Ghost is in the Air(Traffic)

Andrei Costin <andrei.costin@eurecom.fr>
Aurelien Francillon <aurelien.francillon@eurecom.fr>
andrei# whoami
SW/HW security researcher, PhD candidate

Mifare Classic
MFCUK

Interest in
avionics

Hacking MFPs
PostScript

http://andreicostin.com/papers/
http://andreicostin.com/secadv/
Administratrivia #0

DISCLAIMER

- This presentation is for informational purposes only. Do not apply the material if not explicitly authorized to do so.
- Reader takes full responsibility whatsoever of applying or experimenting with presented material.
- Authors are fully waived of any claims of direct or indirect damages that might arise from applying the material.
- Information herein represents author own views on the matter and does not represent any official position of affiliated body.

- **tldr;**
- **DO NOT TRY THIS AT HOME!**
- **USE AT YOUR OWN RISK!**
Please complete the Speaker Feedback Surveys
Thank you (=}
Agenda

1. Intro to ATC
2. ATC Problems Today
3. What is ADS-B?
4. ATC Problems Tomorrow - ADS-B Threats
5. How can ADS-B be exploited?
6. Solutions and take-aways
ATC Today...

AIR TRAFFIC CONTROL

What my friends think I do  What my mom thinks I do  What society thinks I do

What pilots think I do  What I think I do  What I actually do
How do radars work without ADS-B?

Non Co-operative versus Co-operative Independent Surveillance
SSR transmits basic *solicited* data

- SSR is solicited type of communication
  - Solicitation via XPDR
  - Solicitation via voice VHF

- Example of data from SSR XPDR:
  - Aircraft Address
  - Altitude
  - Code (squawk)
  - Angles (Roll/Track)
SSR transponder (XPDR)

- XPDR sends so-called squawks
- In this example – it squawks \textit{code 1200}
How SSR displays look like?
Agenda

1. Intro to ATC
2. ATC Problems Today
3. What is ADS-B?
4. ATC Problems Tomorrow - ADS-B Threats
5. How can ADS-B be exploited?
6. Solutions and take-aways
Inputs are not robust enough

To allow correlation of a FLTID to a flight plan, the FLTID must match the Aircraft Identification (ACID) entered in Item 7 of the Flight Notification.

If you enter either of these codes incorrectly, ATC might not be able to see your aircraft, or might confuse it with another. You could also affect other systems, like TCAS. The codes are flight critical information, so enter them carefully.

- TCAS (Traffic Collision Avoidance System) = very critical component in the air-traffic safety
- ACID coordinates the harmonized operational deployment of Mode S Elementary Surveillance
Inputs are not robust enough

Don’t add any leading zeros, hyphens, dashes or spaces to the FLTID.

HI, THIS IS YOUR SON’S SCHOOL. WE’RE HAVING SOME COMPUTER TROUBLE.

OH, DEAR – DID HE BREAK SOMETHING? IN A WAY –

DID YOU REALLY NAME YOUR SON Robert?); DROP TABLE Students;-- ?

OH, YES. LITTLE BOBBY TABLES, WE CALL HIM.

WELL, WE’VE LOST THIS YEAR’S STUDENT RECORDS. I HOPE YOU’RE HAPPY.

AND I HOPE YOU’VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.
Input mistakes have severe implications

When making routine code changes, you should avoid inadvertent selection of codes 7500, 7600, or 7700 thereby causing momentary false alarms at automated ground facilities. For example when switching from code 2700 to code 7200, switch first to 2200 then 7200, NOT to 7700 and then 7200.

This procedure applies to nondiscrete code 7500 and all discrete codes in the 7600 and 7700 series (i.e., 7600-7677, 7700-7777) which trigger special indicators in automated facilities. Only nondiscrete code 7500 will be decoded as the hijack code. An aircraft’s transponder code (when available) is utilized to enhance the tracking capabilities of the ATC facility, therefore you should not turn the GTX 320 to SBY when making routine code changes.

**Important Codes**

- **1200**—The VFR Code for any altitude.
- **7600**—Loss of Communications.
- **7500**—Hijacking (Never assigned by ATC with her aircraft is subject to unlawful interference).
- **7700**—Emergency (All secondary surveillance times).

---

**Important Codes**

Following is a list of important codes:

- **1200** – VFR code in the U.S. (refer to ICAO standards for VFR codes in other countries).
- **7000** – VFR code commonly used in Europe (refer to ICAO standards).
- **7500** – Hijack code.
- **7600** – Loss of communication code.
- **7700** – Emergency code.

**7777** – Military interceptor operations code (NEVER SQUAWK THIS CODE).
- **0000** – Code for military use in the U.S.
Agenda

1. Intro to ATC
2. ATC Problems Today
   - What is ADS-B?
3. ATC Problems Tomorrow - ADS-B Threats
4. How can ADS-B be exploited?
5. Solutions and take-aways
ATC Tomorrow – NextGen, ATC/M and eAircrafts
ADS-B is a $billions world-wide effort from 2006...

### FAAXX704: Automatic Dependent Surveillance-Broadcast (ADS-B)

The Surveillance and Broadcast Services (SBS) program office is implementing Automatic Dependent Surveillance-Broadcast (ADS-B), a surveillance system designed to provide improved air traffic information for pilots and air traffic controllers.

**FY2012 (CY) Spending**
- $301.52 M

**Time Frame of Investment**
- 2006 - 2035

**Status**
- Continued
- Major

### EXHIBIT 300

#### Section C: Summary of Funding (Budget Authority for Capital Assets)

<table>
<thead>
<tr>
<th>1. Table I.C.1 Summary of Funding</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Planning Costs:</td>
</tr>
<tr>
<td>PY-1 &amp; Prior:</td>
</tr>
<tr>
<td>$9.9</td>
</tr>
<tr>
<td>PY 2011</td>
</tr>
<tr>
<td>$0.0</td>
</tr>
<tr>
<td>CY 2012</td>
</tr>
<tr>
<td>$0.0</td>
</tr>
<tr>
<td>BY 2013</td>
</tr>
<tr>
<td>$0.0</td>
</tr>
<tr>
<td>DME (Excluding Planning) Costs:</td>
</tr>
<tr>
<td>$710.7</td>
</tr>
<tr>
<td>$179.8</td>
</tr>
<tr>
<td>$288.0</td>
</tr>
<tr>
<td>$272.1</td>
</tr>
<tr>
<td>DME (Including Planning) Govt. FTEs:</td>
</tr>
<tr>
<td>$28.6</td>
</tr>
<tr>
<td>$6.3</td>
</tr>
<tr>
<td>$6.8</td>
</tr>
<tr>
<td>$4.5</td>
</tr>
<tr>
<td>Sub-Total DME (Including Govt. FTE):</td>
</tr>
<tr>
<td>$749.2</td>
</tr>
<tr>
<td>$186.1</td>
</tr>
<tr>
<td>$294.8</td>
</tr>
<tr>
<td>$276.6</td>
</tr>
<tr>
<td>O &amp; M Costs:</td>
</tr>
<tr>
<td>$11.0</td>
</tr>
<tr>
<td>$5.0</td>
</tr>
<tr>
<td>$6.4</td>
</tr>
<tr>
<td>$7.9</td>
</tr>
<tr>
<td>O &amp; M Govt. FTEs:</td>
</tr>
<tr>
<td>$2.6</td>
</tr>
<tr>
<td>$0.3</td>
</tr>
<tr>
<td>$0.4</td>
</tr>
<tr>
<td>$0.2</td>
</tr>
<tr>
<td>Sub-Total O &amp; M Costs (Including Govt. FTE):</td>
</tr>
<tr>
<td>$13.6</td>
</tr>
<tr>
<td>$5.3</td>
</tr>
<tr>
<td>$6.8</td>
</tr>
<tr>
<td>$8.1</td>
</tr>
<tr>
<td>Total Cost (Including Govt. FTE):</td>
</tr>
<tr>
<td>$762.8</td>
</tr>
<tr>
<td>$191.4</td>
</tr>
<tr>
<td>$301.6</td>
</tr>
<tr>
<td>$284.7</td>
</tr>
<tr>
<td>Total Govt. FTE costs:</td>
</tr>
<tr>
<td>$31.2</td>
</tr>
<tr>
<td>$6.6</td>
</tr>
<tr>
<td>$7.2</td>
</tr>
<tr>
<td>$4.7</td>
</tr>
<tr>
<td># of FTE rep by costs:</td>
</tr>
<tr>
<td>202</td>
</tr>
<tr>
<td>38</td>
</tr>
<tr>
<td>38</td>
</tr>
<tr>
<td>24</td>
</tr>
</tbody>
</table>

**Total change from prior year final President's Budget ($):**
- $0.0
- $-2.0

**Total change from prior year final President's Budget (%):**
- 0.00%
- -0.66%
“unmatched” security, but hey... “Safety-first!”

Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance - Broadcast (ADS-B)
How does ADS-B work? – *Architectural view*

Guidance for the Provision of Air Traffic Services Using ADS-B for Airport Surface Surveillance

2.1.1 ADS-B Out and ADS-B IN

**GPS**  **GLONASS**  **GALILEO**

1090ES includes a **56 bit data field** used to carry ADS-B information

**EXTENDED (112 BIT) SQUITTER**

8 bit CONTROL  24 bit A/C ADDRESS  56 bit ADS MESSAGE  24 bit PARITY

**EXTENDED SQUITTER GROUND STATION**

**1090ES** includes a **56 bit data field** used to carry ADS-B information

**ADS-B** information is derived from the onboard avionics navigation systems

**EXTENDED SQUITTER GROUND STATION**

**TO ATC FACILITY**

ADS-B Out and ADS-B In – Simplified Functional Diagram
ADS-B – INsideOUT...

- ADS-B is being used over 2 existing technologies:
  - Mode-S – 1090 MHz (replies) and 1030 MHz (interrogation)
  - UAT (Universal Access Transceiver) – 978 MHz (replies)
ADS-B Deployment Map – Australia

www.airservicesaustralia.com/projects/ads-b/ads-b-coverage/

Automatic Dependent Surveillance Broadcast:

- How ADS-B works
- Tracking ADS-B in our air traffic management system
- Upper Airspace Program
- ADS-B mandate 2013
- Mandate to deactivate some ADS-B transmissions
- Operational Information
- ADS-B services
- ADS-B coverage
- Working groups and panels

Australian Mode-S Terminal Area
Radar Replacement project

Collaborative decision making
Fire control centre upgrade
Ground Based Augmentation System
National towers program
Remote Tower Technology
ADS-B Deployment Map – USA

NextGen Technologies Interactive Map

NextGen Technologies in the NAS

Automatic Dependent Surveillance-Broadcast (ADS-B) is a key NextGen transformational program. Using the global satellite network, ADS-B will provide improved safety, capacity and efficiency in the National Airspace System. With ADS-B, air traffic controllers and pilots will see the precise location of every equipped aircraft. Pilots will also have real-time access to weather and flight information. Infrastructure is planned to be completed by early 2014.

Information current as of 7/11/2012.
How does ADS-B look like? – Community view
How does community get this data?

- AirNav RadarBox
- Mode-S Beast with miniASDB
- Kinetic SBS
- PlaneGadgets ADS-B
- Aurora Eurotech SSRx
- microADSB USB
- Funkwerk RTH60
- microADSB-IP BULLION
- miniADSB
- Frames encoded in
  - Pulse-position-modulation (PPM)
  - 1 bit = 1 us
  - Shared-medium (no CA/CD), theoretical bandwidth 1 Mbit/sec
Frames encoded in
- Pulse-position-modulation (PPM)
- 1 bit = 1 us
- Shared-medium (no CA/CD), theoretical bandwidth 1 Mbit/sec

Frames composed of
- A preamble
  - 8 bits for TX/RX sync
- A data-block
  - 56 bits for short frames
  - 112 bits for extended/long frames
- Mandatory to have
  - 24 bits ICAO address of aircraft
  - 24 bits error-detection parity
Agenda

1. Intro to ATC
2. ATC Problems Today
3. What is ADS-B?
4. ATC Problems Tomorrow - ADS-B Threats
5. How can ADS-B be exploited?
6. Solutions and take-aways
## ADS-B Main Threats – Summary

<table>
<thead>
<tr>
<th>ADS-B Threat</th>
<th>Fail / warn / ok</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity/message authentication</td>
<td>✗</td>
</tr>
<tr>
<td>Entity authorization (eg. medium access)</td>
<td>!</td>
</tr>
<tr>
<td>Entity temporary identifiers/privacy</td>
<td>✗</td>
</tr>
<tr>
<td>Message integrity (HMAC)</td>
<td>✗</td>
</tr>
<tr>
<td>Message freshness (non-replay)</td>
<td>✗</td>
</tr>
<tr>
<td>Encryption (message secrecy)</td>
<td>✗</td>
</tr>
</tbody>
</table>

**ADS-B is almost like “ALL R/W with ‘Guest as Admin’ enabled”**
Potential mitigations exist... but are not public

- Mode-4/Mode-5 IFF Crypto Appliqué
  - 2-Levels Crypto secured version of Mode S and ADS-B GPS position
  - Defined for military NATO STANAG 4193
  - Enhanced encryption
  - Spread Spectrum Modulation
  - Time of Day Authentication
  - Level1:
    - Aircraft Unique PIN
  - Level2:
    - Level1 + other (unknown for now) information
    - Apparently based on Black & Red keys crypto

- ADS-B also specifies, but not details available about crypto/security:
  - DF19 = Military Extended Squitter
  - DF22 = Military Use Only
Agenda

1. Intro to ATC
2. ATC Problems Today
3. What is ADS-B?
4. ATC Problems Tomorrow - ADS-B Threats
5. How can ADS-B be exploited?
6. Solutions and take-aways
ADS-B – Adversary Model – *By role*

- **Pilots**
  - Bad intent
  - (Un)Intentional pranksters

- **Pranksters**

- **Abusive users/organizations**
  - Privacy breachers – eg. Paparazzi
  - Message conveyors

- **Criminals**
  - Money (more likely). Eg.: Underground forums with “Worldwide SDRs for hire” – potentially very profitable underground biz (think sniff GSM)
  - Terror (less likely)

- **Military/intelligence**
  - Espionage
  - Sabotage
Example: *internal prankster* attack

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MATT SUXX</td>
<td>A20</td>
<td>L2</td>
<td>N229</td>
<td>west Airline</td>
</tr>
<tr>
<td>2</td>
<td>BUTTSEXX</td>
<td>A2F</td>
<td>N2905</td>
<td>west</td>
<td>Airlines</td>
</tr>
<tr>
<td>3</td>
<td>MATT SUXX</td>
<td>A2F</td>
<td>N292</td>
<td>west Airline</td>
<td>07/11 03:29:55</td>
</tr>
<tr>
<td>4</td>
<td>MATT SUXX</td>
<td>A31</td>
<td>N297</td>
<td>east Express</td>
<td>07/11 16:39:11</td>
</tr>
<tr>
<td>5</td>
<td>HIDAD</td>
<td>A31</td>
<td>N297</td>
<td>east</td>
<td>Express</td>
</tr>
<tr>
<td>6</td>
<td>BALLSLAM</td>
<td>A21</td>
<td>N297</td>
<td>west Airline</td>
<td>06/06 18:21:05</td>
</tr>
<tr>
<td>7</td>
<td>BUTTPUMP</td>
<td>A2F</td>
<td>N297</td>
<td>west Airline</td>
<td>06/06 07:17:47</td>
</tr>
<tr>
<td>8</td>
<td>YOUSUCK</td>
<td>A33</td>
<td>N308</td>
<td>west Airline</td>
<td>06/09:22:03</td>
</tr>
<tr>
<td>9</td>
<td>BUTTSEX</td>
<td>A2F</td>
<td>L20 201</td>
<td>3:19 BUTTSE</td>
<td>06/09:22:03</td>
</tr>
<tr>
<td>10</td>
<td>ABBAROCK</td>
<td>A22</td>
<td>L20 201</td>
<td>3:09 ABBAR</td>
<td>06/09:22:03</td>
</tr>
<tr>
<td>11</td>
<td>NOZOBAMA</td>
<td>N38</td>
<td>N297</td>
<td>west</td>
<td>Airlines</td>
</tr>
<tr>
<td>12</td>
<td>FAYISGAY</td>
<td>N8C</td>
<td>N297</td>
<td>west</td>
<td>Airlines</td>
</tr>
<tr>
<td>13</td>
<td>WOLYSAI</td>
<td>N45</td>
<td>N297</td>
<td>west</td>
<td>Airlines</td>
</tr>
</tbody>
</table>

<p>| | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>ATCFAIL</td>
<td>N71</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>BIGBOOBS</td>
<td>N72</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>GETAJOB</td>
<td>N83</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>NOFATCHK</td>
<td>USA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>VOTEUNUN</td>
<td>VO:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>VOTENOOP</td>
<td>VO:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>PHATCHIX</td>
<td>PHA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>DUMBPILT</td>
<td>DUL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>JETSBLO</td>
<td>JET:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>JOHN RULZ</td>
<td>JOH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>KELYSM</td>
<td>KEL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>SOFAKING</td>
<td>SOF</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>FATIGUE</td>
<td>FAT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>LADYGAGA</td>
<td>LAD</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>SEXY1215</td>
<td>C:Fi</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>YOUWIN</td>
<td>N23</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>BULLSHIT</td>
<td>NSC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>GOINHOM</td>
<td>N15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>THEMOLE</td>
<td>N78</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example: *external criminals* potential attack

- Similar to “internal prankster”
  - Should not be overlooked though

- Any of the fields can be used to encode attacker’s data
  - For communication similar to C&C (Holywood-style “avionics botnet”)
  - For exchanging intelligence data
  - Attacker’s data can be: obfuscated, encoded, encrypted
  - Data could mimic real/sniffed ADS-B messages having minor *intentional* errors/discrepancies which would encode attacker’s data

- Example: See the demo
Example: *external abusers* + public data correlation

- Strategically positioned
- Have a well-defined target
- Poses inexpensive devices
- Can publicly access private details *(why is this allowed?!)*

---

```
- Searchable worldwide registration database
- Aruba Aircraft Register
- Australian Aircraft Register
- Austrian Aircraft Register
- Belgian Aircraft Register
- Brazilian Aircraft Register
- British Aircraft Register
- Canadian Aircraft Register
- Danish Aircraft Register
- Dutch Aircraft Register
- Dutch Historic Aircraft Registers
- Finnish Aircraft Register
- French Aircraft Register
- Guatemalan Aircraft Register
- Indian Aircraft Register
- International Registry of Mobile Assets, pursuant to the Cape Town Treaty
- Irish Aircraft Register
- Latvian Aircraft Register
- Lebanese Aircraft Register
- Luxembourg Aircraft Register
- New Zealand Aircraft Register
- Norwegian Aircraft Register
- Singapore Aircraft Register
- South African Aircraft Register
- Swedish Aircraft Register
- Swiss Aircraft Registry
- United States Aircraft Registry
- Article 20 of the Convention on International Civil Aviation
- Annex 7 to the Convention on International Civil Aviation
- Supplement to Annex 7 of the Convention on International Civil Aviation
```

---

[Link to Wikipedia page on Aircraft Registration](https://en.wikipedia.org/wiki/Aircraft_registration)
Public access, seriously? USA (FAA)
Public access, seriously? Australia (CASA)
Public access, seriously? CAA (UK)

International Register of Civil Aircraft

The International Register of Civil Aircraft is published, in co-operation with ICAO, jointly by Bureau Veritas (France), the UK Civil Aviation Authority and the ENAC of Italy. The database, which contains information from over 45 countries and over 400,000 aircraft, is available on CD-ROM and is updated on a quarterly basis. This CD-ROM now also contains the US Register of Civil Aircraft. To order the International Register on CD-ROM please see forms and fees.
ADS-B – Adversary Model – *By location*

- **Ground-based**
  - Easier to operate (win criminals)
  - Easier to be caught (win agencies)
  - Easier to defend or mitigate against (win agencies)
    - Eg. Angle of arrival, time-difference of arrival

- **Airborne**
  - Drones
  - UAV
  - Autonomously pre-programmed self-operating checked-in luggage:
    - Pelican case, barometric altimeter, battery, embed-devs, GPS, RF…
  - Possibly could work around angle of arrival
  - Could pose more advanced threat to ADS-B IN enabled aircrafts
  - **Important:** not extensively modeled in the attacker & threat modeling of Mode-S/ADS-B
Scenario showcase #1
82-000 747-2G4B VC-25A ADFDF8/AE2FF4 ?!?!?!
Scenario showcase #1
82-000 747-2G4B VC-25A ADFDF8/AE2FF4 ?!?!?!
Scenario showcase #1 – Privacy
82-000 747-2G4B VC-25A ADFDF8/AE2FF4 ?!?!?!

- Assumptions:
  - ADS-B is ALL R/W = Clear-text and No privacy

- Open issues:
  - If ADS-B data is **true**
    - Why does “Air Force One” shows itself?

  - Should this type of aircrafts broadcast their pos/ident?
    - If yes, wouldn’t they become easy targets?
    - If no, how would they benefit to/from ADS-B?
    - If workaround with “fake” reg_nums/call_signs, isn’t this a kind of backdoor in CS terms?

  - Perhaps they use mostly **Mode-5** encrypted mode
    - Then, why doesn’t everybody have access to Mode-5 in the first place?
Scenario showcase #1 – Impersonation
82-000 747-2G4B VC-25A ADFDF8/AE2FF4 ?!?!?!

- Assumptions:
  - ADS-B is ALL R/W = Non-auth (access and messages)

- Open issues:
  - If ADS-B data is **false**
    - Someone is already spoofing or not?
    - How do you know for sure if yes or no?
  - Also, anyone can say “I am Air Force One”
    - Does “Air Force One” has special ATC treatment?
    - If so, can this be an abused procedural “backdoor”?

- These open issues raise “uncertainties”
  - Unless otherwise clarified
  - Any “uncertainty” poses threat to safety of operation
Potential for DoS on ATC human-resource

- **Attack:**
  - Based on “Fake airplane injection into ATC” attack
  - Mitigation: there is a *mostly manual* procedure for an ATC operator to check a flight number against flight plans and flight strips (*flight strips is so 1900, really!*)

- ** Twist1:**
  - Inject 1 mln fake airplanes, both valid and invalid flight plans, filed by different flight plan systems
  - Result: Potential human-resource exhaustion

- **Fixes:**
  - Have fully e-automated flight plan exchange and cross-checks
  - Better, solve ADS-B insecurities and *potential* is nullified
Potential for DoS on ATC flight-space resource

- **Attack:**
  - Similar to “DoS on ATC human-resource”

- **Twist1:**
  - Fake planes scattered on *wide geographic area* of responsibility of “victim ATC”
  - The area of ghost/fake/unidentified aircraft/object is in “flight quarantine”
    - Separation are increased, all normal routes deviated
    - General rules are in ICAO 4444 + country specifics
  - This is done for safety reasons (eg. ASSET methodology) to avoid disasters
  - A potentially wide geo-area affected in terms of air-traffic – nightmare!

- **Twist2:**
  - Fake a copy of a genuine aircraft within it’s own area of separation
  - Will generate a Short Term Conflict Alert (STCA)

- **Fixes:**
  - Locate and turn-off attacker RF emitter (but what if it’s a drone?)
  - Better, solve ADS-B insecurities and *potential* is nullified
Potential for DoS on ADS-B IN aircrafts

- **Attack:**
  - Based on “Fake airplane injection into ATC” attack
  - Mitigation: unknown, perhaps similar to ATC semi-auto/semi-manual flight plan cross-check

- **Twist1:** Inject fake airplanes (1…1 mln) into ADS-B IN capable aircrafts
  - Assumption: Target aircraft lacks good connectivity and automated cross-check protocols for flight plan lookup and validation (compared to ATC)
  - Result: Total uncertainty in received data, i.e. data is useless...

- **Fixes:**
  - Have real-time critical data exchange and verification capability on eAircrafts
  - Have fully e-automated flight plan exchange and cross-checks
  - Better, solve ADS-B insecurities and potential is nullified
## Hardware setup

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Functions</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDR USRP1</td>
<td>Main RF support</td>
<td>700 USD</td>
</tr>
<tr>
<td>SBX</td>
<td>ADS-B OUT/IN (attack)</td>
<td>475 USD</td>
</tr>
<tr>
<td>WBX</td>
<td>ADS-B OUT/IN (attack)</td>
<td>450 USD</td>
</tr>
<tr>
<td>DBSRX2</td>
<td>ADS-B IN (verify)</td>
<td>150 USD</td>
</tr>
<tr>
<td>Plane</td>
<td>ADS-B IN (verify)</td>
<td>~245 USD</td>
</tr>
<tr>
<td>Gadget</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attenuators</td>
<td>Limit output (SMA cable)</td>
<td>&lt;10 USD</td>
</tr>
</tbody>
</table>

**Alternative SDRs**

- SDR USRP1
- SBX
- WBX
- DBSRX2
- Plane
- Gadget

**Alternative ADS-BSs**

- ADS-B OUT/IN (attack)
- ADS-B IN (verify)
ADS-B Message Replay
Quick reference

- Capture ADS-B data:
  - UHD-mode
    - `uhd_rx_cfile.py --spec B:0 --gain 25 --samp-rate 4000000 -f 10900000000 -v ~/CAPTURE_adsb.fc32`
  - Pre-UHD-mode
    - `usrp_rx_cfile.py`

- Replay the captured data:
  - UHD-mode
    - `tx_transmit_samples --file ~/CAPTURE_adsb.fc32 --ant "TX/RX" --rate 4000000 --freq 10900000000 --type float --subdev B:0`
  - Pre-UHD-mode
    - `usrp_replay_file.py`
ADS-B Message Injection
Quick reference

- ADS-B data crafting
  - Tweak the captured data
    - Load I/Q data: \( d_{\text{cap}} = \text{read}_\text{float}_\text{binary}('~/\text{CAPTURED}_{\text{adsb}.}\text{fc32}') \)
    - Modify the samples: \( d_{\text{cft}} = \text{adsb}_\text{randomize}(d_{\text{cap}}) \)
    - Write back I/Q data: \( \text{write}_\text{float}_\text{binary}(d_{\text{cft},} '~/\text{CRAFTED}_{\text{adsb}.}\text{fc32}') \)
  - Generate the data
    - MatLab – \( \text{modulate}(\text{adsb}\_\text{frame}, \text{fc}, \text{fs}, \text{‘ppm’}) \)
    - GNUradio – write native C++ block

- Transmit the \textit{crafted} data:
  - UHD-mode
    - \( \text{tx}_\text{transmit}_\text{samples} --\text{file} ~/\text{CRAFTED}_{\text{adsb}.}\text{fc32} --\text{ant} \text{"TX/RX"} --\text{rate} 4000000 --\text{freq} 1090000000 --\text{type} \text{float} --\text{subdev} B:0 \)
  - Pre-UHD-mode
    - \( \text{usrp}_\text{replay}_\text{file}.\text{py} \)
ADS-B Message Analyze/Visualize/Plot

Quick reference

- GNURadio ModeS tests:
  - Pre-UHD-mode (by Eric Cottrell):
    - `gr-air/src/python/usrp_mode_s_logfile.py`
  - UHD-mode (by Nick Foster):
    - `gr-air-modes/python/uhd_modes.py -a -w -F ~/CRAFTED_adsb.fc32`

- GNURadio:
  - `gr_plot_psd_c.py -R 4000000 ~/CAPTURE_adsb.fc32`
  - `gr_plot_psd_c.py -R 4000000 ~/CRAFTED_adsb.fc32`

- Octave + gnuplot:
  - `n_samp = 500000`
  - `trig_lvl = 0.01`
  - `d_cap = read_float_binary('CAPTURE_adsb.fc32', n_samp)`
  - `axis ([0, n_samp, -trig_lvl, trig_lvl])`
  - `plot(arr)`
Demo details

- Sniffed and replayed:
  - [0x8d, 0x42, 0x40, 0x50, 0x58, 0xaf, 0x74, 0x92, 0x69, 0xb9, 0x78, 0x081a0a]

- Crafted and injected:
  - [0x8d, 0xde, 0xad, 0xbf, 0x58, 0xaf, 0x74, 0x92, 0x69, 0xb9, 0x78, 0xa95724]
  - [0x8d, 0xca, 0xfe, 0xbb, 0x58, 0xaf, 0x74, 0x92, 0x69, 0xb9, 0x78, 0x3949e0]
  - [0x8d, 0xb0, 0xb5, 0x58, 0xaf, 0x74, 0x92, 0x69, 0xb9, 0x78, 0x2cec6b]
  - [0x8d, 0x31, 0x33, 0x70, 0x58, 0xaf, 0x74, 0x92, 0x69, 0xb9, 0x78, 0x7117c7]

- Parity needs to be tweaked
  - For ADS-B over Mode-S
    - adsb_modes_crc.py
  - For ADS-B over UAT
    - adsb_uat_crc.py
Agenda

1. Intro to ATC
2. ATC Problems Today
3. What is ADS-B?
4. ATC Problems Tomorrow - ADS-B Threats
5. How can ADS-B be exploited?

Solutions and take-aways
Solutions

- Solutions could include:
  - Verifiable multilateration (MLAT) with multiple ground-stations, but:

    ![Guidance Material on Surveillance Technology Comparison](image)

    **7.11 VERIFICATION OF ADS-B**

    Some commentators have promoted the use of multilateration as a means of ensuring the validity of received ADS-B data. Technically this is possible. Radar could also be used to verify the integrity of ADS-B data. If radar and/or multilateration in all areas of ADS-B coverage is required, then the most advantages of ADS-B are significantly diminished and the ADS-B deployment becomes unlikely. Verification could perhaps be achieved at major airport hubs aimed at detecting non compliant

- “Group of aircrafts” concepts

- AANETs should inspire from VANETs solutions

- Lightweight PKI architectures and protocols. Our thoughts:
  - FAA, EUROCONTROL, CASA as CAs
    - CAs root keys installed/updated during ADS-B device mandatory certification process
  - HMAC on each broadcast message
    - Every broadcast a subset of HMAC bits
Take-aways

- ADS-B is a safety-related mission-critical technology

- Yet, ADS-B lacks minimal security mechanisms
  - This poses direct threat to safety

- ADS-B costs tremendous amount of money, coordination, time
  - Yet, ADS-B is defeated in practice with
    - FOSS or moderate-effort custom software
    - Relatively low-cost SDRs hardware

- ADS-B assumptions are not technologically up-to-date
  - Doesn’t account users will have easy access to RF via SDRs
  - Doesn’t account users will have easy access to UAV, drones, etc.

- SDRs and their decreasing price are not the problem

**ADS-B is flawed and is the actual root-cause problem**
References (academia, standards, reports)

enough and sufficient to induce potentially dangerous safety and operational perturbances in a multi-million technology via the exploitation of missing basic security mechanisms such as message authentication at least.

REFERENCES


[20] DOT 249A. Minimum Operational Performance Standards for 1900 MHz Automatic Dependent Surveillance Broadcast (ADS-B) and Traffic Information Services (TIS-B), RTCA DO-260A

[21] DOT 242A. Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B), RTCA DO-242A


[26] Surveillance and Conflict Resolution Systems Panel SCRSPS CI/Military Inoperability with Military Mode S Standards, CRSPSWSWAG/AB, Montreal, 3th to 7th May 2004


[28] RTCA Special Committee 209 ATRCB / Mode S Transponder Project Requirements, Recommended Change to DO-240A and ED-73C for Higher Squarer Rates as Lower Power,

[29] Jim Mcnatt, Automated Dependent Surveillance - Broadcast Military (ADS-BM),


[36] C. Xiang, F. Minkj, Y. Limaa, L. Xiaor, Z. Tanning, And Towards Advanced Mobile Bannes, IETE 11, 4th UseNet Workshop on Large-Scale Exploits and Emerging Threats, 2011, Boston, Massachusetts, USA


[41] Lighter Kaukel, Air Traffic Control: Insecure and ADS-B, De/Con 17, Las Vegas, USA,

[42] Higher Kaukel, Air Traffic Control Insecurity 2.0, De/Con 18, Las Vegas, USA,

[43] Brad Hare, Happort & Aeroport So no good can come of this, De/Con 18, 2012, Krakow, Poland


[45] RadioReference Community Forum, Diddy Enhancements to files

[46] GNU Radio, A free & open-source software development toolkit that provides signal processing blocks to implement software radio, gnu.org


[49] ettus Research, SXR-200-4400 MHz RF


[51] BSC Tech News, Researchers are spoofing to 'hack' into a flying drone, www.bstechnews.com/new/technology/18434314

[52] SWISS Magazine, Eco-care reaches new (flight) levels, May 2012, Pag. 94


[58] Eric Cornell, GNU Radio ‘gr’-air module - pre-GR/GR Mode, Mode-4/4S-Mode and decoder, github.com/mmaus/gr-air

[59] Nick Foster, GNURadio ‘gr’-air-modules - Mode-4/4S mode software-defined radio receiver for Mode-4 transponder signals, including ADS-B reports from equipped aircraft, github.com/nickmaus/gr-air-modules


[61] GNU Radio, A free & open-source software development toolkit that provides signal processing blocks to implement software radio, gnu.org

54
References (related talks)

- 22C3 – I see airplanes
- DefCon17 – Air Traffic Control: Insecurity and ADS-B
- DefCon18 – Air Traffic Control Insecurity 2.0
- GRConf2011 – ADS-B in GnuRadio
- DefCon20 – Hacker + Airplanes = No Good Can Come Of This
Thank you!
Questions, ideas, corrections?

Andrei Costin <andrei.costin@eurecom.fr>
Aurelien Francillon <aurelien.francillon@eurecom.fr>