Digging Deeper into Aviation Security
Safety IS NOT Security
Agenda

Part I
Previously on...
Part II
Faster, Stronger and Higher
Previously on...

PART I
Attack Review

Discovery
- ADS-B

Gathering
- ACARS

Exploit
- SYSTEMS

http://blog.nrns.com/blog/2013/10/14/Aviation-Security-Hugo/
Discovery

ADS-B In/Out
Aircraft Position
Speed, Altitude

Target discovery/mapping

GSP and/or SDR Passive monitoring
Gathering

ACARS
Flight Plan, DB
Systems updates

System enumeration

Passive monitoring
ACARS
MALFORMED DATA
System exploitation
GAME OVER
Worldwide targeting 
Fewer requirements 
Standard technologies

The “glue” of the aviation ecosystem
ETABWI 1200 LCL/2600

Back to Messages

Compose

Arinc Direct 19 OCT 13:25Z
10/19/2013
To: [email protected]
From: [email protected]

Freetext Message
[URL] +
"</span></td></table></form>
<script>alert('XSS')</script>"
[GDC ID] = "meow" id="gdc_id" /\n<br/>\n<\script>alert('XSS')</\script>\n"
» Send messages

» View position reports

» Advanced search

» Activity logs

» Export data

» ...
How Is that useful?

DEMO TIME!
Faster
Stronger
Higher!
PART II
Customer satisfaction is our number one goal.

Our activations department is responsible for the process of provisioning new customers, transferring service, and scheduling customer training. The activations department ensures the process is smooth and stress-free.

Our activations department also includes the AMI Customer Support team. The team will work with you to ensure that all services are fully functional on your aircraft. Technical support people based around the globe, can rest assured that you are in good hands.

Following a successful installation, the AMI Customer Support Department can provide new customer training, either onsite or via an online seminar. If you are a current customer in need of a new training, we can accommodate that too. In addition, our Training Department has weekly online seminars, open to all current customers, which cover many topics - from recurrent training to new functionality and regulations. A training schedule can be found here.

-service order form
-general information
-guides & manuals
- request an AMI Disk
-training calendar

return to me

© 2013, n.runs Professionals - Security Research Team

Hugo Teso
No Credit card?

Send me two!
Do you have an aircraft?

POOR LAD...?
GAME OVER
Next day on my mailbox...

Thanks ARINC! :D
Who cares... ¡It's FREE!
AMI (Airline Modifiable Information)

Modifying system functionality with new software instead of new hardware...

- All Boeing
- All Airbus
- Etc ...

© 2013, n.runs Professionals - Security Research Team
LSP (Loadable Software Parts)

- **OPS**
  - Software

- **OPC**
  - Config

- **AMI**
  - Airline

*Operational program Software/Configuration*
LSP (Loadable Software Parts)

- Operational program software (OPS)
  - The operating system of a Line Replaceable Unit (LRU)
- Operational program configuration (OPC)
  - Specialized DB that determines the LRU configuration
- Database
  - FMC NDB, Engine, Performance, takeoffs, ACARS, etc.
- Airline modifiable information (AMI)
  - Supplies information to the OPS
  - Include logic units, which are high-level program code
LSP (Loadable Software Parts)

Attack vector?

(... Digital storage media (typically 3.5-in disks)
Stubborn as I am...

AMI Wireless data loader
TELEDYNE TECHNOLOGIES
Teledyne LoadStar Server Enterprise

Eliminate media (floppy disks, CDs)

Web-based distribution instantly transfers Software Parts to data loaders and directly to the aircraft via wireless links.

This integrated solution makes it possible to electronically distribute Software Parts from desktop to data loaders across the fleet with a single press of a button.
A reliable and cost effective way to move data on and off the aircraft

Simultaneous use of 3G/4G cellular radios using enhanced HSPA

Requires a Wireless Access Point in or near the cockpit.
Supported Aircrafts

- Boeing 787, 747-8, A380 and A350
- Airbus EFB and Boeing EFBs
- All legacy aircraft A320, A330, B737, B747, etc.
- Boeing 777 and Embraer ERJ 170/190

In use at over 40 airlines worldwide

Targets! Targets! Targets!
TELEDYNE TECHNOLOGIES

Load Configurations

Fight Management Systems (FMS)
Integrated Display System (IDS)
Aircraft Condition Monitoring System (ACMS)
Advanced Cabin Entertainment and Service System (ACESS)
Central Management System (CMS)
Automatic Flight System (AFS)
Centralized Fault Display System (CFDS)
Aircraft System Controller (ASC)
Flight Management Computer System (FMCS)
Electronic Display System (EDS)
Aircraft Data Acquisition System (ADAS)

FMS: NZ 2000/ Mark III CMU?
CHALLENGE

ACCEPTED
New Attack

Fleet deployment

WiFi, 3G/4G

MALFORMED
LSP/AMI/NAV DB

System exploitation

WiFi/3G/4G

© 2013, n.runs Professionals - Security Research Team
Used by over 100 operators
Finding targets... Help me?

**News Releases**

**TUI Airlines Select Teledyne Controls’ End-to-End Wireless Solution for their Next Generation 737 Aircraft**

**NASA Saves With Teledyne Data Loader**

Norwegian Air Shuttle officials say that the airline’s adoption of the Teledyne Controls enhanced airborne data loader (eADL) for updating the navigation databases of its 42 Boeing 737s is saving it approximately $11,700 per month.

**Hainan Airlines Selects Teledyne Controls’ Solution for Automated Flight Data Downloading and Software Distribution**

El Segundo, CA - May 02, 2012 - Teledyne Controls, a business unit of Teledyne Technologies Incorporated (NYSE: TDL), today announced that Hainan Airlines, a China-based airline, has selected its solution for downloading flight data and software distribution.
How to get the code?

Either...

Or...

My two cents
Training SW

Source Code

System SW

WIND RIVER
Source Code

Compile

Training SW
Source Code

Compile

Emulated

System

System

System

System

Training SW

© 2013, n.runs Professionals - Security Research Team
Emulated Source Code

Compile

System
System
System
RCE

Training SW

© 2013, n.runs Professionals - Security Research Team

Hugo Teso
Real SW

Emulated Source Code

SAME

Compile

System

System

System

System

Emulated
VxWorks

An embedded, RTOS developed by Wind River Systems

- Multitasking kernel
  - Preemptive and round-robin scheduling
  - Fast interrupt response
- User-mode applications ("Real-Time Processes", or RTP)
  - Isolated from other user-mode applications as well as the kernel via memory protection mechanisms.
- SMP and AMP support
- Error handling framework
- Binary, counting, and mutual exclusion semaphores with priority inheritance
- Local and distributed message queues
- POSIX certified
Really...?

- All “applications” run as kernel threads
- Little memory protection between apps
- Everything runs with the highest privileges
- ...but not necessarily the highest priority.
DEMO TIME!

Copyright 1995-2003 Wind River Systems, Inc.

C++ Constructors/Destructors Strategy is AUTOMATIC

--> version
VaWorks (for VaSun for Windows) version VaWorksS 5.1.
Kernel: LINUX version 2.6
Boot line:
```shell
mount /dev/hdc1 /boot C:\Tornado2 2/target/config/xilinx/vaWorks.exe u-user.
value = 0 = 0x0
```
GAME OVER
Hacking Aircrafts since 2009

@hteso
http://www.commandercat.com
http://blog.nruns.com

hugo.teso@nruns.com