Aircraft Hacking
Practical Aero Series
Agenda

✈ Part 1: The $PATH to the exploit
✈ Part 2: The $PATH to exploit

Disclaimer

✈ Time constraints
 » Too much to explain
   ✱ Aircrafts != Computers

✈ Safety reasons
 » Still too much to fix
Part 1
The $PATH$ to the exploit
The Target

In the beginning there was “The Question”

Would I be able to convert THIS... ...into THIS?
The Answer
Attack Overview

**DISCOVERY:**
- ADS-B

**INFO GATHERING:**
- ACARS

**EXPLOITATION:**
- Via ACARS
- Against on-board systems vulns.

**POST-EXPLOITATION:**
- Party hard!
ADS-B 101

- Automatic Dependent Surveillance-Broadcast
- Radar substitute
- Position, velocity, identification, and other ATC/ATM-related information.
- ADS-B has a data rate of 1 Mbit/sec.
- Used for locating and plotting targets
ADS-B Security

- None at all
- Attacks range from **passive attacks** (eavesdropping) to **active attacks** (message jamming, replaying, injection).
- Target selection
  - Public Data
  - Local data (SDR*)
  - Virtual Aircrafts

* Software Defined Radio
ACARS 101

✈ Aircraft Communications Addressing and Reporting System

✈ Digital datalink for **transmission of messages between aircraft and ground stations**

✈ Multiple data can be sent from the ground to the A/C *

✈ Used for passive “OS fingerprinting” and plotting targets

* Aircraft
ACARS Security

- None at all
  - sometimes monoalphabetic ciphers

- Detailed flight and Aircraft information
  - Public DB
  - Local data (SDR)
  - Virtual Aircrafts

- Ground Service Providers
  - Two main players
  - Worldwide coverage
FMS 101

Flight Management System typically consists of two units:
» A computer unit
» A control display unit

Control Display Unit (CDU or MCDU) provides the primary human/machine interface for data entry and information display.

FMS provides:
» Navigation
» Flight planning
» Trajectory prediction
» Performance computations
» Guidance
Goal: Exploit the FMS
  » Using ACARS to upload FMS data
  » Many different data types available

Upload options:
  » Software Defined Radio
  » Ground Service Providers

The path to the exploit:
  » Audit aircraft code searching for vulnerabilities

We use a lab with virtual airplanes
  » but real aircraft code and HW
Aircraft Hardware and Software

✈ The good old...
  » eBay!!

✈ Russian scrapings
  » You name it

✈ Loving salesman
  » Value-added products

✈ Third party vendors
  » /wp-admin... Sigh

✈ Resentful users or former employees
A truly effective solution is the Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.
Key advantages

The PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

A truly effective Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.
A truly effective solution is the Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.
The PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

A truly effective Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.
Key advantages

The PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

A truly effective Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.
Honeywell's CMUs and ATSU AOC products are supported by a ground based tool called Airsim. The Airsim tool is a PC-based program that is designed to simulate a datalink system. The Airsim incorporates over 95% of the actual CMU and ATSU AOC software. This allows it
Honeywell offers tools using actual aircraft FMS code...for your genuine training experience.

Honeywell’s PC-FMS™ free play software provides simulation based on actual flight code software.

Key advantages

The PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

A truly effective Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.

Honeywell's CMUs and ATSU AOC products are supported by a ground based tool called Airsim. The Airsim tool is a PC-based program that is designed to simulate a datalink system. The Airsim incorporates over 95% of the actual CMU and ATSU AOC software. This allows it...
Honeywell offers tools using actual aircraft FMS code...for your genuine training experience.

Honeywell’s PC-FMS™ free play software provides simulation based on actual flight code software.

Key advantages

The PC-Primus Apex familiarization tool provides a detailed presentation of the FMS and display windows. High-resolution graphics are combined with actual aircraft code to create a training environment that looks just like the aircraft.

A truly effective Rockwell Collins FMS desktop trainer (DTT). Our solution uses the same software that is used by the actual Rockwell Collins FMS and display avionics software.

Honeywell's CMUs and ATSU AOC products are supported by a ground based tool called Airsim. The Airsim tool is a PC-based program that is designed to simulate a datalink system. The Airsim incorporates over 95% of the actual CMU and ATSU AOC software. This allows it
The Lab

A/C == Aircraft
SDR == Software Defined Radio
The Lab
FMS vulnerabilities

✈ Many different data types to upload
✈ Many FMS manufacturers, models and versions.
✈ Architectures: PPC (Lab x86)
✈ Language: mostly ADA (old ones)
✈ SO – RTOS realm:
   » DeOS
   » VxWorks
✈ ACARS:
   » ACARS datalink allows real time (avg of 11s delay) data transmission
   » Size: Max 220 chars * 16 blocks :S
## ACARS Messages during flight

<table>
<thead>
<tr>
<th>Stage</th>
<th>From A/C</th>
<th>To A/C</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Taxi</strong></td>
<td>OUT</td>
<td></td>
<td>Link Test, Clock Update, Delay Reports</td>
</tr>
<tr>
<td></td>
<td>Engine Data</td>
<td>Flight Plan Update</td>
<td>Weight and Balance, Airport Analysis, V-Speeds, Flight-Plan, Loaf FMC</td>
</tr>
<tr>
<td><strong>Take-Off</strong></td>
<td>OUT</td>
<td></td>
<td>PDC, and ATIS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Flight Plan Update</td>
<td></td>
</tr>
<tr>
<td><strong>Departure</strong></td>
<td>From A/C</td>
<td>Weather Reports</td>
<td>ATC Oceanic Clearance, Weather Reports, Reclearance, Ground Voice Request</td>
</tr>
<tr>
<td><strong>En Route</strong></td>
<td>From A/C</td>
<td></td>
<td>Position Reports, Weather Reports, Delay Info/ETA, Voice Request, Engine Information, Maintenance Reports</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Catering Requests, Gate Requests, ETA, Special Requests, Engine Information</td>
</tr>
<tr>
<td><strong>Approach</strong></td>
<td>From A/C</td>
<td></td>
<td>Maintenance Reports, Connecting Gates, Pax and Crew, ATIS</td>
</tr>
<tr>
<td><strong>Land</strong></td>
<td>From A/C</td>
<td></td>
<td>IN, Fuel Information, Crew Information, Fault Data from CMC</td>
</tr>
<tr>
<td><strong>Taxi</strong></td>
<td>From A/C</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Part II
The $PATH$ to exploit
SITA/ARINC

✈ Société Internationale de Télécommunications Aéronautiques (SITA)
  » IT and telecommunication services to the air transport industry.
  » 90% of the world’s airline business.

✈ Aeronautical Radio, Incorporated (ARINC)
  » Major provider of transport communications and systems solutions:
  » Aviation, airports, defense, government, healthcare, networks, security, and transportation.
Be my guest...

What could possibly go WRONG?

Access methods:

✈ E-Mail Clients
   » SMTP / POP3
   » Lotus Notes

✈ Desktop Apps, connection over:
   » X.25
   » TCP
   » MQ Series (IBM WebSphere)
   » MSMQ (Microsoft queues)
   » MS SQL Database
   » ORACLE Database

✈ Web App

✈ Mobility
   » Mobile App
   » Pager/SMS
   » Printer
   » SDK
   » Stations

Software Defined Radio 101

✈ A radio communication system where components that have been typically implemented in hardware are instead implemented by means of software.

✈ HW: USRP1/USRP2
   » Universal Software Radio Peripheral
   » USB or Gigabit Ethernet link

✈ SW: GNU Radio
   » LabVIEW, MATLAB and Simulink
   » SDK that provides signal processing blocks to implement software radios.
   » Python/C++
Post-Exploitation

✈ Consolidation
  » Protection & Monitoring

✈ Communication
  » Two way communication

✈ Expansion
  » Other systems
  » Back to Discovery

“Smiths Aerospace chose Wind River Systems' VxWorks 653 RTOS for the B787's common core system (CCS), a cabinet that will host 80 to 100 applications, including Honeywell's FMS and health management software and Collins' crew alerting and display management software”
Aircraft Post-Exploitation

✈ Aircraft and Pilots
   » Predictables
   » Checklists and procedures

✈ Exploiting other comm and nav systems or protocols

✈ Planning and timing!

✈ C&C
   » Two way communication
   » Actions
   » Limitations

---

- AP (if engaged) ............... OFF
- BOTH FDs .................... OFF
- Respond promptly and smoothly to an RA by adjusting or maintaining the vertical speed, as required, to reach the green area and/or avoid the red area of the vertical speed scale.

Note: Avoid excessive manoeuvres while aiming to keep the vertical speed just outside the red area of the VSI, and within the green area. If necessary, use the full speed range between \( V_{\alpha\text{ max}} \) and \( V_{\text{max}} \).

- Respect stall, GPWS, or windshear warning.
- Notify ATC.
- When “CLEAR OF CONFLICT” is announced:
  - Resume normal navigation in accordance with ATC clearance.
  - AP/FD can be re-engaged as desired.
SIMON

✈ Why SIMON?
✈ Multi-stage payload
✈ Control ADS-B/ACARS
   » Upload via ADS-B/ACARS
✈ Persistence
✈ Stealthness (No Rootkit)
✈ Accept and inject:
   » FP/DB
   » Payloads (scripts)
   » Plugins (code)
   » Commands
   » Two way comm
Conclusions
Remediation
Safety != Security

✈ Where to start from?
» NextGen Security
» On-board systems security audit

✈ Who is affected?
» Manufacturers
» Ground Service Providers
» Airlines

✈ We are working with EASA to improve the situation
Aviation 101

ADS-B
» http://en.wikipedia.org/wiki/Automatic_dependent_surveillance-broadcast
» https://www.blackhat.com/html/bh-us-12/bh-us-12-briefings.html#Costin

ACARS
» http://en.wikipedia.org/wiki/Aircraft_Communications_Addressing_and_Reporting_System
» http://spench.net/

FMS
» http://en.wikipedia.org/wiki/Flight_management_system
» http://www.b737.org.uk/fmc.htm

SDR
» http://en.wikipedia.org/wiki/Software-defined_radio
» http://gnuradio.org
THANKS TO:

✈ @d0tslash
✈ @vierito5
✈ @searchio
✈ @48bits
✈ @kuasar
✈ Many others


Hugo Teso
hugo.teso@nruns.com