Civil Aviation and CyberSecurity

Dr. Daniel P. Johnson
Honeywell Aerospace Advanced Technology
Outline

• Scope
• Civil aviation regulation
• History
• Cybersecurity threats
• Cybersecurity controls and technology areas
• Unique features of civil aviation and autonomy
• Research considerations

...cybersecurity stories interspersed...
Air Transportation System

Manufacturers

Service Provider Networks

Internet

Passenger Services

Airline IT Infrastructure

Airline Flight Operations

Airline Ground Operations

Wide Area Network

Local Area Network

Maintenance Operations

Airport Operations

ATS Operations

Copyright by Honeywell 2013.
Scope of Cybersecurity Issues in Civil Aircraft

• Cybersecurity Issues in Civil Aircraft
  - Aircraft
    ◆ Flight Safety
    ◆ Mission/Economic
  - Aircraft Traffic Control
    ◆ Flight Safety
    ◆ Traffic Flow
  - Airports
    ◆ Security
    ◆ Flight Safety
    ◆ Mission/Economic

• Regulators
  - National agencies
    ◆ FAA, EASA, Transport Canada, JAA, CAAC, ...
  - International Coordination
    ◆ ICAO

This talk is focused on Aircraft Flight Safety
Securing Civil Aircraft

• Scope of this presentation
  - Aircraft Type Design and Continuing Airworthiness
  - Aircraft Service Providers to aircraft, including Air Traffic Control Services

• Areas not covered:
  - Securing Air Traffic Control Ground Systems
    - In US, regulated under Federal Information Management Security Act (FISMA)
    - Cybersecurity issues similar to other economic sectors
  - Securing Airports
    - Under FAA/ICAO oversight
    - Cybersecurity issues dominated by physical security concerns, otherwise similar to other economic sectors
  - Military and Defense
    - Cybersecurity issues dominated by confidentiality and security classification concerns, otherwise similar to other economic sectors
Airworthiness Cyber Security Scope

ADN Cyber Security Issues

VIRUSES
WORMS
TROJAN HORSES

Mission-critical systems are potentially susceptible to attack

Hackers
Cyber Criminals
Cyber Terrorists
Cybersecurity Regulation for Aircraft

- **Type Certification**
  - Justification that Aircraft design is sufficient to operate in its environment
    - Cyberattack is now part of that environment

- **Continuing Airworthiness**
  - Justification that each aircraft is in a condition sufficient to operate in its environment
    - Documented through log of maintenance problems and actions, and adherence to operating standards

- **RTCA Special Committees develop standards for industry to be invoked by FAA regulation**
How to crash an in-flight entertainment system

Submitted by Hugh Thompson on Fri, 2007-02-09 16:09

Topic(s): Information Security

One of the most interesting examples of a software "abuse case" came to me rather abruptly on an airplane flight from Las Vegas to Orlando in mid 2005.

Each seat in the airplane had a small touch screen monitor built into the head rest of the chair in front, and on this small screen was a touch sensitive keypad that could be used to control the entertainment system.  I happened to have a 2005 model Dell laptop with a touch screen display and a QWERTY keyboard.  I discovered that I could use the touch sensitive keypad to simulate the keyboard.  The keypad had a choice of 14 keys (up, down, left, right, numbers 0-9, and letters A, B, C, D, E, F, and G) and a space bar.  These keys could be configured to simulate keys on the laptop keyboard.

I decided to see if I could configure the keypad to simulate the keys used for a "hot key" on a laptop.  Specifically, I wanted to see if I could make the keypad simulate the "function" key (the key labeled with the symbols for addition, subtraction, multiplication, and division).  After a few minutes of trying, I was able to configure the keypad to simulate the function key.

I then decided to see what other things I could do with the keypad.  I tried to simulate the space bar and the number keys 0-9.  However, I was not able to simulate the other keys on the keyboard, such as the letter keys or the backspace key.

After a couple of seconds the entertainment system crashed.  It turned out to be a Redhat based system that ran from ancient times.
History

- Historically, aircraft only connected through governmentally regulated service providers
  - Flight Plans, ATC directions
  - Radio
  - ACARS (text messages over radio and satellite)
  - Maintenance technicians hand-carry CDs with software updates or navigation database updates
- Engine vendors adding "call home" functions
  - Cell phone units to download engine diagnostic information
- IFE vendors adding cellular service for passengers
  - Not a problem until IFE systems started talking to other avionics
- Boeing and Airbus started providing WiFi for maintenance
  - Remote control of maintenance functions - initiated test, diagnostic information
  - Electronic loading of Navigation Databases and Software Parts
- Vendors adding Flight Planning applications on portable devices
  - Electronic Flight Bags
  - Not a problem until EFB started talking to other avionics
  - Moved to iPads and tablets.
In 2005, FAA issued "Special Condition" for Cybersecurity as part of B787 Type Design
- Special Conditions are additional requirements specific to a proposed aircraft design

In 2006, RTCA formed the SC216 Committee on Aeronautical Security, in cooperation with EUROCAE WG72 Working Group on Aeronautical Security

FAA and EASA continue to issue special conditions for cybersecurity for aircraft and aircraft equipment deemed to have a cybersecurity component


In 2014, SC216 plans to publish revised DO-326A along with new standards on "Airworthiness Security Methods and Guidelines", and "Continuing Airworthiness Guidance for Security"
DO-326 Airworthiness Security Process Specification

- Development process standard
  - Security risk assessment of design and implementation
    - Show that the technical requirements are sufficient
  - Assurance of quality of design and implementation
    - Show that the technical requirements were implemented correctly

- Not a technical standard
  - Committee felt that we do not know the final word on cybersecurity technology
False GPS signals could threaten transportation security

Todd Humphreys from UT’s White Rose of Drachs, an $8.2 million research vessel, international waters about 300 miles southeast of the British Virgin Islands, on October 29, 2013, graduate student and research assistant on the deck of the yacht, transmitting false GPS signals that was about the size of a piece of paper, then gradually increasing the area of the false signal to cover the entire island of St. Thomas.

Truck driver has GPS jammer, accidentally jams Newark airport

An engineering firm worker in New Jersey has a GPS jammer so his bosses don’t know where he is all the time. However, his route takes him close to Newark airport, and his jammer affects its satellite systems.
Cybersecurity Attack Vectors

- Remote connections from aircraft to ground websites
  - Any traverse of Internet results in exposure to attack
- Network connections between aircraft systems and vulnerable equipment
  - Vulnerable due to external connections
  - Vulnerable due to being a portable device such as a laptop, iPad, or USB device
- Interference with Governmental or Non-Governmental Services
  - Command radio
  - GPS
  - ACARS
  - ADS-B
  - Digital Weather
  - Broadband Satellite
  - WiFi/Cellular connections
Cybersecurity Threats

- **Spoofing**
  - Modifying data that otherwise appears to be from a legitimate source
  - Uses protocol weaknesses, compromised security data, or compromised ground systems
    - Flight plans
    - GPS navigation data

- **Exploiting**
  - Using a digital connection to execute malicious instructions on installed equipment
  - Uses software vulnerabilities such as buffer overflows
    - Bots
    - Automated sabotage

- **Denial of Service**
  - Using a digital connection to disrupt service
  - Often uses inherent protocol features
    - Flooding
    - ARP poisoning

- **Counterfeiting**
  - Inserting malicious content into a legitimate part, software component, or database
    - Trojan, backdoor, rootkit
    - Wrong flight approach
ACARS Hacking

Aircraft Hacking
Practical Aero Series

ACARS messages benefit to all groups:
Dispatch, Operations, Maintenance, Engineering, Catering, Customer Service

<table>
<thead>
<tr>
<th>Taxi</th>
<th>Take-Off</th>
<th>Departure</th>
<th>En Route</th>
<th>Approach</th>
<th>Land</th>
<th>Taxi</th>
</tr>
</thead>
<tbody>
<tr>
<td>From A/C</td>
<td>From A/C</td>
<td>From A/C</td>
<td>From A/C</td>
<td>From A/C</td>
<td>From A/C</td>
<td>From A/C</td>
</tr>
<tr>
<td>OUT</td>
<td>OFF</td>
<td>Engine Data</td>
<td>Position Reports</td>
<td>Catering Requests</td>
<td>ON</td>
<td>IN</td>
</tr>
<tr>
<td>Link Test</td>
<td></td>
<td></td>
<td>Weather Reports</td>
<td>Gate Requests</td>
<td></td>
<td>Fuel Information</td>
</tr>
<tr>
<td>Clock Update</td>
<td></td>
<td></td>
<td>Delay Info/ETA</td>
<td>ETA</td>
<td></td>
<td>Crew Information</td>
</tr>
<tr>
<td>Delay Reports</td>
<td></td>
<td></td>
<td>Voice Request</td>
<td>Special Requests</td>
<td></td>
<td>Fault Data</td>
</tr>
<tr>
<td>To A/C</td>
<td></td>
<td></td>
<td>Engine Information</td>
<td>Engine Information</td>
<td></td>
<td>from CMC</td>
</tr>
<tr>
<td>PDC, and ATIS</td>
<td></td>
<td></td>
<td>Maintenance Reports</td>
<td>Maintenance Reports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weight and Balance</td>
<td></td>
<td></td>
<td>To A/C</td>
<td>To A/C</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Airport Analysis</td>
<td></td>
<td></td>
<td>Flight Plan Update</td>
<td>Flight Plan Update</td>
<td></td>
<td></td>
</tr>
<tr>
<td>V-Speeds</td>
<td></td>
<td></td>
<td>Weather Reports</td>
<td>Weather Reports</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flight-Plan, Loaf</td>
<td></td>
<td></td>
<td>Reclearance</td>
<td>Reclearance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FMC</td>
<td></td>
<td></td>
<td>Ground Voice Request</td>
<td>Ground Voice Request</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SITA
Cybersecurity Controls and Technologies

- NIST 800-53 Rev3 list 337 different controls.
- SANS documents 20 "critical" controls.
- There is an Australian study that tried to reduce this to 3 controls.
## National Cyber Security Workforce Framework

<table>
<thead>
<tr>
<th>Cyber-security Categories</th>
<th>Specialty Areas</th>
<th>Cyber-security Categories</th>
<th>Specialty Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Securely Provision</td>
<td>IA Compliance</td>
<td>Investigate</td>
<td>Digital Forensics</td>
</tr>
<tr>
<td></td>
<td>SW Assurance and Security Engineering</td>
<td></td>
<td>Investigation</td>
</tr>
<tr>
<td></td>
<td>Systems Security Arch.</td>
<td>Collect and Operate</td>
<td>Collection Operations</td>
</tr>
<tr>
<td></td>
<td>Technology R&amp;D</td>
<td></td>
<td>Cyber Operations Planning</td>
</tr>
<tr>
<td></td>
<td>Systems Requirements Planning</td>
<td></td>
<td>Cyber Operations</td>
</tr>
<tr>
<td></td>
<td>Test and Evaluation</td>
<td>Analyze</td>
<td>Threat Analysis</td>
</tr>
<tr>
<td></td>
<td>Systems Development</td>
<td></td>
<td>Exploitation Analysis</td>
</tr>
<tr>
<td>Operate</td>
<td>Data Administration</td>
<td></td>
<td>All-Source Intelligence</td>
</tr>
<tr>
<td></td>
<td>Knowledge Management</td>
<td></td>
<td>Targets</td>
</tr>
<tr>
<td></td>
<td>Customer Service and Technical Support</td>
<td>Oversight and Development</td>
<td>Legal Advice</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network Services</td>
<td></td>
<td>Strategic Planning</td>
</tr>
<tr>
<td></td>
<td>Systems Administration</td>
<td></td>
<td>Education and Training</td>
</tr>
<tr>
<td></td>
<td>Systems Security Analysis</td>
<td></td>
<td>Information Systems Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Operations</td>
</tr>
<tr>
<td>Protect and Defend</td>
<td>Computer Network Defense Analysis</td>
<td></td>
<td>Security Program Management</td>
</tr>
<tr>
<td></td>
<td>Incident Response</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Computer Network Defense Infrastructure Support</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Vulnerability Assessment and Management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Cyber Security Research Alliance

• Industry-lead non-profit consortium on research and development strategies for cyber security

• In April of 2013, CSRA in partnership with NIST held industry/academia/government workshop on "Designed-In Cyber Security for Cyber-Physical Systems"

• Main Areas of Concern:
  - Supply Chain
  - Assurance
  - Reliable Information on Threats and Vulnerabilities
  - Securing Legacy Systems
  - Acquisition and Implementation
  - Trustworthy Operations

• Have identified 43 recommendations for industry and government
CSRA Research Areas

11 themes identified in workshop on Cyber Physical Systems (CPS)

1. Understanding the CPS field by creating taxonomy
2. Develop a notion of valid and optimal CPS architectures
3. Develop more resilient and responsive CPS
4. Establish approaches to security and trust composition for coherent in-domain and cross-domain operations
5. Establish new approaches to security assessment and certification
6. Establish metrics and assessment models for CPS
7. Establish new methodologies to study CPS supply chain and provisioning
8. Collect and streamline best practices in CPS
9. Define standards for greater uniformity of security functions and better interoperability
10. Define economic and business incentives for secure CPS
11. Establish cyber security curricula for studying CPS to ensure supply of skills and expertise
Some Traditional Cybersecurity Controls

- Secure protocols
  - Encryption/Decryption, Digital Certificates and Signatures
  - HTTPS, IPSEC (VPN)
  - WiFi WPA2 for 803.11i, GSM Elliptical Curve Cryptography

- Access Control
  - Authentication mechanisms

- System Maintenance
  - Patch control

- Firewalls and Network Architecture

- Network Intrusion Detection

- Software and Hardware Quality Assurance
  - Code inspection
  - Validation and verification
  - Security testing

- Organizational Controls
  - Trusted personnel
  - Access control
  - Control of portable devices
Unique Aspects in Civil Aviation for Cybersecurity

• Fail-Operational
  - Essential systems must not have a single point of failure
    ♦ Built-in protection for availability means protection against denial-of-service and interference

• Pilot-in-the-loop
  - Pilot Awareness
    ♦ Monitoring of radio, flight plans, traffic
  - Pilot Control
    ♦ Able to land even if all ATC and all non-essential equipment are shut down

• Mobility
  - No System Administrator
  - Roams world-wide to varying infrastructure
Unique Aspects in Civil Aviation for Cybersecurity

- **Configuration Control**
  - **Controlled Software Loading**
    - SW executed from persistent store, only changed during authorized maintenance actions
    - Always (even during flight) able to reboot into clean configuration
  - **Configuration Compliance**
    - Aircraft not authorized to operate unless critical SW/HW is up-to-date
  - **Quality Assurance**
    - Level A assurance is extremely high-quality, but extremely expensive to develop
Implications for Autonomy

• High cost of configuration control is most easily justified by flight safety of passengers, may be less easily justified for co-operative operations in civil airspace

• Loss of configuration control means loss of control over many forms of exploitation, denial of service, and counterfeiting

• Loss of pilot means loss of control to prevent spoofing

• Mobility means that active detection and response to cyberattack is currently difficult or impossible
Open Source Drones

Report from the DroneGames (formerly Drc)

We had a great time at the Drone Games Drone Olympics until they got a cease-and-desist letter from another AR.Drones and caused them a big problem. The winners were:

1. (substack), who hacked the AR.Drones to make them a weapon
2. A Stanford freshman who added a payload to the AR.Drones. (Not yet on Github but will be)

The payload virus.tar includes:

- virus.js
  - checkervisor
- virus.tar
  - lump everything into virus.tar

virus-copter

Infect other AR drones with this program.

Deploying code to AR drones is annoying. This program makes it more interesting to deploy software onto AR drones when it works at all.
Research Status, Views

- **Vulnerability Assessment**
  - Major source of new major vulnerabilities is through independent security researcher
  - Black market for vulnerabilities
  - Bounty system developing
  - Automated scanning tools

- **Secure protocols**
  - Very technical and tricky, must be expert, must use expert community
  - NIST governance
  - Room for protocols specific to aviation needs (e.g. existing secure ACARS)

- **Access Control**
  - Much active research and product offerings, biometrics, tokens, etc,

- **System Maintenance**
  - Many tools in market, issue is organizational discipline

- **Firewalls and Network Architecture**
  - Not much new research except in QA (e.g. validating firewall rules)
Research Status, Views

- **Organizational Controls**
  - Little research, lots of guidance

- **Network Intrusion Detection**
  - Extremely poor performance, manual intervention required
  - Botnets often only found through honeypots and reverse-engineering analysis
  - Needs fundamental research

- **Software and Hardware Quality Assurance**
  - OS vendors seeking high-assurance certifications
  - Virtualization touted, but may be just another example of "security by obscurity"
  - Current validation tools and methodologies costly to use, and are not specific to security concerns
  - Needs fundamental research

- **Supply Chain Control**
  - Have secure transmission if suppliers are trusted
  - Difficult to prevent counterfeiting
  - Difficult to detect counterfeit parts
  - Need fundamental research
El ordenador de Spanair que anotaba los fallos en los aviones tenía virus

La computadora no operaba correctamente por unos programas 'troyanos'

José Antonio Hernández - Madrid - 20/08/2010

El ordenador central de la compañía Spanair en el que se anotaban las averías de los aviones estaba contaminado con programas informáticos maliciosos cuando se produjo, hace hoy dos años, el accidente del vuelo JK 5022. La computadora, situada en la sede de la aerolínea en Palma de Mallorca, emite una señal de alarma en el monitor cuando registra tres problemas técnicos similares en el mismo aparato. El avión que se estrelló en Barajas hace hoy dos años -murió 154 de sus 172 ocupantes- acumulaba tres incidencias, que no fueron registradas a tiempo en el ordenador.

La primera vez que volví a volar tuve un ataque de pánico

Las víctimas del accidente de Spanair denuncian que el Estado las abandonó

“Viajábamos dos personas desde Suecia, la otra murió”

Supervivientes de un vuelo sin destino

Spanair tardaba 24 horas en anotar en el ordenador los fallos de sus aviones

Las víctimas del accidente de Spanair piensan denunciar en

Un parte interno de la compañía, datado el mismo día de accidente, indica que el monitor estaba contaminado “de troyanos”. Estos programas maliciosos pueden ocasionar daños y facilitar los ataques de piratas informáticos. Precisamente, la asociación de víctimas del accidente, personada en la causa, ha pedido al juez instructor, Juan David Pérez, que pida a Spanair todas las anotaciones registradas en ese ordenador en los días anteriores y posteriores al siniestro. El magistrado acaba de dictar un auto en el que ordena a la aerolínea que le facilite tales datos.