Cyber-Vulnerabilities in Aviation Today

Robert F. Behler
Deputy Director and COO

CERT | Software Engineering Institute | Carnegie Mellon University
The aircraft industry is in the software business whether they realize it or not.
The aircraft industry is in the software business

whether they realize it or not

Source: U.S. Air Force, Global Horizons (AFST TR 13-01), June 2013
F-35
30M SLOC
15M on plane
15M for ground support equipment
Potential Cyber-Vulnerability Pathways

Distributed Aperture System
Advanced Sensor Fusion
Multifunction Advanced Data Link
Advanced Electronically Scanned Radar
Electro-Optical Targeting System
Health Monitoring: Automated Pilot/Maintenance Debrief

26 suppliers provide components for the avionics
### Defects in software may be exploited

#### Software defects per KSLOC in a recent aircraft program

<table>
<thead>
<tr>
<th>Type of Development</th>
<th>Number of Defects Discovered</th>
<th>KSLOC</th>
<th>Defects per KSLOC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Project 1</td>
<td>36</td>
<td>32</td>
<td>1.13</td>
</tr>
<tr>
<td>Software Project 2</td>
<td>66</td>
<td>89</td>
<td>0.74</td>
</tr>
<tr>
<td>Software Project 3</td>
<td>260</td>
<td>443</td>
<td>0.59</td>
</tr>
</tbody>
</table>

Adapted from: NAVAIR report, NAWCWD TP 8642
The supply chain creates vulnerabilities
Aircraft operate in a very complex environment
Automatic Dependent Surveillance-Broadcast (ADS-B) will replace radar with GPS.

Greater functionality

Greater complexity

Increased attack surface and lack of security
Every aircraft will be a node on a network.
Trucks jam GPS, close Newark airport
Engineering Perspectives

- Propulsion Engineer
- Aero Engineer
- Armaments Engineer
- Avionics Engineer
Engineering Perspectives

Cyber-Vulnerabilities
Engineer
Taxonomy of Cyber-Threats

Exploits pre-existing known vulnerabilities

$10K's

- Password theft
- Insider threat
- Credit card fraud
- Malware
- Spear fishing
- Identity theft

NUISANCE  EXISTENTIAL

Taxonomy of Cyber-Threats

Exploits pre-existing known vulnerabilities

$10K's
- Password theft
- Insider threat
- Credit card fraud
- Malware
- Spear fishing
- Identity theft

Discovers unknown vulnerabilities

$1M's
- Zero day attacks
- Logic bombs
- Supply chain issues
- Intellectual property theft - aircraft designs
- Fuzz testing to identify vulnerabilities

NUISANCE  EXISTENTIAL

Taxonomy of Cyber-Threats

- **Exploits pre-existing known vulnerabilities**
  - $10K's
    - Password theft
    - Insider threat
    - Credit card fraud
    - Malware
    - Spear fishing
    - Identity theft

- **Discovers unknown vulnerabilities**
  - $1M's
    - Zero day attacks
    - Logic bombs
    - Supply chain issues
    - Intellectual property theft - aircraft designs
    - Fuzz testing to identify vulnerabilities

- **Creates vulnerabilities using full spectrum**
  - $1B's
    - Russia
    - China
    - North Korea
    - Iran

---

"Cyber poses a very complex set of threats, because profit-motivated criminals, ideologically motivated hackers or extremists, and variously capable nation-states like Russia, China, North Korea, and Iran are all potential adversaries who, if they choose, can all do great harm."

James Clapper in testimony to the Senate Intelligence Committee on February 26, 2015
Software-reliant platforms need to be tested to minimize the maximum regret.