unauthenticated connections on TCP port 1827 from the local ethernet port. This port utilizes an insecure proprietary protocol which can be used to perform privileged operations on the device, such as reading and writing arbitrary memory. An unauthenticated local attacker could leverage this protocol to execute arbitrary code on vulnerable devices.

The satellite terminals from the following vendors use the affected firmware, however specific implementations may vary the exploitability of these vulnerabilities.

Harris Corporation:

- BGAN RF-7800B-VU204
- BGAN RF-7800B-DU204

Hughes Network Systems:

- 9502
- 9201
- 9450

Thuraya Telecommunications Company:

- IP

Japan Radio Corp., Ltd.:

- JUE-250
- JUE-500

CERT/CC has confirmed that the affected firmware is developed by Hughes Network Systems. GateHouse produces a BGAN network stack that is licensed to Hughes Network Systems, but the GateHouse software does not provide either of the vulnerable features. Please see the "Vendor Information" below for more details.

The CVSS score reflects CVE-2013-6035.

Impact

Depending on implementation, an unauthenticated attacker may be able to gain privileged access to the device. Additionally, an unauthenticated attacker on the local network may be able to execute arbitrary code on the device.

Solution

We are currently unaware of a practical solution to this problem.

Vendor Information [\(Learn More\)](#)

Vendor	Status	Date Notified	Date Updated
Harris Corporation	Affected	25 Nov 2013	24 Jun 2014
Hughes Network Systems, Inc.	Affected	10 Oct 2013	24 Jun 2014
GateHouse	Not Affected	11 Dec 2013	06 Jun 2014
Inmarsat	Not Affected	10 Oct 2013	12 Jun 2014
Japan Radio Co Ltd	Unknown	10 Oct 2013	25 Nov 2013
Thuraya	Unknown	10 Oct 2013	25 Nov 2013

If you are a vendor and your product is affected, let us know.

CVSS Metrics [\(Learn More\)](#)

Group	Score	Vector
Base	5.7	AV:A/AC:M/Au:N/C:C/I:N/A:N
Temporal	4.8	E:U/RL:U/RC:C
Environmental	1.2	CDP:N/TD:L/CR:ND/IR:ND/AR:ND

References

- <http://rf.harris.com/capabilities/tactical-radios-networking/rf-7800b/default.asp>
- <http://www.hughes.com/technologies/mobilesat-systems/mobile-satellite-terminals>
- <http://www.thuraya.com/thuraya-ip>
- http://www.jrc.co.jp/eng/product/marine/application/comm_inmarsat.html

- <http://www.inmarsateu.net/>
- <http://www.inmarsat.com/Support/detailsupport/bgan/Firmware/index.htm>
- <http://www.inmarsat.com/Support/detailsupport/FleetBroadband/Firmware/index.htm>
- http://www.thuraya.com/product_upgrades/41
- <http://www.gatehouse.dk/>
- <http://www.inmarsat.com/service/bgan/>
- <http://en.wikipedia.org/wiki/BGAN>

Credit

Thanks to IOActive researcher Ruben Santamarta for reporting this vulnerability.

This document was written by Todd Lewellen and Chris King.

Other Information

CVE IDs: CVE-2013-6034 CVE-2013-6035

Date Public: 31 Jan 2014

Date First Published: 31 Jan 2014

Date Last Updated: 14 Aug 2014

Document Revision: 67

Feedback

If you have feedback, comments, or additional information about this vulnerability, please send us email.