

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

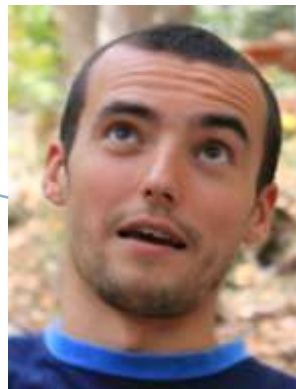
Mifare Classic
MFCUK



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!**

Agenda

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

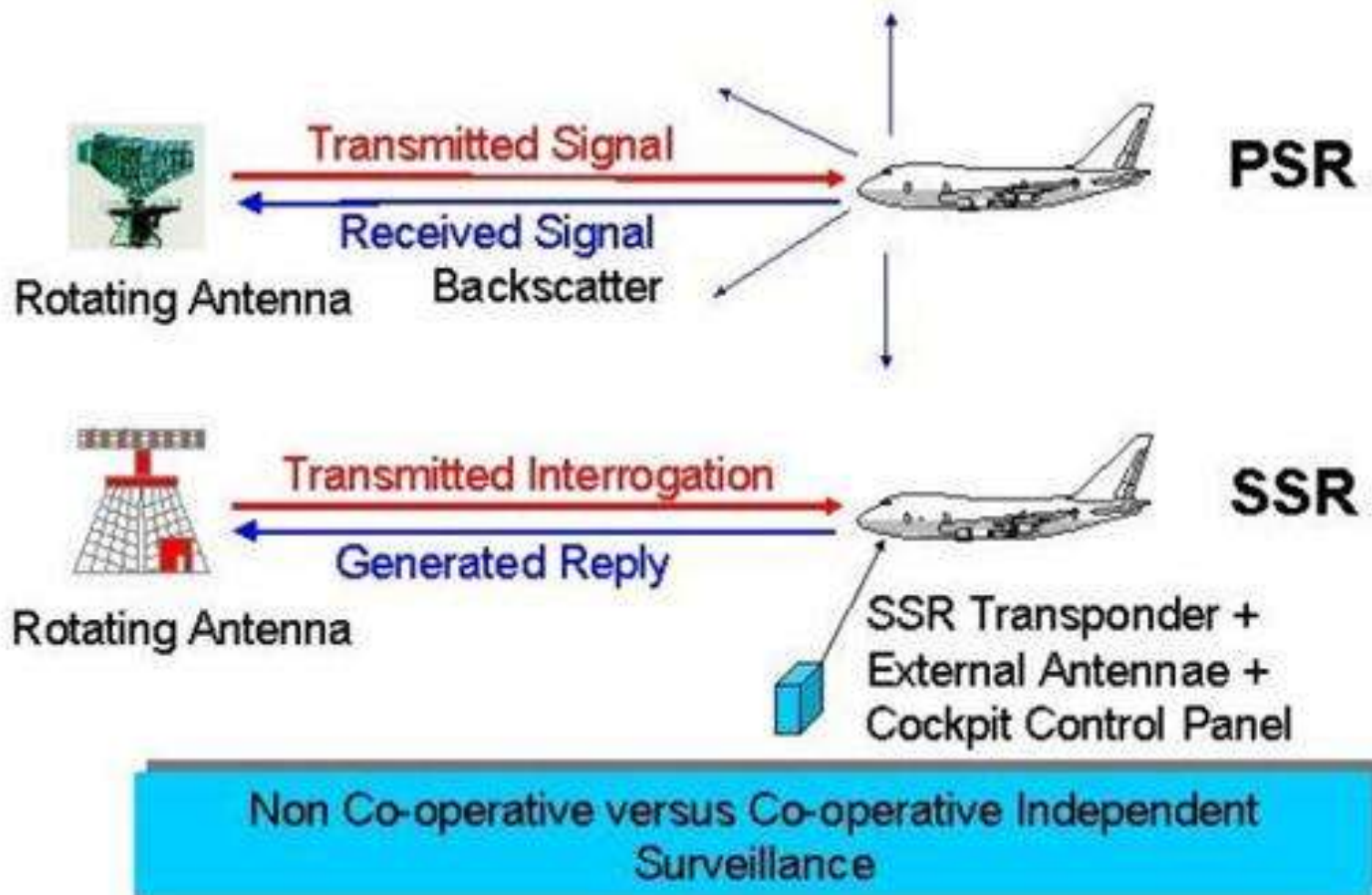


What I think I do

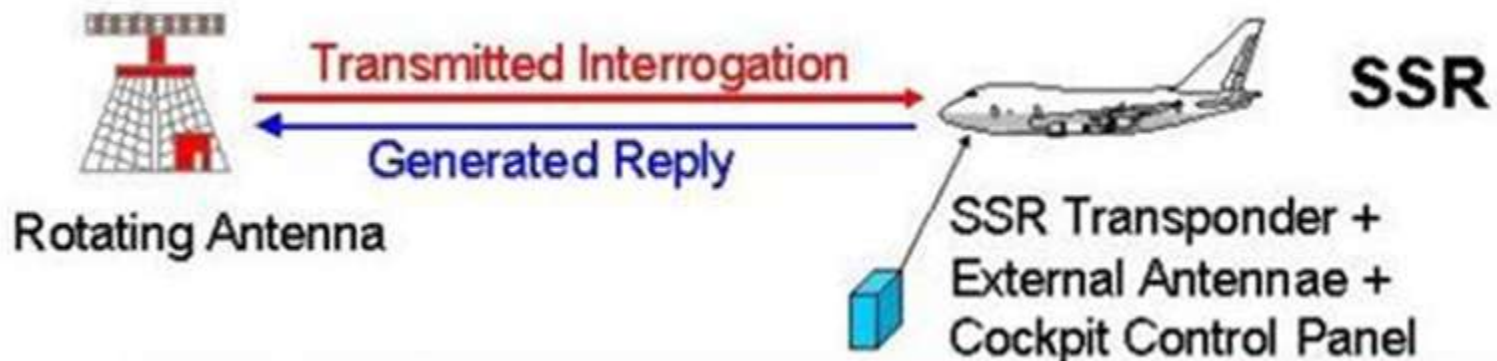


What I actually do

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

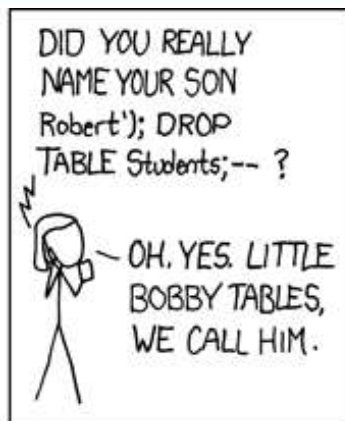
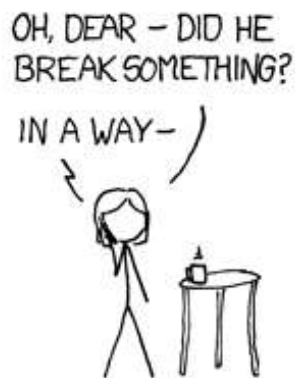
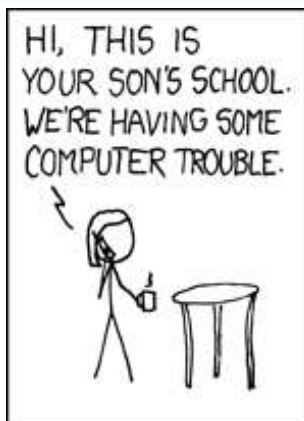
6. Solutions and take-aways

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)

4. "Tomorrow"s Problems

5. Exploit scenarios & Demos

6. Solutions and take-aways

ADS-B is a \$billions world-wide effort from 2002...

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

Investment Description: 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. ADS- More...

FY2012 (CY) Spending: \$301.52 M
Time frame of investment: 2006 - 2035

Status: Continued Major

[Projects](#)
[Current Exhibit 300](#)
[FY12 Exhibit 300](#)
[Contracts](#)
[Baseline Change History](#)
[Evaluation History](#)

EXHIBIT 300

UII 021-142305975

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

1.

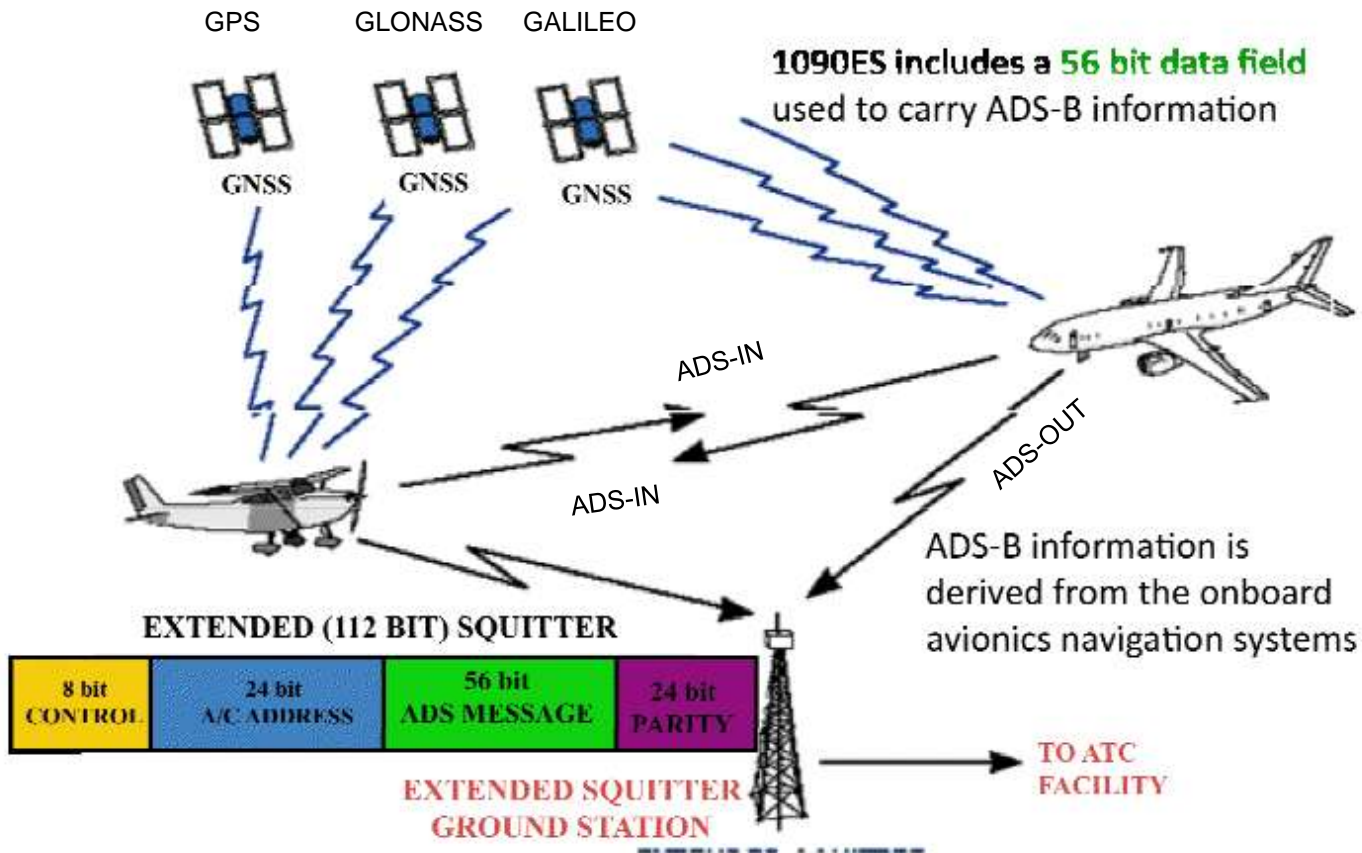
Table I.C.1 Summary of Funding

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

How does ADS-B work? – Architectural view

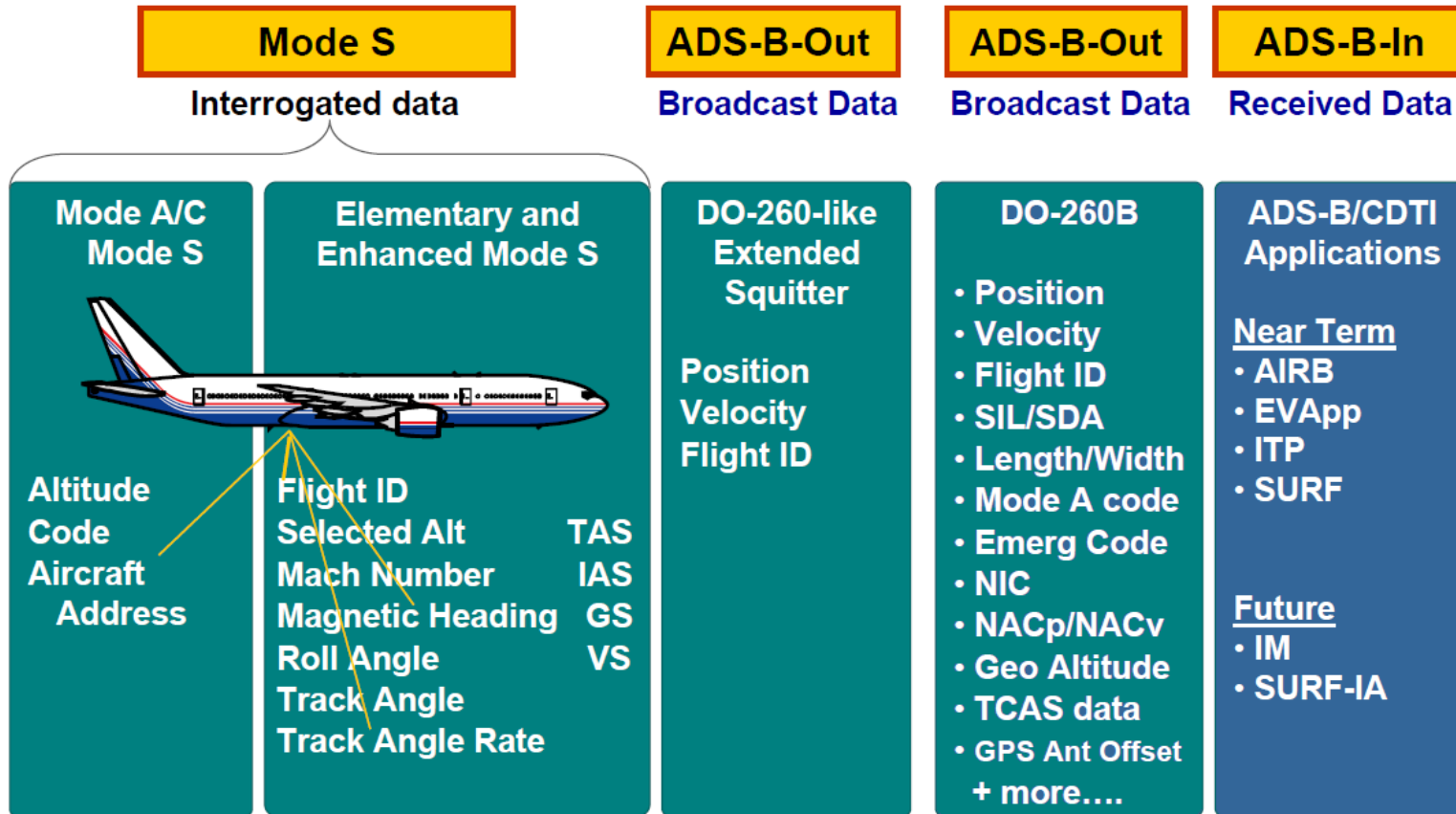
Guidance for the Provision of Air Traffic Services Using ADS-B for Airport Surface Surveillance

2.1.1 ADS-B Out and ADS-B IN



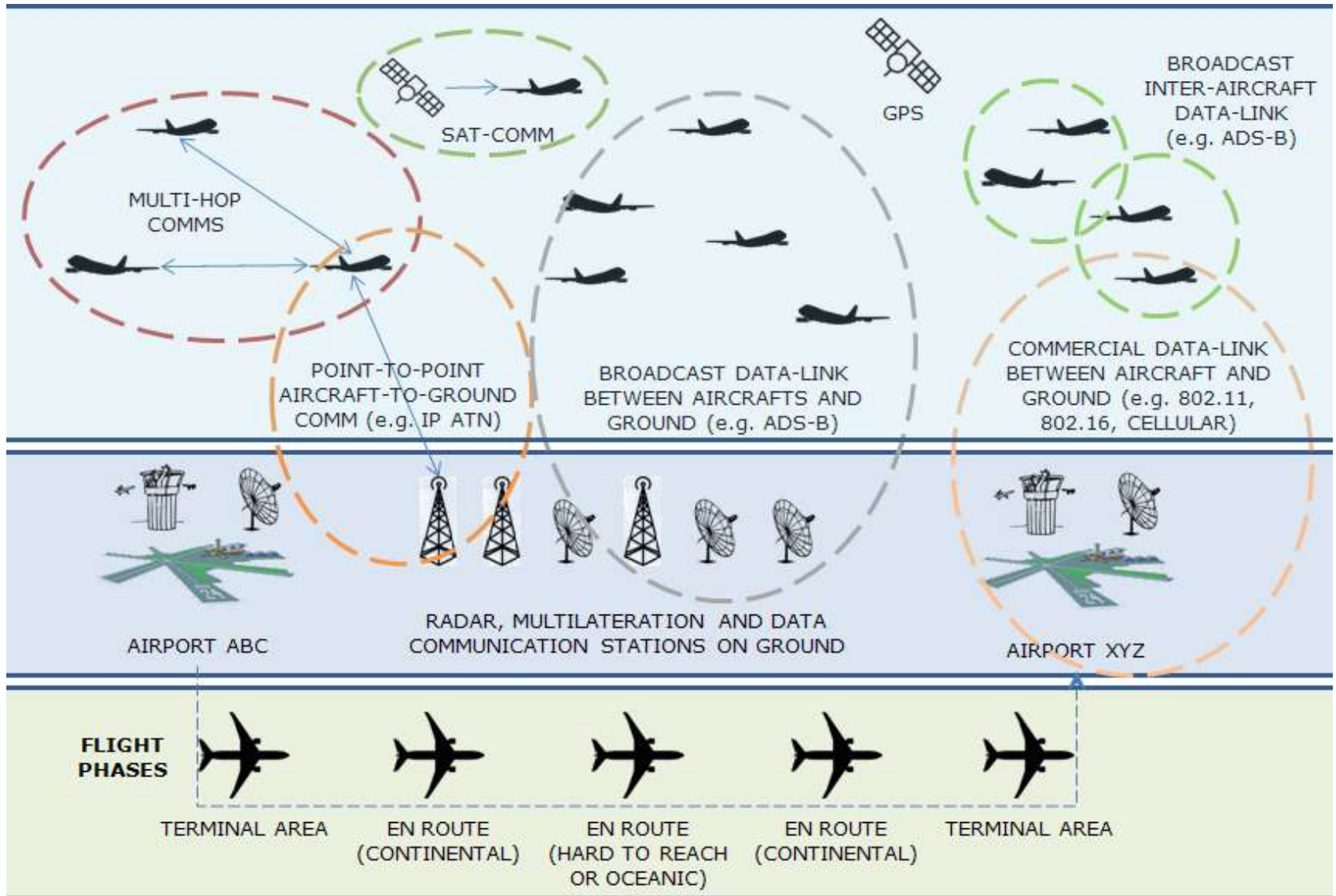
ADS-B Out and ADS-B In – Simplified Functional Diagram

ADS-B – INsideOUT...



- ADS-B is being used over 2 existing technologies:
 - Mode-S – 1090 MHz (replies) and 1030 MHz (interrogation)
 - 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/

portals network status

[Home](#) [About us](#) [Careers](#) [Flight briefing](#) [Publications](#) [Media](#) **Projects** [Services](#) [Environment](#) [Aircraft noise](#) [Online store](#) [Contact us](#)

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](#)

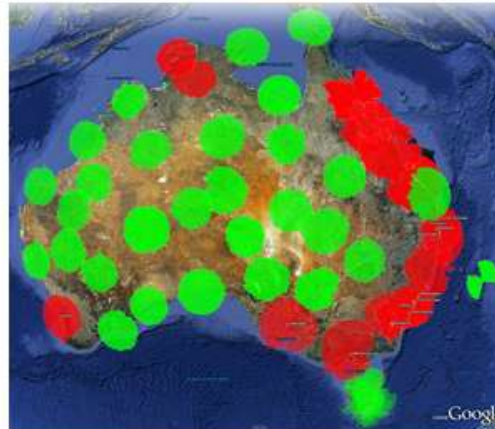
[Collaborative decision making](#)

[Fire control centre upgrade](#)

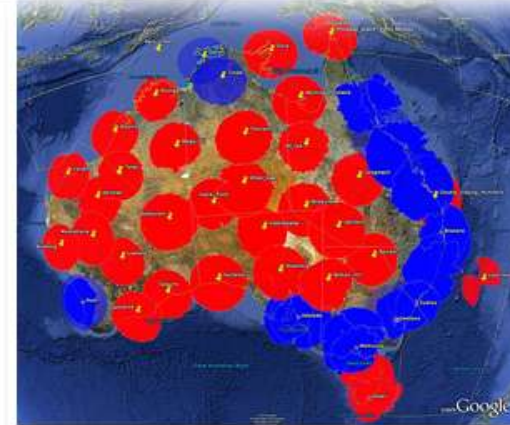
[Ground Based Augmentation System](#)

[National towers program](#)

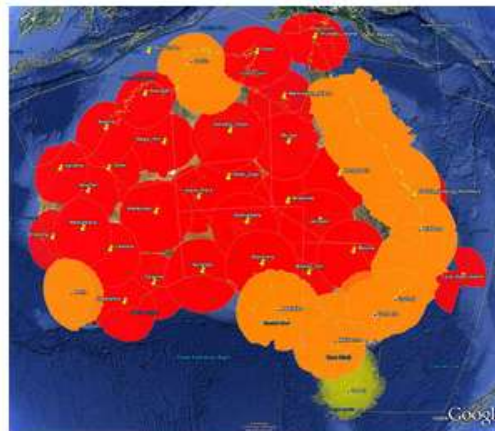
[Remote Tower Technology](#)



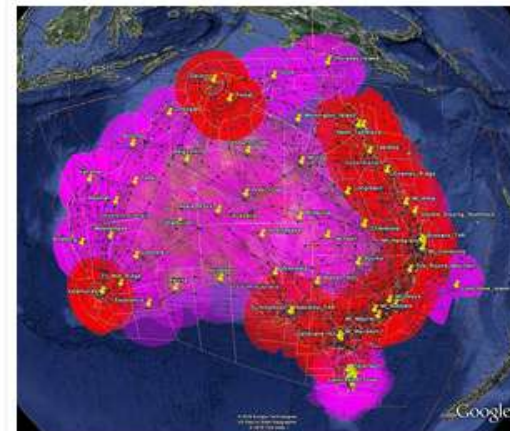
ADS-B End State Coverage at 5,000 feet



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

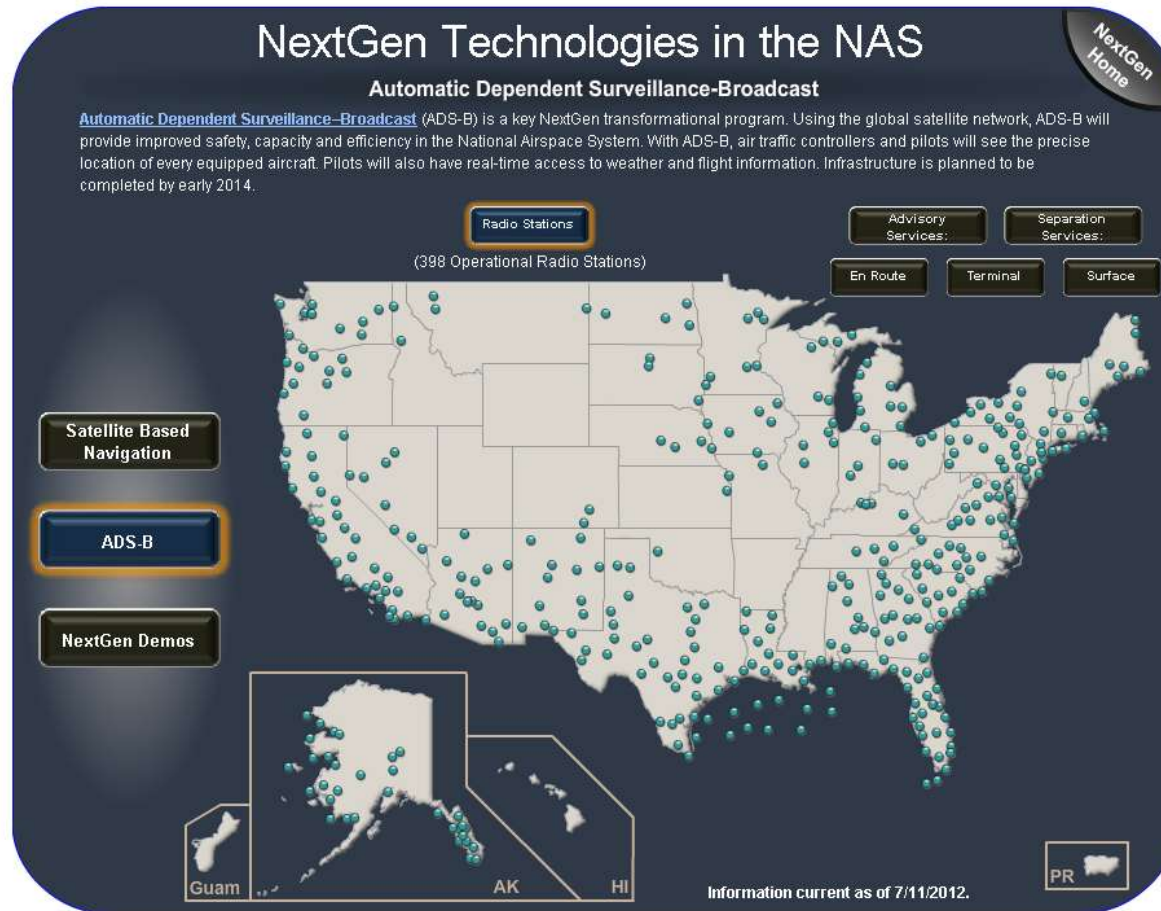
ADS-B Deployment Map – USA

www.faa.gov/nextgen/flashmap/

FAA Home » NextGen » NextGen Technologies Interactive Map

NextGen Technologies Interactive Map

 Print  Email



Page Last Modified: 08/09/10 11:06 ET

How does community get this data?

AirNav RadarBox



Mode-S Beast with miniASDB



Kinetic SBS



PlaneGadgets ADS-B



Aurora Eurotech SSRx



microADS-B USB



miniADS-B



Funkwerk RTH60



microADS-B-IP BULLION



How does ADS-B look like? – Community view

www.flightradar24.com

flightradar24
LIVE AIR TRAFFIC

APPS INCREASE COVERAGE ABOUT FORUM CHAT

BAW164

Airline: British Airways
Flight: BA164
From: Tel Aviv, Ben Gurion (TLV)
To: London, Heathrow (LHR)
Aircraft: Boeing 777-236 (B772)
Reg: G-VIII
Altitude: 40000 ft (12102 m)
Speed: 435 kt (806 km/h, 501 mph)
Track: 297°
Hex: 4005BB
Squawk: 2767
Pos: 48.0048 / 5.7793
Radar: EDDF4

Aircraft view (BEV) Report track error

flight diary users on board this flight

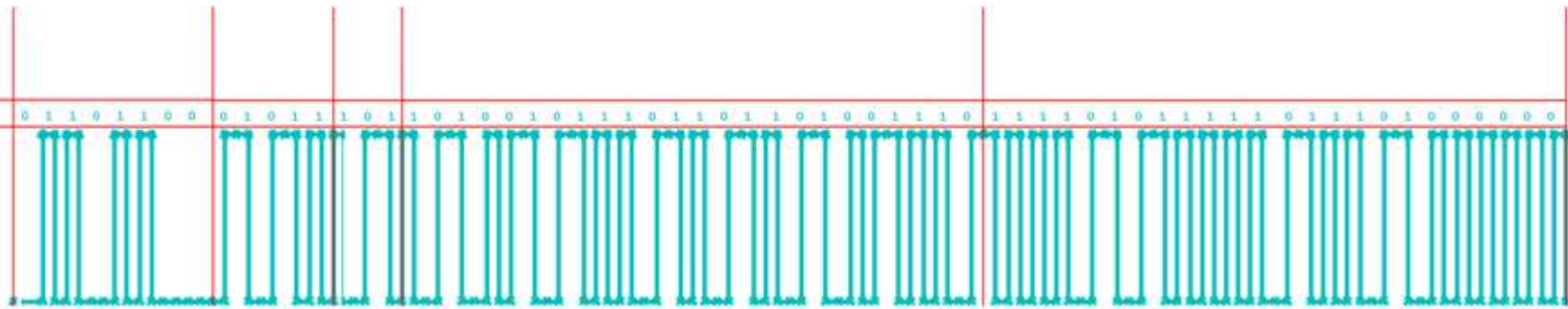
None

What's happening?

Aircraft View - BAW164
<http://www.flightradar24.com/BAW164View>

Google Earth
Data: SIO NOAA US Navy NGA GEBCO
© 2012 Cesium Software
Image © 2012 TerraMetrics
Image © 2012 CN-France

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

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

Agenda

1. ATC Today (SSR)
2. Today's Problems
3. ATC "Tomorrow" (ADS-B)

▶ "Tomorrow"s Problems

5. Exploit scenarios & Demos
 6. Solutions and take-aways
-

ADS-B Main Threats – Summary

ADS-B Threat

Entity/message authentication



Entity authorization (eg. medium access)*



Entity temporary identifiers/privacy



Message integrity (HMAC)



Message freshness (non-replay)



Encryption (message secrecy)



Massive public DBs with private detail*



Fail / warn / ok

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 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

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: *external abusers* + public data correlation



Have a well-defined target

Poses inexpensive devices

Strategically positioned



Can publicly access private details (**why is this allowed?!**)

en.wikipedia.org/wiki/Aircraft_registration

- 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 [📄](#)

Public access, seriously? USA (FAA)



Federal Aviation
Administration

Aircraft Inquiries

- N-number
- Serial Number
- Name
- Make / Model
- Engine Reference
- Dealer
- Document Index
- State and County
- Territory and Country
- Pending / Expired / Canceled Registration Reports
- Recent Registration
- N-number Availability
 - Request A Reserved N-Number
 - Online
 - In Writing
 - Reserved N-Number Renewal
 - Online
 - Request for Aircraft Records
 - Online
- Help
- Main Menu
- Aircraft Registration
- Aircraft Downloadable Database
- Definitions
- N-Number Format
- Registrations at Risk
- Contact Aircraft Registration

FAA Home » Licenses & Certificates » Aircraft Certification » Aircraft Registration » Aircraft Inquiry » N-Number Inquiry

Warning:

NOTICE

The FAA Registry will be performing maintenance on its web servers beginning Saturday, July 21st. This website will be unavailable from 06:00 AM CDT Saturday morning through 11:30 PM CDT Sunday night. We apologize for the inconvenience.

FAA REGISTRY N-Number Inquiry Results

N1 is Assigned

Data Updated each Federal Working Day at Midnight

[Download the Aircraft Registration Database \(29 MB\)](#)
Aircraft Certificate Expiration Date has been added to the Master Download file.

Aircraft Description

Serial Number	1071	Type Registration	Government
Manufacturer Name	GULFSTREAM AEROSPACE	Certificate Issue Date	02/14/1990
Model	G-IV	Expiration Date	12/31/2013
Type Aircraft	Fixed Wing Multi-Engine	Status	Valid
Pending Number Change	None	Type Engine	Turbo-fan
Date Change Authorized	None	Dealer	No
MFR Year	1988	Mode S Code	50000001
		Fractional Owner	NO

Registered Owner

Name	FEDERAL AVIATION ADMINISTRATION		
Street	NATL FLIGHT PROGRAM OVERSIGHT OFC		
	6125 SW 68TH ST RM 137N		
City	OKLA CITY	State	OKLAHOMA
County	OKLAHOMA	Zip Code	73169-1225
Country	UNITED STATES		

Airworthiness

Engine Manufacturer	ROLLS-ROYCE	Classification	Standard
Engine Model	TAY MK 610-8	Category	Transport
		AW Date	09/09/1988

Public access, seriously? Australia (CASA)

safe skies for all

Australian Government
Civil Aviation Safety Authority

Search CASA

HOME OPERATIONS AIRWORTHINESS REGULATIONS AND POLICY MANUALS AND FORMS EDUCATION SERVICES ABOUT CASA

Menu
Home
Site Map

Registered Operator State
ACT (187)
Brunei (1)
Hong Kong (1)
Island (1)
Minnesota (2)
Morobe (1)
N.T. (5)
NSW (4019)
NT (536)
Other (1)
more...

Year of Manufacture
2012 (107)
2011 (307)
2010 (293)
2009 (239)
2008 (387)
2007 (397)
2006 (320)
2005 (334)
2004 (307)
2003 (267)
more...

Year First Registered
1925 (1)
1927 (1)
1928 (2)
1930 (1)
1935 (1)
1936 (7)
1937 (6)
1938 (1)
1939 (2)

Aircraft type
Glider (979)
Manned Free Balloon (383)
Motor-Glider (218)
Power Driven
Aeroplane (11244)
Rotorcraft (1971)

Manufacturer
Aero Commander (62)
Aero Engine Service Ltd (18)
Aero Vodochody (16)
Aerospatiale Industries (111)
Aerostar Aircraft Corporation (15)
Agusta, Spa, Costruzioni Aeronautiche (52)
Air Tractor Inc (148)
Airbus Industrie (112)
Airparts Nz Ltd (24)
Alexander Schleicher Segelflugzeugbau (146)
more...

Registration Holder State
(6)
ACT (185)
Berm (1)
Brunei (1)
Ca (6)
California (3)
Chi (2)
Clare (2)
Ct (2)
Delaware (2)

Home > Search

Search results

14773 aircraft match your search criteria.

Search again

Note: A record on the Civil Aircraft Register does not constitute proof of ownership for either the certificate of registration holder or property interest holders.

Fully matching documents

[Download results as CSV](#)

Registration holder as of 07 March 2012
Michael HOPPERS CROSSING VIC 3029 AUSTRALIA
Registered operator as of 07 March 2012
Michael HOPPERS CROSSING VIC 3029 AUSTRALIA
Registration holder as of 27 June 2012
GEORGES HALL NSW 2198 AUSTRALIA
Registered operator as of 27 June 2012
PO Box 121 GEORGES HALL NSW 2198 AUSTRALIA

Power Driven Aeroplane with TAILWHEEL-FIXED landing gear
Single Piston engine
Manufacturer: AMATEUR BUILT AIRCRAFT
Model: VANS RV-7A
Serial number: 72919
Aircraft first registered in Australia: 07 March 2012
Year of manufacture: 2012
Full Registration

Rotorcraft with SKID landing gear
Single Piston engine
Manufacturer: ROBINSON HELICOPTER CO
Model: R22 BETA
Serial number: 4567
Aircraft first registered in Australia: 27 June 2012
Year of manufacture: 2012
Full Registration

Public access, seriously? UK (CAA)

Civil Aviation Authority feedback text-only print

GINFO Database Search

Search for an aircraft's details by entering your search criteria into any number of the fields displayed below. **Data Extracted:** 21/07/2012 at 19:30

Search

Operations and Safety

Aircraft

Aircraft Register

What's New

FAQs

Web Links

E-Mail Contact

Registration Information

Mortgage Information

Registration (without "G-" prefix):

Serial Number:

Aircraft Type or Name:

Registered Owner:

ICAO 24 bit aircraft address (hex):

View De-Registered Aircraft

Search Report



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](#).

Photographs

International Register of Civil Aircraft

DoS constraints

- ADS-B over 1090 MHz Mode-S ES has is PPM @ 1 MHz
 - It means bandwidth 1 Mbps

- For 112 bit messages
 - Upper limits
 - MAX different 9000 fake airplanes
 - OR same fake airplane in 9000 different positions/sec
 - Pretty damn fast UFOs!
 - Assumptions
 - Nobody else (il)legitimately transmits
 - OR the upper limit is decreasing over-linearly with linear increase in transmitters

Hardware setup

Hardware

Functions

Price

SDR USRP1



Main RF support

700 USD

SBX



ADS-B **OUT**/IN (attack)

475 USD

WBX



ADS-B **OUT**/IN (attack)

450 USD

DBSRX2



ADS-B **IN** (verify)

150 USD

Plane
Gadget



ADS-B **IN** (verify)

~245 USD

Attenuators
Cables



Limit output (**SMA cable**)

<10 USD

Alternative SDRs

Alternative ADS-Bs

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 1090000000 -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 1090000000 --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 = read_float_binary('~ /CAPTURED_adsb.fc32')`
 - Modify the samples: `d_cft = adsb_randomize(d_cap)`
 - Write back I/Q data: `write_float_binary(d_cft, '~ /CRAFTED_adsb.fc32')`
 - Generate the data
 - MatLab – `modulate(adsb_frame, fc, fs, 'ppm')`
 - GNUradio – write native C++ block
- Transmit the *crafted* data:
 - UHD-mode
 - `tx_transmit_samples --file ~/CRAFTED_adsb.fc32 --ant "TX/RX" --rate 4000000 --freq 1090000000 --type float --subdev B:0`
 - Pre-UHD-mode
 - `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)`

Code showcase

```
adbsb_modes_crc.py
0 10 20 30 40 50 60
40 def adbsb_112bits_crc(adbsb_payload_11_bytes):
41     POLY = 0xFFFFA0480
42
43     data = \
44         (adbsb_payload_11_bytes[0] << 24) | \
45         (adbsb_payload_11_bytes[1] << 16) | \
46         (adbsb_payload_11_bytes[2] << 8) | \
47         (adbsb_payload_11_bytes[3] << 0)
48
49     data1 = \
50         (adbsb_payload_11_bytes[4] << 24) | \
51         (adbsb_payload_11_bytes[5] << 16) | \
52         (adbsb_payload_11_bytes[6] << 8) | \
53         (adbsb_payload_11_bytes[7] << 0)
54
55     data2 = \
56         (adbsb_payload_11_bytes[8] << 24) | \
57         (adbsb_payload_11_bytes[9] << 16) | \
58         (adbsb_payload_11_bytes[10] << 8)
59
60     logging.info('init dataX', hex(data), hex(data1), hex(data2))
61
62     result = 0x00000000
63
64     for i in range(0, 88):
65         logging.info('data', hex(data))
66         if (data & 0x80000000) <> 0:
67             data = data ^ POLY
68             logging.info('data (if)', hex(data))
69
70         data = data << 1
71         logging.info('data (<<)', hex(data))
72
73         logging.info('data1', hex(data1))
74         if (data1 & 0x80000000) <> 0:
75             data = data | 1
76             logging.info('data (if)', hex(data))
77
78         data1 = data1 << 1
79         logging.info('data1 (<<)', hex(data1))
80
81         logging.info('data2', hex(data2))
82         if (data2 & 0x80000000) <> 0:
83             data1 = data1 | 1
84             logging.info('data1 (if)', hex(data1))
85
86         data2 = data2 << 1
87         logging.info('data2 (<<)', hex(data2))
88
89     result = result ^ data
90     logging.debug(hex(data >> 8), hex(result >> 8))
91
92     return result >> 8
```


ADS-B Fuzzing notes

- PlanePlotter doesn't show at all planes whose ICAO24 starts with 0xxxxx like **031337**
- No indication in the standard it should be this way
- We don't know how real-world radars behave to such fuzzing
 - Anyone in the audience?

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 Hoehner and Helmut 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>)
 - 13 Jan 2010 (Ettus) - WBX Transceiver board available (<http://lists.gnu.org/archive/html/discuss-gnuradio/2010-01/msg00146.html>)
 - 23 Mar 2011 (Ettus) - USRP N200 \$US1500 and USRP N210 \$US1700 available (http://lists.ettus.com/pipermail/usrp-announce_lists.ettus.com/2011-March/000007.html)
 - 15 Apr 2011 (Ettus) - SBX Transceiver board available (http://lists.ettus.com/pipermail/usrp-announce_lists.ettus.com/2011-April/000008.html)
 - February 2012 (Antti Palosaari) - RTL-SDR discovered (<http://thread.gmane.org/gmane.linux.drivers.video-input-infrastructure/44461/focus=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)"
 - Jul 2004 (RTC) - DO-282A "Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance – Broadcast."
 - 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 - First public 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:

Guidance Material on Surveillance Technology Comparison

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

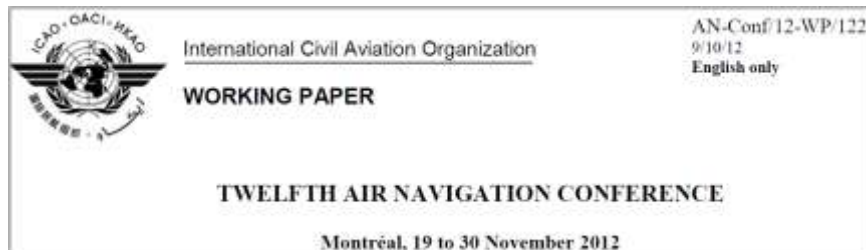
Edition 1.0

September 2007

Page 41

- “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 – THE GOOD



2. DISCUSSION

2.1 There are already a number of examples of cyber security incidents and vulnerabilities:

- a) vulnerability: An extract from the media in July 2012: “At a recent conference ~~Dr.~~ Andrei Costin gave an unnerving demonstration of weaknesses in the air traffic control systems coming into use. He showed that with just \$2 000 worth of store-bought electronics an ADS-B beacon could be ‘spoofed’ to show that a non-existent aircraft was coming in to land. This ‘Ghost Plane’ presentation was possible because air traffic control systems have no way of verifying where messages are coming from”;

Cost (Euros)	Reason
1.3 Billion	Loss of airlines earnings - reported by IATA
12,700	Estimated financial damage per cancelled flight in Germany.
3M per day	Estimated loss of ATM earnings.
1-1.5 million euros per hour	Estimated cost of a complete ATM failure (this figure includes the airline, airport and ATM losses), made by a major European airport.

The Conference is invited to:

- a) recognize the risks in the current situation and the potential for future problems;
- b) create a Cyber Security Task Force (CSTF) to evaluate the extent of the problem and draw up a global cyber security architecture, which includes contributions from industry;
- c) encourage states to provide the Aeronautical Communications Panel (ACP) with the resources to complete its work in developing a robust, secure aeronautical telecommunication network (ATN) using IPV6 as a foundational part of the next generation air traffic management systems; and
- d) encourage States and industry to contribute to the work of the CSTF to ensure aircraft can interoperate with air navigation service providers (ANSPs) around the globe.

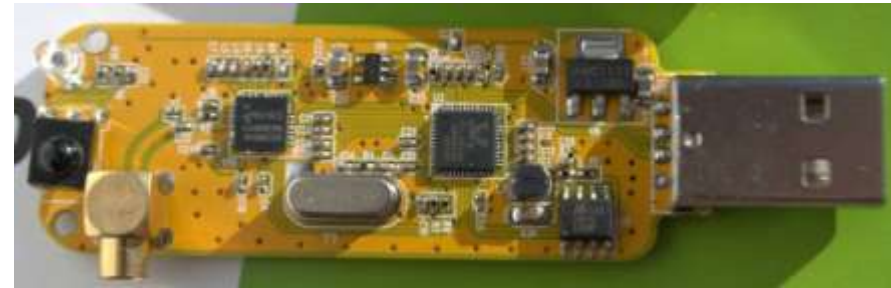
Take-aways – THE BAD

- 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 architectural root-cause

Take-aways – THE UGLY

- Portable RF sniffer
 - Uber cheap (25 USD)
 - few MHz ~ 2.x GHz
 - RTL-SDR via RTL 2832U + E4000



- Portable 'universal' RF transceiver
 - Cheap (300 USD)
 - few MHz ~ 2.x GHz
 - [HackRF](#) by mossmann
 - Exponentially more functionality
 - Compared to 2009 PM3 price



- TCAS
 - 100% affected user base vs ~30% on ADS-B
 - Involves TAs & Ras
 - *pilots are expected to respond immediately to the RA*
 - *aircraft will at times have to manoeuver contrary to ATC instructions or disregard ATC instructions*
 - Custom Verilog required
 - More stable/precise timing required

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

- [1] K. Sampigethaya, R. Poovendran, L. Bushnell, *Assessment and Mitigation of Cyber Exploits in Future Aircraft Surveillance*, Aerospace Conference (AC), 2010 IEEE
- [2] K. Sampigethaya, R. Poovendran, *Visualization & Assessment Of ADS-B Security For Green ATM*, Digital Avionics Systems Conference (DASC), 2010 IEEE/AIAA 29th
- [3] K. Sampigethaya, R. Poovendran, L. Bushnell, *A Framework for Securing Future e-Enabled Aircraft Navigation and Surveillance*, AIAA Proceedings, 2009
- [4] K. Sampigethaya, R. Poovendran, S. Shetty, T. Davis, C. Royalty *Future E-Enabled Aircraft Communications and Security: The Next 20 Years and Beyond*, Proceedings of the IEEE, Vol. 99, No. 11, November 2011
- [5] K. Sampigethaya, R. Poovendran, *Privacy of future air traffic management broadcasts*, Digital Avionics Systems Conference, 2009. DASC '09. IEEE/AIAA 28th
- [6] K. Sampigethaya, R. Poovendran, L. Bushnell, *Secure Operation, Control, and Maintenance of Future E-Enabled Airplanes*, Proceedings of the IEEE, Dec 2008
- [7] K. Sampigethaya, R. Poovendran, *Security and Privacy of Future Aircraft Wireless Communications with Offboard Systems*, Communication Systems and Networks (COMSNETS) 2011, IEEE
- [8] K. Sampigethaya, R. Poovendran, L. Bushnell, *Secure Wireless Collection and Distribution of Commercial Airplane Health Data*, IEEE Aerospace and Electronic Systems Magazine, 2009, 34(7): 14, 20
- [9] L. Kenney, J. Dietrich, J. Woodall, *Secure ATC surveillance for military applications*, Military Communications Conference, MILCOM 2008, IEEE
- [10] D. McCallie, J. Butts, R. Mills, *Security analysis of the ADS-B implementation in the next generation air transportation system*, International Journal of Critical Infrastructure Protection, No. 4 (2011), Pag. 7887
- [11] J. Krozel, D. Andrisani, M. A. Ayoubi, T. Hoshizaki, C. Schwalm, *Aircraft ADS-B Data Integrity Check*, AIAA Aircraft Technology, Integration, and Operations Conf., Chicago, IL, Sept., 2004
- [12] A.C. Drumm, E.M. Shank, *Validation techniques for ADS-B surveillance data*, Digital Avionics Systems Conference, 2002. Proceedings. The 21st
- [13] S. Thompson, D. Spencer, J. Andrews, *An Assessment of the Communications, Navigation, Surveillance (CNS) Capabilities Needed to Support the Future Air Traffic Management System*, Project Report ATC-295, 10 January 2001, Massachusetts Institute Of Technology, Lexington, Massachusetts
- [14] B. Nuseibeh, C.B. Haley, C. Foster, *Securing the Skies: In Requirements We Trust*, Computer, IEEE Journals & Magazines, Sept. 2009
- [15] B. Nuseibeh, C.B. Haley, C. Foster, *Securing the Skies: In Requirements We Trust*, Computer, IEEE Journals & Magazines, Sept. 2009
- [16] L. Purton, H. Abbass, S. Alam, *Identification of ADS-B System Vulnerabilities and Threats*, Australian Transport Research Forum, Canberra, October, 2010
- [17] Federal IT Dashboard - An Official Website of the United States Government FAAXX704: *Automatic Dependent Surveillance-Broadcast (ADS-B)*, www.itdashboard.gov/investment?buscid=3
- [18] Federal Aviation Administration (FAA), *Air Traffic Bulletin, Special Issue 2005-3, August 2005*, www.faa.gov/air_traffic/publications/bulletins/mc/ia/ath_aug_05.pdf
- [19] *DO-282B, Minimum Operational Performance Standards for Universal Access Transceiver (UAT) Automatic Dependent Surveillance-Broadcast (ADS-B)*, RTCA Paper Number 190-09/SC186-286, RTCA DO-282B, 2009
- [20] *DO-249, Development and Implementation Planning Guide for Automatic Dependent Surveillance Broadcast (ADS-B) Applications*, RTCA DO-249
- [21] *DO-260A, Minimum Operational Performance Standards for 1090 MHz Automatic Dependent Surveillance Broadcast (ADS-B) and Traffic Information Services (TIS-B)*, RTCA DO-260A
- [22] *DO-242A, Minimum Aviation System Performance Standards for Automatic Dependent Surveillance Broadcast (ADS-B)*, RTCA DO-242A
- [23] *DO-263, Application of Airborne Conflict Management: Detection, Prevention, & Resolution*, RTCA DO-263
- [24] DoT, FAA, Technical Standard Order, *Airborne Navigation Sensors Using The Global Positioning System (GPS) Augmented By The Wide Area Augmentation System (WAAS)*, TSO-C145a
- [25] End-to-End System Preliminary Hazard Analysis Matrix of Scenarios, *FAA Capstone Safety Engineering Report #1 ADS-B Radar-Like Services*, Volume 2
- [26] Electronic Code of Federal Regulations, Title 47: Telecommunication, *PART 15RADIO FREQUENCY DEVICES, Subpart B Unintentional Radiators*,
- [27] *Surveillance and Conflict Resolution Systems Panel (SCRSP), Civil-Military Interoperability with Military Mode S Format 22*, SCRSP/WG-A/B, Montreal, 26th to 7th May 2004,
- [28] R.D. Grappel, R.T. Wiken, *Guidance Material for Mode S-Specific Protocol Application Avionics*, Project Report ACT-334, Lincoln Laboratory, MIT,
- [29] RTCA Special Committee 209 ATCRBS / Mode S Transponder MOPS Maintenance, *Proposed Change to DO-181D and ED-73C for Higher Squitter Rates at Lower Power*,
- [30] Jim McMath, *Automated Dependent Surveillance - Broadcast Military (ADS-M)*,
- [31] Vincent Orlando, *Extended Squitter Update*, adsh.tc.faa.gov/WG3_Meetings/Meeting1/1090-WP-1-01.pdf
- [32] N. O. Tippenhauer, C. Pper, K. B. Rasmussen, S. Capkun, *On the Requirements for Successful GPS Spoofing Attacks*, CCS11, October 1721, 2011, Chicago, Illinois, USA
- [33] E. Lester, J. Hansman, *Benefits and incentives for ADS-B equipage in the national airspace system*, MIT ICAT Report, ICAT-2007-2, 2007
- [34] W. Ochieng, K. Sauer, D. Walsh, G. Brodin, S. Griffin, M. Denney, *GPS integrity and potential impact on aviation safety*, The Journal of Navigation Vol. 56, 2003
- [35] H.R. Zeidanloo, *Borneo Command and Control Mechanisms*, ICCEE '09, Second International Conference on Computer and Electrical Engineering, 2009
- [36] Yuanyuan Zeng, Kang G. Shin, Xin Hu, *Design of SMS Commanded-and-Controlled and P2P-Structured Mobile Borneo*, WiSec'12, April 1618, 2012, Tucson, Arizona, USA
- [37] C. Xiang, F. Binxing, Y. Lihua, L. Xiaoyi, Z. Tianning, *Andbox: Towards Advanced Mobile Borneo*, LEET'11, 4th Usenix Workshop on Large-Scale Exploits and Emerging Threats, 2011, Boston, Massachusetts, USA
- [38] A. Khalili, J. Katz, W.A. Arbaugh, *Toward secure key distribution in truly ad-hoc networks*, Proceedings of IEEE Symposium on Applications and the Internet Workshops, 2003
- [39] M. Torani, A. Beheshti, *LPKI - A lightweight public key Infrastructure for the mobile environments*, 11th IEEE Singapore International Conference on Communication Systems, 2008
- [40] Ki-Woong Park, Hyunchul Seok, Kyu-Ho Park, *pKASSO: Towards Seamless Authentication Providing Non-Repudiation on Resource-Constrained Devices*, AINAW Advanced Information Networking and Applications Workshops, 2007
- [41] B. Kadri, M. Feham, A. M'hamed, *Lightweight PKI for WSN uPKI*, International Journal of Network Security, 2010
- [42] Righter Kunkel, *Air Traffic Control: Insecurity and ADS-B*, DefCon 17, Las Vegas, USA,
- [43] Righter Kunkel, *Air Traffic Control Insecurity 2.0*, DefCon 18, Las Vegas, USA,
- [44] Brad Haines, *Hacker + Airplanes = No good can come of this*, Confidence X, 2012, Krakow, Poland,
- [45] *A comprehensive summary of existing radio-enthusiasts-level ADS-B devices*, www.andreicostin.com/papers/AdsbComprehensiveDeviceList.xlsx
- [46] RadioReference Community Forum, *Dodgy callsigns from flights*,
- [47] GNU Radio, *A free & open-source software development toolkit that provides signal processing blocks to implement software radios*, gnuradio.org
- [48] CGRAN, *Comprehensive GNU Radio Archive Network*, www.cgran.org
- [49] Ettus Research, *USRP (Universal Software Radio Peripheral)*, www.ettus.com/product/details/USRP-PKG
- [50] Ettus Research, *SBX 400-4400 MHz Rx/Tx transceiver daughterboard*, www.ettus.com/product/details/SBX
- [51] Radar Gadgets, *Plane Gadget ADS-B Virtual Radar*, www.radargadgets.com
- [52] Mini-Circuits, *VAT-10W2+ SMA Fixed Attenuator*, 217.34.103.131/pdfs/VAT-10W2+.pdf
- [53] Discovery Tech News, *Iran's Military Hacks U.S. Stealth Drone*, news.discovery.com/tech/irans-military-hacks-us-stealth-drone.html
- [54] BBC Tech News, *Researchers use spoofing to 'hack' into a flying drone*, www.bbc.com/news/technology-18643134
- [55] SWISS Magazine, *Eco-care reaches new (flight) levels*, May 2012, Pag. 94
- [56] NewScientist Tech, *Air traffic system vulnerable to cyber attack*, www.newscientist.com/article/mg21128295.600-air-traffic-system-vulnerable-to-cyber-attack.html
- [57] USA Today 27 May 2011, *Air France jet's final minutes a free-fall*, www.usatoday.com/news/world/2011-05-27-air-france-crash_n.htm
- [58] Bureau d'Enquêtes et d'Analyses (BEA), *Final Report On the accident on 1st June 2009 to the Airbus A330-203 registered F-GZCP operated by Air France flight AF 447 Rio de Janeiro - Paris*, http://www.bea.aero/en/enquetes/flight.af.447/rapport.final.en.php
- [59] Garmin, *Garmin GDL 90*, www8.garmin.com/specs/gdl90_0903.pdf
- [60] FreeFlight Systems, *Freeflight 1201, 1204, 1203 GPS/WAAS SENSOR SYSTEMS*, www.freeflightsystems.com/docs/FFS_GPS_WAAS.pdf
- [61] Eric Cottrell, *GNURadio 'gr-air' module - pre-UHD-mode Mode-S/ADS-B demodulator and decoder*, github.com/russss/gr-air
- [62] Nick Foster, *GNURadio 'gr-air-modes' module - UHD-mode software-defined radio receiver for Mode S transponder signals, including ADS-B reports from equipped aircraft*, github.com/bistromath/gr-air-modes
- [63] [Discuss-gnuradio] A Chunks to Symbols Related Question, *GNURadio PPM native transmitter block implementation hints*, lists.gnu.org/archive/html/discuss-gnuradio/2012-01/msg00144.html

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](#)

Acknowledgements

- Thanks to Aurelien Francillon, my PhD professor & advisor, for his tremendous support on this research
- Thanks to EURECOM for time offered to finalize this research and whitepaper

Challenge for all POC hackers and not only!

- Check out: code.google.com/p/libadsb
 - Library for ADS-B encoding/decoding and utilities
- Help community – write ASN.1 specifications for ADS-B
 - Easy Wireshark integration + core of libadsb
 - Provide formal specification of lengthy documents
- Teach yourself – improve the demo code above
- Top 4+1 contributors get either one of these:
 - Rtl-sdr dongle
 - Arduino baseboard
 - Raspberry Pi

Fell free to shout: zveriu@gmail.com

Thank you!
Questions, ideas, corrections?



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

