



Air Traffic Control: Insecurity and ADS-B

Righter Kunkel, CISSP, CISA
Security Researcher
defcon 17



Agenda

- Who am I?
- ATC Background
- DOS on a Tower
- State of Airline Security
- Where are we going?
- ADS-B



Who am I?

- Security Field for >12 years
- Worked with secure operating systems: B1, B2
- Firewalls, proxies
- Trainer
- CISSP, CISA
- Ham Radio
- Private Pilot



First

- Is flying safe? YES
- Are planes going to fall out of the sky after this talk? NO
- Is flying safe after this talk? YES
- Is some of this talk illegal? YES

Disclaimer: Don't do this!



Pilots?

- Is any one a pilot?



Our Focus

- We are not going to focus on:
 - Airport physical security
 - Cockpit door security
 - X-Ray security
- Our focus:
 - Computers used by ATC
 - How airplanes report their position to ATC
 - NexGen ATC



Why?

- ATC is busy moving planes through the air
- ATC not focused on network security of equipment being used
 - Who would want to hack a radar scope?

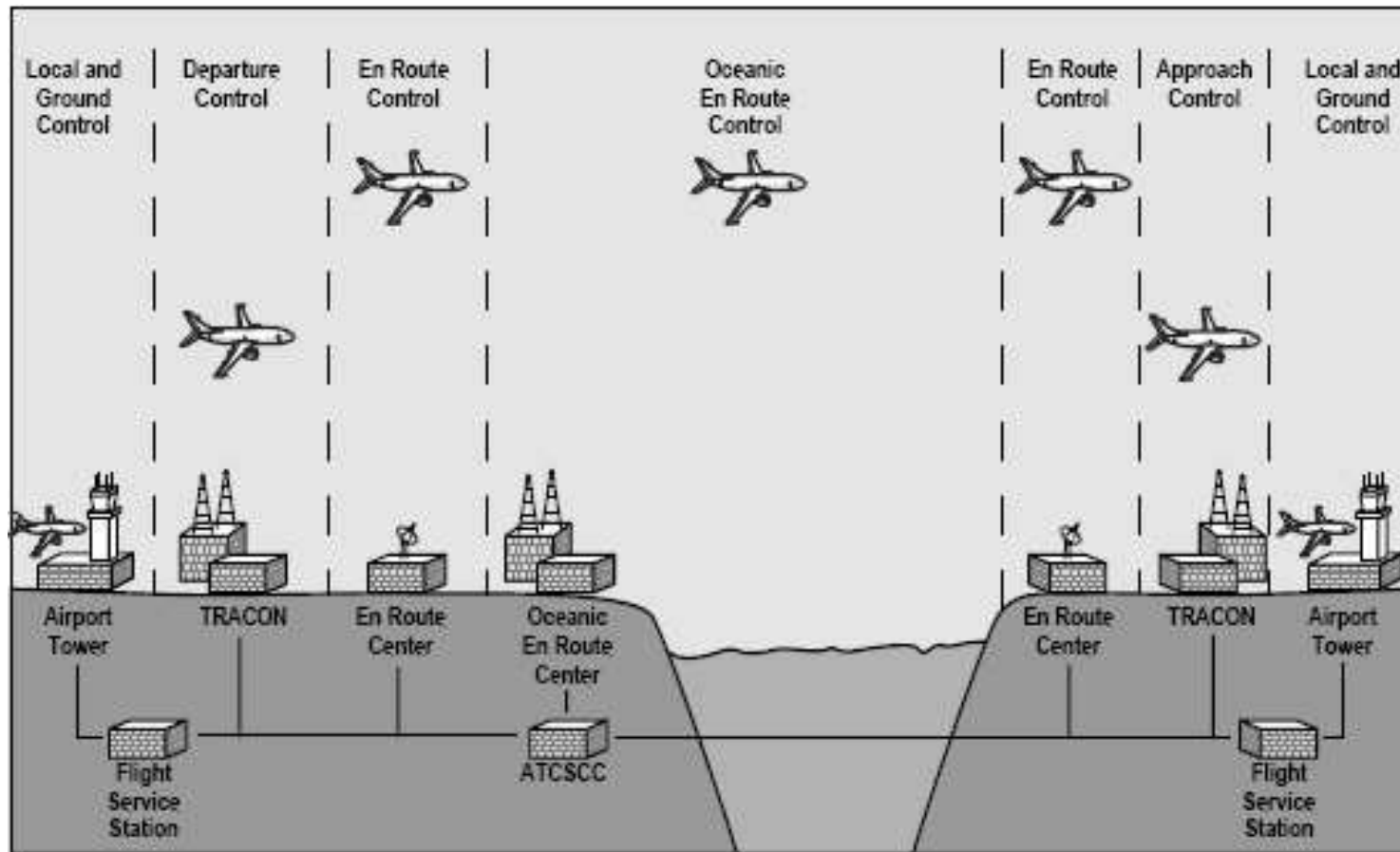


Some ATC Background

- ATC
- VOR
- Transponders
- Flight Plans

ATC

- What is ATC?



Source: GAO/T-AIMD-00-330 FAA Computer Security

VOR

- What are VOR's?
 - VHF Omni-directional Radio Range



Source: Wikipedia

Airplane Transponder



Source: Wikipedia

Mode-S Transponders

- Primary Surveillance Radar (PSR)
 - Paint the skin
- Secondary Surveillance Radar (SSR)
 - Asks planes transponder to send out a signal and data, time based
 - Get unconfirmed ALT from plane



Source: Wikipedia

How do Flight Plans Work?

- Pilot submits a requested route
- Goes into a central computer
- Real flight plan gets printed out at ATC

Form Approved: UMS No. 2120-102/0

U.S. DEPARTMENT OF TRANSPORTATION FEDERAL AVIATION ADMINISTRATION		(FAA USE ONLY) <input type="checkbox"/> PILOT BRIEFING <input type="checkbox"/> VNR			TIME STARTED		SPECIALIST INITIALS	
FLIGHT PLAN				<input type="checkbox"/> STOPOVER				
1. TYPE	2. AIRCRAFT IDENTIFICATION	3. AIRCRAFT TYPE / SPECIAL EQUIPMENT	4. TRUE AIRSPEED	5. DEPARTURE POINT	6. DEPARTURE TIME		7. CRUISING ALTITUDE	
VFR					PROPOSED (Z)	ACTUAL (Z)		
IFR			KTS					
DVFR								
8. ROUTE OF FLIGHT								
9. DESTINATION (Name of airport and city)			10. EST. TIME ENROUTE HOURS MINUTES		11. REMARKS			
12. FUEL ON BOARD HOURS MINUTES		13. ALTERNATE AIRPORT(S)		14. PILOT'S NAME, ADDRESS & TELEPHONE NUMBER & AIRCRAFT HOME BASE			15. NUMBER ABOARD	
				17. DESTINATION CONTACT/TELEPHONE (OPTIONAL)				
16. COLOR OF AIRCRAFT			CIVIL AIRCRAFT PILOTS. FAR Part 91 requires you file an IFR flight plan to operate under instrument flight rules in controlled airspace. Failure to file could result in a civil penalty not to exceed \$1,000 for each violation (Section 901 of the Federal Aviation Act of 1958, as amended). Filing of a VFR flight plan is recommended as a good operating practice. See also Part 99 for requirements concerning DVFR flight plans.					

FAA Form 7233-1 (8-82)
Electronic Version (Adobe)

CLOSE VFR FLIGHT PLAN WITH _____ FSS ON ARRIVAL

Source: Wikipedia



Some interesting attacks in the past

- D.B. Cooper
- 9/11
- People trying to fake their own death

Who Was D.B. Cooper?

- Legendary Skyjacker
- \$200,000
- Parachuted out the back of a 727 in flight
- Never found



Source: Wikipedia



9/11

- I only want to focus on one fact:
 - They turned the transponder off
- We have not developed anything to mitigate that attack country wide
 - ADIZ in DC only defense



Faking Your Own Death

- A Pilot tried to bluff ATC about an emergency
 - Set plane on autopilot
 - Parachuted out of plane
 - Plane intercepted by F16s
 - Plane crashed
 - Pilot got caught



Switching Gears

- My proposed attack:
 - DOS on an ATC tower



A DOS on an ATC Tower

1. Get a fake ID (Of course this is illegal)
2. Get an aviation medical using fake id (also illegal)
3. Get issued a student pilot certificate with certificate number
4. Log into duat.com
5. Create multiple flight plans and submit
6. All flight plans get printed at tower

Medical Cert

Copy of FAA Form 8500-9 (Medical Certificate) or FAA Form 8420-2 Medical Student Pilot Certificate) issued.						FF-		
MEDICAL CERTIFICATE <u>FIRST</u> CLASS AND STUDENT PILOT CERTIFICATE								
This certifies that <i>(Full name and address)</i> : JOHN DOE 123 STREETNAME DR. ANYTOWN, IN 37130								
12/17/03		70		170		BR	BR	M
Date of Birth		Height		Weight		Hair	Eyes	Sex
has met the medical standards prescribed in part 67, Federal Aviation Regulations, for this class of Medical Certificate.								
Limitations	MUST WEAR CORRECTIVE LENSES							
Examiner	Date of Examination 10/17/42		Examiner's Designation No 1013-2					
Signature								
Typed Name JOE DOCTOR, D.O.								
Airman's Signature								

Source: Wikipedia



Web Sites

- Web based way to get weather briefings and enter flight plans
 - Duat.com
 - Duats.com

DTC WEATHER & FLIGHT PLANNING SERVICES
WWW.DUAT.COM

www.duat.com

IMPORTANT NOTICE

At the direction of the FAA, the DUAT service is no longer permitted to file Defense Visual Flight Rules flight plans. These flight plans must now be filed with a Flight Service Station. We regret any inconvenience that this may cause.

Introducing! **DUAT Mobile** Now access **DUAT Mobile** from your Smart Phone or PDA
www.duat.com/mobile

[Notices](#) **DUAT Mobile** [What is DUAT?](#) [Who can use DUAT?](#) [Need Access?](#) [How do I...](#)

Weather SnapShot

Flight Views Tutorial
[Tips & FAQ](#)
[News/Updates](#)
[Windows Software](#)

[Feedback](#)
[QICP](#)
[Contact Us](#)

Access Code: *
Password: *
Aircraft ID: *
* required field
Login



FAA WArning




The DUAT service is an FAA sponsored free service to pilots and dispatchers and other authorized users. Users are encouraged to use the DUAT system as much as is needed and without reservation. Please note that the following statement is directed at potential abusers/hackers and is not meant to discourage legitimate users in any way.

WARNING WARNING WARNING

This is a Federal Aviation Administration (FAA) computer system. FAA systems, including all related equipment, networks, and network devices (specifically including Internet access) are provided for the processing of official U.S. Government information. Unauthorized access or use of this computer system may subject violators to criminal, civil, and/or administrative action. All information on this computer system may be intercepted, recorded, read, copied, and disclosed by and to authorized personnel for official purposes, including criminal investigations. Access or use of this computer system by any person whether authorized or unauthorized, constitutes consent to these terms.

WARNING WARNING WARNING

duat.com



File Flight Plan Tue Jun 16 0432Z

MyDUAT Shortcuts: Pilot Info: Aircraft Info: Route Info:

Flight Plan

Type: Aircraft ID: Departure: Destination: ETD (HHMMz): ETE (HHMM): ETA (DDHHMM):

Aircraft Type: Aircraft Color: Alternate: Fuel (HHMM): Altitude: Airspeed:

Route: Number Aboard:

Remarks: Destination Contact:

Departure Name: Destination Name:

Pilot's Name: Pilot's Address: Pilot's Phone: Home Base:

Save Copy in Stored Requests

Welcome to CSC DUATS on the Web

Please review the [Special Notice](#) (revised 9/24/2004), the [Security Bulletin](#) (revised 8/13/2002), and the [Security Information and Conditions of Use](#) below.

Registered Users



Access Code Password

Main Menu

Close Flight Plan

[Non-SSL DUATS](#)

Forgot your CSC DUATS access code? [Click here.](#)

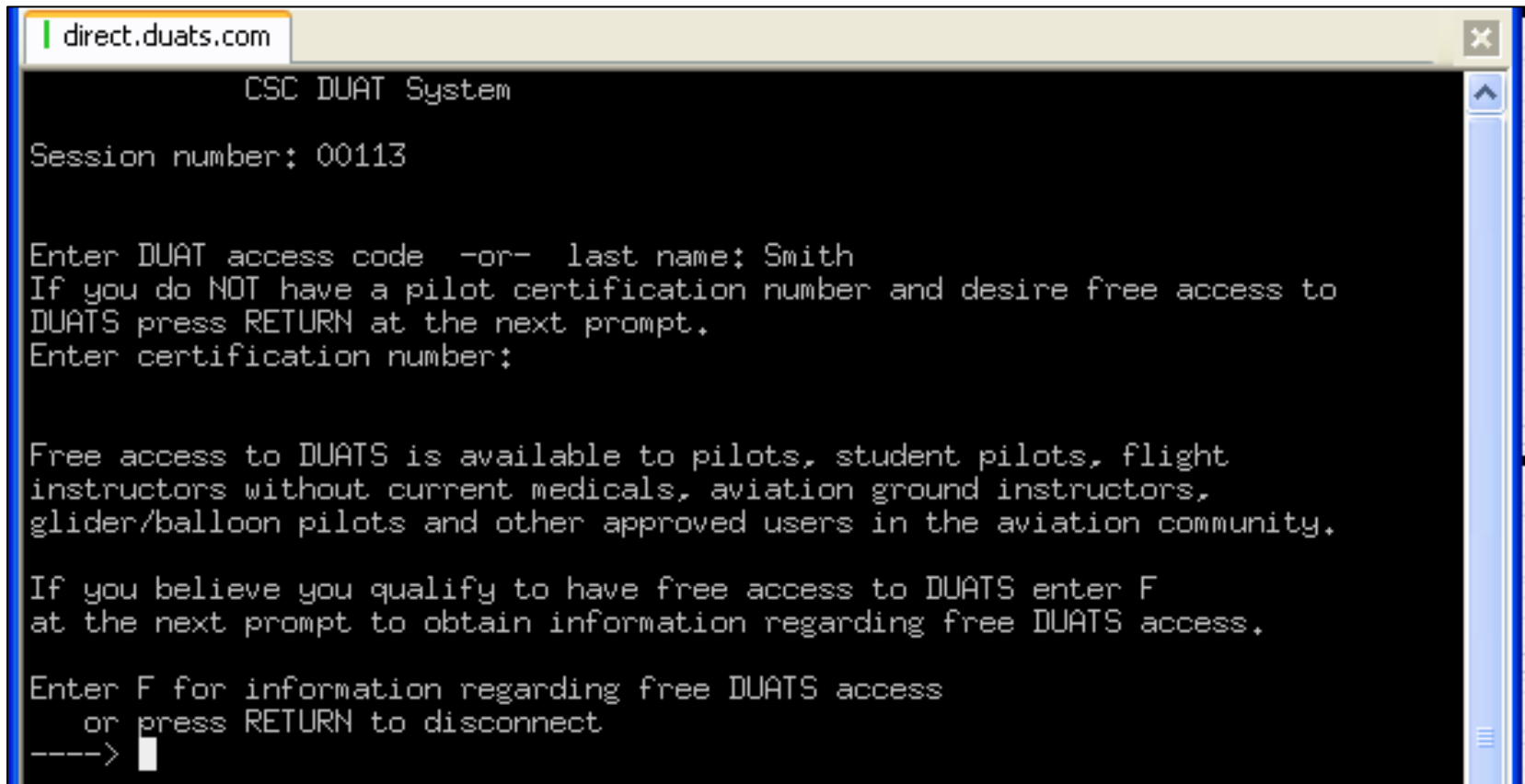
Forgot your password? [Click here.](#)

New Users

Free access to CSC DUATS is available to U.S. pilots and student pilots who hold current medical certificates, flight instructors without current medicals, aviation ground instructors, glider/balloon pilots and other approved users in the U.S. aviation community.

[New User Registration](#)

Telnet access to duats.com



```
direct.duats.com
CSC DUAT System

Session number: 00113

Enter DUAT access code -or- last name: Smith
If you do NOT have a pilot certification number and desire free access to
DUATS press RETURN at the next prompt.
Enter certification number:

Free access to DUATS is available to pilots, student pilots, flight
instructors without current medicals, aviation ground instructors,
glider/balloon pilots and other approved users in the aviation community.

If you believe you qualify to have free access to DUATS enter F
at the next prompt to obtain information regarding free DUATS access.

Enter F for information regarding free DUATS access
  or press RETURN to disconnect
----> █
```

Or Telephone Numbers

Air Traffic Control System Command Center

Main Number.....703-904-4400

RGNL AIR TRAFFIC DIVISIONS

REGION	TELEPHONE
Alaskan	907-271-5464
Central	816-329-2500
Eastern	718-553-4502
Great Lakes	847-294-7202
New England	781-238-7500
Northwest Mountain	425-227-2500
Southern	404-305-5500

Source: A/FD

AIR ROUTE TRAFFIC CONTROL CENTERS (ARTCCs)

ARTCC NAME	*24 HR RGNL DUTY OFFICE TELEPHONE #	BUSINESS HOURS	BUSINESS TELEPHONE #
Albuquerque	817-222-5006	7:30 a.m.-4:00 p.m.	505-856-4300
Anchorage	907-271-5936	7:30 a.m.-4:00 p.m.	907-269-1137
Atlanta	404-305-5180	7:30 a.m.-5:00 p.m.	770-210-7601
Boston	617-238-7001	7:30 a.m.-4:00 p.m.	603-879-6633
Chicago	847-294-8400	8:00 a.m.-4:00 p.m.	630-906-8221

Source: A/FD
defcon 17



Or Radio

- Jam the ATC tower frequencies



State of Airline Insecurity

- I then stepped back and looked around.



FAA Insecurity

- A published report came out:
 - ATC_Web_report.pdf
 - Included on the CD

**REVIEW OF WEB APPLICATIONS SECURITY
AND INTRUSION DETECTION
IN AIR TRAFFIC CONTROL SYSTEMS**

Federal Aviation Administration

Report Number: FI-2009-049

Date Issued: May 4, 2009

Test Results

- Wow!

Table 1. Internet-based and Internal Security Testing Results

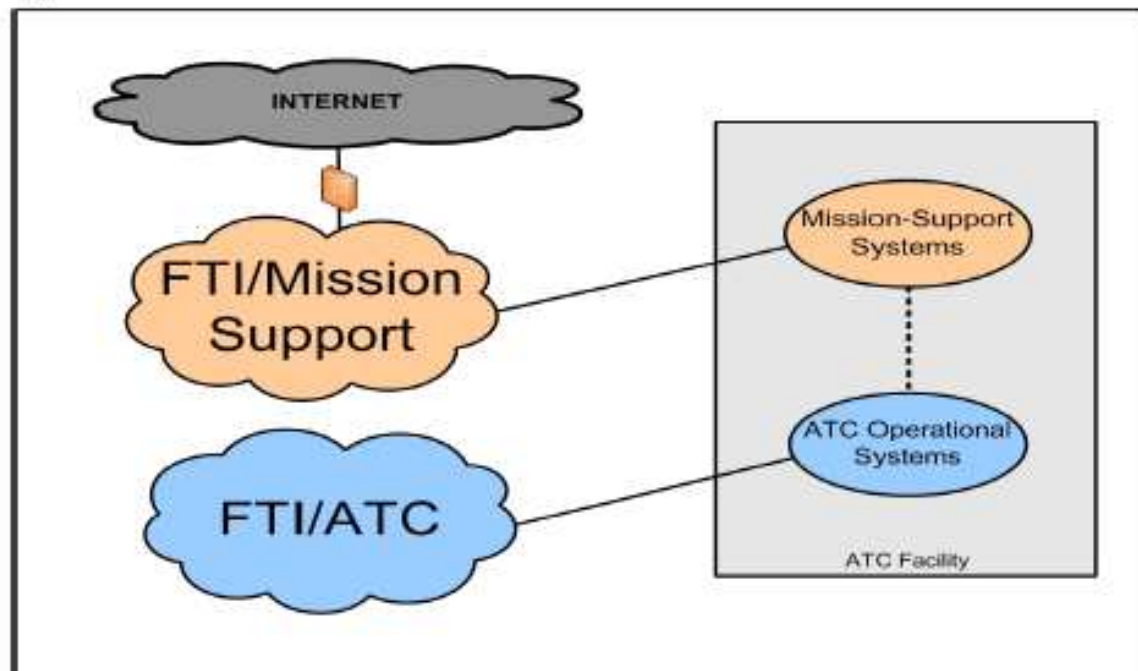
	Number of Web Applications Tested	Number of Vulnerabilities and Risk Level		
		High	Medium	Low
Internet-based (Public Use)	35	212	169	1,037
Internal (FAA Use)	35	551	335	1,553
Total	70	763	504	2,590

Source: KPMG

FAA Network Infrastructure

- The connection that should never happen

Figure 1. ATC IP-based Network Infrastructure^a



^a This infrastructure consists primarily of the backbone FAA Telecommunications Infrastructure (FTI) and several local area networks; FAA relies on this infrastructure to conduct ATC operations. ATC systems are hosted on local area networks at ATC facilities, which have connections to both FTI operational and mission-support networks. (Source: OIG)

IDS Sensors

- Who needs IDS

Table 2. CSMC IDS Sensor Coverage

	Total Number of Facilities	Number of Facilities with IDS Sensors Installed	
		ATC Network	Mission-support Network
Major ATC Facilities			
En route centers	21	0	5
Terminal radar approach control facilities	166	0	4
Airport traffic control towers	512		
Flight service stations	33	0	0
FAA Technical Center	1	0	1
Mike Monroney Aeronautical Center	1	0	1
Remote Sites	*	0	0
Total	734[#]	0	11

* in the thousands

excluding remote sites

Source: FAA

Leaked Data From Report

- ATC_Web_report.pdf
 - I guess we now know what networks are vulnerable

³ While Web technologies are used to support many ATC systems, this audit covered only the following eight systems: FAA's Air Route Traffic Control Center Critical Essential Power System Power Monitoring System (APMS), TECHNET, En Route Automation Modernization/En Route Information Display System (ERAM/ERIDS), Computer-Aided Engineering Graphics (CAEG), Automated Inventory Tracking System ver. 2 (AITSv2), Airport Surveillance Radar—Local Area Network (ASRLAN), Juneau Aviation Weather System (JAWS), and Traffic Flow Management Infrastructure (TFM-I).

S:\\ABU-100\\Share\\OIG GAO\\08-30 Web Applications Security doc:ARWilliams 4/16/09

Appendix A. Management Comments



Where are We Going?

- IDS by Feb. 2010
- NextGen ATC
- ADS-B



NextGen ATC

- Converting from proprietary hardware to commercial off the shelf hardware
- Phasing out radar
- Airplanes transponder will report Lat., Long., and Alt. in clear txt
 - ADS-B



ADS-B Insecurity

- Who am I and where am I in one unencrypted packet
- GPS will be the backbone of NextGen
 - Oh, and GPS sats are failing faster than expected
- One could easily fake an ADS-B transmission
 - No radar to verify true position



Call to Action

- Listen to ATC
- View ADS-B broadcasts
- Become a Pilot



Conclusion

- ATC Background
- DOS on a Tower
- State of Airline Security
- Where are we going?
- ADS-B

Questions





References

- http://en.wikipedia.org/wiki/D._B._Cooper
- http://www.oig.dot.gov/StreamFile?file=/data/pdfdocs/ATC_Web_Report.pdf
- <http://www.airsport-corp.com/adsb2.htm>
- <http://online.wsj.com/article/SB124165272826193727.html#>
- http://en.wikipedia.org/wiki/Pilot_certification_in_the_United_States
- Airport/Facility Directory; FAA Product ID:AFDSW ; www.naco.faa.gov
- http://en.wikipedia.org/wiki/Air_traffic_control_radar_beacon_system
- http://en.wikipedia.org/wiki/VHF_omnidirectional_range
- GAO, FAA COMPUTER SECURITY, GAO/T-AIMD-00-330 FAA Computer Security, Sept. 2000