

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.

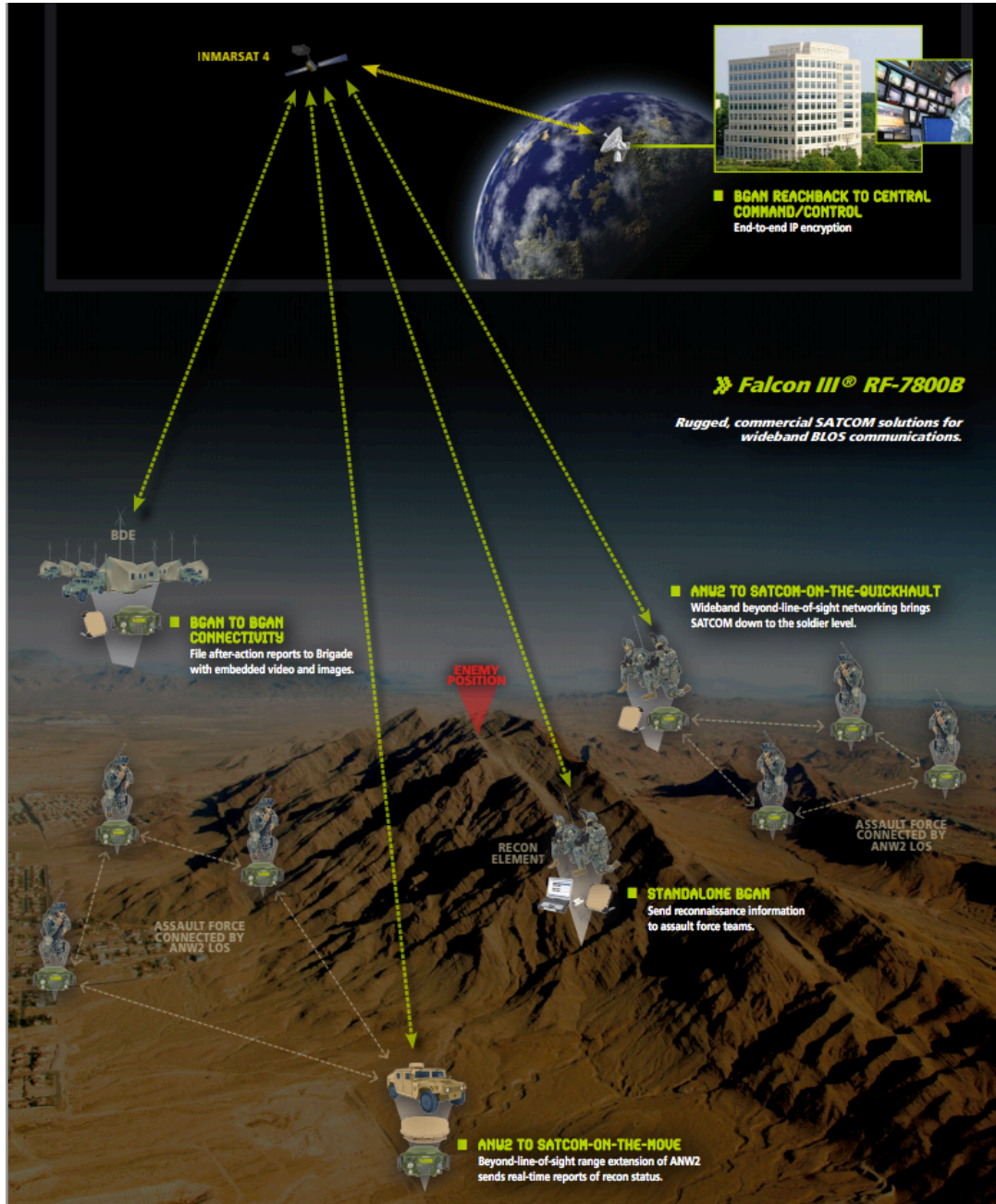


Figure 3: Harris' Tactical Schema

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

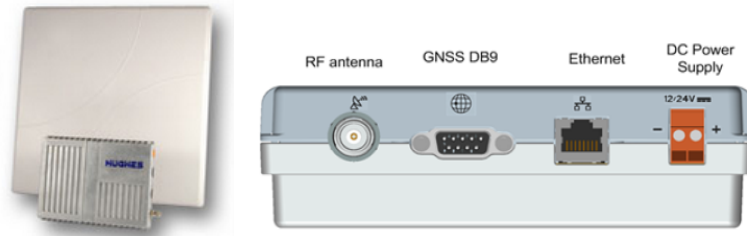


Figure 5: Hughes 9502 BGAN M2M Antenna and Indoor Unit

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.

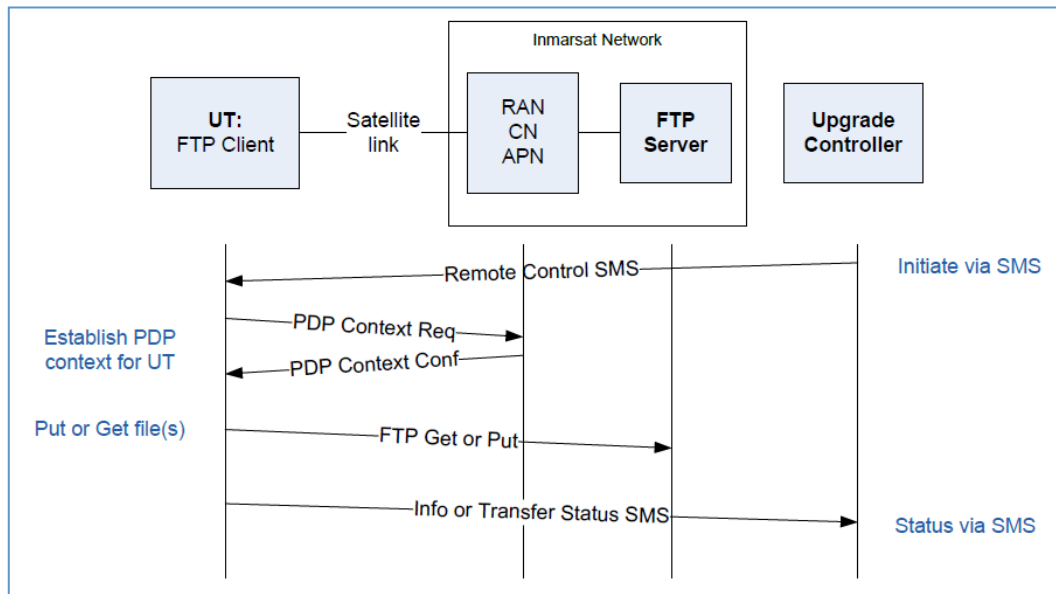


Figure 6: Remote Control of the Hughes BGAN M2M UT via SMS

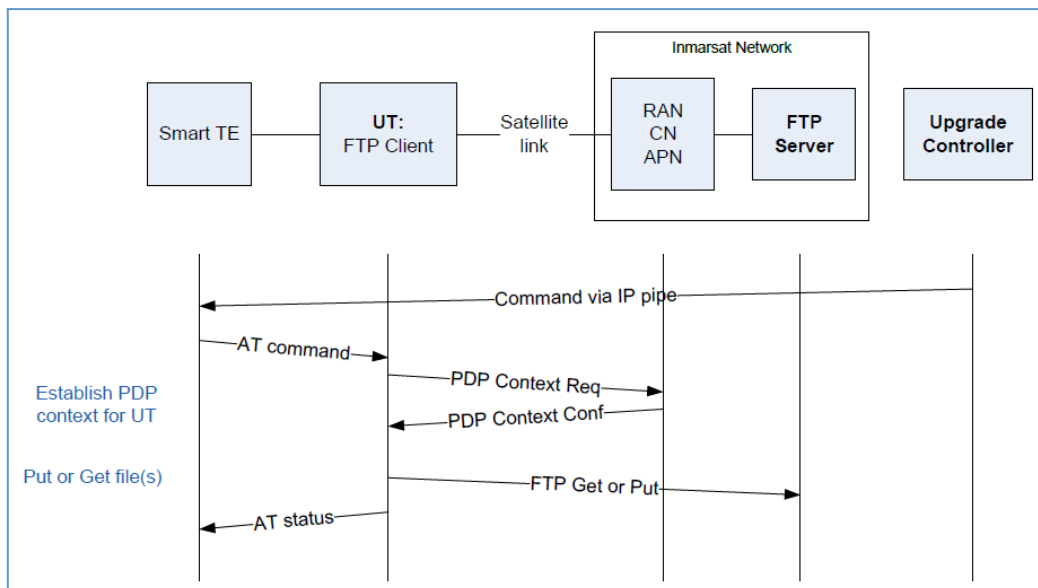


Figure 7: Remote Control of the HUGHES BGAN M2M UT via AT Commands

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.

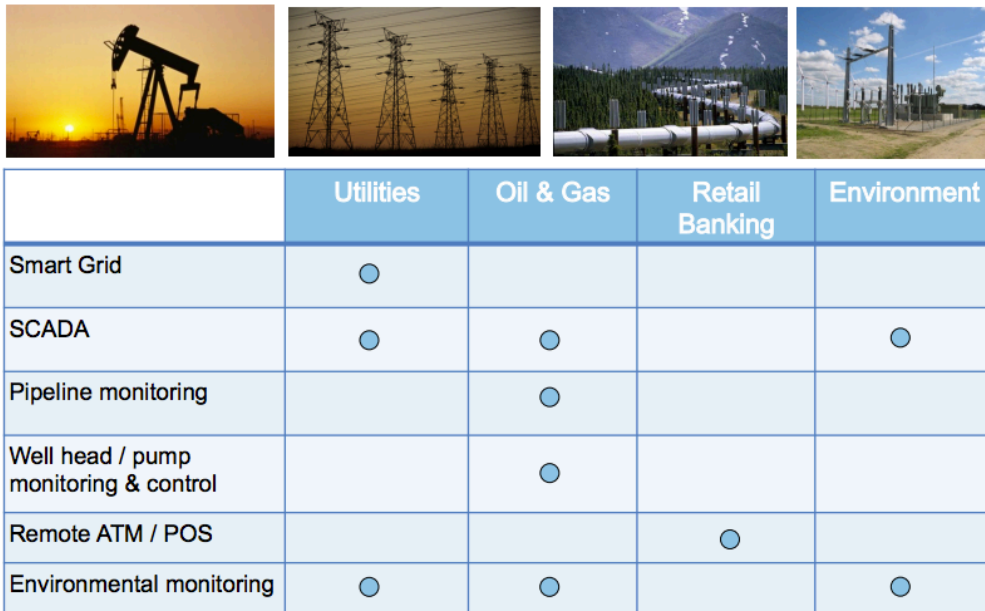


Figure 8: Hughes BGAN M2M Target Market Overview

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.

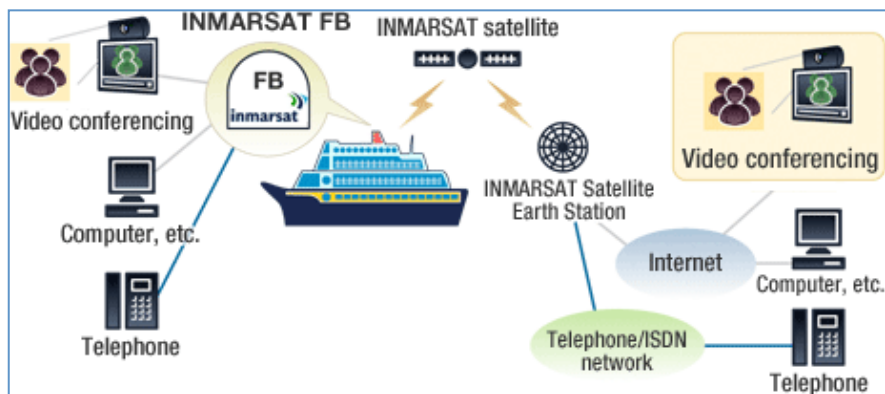


Figure 14: Inmarsat FB System

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

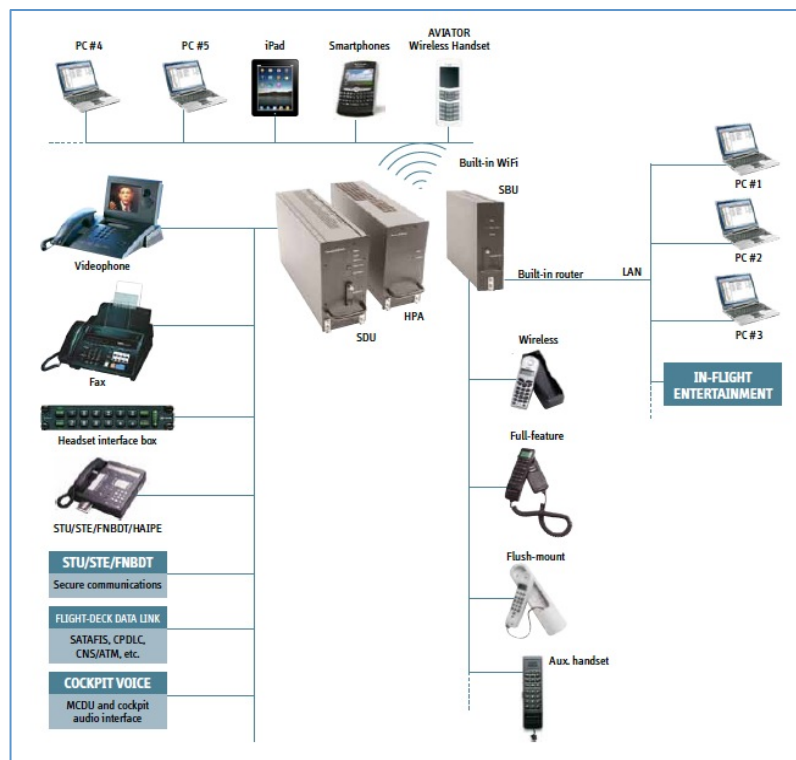


Figure 16: AVIATOR 700 System Interactions

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.

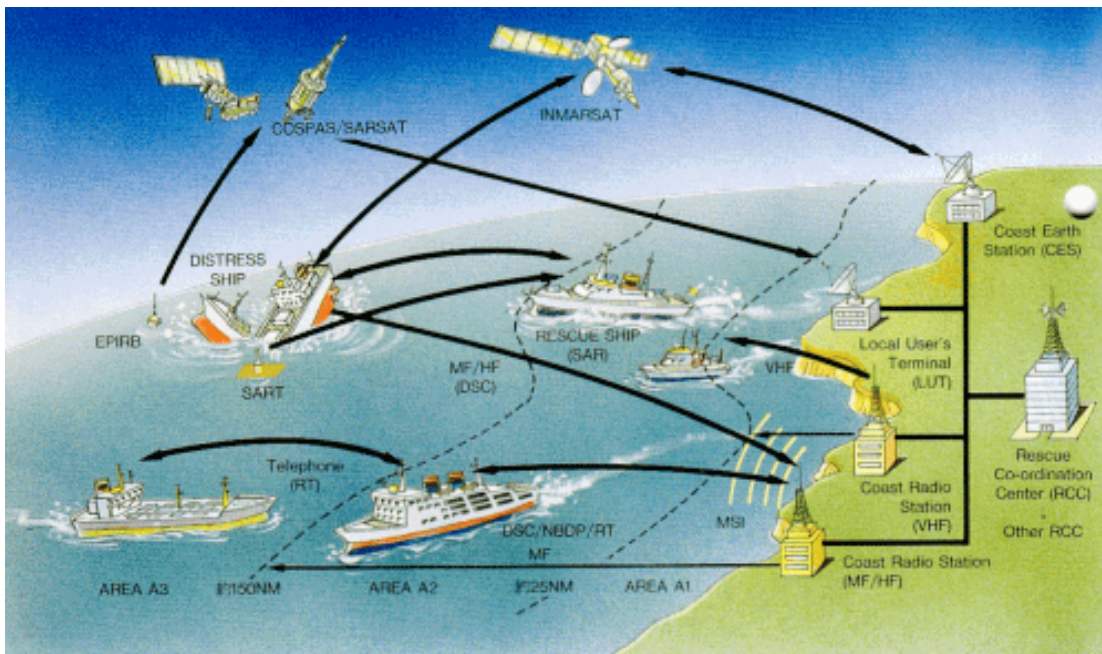


Figure 18: Sea Areas for GMDSS Communication Systems

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>.
