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

Airplane Transponder

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

How do Flight Plans Work?

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

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
Web Sites

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

Weather SnapShot
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.

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.
defcon 17

Righter Kunkel
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

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

<table>
<thead>
<tr>
<th>REGION</th>
<th>TELEPHONE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alaskan</td>
<td>907–271–5464</td>
</tr>
<tr>
<td>Central</td>
<td>816–329–2500</td>
</tr>
<tr>
<td>Eastern</td>
<td>718–553–4502</td>
</tr>
<tr>
<td>Great Lakes</td>
<td>847–294–7202</td>
</tr>
<tr>
<td>New England</td>
<td>781–238–7500</td>
</tr>
<tr>
<td>Northwest Mountain</td>
<td>425–227–2500</td>
</tr>
<tr>
<td>Southern</td>
<td>404–305–5500</td>
</tr>
</tbody>
</table>

Source: A/FD

AIR ROUTE TRAFFIC CONTROL CENTERS (ARTCCs)

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

Source: A/FD
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>
<thead>
<tr>
<th>Table 1. Internet-based and Internal Security Testing Results</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Table Image" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Web Applications Tested</th>
<th>Number of Vulnerabilities and Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>High</td>
</tr>
<tr>
<td>Internet-based (Public Use)</td>
<td>35</td>
</tr>
<tr>
<td>Internal (FAA Use)</td>
<td>35</td>
</tr>
<tr>
<td>Total</td>
<td>70</td>
</tr>
</tbody>
</table>

Source: KPMG
FAA Network Infrastructure

- The connection that should never happen

Figure 1. ATC IP-based Network Infrastructure

---

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

<table>
<thead>
<tr>
<th>Major ATC Facilities</th>
<th>Total Number of Facilities</th>
<th>Number of Facilities with IDS Sensors Installed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>ATC Network</td>
</tr>
<tr>
<td>En route centers</td>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>Terminal radar approach control facilities</td>
<td>166</td>
<td>0</td>
</tr>
<tr>
<td>Airport traffic control towers</td>
<td>512</td>
<td>0</td>
</tr>
<tr>
<td>Flight service stations</td>
<td>33</td>
<td>0</td>
</tr>
<tr>
<td>FAA Technical Center</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Mike Monroney Aeronautical Center</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Remote Sites</td>
<td>*</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>734#</strong></td>
<td>0</td>
</tr>
</tbody>
</table>

* 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).

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://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