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/
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!
Agenda

1. ATC Today (SSR)
2. Today’s Problems
3. ATC “Tomorrow” (ADS-B)
4. “Tomorrow”s Problems
5. Exploit scenarios & Demos
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?
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)
Agenda

1. ATC Today (SSR)
2. Today’s Problems
3. ATC “Tomorrow” (ADS-B)
4. “Tomorrow”s Problems
5. Exploit scenarios & Demos
6. Solutions and take-aways
Inputs are not robust enough

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

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.
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. ATC Today (SSR)

2. Today’s Problems

ATC “Tomorrow” (ADS-B)

3. ATC “Tomorrow” (ADS-B)

4. “Tomorrow”s Problems

5. Exploit scenarios & Demos

6. Solutions and take-aways
ADS-B is a $billions world-wide effort from 2002...

### Table I.C.1 Summary of Funding

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

| Change from prior year final President's Budget ($) | $0.0 | $-2.0 |
| Change from prior year final President's Budget (%) | 0.00% | -0.66% |
How does ADS-B work? – Architectural view
ADS-B is being used over 2 existing technologies:
- Mode-S – 1090 MHz (replies) and 1030 MHz (interrogation)
  - PPM @ 1 Mbps
- UAT (Universal Access Transceiver) – 978 MHz (replies)
  - CP-2FSK @ 1.041667 Mbps (modulation index \( h \geq 0.6 \))
ATC Tomorrow – NextGen, ATC/M and eAircrafts
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 End State Coverage at 6,000 feet

 ADS-B End State Coverage at 10,000 feet

 ADS-B End State Coverage at 20,000 feet

 ADS-B End State Coverage at 30,000 feet
ADS-B Deployment Map – USA

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.

(398 Operational Radio Stations)

Information current as of 7/11/2012.
How does community get this data?

AirNav RadarBox

Mode-S Beast with miniASDB

Kinetic SBS

PlaneGadgets ADS-B

Aurora Eurotech SSRx

microADSB USB

miniADSB

Funkwerk RTH60

microADSB-IP BULLION

Summarized list of enthusiast-level ADS-B radar receivers
How does ADS-B look like? – Community view
Frames encoded in
  - Pulse-position-modulation (PPM)
  - 1 bit = 1 us
  - Shared-medium (no CA/CD), theoretical bandwidth 1 Mbit/sec
### ADS-B Frame – Modulation, Format, Security

- 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
ADS-B frame – modulation, format, security

Page intentionally left blank
1. ATC Today (SSR)
2. Today’s Problems
3. ATC “Tomorrow” (ADS-B)
4. “Tomorrow”s Problems
5. Exploit scenarios & Demos
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>
<tr>
<td>Massive public DBs with private detail*</td>
<td>✗</td>
</tr>
</tbody>
</table>
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. ATC Today (SSR)
2. Today’s Problems
3. ATC “Tomorrow” (ADS-B)
4. “Tomorrow”s Problems

Exploit scenarios & Demos

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*

- **Already happening** – Callsigns/FlighIDs used in real-life!
- Check them on Google or RR forum

<table>
<thead>
<tr>
<th>Callsign</th>
<th>Identifier</th>
<th>Type</th>
<th>Location</th>
<th>Date/Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>MATTUXX</td>
<td>A20</td>
<td>[N2255]west Airline</td>
<td>07/11 17:57:04</td>
<td></td>
</tr>
<tr>
<td>MATSUXX</td>
<td>A2F</td>
<td>[N292]west Airline</td>
<td>07/11 03:29:55</td>
<td></td>
</tr>
<tr>
<td>MATTUXX</td>
<td>A31</td>
<td>[N2972]ed Express</td>
<td>07/11 16:39:11</td>
<td></td>
</tr>
<tr>
<td>HIDAD</td>
<td>A31</td>
<td>[IIDAD]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BALLSLAM</td>
<td>A21</td>
<td>[N231]west Airline</td>
<td>06/06 18:21:05</td>
<td></td>
</tr>
<tr>
<td>BUTTPUMP</td>
<td>A2F</td>
<td>[N29]west Airline</td>
<td>06/06 07:17:47</td>
<td></td>
</tr>
<tr>
<td>YOU SUCK</td>
<td>A33</td>
<td>[N308F]west Airline</td>
<td>06/09 22:03</td>
<td></td>
</tr>
<tr>
<td>BUTTSEXX</td>
<td>A2F</td>
<td>[L2020]5:19 BUTTSE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ABBAROCK</td>
<td>A22</td>
<td>[L2020]3:09 ABBAR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NO2OBAMA</td>
<td>N3E</td>
<td>[A]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FAYISGAY</td>
<td>N8C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WOLYSAI</td>
<td>N45</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATCFAIL</td>
<td>N71</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BIGBOOPS</td>
<td>N72</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GETJOB</td>
<td>N82</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>NOFATCH</td>
<td>USA</td>
<td>[NOF]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VOTEUNUN</td>
<td>VO</td>
<td>[B8 - N]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VOTENDO</td>
<td>VO</td>
<td>can Ea at probably</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PHATCHIX</td>
<td>PH4</td>
<td>[N29]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DUMBPILT</td>
<td>DU</td>
<td>[A302]</td>
<td>15W</td>
<td></td>
</tr>
<tr>
<td>JETSBLOW</td>
<td>JET</td>
<td>[N29]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>JOHN RULZ</td>
<td>JOH</td>
<td>[V (A301)]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KELYSMLS</td>
<td>KEL</td>
<td>[N (A305)]</td>
<td>miles, or Ke You be the judge.</td>
<td></td>
</tr>
<tr>
<td>SQFAKING</td>
<td>SOF</td>
<td>[N29]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FATIGUE</td>
<td>FAT</td>
<td>[N29]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LADY GAGA</td>
<td>LAC</td>
<td>[N29]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SEXY1215</td>
<td>C-FI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>YOU WIN</td>
<td>N2</td>
<td>- send YOUWIN&quot; &amp; &quot;</td>
<td></td>
<td></td>
</tr>
<tr>
<td>BULLSHIT</td>
<td>N5C</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GOINHOM</td>
<td>N15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>THEMOLE</td>
<td>N7E</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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?!)*

<table>
<thead>
<tr>
<th>Searchable worldwide registration database</th>
<th>International Registry of Mobile Assets, pursuant to the Cape Town Treaty</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Aruba Aircraft Register</td>
<td>- Irish Aircraft Register</td>
</tr>
<tr>
<td>- Australian Aircraft Register</td>
<td>- Latvian Aircraft Register</td>
</tr>
<tr>
<td>- Austrian Aircraft Register</td>
<td>- Lebanese Aircraft Register</td>
</tr>
<tr>
<td>- Belgian Aircraft Register</td>
<td>- Luxembourg Aircraft Register</td>
</tr>
<tr>
<td>- Brazilian Aircraft Register</td>
<td>- New Zealand Aircraft Register</td>
</tr>
<tr>
<td>- British Aircraft Register</td>
<td>- Norwegian Aircraft Register</td>
</tr>
<tr>
<td>- Canadian Aircraft Register</td>
<td>- Singapore Aircraft Register</td>
</tr>
<tr>
<td>- Danish Aircraft Register</td>
<td>- South African Aircraft Register</td>
</tr>
<tr>
<td>- Dutch Aircraft Register</td>
<td>- Swedish Aircraft Register</td>
</tr>
<tr>
<td>- Dutch Historic Aircraft Registers</td>
<td>- Swiss Aircraft Registry</td>
</tr>
<tr>
<td>- Finnish Aircraft Register</td>
<td>- United States Aircraft Registry</td>
</tr>
<tr>
<td>- French Aircraft Register</td>
<td>- Article 20 of the Convention on International Civil Aviation</td>
</tr>
<tr>
<td>- Guatemalan Aircraft Register</td>
<td>- Annex 7 to the Convention on International Civil Aviation</td>
</tr>
<tr>
<td>- Indian Aircraft Register</td>
<td>- Supplement to Annex 7 of the Convention on International Civil Aviation</td>
</tr>
</tbody>
</table>
Public access, seriously? USA (FAA)
Public access, seriously? Australia (CASA)
Public access, seriously? UK (CAA)

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
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 <strong>OUT</strong>/IN (attack)</td>
<td>475 USD</td>
</tr>
<tr>
<td>WBX</td>
<td>ADS-B <strong>OUT</strong>/IN (attack)</td>
<td>450 USD</td>
</tr>
<tr>
<td>DBSRX2</td>
<td>ADS-B <strong>IN</strong> (verify)</td>
<td>150 USD</td>
</tr>
<tr>
<td>Plane Gadget</td>
<td>ADS-B <strong>IN</strong> (verify)</td>
<td>~245 USD</td>
</tr>
<tr>
<td>Attenuators</td>
<td>Limit output (<strong>SMA cable</strong>)</td>
<td>&lt;10 USD</td>
</tr>
<tr>
<td>Cables</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Alternative SDRs
SDR USRP1

### Alternative ADS-Bs
ADS-B OUT/IN (attack)
ADS-B IN (verify)
Limit output (**SMA cable**)
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 guide

- ADS-B data crafting
  - Tweak the captured data
    - Load I/Q data: \( d\_cap = \text{read\_float\_binary}('~/\text{CAPTURED\_adsb.fc32}') \)
    - Modify the samples: \( d\_cft = \text{adsb\_randomize}(d\_cap) \)
    - Write back I/Q data: \( \text{write\_float\_binary}(d\_cft, '~/\text{CRAFTED\_adsb.fc32}') \)
  - Generate the data
    - MatLab – \( \text{modulate}(\text{adsb\_frame}, fc, fs, 'ppm') \)
    - GNUradio – write native C++ block

- Transmit the crafted data:
  - UHD-mode
    - \( \text{tx\_transmit\_samples} --file ~/\text{CRAFTED\_adsb.fc32} --ant "TX/RX" --rate 4000000 --freq 10900000000 --type float --subdev B:0 \)
  - Pre-UHD-mode
    - \( \text{usrp\_replay\_file.py} \)
ADS-B Message Analyze/Visualize/Plot
Quick reference guide

- 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)
```python
def edsh_16BitsCRC(edsh_payload_16_bytes):
    POLY = 0x8F0A4C10
    data = \
        | edsh_payload_16_bytes[3] << 24 | \
        | edsh_payload_16_bytes[1] << 16 | \
        | edsh_payload_16_bytes[2] << 8  | \
        | edsh_payload_16_bytes[3] << 0  |
    data1 = \
        | edsh_payload_16_bytes[3] << 24 | \
        | edsh_payload_16_bytes[1] << 16 | \
        | edsh_payload_16_bytes[4] << 8  | \
        | edsh_payload_16_bytes[7] << 0  |
    data2 = \
        | edsh_payload_16_bytes[3] << 24 | \
        | edsh_payload_16_bytes[3] << 16 | \
        | edsh_payload_16_bytes[10] << 8 |
    logging.info('init dataX', hex(data), hex(data1), hex(data2))
    result = 0x00000000
    for i in range(0, 80):
        logging.info('data', hex(data))
        if (data & 0x80000000) <> 0:
            data = data ~ POLY
            logging.info('data (if)', hex(data))
        data = data << 1
        logging.info('data <<', hex(data))
        logging.info('data1', hex(data1))
        if (data1 & 0x80000000) <> 0:
            data1 = data1 | 1
            logging.info('data1 (if)', hex(data1))
        data1 = data1 << 1
        logging.info('data1 <<', hex(data1))
        logging.info('data2', hex(data2))
        if (data2 & 0x80000000) <> 0:
            data2 = data2 | 1
            logging.info('data2 (if)', hex(data2))
        data2 = data2 << 1
        logging.info('data2 <<', hex(data2))
    result = result ^ data
    logging.debug(hex(data >> 8), hex(result >> 8))
    return result >> 8
```
Demo showtime

- [Link](http://www.youtube.com/zveriu)
Agenda

1. ATC Today (SSR)
2. Today’s Problems
3. ATC “Tomorrow” (ADS-B)
4. “Tomorrow”s Problems
5. Exploit scenarios & Demos

Solutions and take-aways
High-level perspective – Timelines

- **SDR Community**
  - 1988 (Peter Hoeher and Helmuth Lang) - SDR prototype
  - 1991/1992 (Joseph Mitola) - SDR theory and paper
  - October 2003 (Ettus) - USRP1 available $US750
  - September 2008 (Ettus) - USRP2 available $US1700 (http://www.ruby-forum.com/topic/165227)
  - February 2012 (Antti Palosaari) - RTL-SDR discovered (http://thread.gmane.org/gmane.linux.drivers.video-input-infrastructure/44461/topic=44461)

- **ADS-B Standardization/Regulatory**
  - Jul 2002 (FAA) - Federal Aviation Administration (FAA) announced a dual link decision using 1090 MHz ES for air carrier and private/commercial operators of high performance aircraft and UAT for the typical general aviation user as media for the ADS-B system in the United States (http://www.faa.gov/news/press_releases/news_story.cfm?newsId=5520&print=go)
  - March 2003 - First ADS-B demonstrations (AOPA for CAP)
  - April 2003 (RTC) - DO-260A "Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B)"
  - 2004 - US Development & testing stations deployed
  - 2007 - Early estimates stated the cost to equip a general aviation aircraft ranged from $7,644 to $10,920 for ADS-B Out and from $10,444 to $29,770 for ADS-B Out and ADS-B In, depending on aircraft type.
  - 2009 - US Ground segment implementation and deployment
  - 2009 - Assuming 2009 market prices for individual system components, a UAT retrofit was estimated at $18,000 and new at $25,000. For a 1090ES retrofit $4,200 and new at $18,000.
  - Dec 2009 - Australia in world first for nationwide ADS-B coverage

- **Research community**
  - Jan 2001 - An Assessment of the Communications, Navigation, Surveillance (CNS) Capabilities Needed to Support the Future Air Traffic Management System
  - Oct 2001 - Vulnerability assessment of the transportation infrastructure relying on GPS
  - 2002 - Validation techniques for ADS-B surveillance data
  - 2003 - GPS integrity and potential impact on aviation safety
  - Sept 2004 - Aircraft ADS-B Data Integrity Check
  - 2008/2009 - Vast security research on Future eEnabled Aircraft and their support infrastructure
  - Oct 2010 - Identification of ADS-B System Vulnerabilities and Threats
  - 2010 - Assessment and Mitigation of Cyber Exploits in Future Aircraft Surveillance
  - 2010 - Visualization \& Assessment Of ADS-B Security For Green ATM
  - 2011 - Security analysis of the ADS-B implementation in the next generation air transportation system
  - Oct 2011 - Aircraft Systems Cyber Security
  - Oct 2011 - On the Requirements for Successful GPS Spoofing Attacks
  - Jul 2012 - Practical setups and demonstrations on ADS-B attacks (BH12US, DC19)
ADS-B Security Solutions

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

    "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)

- DOT268, Minimum Performance Standards for 1090 MHz Automatic Dependent Surveillance Broadcast (ADS-B) and Traffic Information Services (TIS-B), RTCA DO-268A.
- DOT282B, Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B), RTCA DO-282B.
- DOT236, Application of Airborne Conflict Management: Detection, Prevention, & Resolution, RTCA DO-236.
- RTCA Special Committee 209 ATCRBS / Mode S Transponder Project Requirements, Proposed Change to DO-209D and ED-72C for Higher Speed Levels as Lower Power.
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>