Abstract

Aircraft manufacturers, avionics/electronics vendors, and owners/operators are implementing technologies (e.g. packet switching devices, wireless interfaces) that are easier to implement, reduce cost/size/weight/power, and increase connectivity but could potentially introduce cyber security vulnerabilities that affect aircraft safety.

Introduction

The purpose of this paper is to provide an overview of the transition of aircraft systems, differentiate cyber security in aircraft systems from terrestrial IT systems, identify some cyber security vulnerabilities/threats that could affect aircraft safety, and identify current and future Federal Aviation Administration (FAA) activities to mitigate cyber security risk. This paper will also provide an overview of research and development activities such as the Aeronautical Network Security Simulator.

Transition of Aircraft Systems

Aircraft systems are transitioning to net-centric architectures based upon the IEEE 802.3 Ethernet standard [1] and implementing Internet Protocols (e.g. IP [2], ICMP [3], TCP [4], UDP [5], SAP [6], tFTP [7], SNMP [8], etc.) with COTS components (e.g. ARINC 664 AFDX [9]). Also, various wireless interfaces (e.g. IEEE 802.11 [10], cellular [11], IEEE 802.15–Bluetooth [12], IEEE 802.16-WiMax [13], etc.) are being implemented internal and external to the aircraft.

Differentiating Cyber Security in Aircraft Systems and IT Systems

The tenants of Information Technology (IT) systems are Confidentiality, Integrity, and Availability (CIA). Confidentiality defined as “ensuring information is accessible only to those authorized to have access”. Integrity defined as “data has a complete or whole structure”. Availability defined as “proportion of time a system is in a functioning condition”. The primary focus of aircraft systems is Integrity and Availability but can include Confidentiality. The primary focus of IT systems is Availability and Confidentiality but can include Integrity.

Table 1 provides some discrete differences between IT and aircraft systems.

Table 1. Information Technology vs. Aircraft/Control Systems [14]
**Potential Cyber Security Threat**

Exploits to IT systems are becoming more sophisticated over time. Exploits such as morphing, zombies, malicious code, and BOTS/BOTNETS are becoming common occurrences. The intruder knowledge is decreasing over time due to the increase of functionality and automation of hacking tools.

Exploits of specific systems include the following:

**Automobiles**
- March 2011 - Research team hacks into cars through GM OnStar [15], Ford Sync [16], and Bluetooth wireless interfaces [17]

**Industrial Control Systems**
- July 2010 - Stuxnet worm delivered to Programmable Logic Controller – sabotaged Iran’s uranium enrichment program centrifuges

**Aviation**
- 2009 – FAA Server Compromised
  - 48,000 employee Name and Social Security numbers stolen
- 2008 – 800 Cyber Incident Alerts at ATO/ATC Facilities
  - Over 150 incidents not remediated
- 2007 – Virus Loaded into Thai Airways EFB
  - Virus disabled EFB and spread to other EFBs
- 2006 – Virus Spread to FAA’s ATC Systems
  - FAA forced to shut down a portion of its ATC systems in Alaska
- 1997 - Hacker broke into a Bell Atlantic Computer System
  - FAA tower's main radio transmitter and another transmitter that activates runway lights were shut down

New aircraft systems have been defined by the ARINC 811 Commercial Aircraft Information Security Concepts of Operation and Process Framework [18]. The ARINC 811 standard has divided the aircraft systems into domains (Aircraft Control Domain, Airline Information systems, and Passenger Info/Entertainment Systems). These aircraft domains can have connectivity (direct or indirect) internally to crew/passenger-owned devices and to external connections (e.g. Internet, SatComm links, Gatelink) that may introduce exploitable vulnerabilities.

**FAA Aircraft Systems Cyber Security Activities**

FAA regulations, standards, and guidance do not address cyber security vulnerabilities. The FAA has developed and published Special Conditions for a number of aircraft and systems. Special Conditions have been implemented in regards to cyber security vulnerabilities for the following rationale:

- May be issued when the current FAA regulations do not contain adequate or appropriate safety standards for protection and security of aircraft systems.
- Contain the additional safety standards that the FAA Administrator considers necessary to establish an equivalent level of safety.
- Are issued for specific airplane models.
- Address new or novel design features.
- Are published in the Federal Register for public comment

The FAA participates on RTCA SC-216 Aeronautical Systems Security. RTCA, Inc. is a private, not-for-profit corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management (CNS/ATM) system issues. RTCA functions as a Federal Advisory Committee. Its recommendations are used by the Federal Aviation Administration (FAA) as the basis for policy, program, and regulatory decisions and by the private sector as the basis for development, investment and other business decisions. RTCA SC-
216 has published and/or has plans to publish the following:


DO-326 methods document (how to) planned for publication June 2012

Guidance for Instructions for Continued Airworthiness planned for publication – June 2012

The FAA has developed the following cyber security training:

- Aircraft Systems Cyber Security Designated Engineering Representative (DER) Seminar (first course given in March 2011)
- Aircraft Systems Cyber Security Orientation in the electronic Learning Management System (eLMS)

The FAA is developing a National Aircraft Systems Cyber Security Plan that will address topics such as:

- Rulemaking
- Aircraft Systems Cyber Security Advisory Circular (s)
- The implementation of the SC-216 products
- The need for development of other FAA policy, standards and guidance
- The need for additional training
- Workforce needs
- Research and Development needs – such as Aeronautical Network Security Simulator – The Volpe Center

**Aeronautical Network Security Simulator**

The Aerospace Network Security Simulator (ANSS) project integrates industry and government aeronautical simulators to assess and identify network security threats in airborne network environments. The ANSS project addresses key cyber security-related concerns of Next Generation Air Transportation System (NextGen) and will identify potential gaps in information security of key data-enabled systems.

With NextGen technologies on the horizon and the emergence of E-enabled aircraft (e.g. B787, B747-8, A380, A350, and upgraded legacy aircraft), a dependency on cyber security related issues will increase by an order of magnitude. The mobility of the aircraft and the number of trust partners involved in normal operations increases the risk to aircraft and its infrastructure (ground systems, airports, satellites, etc). Unlike today’s commercial aircraft operational environment where the primary means of obtaining information is through voice, our new key operational systems will depend on timely, accurate and un-tampered information from mobile, digital networks.

From this current environment, the need for the ANSS was realized. Aircraft operators, manufacturers and regulators jointly identified this common need and participate jointly in the endeavor. ANSS co-operative partnership approach allows stakeholders to identify security issues of immediate concern, test scenarios in an airborne network environment and develop implementable recommendations. Key stakeholders in the US and world-wide include: FAA, DOD/USAF, DISA, UK-CPNI/CESG, aircraft/avionics manufactures, aircraft IT component vendors, airlines, and academia.

The goals of ANSS are detailed in its Concept of Operations Document and summarized below:

- Identify potential information security threats in synthetic environment by simulating next generation aircraft communications systems.
- Share knowledge, tools and methodologies with academia and other interested stakeholders to extend research value.
- Act as coordinating authority for cyber security risk mitigation within the international aerospace & aviation community.
- Recommend appropriate technical & procedural standards for security risks to aid in the development of regulatory guidelines and policies.
- Influence industry bodies on cyber security best practice with respect to specifications,
procedures, and recommendations used by the industry.

ANSS has taken a phased approach to the implementation of the simulator where each phase leverages the capabilities developed in the previous phase. The remainder of this document outlines the goals for each phase accompanied by background and justification of its importance.

Phase 1

The initial goal of the Airborne Network Security Simulator (ANSS) is to engage commercial, academic and government stakeholders in cyber security experiments within a simulated airborne network environment. Participation of stakeholders has been exceptional as each group can easily identify and utilize the benefits ANSS is providing. Through its vulnerability and threat assessment experiments, ANSS is able to simulate real-world functionality and identify cyber vulnerabilities that could potentially impact safety of flight and business reputations. Interconnected with external simulators, ANSS leverages industry information flows to assess impact of corrupt and un-timely data. Experiment findings are discussed with stakeholders and mitigation strategies discussed before recommendations are made.

Airborne network environments differ from classical terrestrial networks in that they are highly mobile, operate in multiple flight phases and interact with a diverse user base (flight crew, third party maintenance, multiple airports, air traffic control and the general public). Much of today’s cyber security research focuses on behavior of terrestrial networks and typically does not consider the differences present in an airborne environment. To address this gap, ANSS:

- Simulates a standard airborne network architecture including real and synthetic components
- Interconnects with disparate aviation simulators to include real-world information in its experiments
- Engages industry, academia and government in its experiments and recommendations
- Design experiments to explore stakeholder identified issues and concerns

Figure 1 depicts the ANSS configuration for its Phase 1 experiment. The scenario under test sends load and balance data from an airline operations center over a wireless network at the airport’s gate to the airplane’s electronic flight bag where the data is used by the pilots to configure the aircraft for take-off.

Figure 1. ANSS Configuration for Its Phase 1 Experiment

Phase 2

An understanding of the Common Operational Picture (COP) between FAA, DOD and DHS will become critical in the identification, containment and prevention of distributed cyber threats across this environment. ANSS will contribute to the research in this area by engaging in NextGen experimentation to understand the impact on commercial E-enabled Aircraft.

In the next generation air traffic control system E-enabled aircraft will play a critical network roll providing situational awareness and communications to their environment around them. Air to air and air to ground will be the common mode of operation in this net-centric, mobile environment in a similar way to ground to ground operate in a terrestrial environment. Service oriented architectures (SOA) will provide the common infrastructure where aircraft are both service consumers and providers.
Critical to this success will be global trust, federated services and real-time, dynamic construction of trusted spaces. Although most of this architecture is futuristic, SOA is a common technology thread. NextGen is incorporating new and innovative technologies within the air transportations system. New aircraft, advanced avionics and complex support systems are planned to be introduced. Many of the planned technologies include advanced networking, remote operations, remote maintenance services, and automated detection are potential issues that may arise within the air vehicle as it operates or during maintenance operations. Given that the air carriers and FAA program offices are attune to the security issues as systems are developed, deployed and integrated into the air transportation system, it is anticipated that complex technologies to ensure the safe and secure operation of air vehicles and NAS functions will accompany NextGen capabilities as they are deployed. From a safety perspective, this creates potential new issues related to the ability to oversee air carrier and NAS operations that have employed complex IT infrastructure to meet the needs of NextGen. As a critical national infrastructure asset, the air transportation system needs to have proper monitoring and safeguards against cyber security attacks. As infrastructure and technologies advance to accommodate NextGen, so do the tools and workforce knowledge, skills and abilities to oversee the changes.

Security vulnerabilities are not just an FAA related issue. Cyber attacks typically arise from multiple sources, threatening a variety of assets across multiple organizational infrastructures. There needs to be a cooperative approach to the detection, reporting, assessment, and mitigation of security risks among all NextGen stakeholders (including DOD, DHS/TSA, Airlines/AOCs, intelligence agencies, etc). The air operators need to incorporate technologies to detect cyber threats to air vehicles while the FAA needs workforce tools to oversee, detect and share cyber threats with DHS and other NextGen stakeholders. The NextGen community needs to be aware and work cooperatively to ensure that security vulnerabilities do not affect the safety of the air transportation system.

To address this emerging need, ANSS will implement a SOA interface to interact with other NextGen simulators and participate in joint NextGen Test & Evaluation (T&E) experimentation. To address these needs ANSS will:

- Include a SOA interface based on current Nextgen Standards
- Build synthetic capabilities to evaluate cyber issues when the aircraft is both a SOA provider and consumer
- Participate in FAA/DOD experiments to understand the commercial impact of cyber security in this environment
- Identify issues and restrictions of global trust in the AN environment
- Identity issues associated with centralized auditing, intrusion detection/prevention and a global view of the operation’s theater.

**Phase 3**

Skill development will play a critical role in the cyber protection of this airborne network environment. Other programs are currently underway to train the next generation cyber warrior; however; special skills will be needed to address the mobility, public safety and critical infrastructure components of this environment.

Training defenders (e.g. FAA, DOD, manufactures and airlines) while anticipating the next level of cyber attack is a challenge that must be addressed in an iterative fashion.

Gaming technology is successfully used to build virtual worlds and train workforces through realistic scenarios. Scenario based training also allows researcher to observe student attack strategies in anticipation of the next level of attack. Learning attack approaches and exploits in a controlled environment feeds the development of predictive and adaptive defense strategies. ANSS is uniquely positioned to meet these needs through its public, private, academic partnerships, realistic synthetic aircraft network environment, flexible connectivity with external simulators and cyber security tool set.

Leveraging all of these assets, ANSS would develop a gaming environment where security teams from government, academia and industry will compete in “capture the flag” type scenarios. In addition to providing a training facility for first line defenders, modes, methods and approaches captured
in the experiments would prove invaluable to researchers in the development of strategies to proactively protect the AN environment.

The advantages of a game based approach is that it quickly allows the player to visualize and understand complex infrastructures, resources and external factors that come into play during normal operations. Through this innovation, ANSS will build on the growing use of low-cost game technology for visualization and training.

Among the most proven and pragmatic of methods for testing the efficiency and adequacy of cyber security safeguards is the red-blue team concept in which players form teams enact offensive or defensive roles with respect to a protected asset, in this case the aircraft. This approach implicitly captures the elements of human creativity and unpredictability which more analytic methods of security assessment often lack. ANSS will develop a serious red-blue team gaming environment for enacting cyber attacks, with a focus on airborne networks. Specifically, the game will be developed with the intent of evaluating the predictive and adaptive attributes of cyber defense systems.

The means of achieving this airborne cyber domain will be to establish a virtual space as a representation of cyber functionalities and security systems within the next generation aircraft. Attacks on cyber system functionality and the defensive responses of the system will then be played-out within the arena of this virtual domain. This gaming tool will allow researchers and administrators to model network scenarios that mirror real-world configurations. These models will be played at variable rates of simulation so that analysts have an opportunity to both examine and train the computer algorithms representing both sides of the scenario.

### Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC</td>
<td>Advisory Circular</td>
</tr>
<tr>
<td>ACARS</td>
<td>Aircraft Communication Addressing and Reporting System</td>
</tr>
<tr>
<td>ACD</td>
<td>Aircraft Control Document</td>
</tr>
<tr>
<td>ADS-B</td>
<td>Automatic Dependent Surveillance-Broadcast</td>
</tr>
<tr>
<td>AFG&amp;CS</td>
<td>Automatic Flight Guidance &amp; Control Systems</td>
</tr>
<tr>
<td>AISD</td>
<td>Airlines Information Services Domain</td>
</tr>
<tr>
<td>AOC</td>
<td>Airline Operations Center</td>
</tr>
<tr>
<td>ARINC</td>
<td>Aeronautical Radio Incorporated</td>
</tr>
<tr>
<td>ARP</td>
<td>Aerospace Recommended Practices</td>
</tr>
<tr>
<td>ASIC</td>
<td>Application Specific Integrated Circuit</td>
</tr>
<tr>
<td>ATC</td>
<td>Air Traffic Control</td>
</tr>
<tr>
<td>ATS</td>
<td>Air Traffic Service</td>
</tr>
<tr>
<td>ATS-P</td>
<td>Air Traffic Service-Provider</td>
</tr>
<tr>
<td>CAA</td>
<td>Civil Aviation Authorities</td>
</tr>
<tr>
<td>CDU</td>
<td>Control Display Unit</td>
</tr>
<tr>
<td>CFR</td>
<td>Code of Federal Regulations</td>
</tr>
<tr>
<td>COTS</td>
<td>Commercial Off-The-Shelf</td>
</tr>
<tr>
<td>CPDLC</td>
<td>Controller Pilot Data Link Communications</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic Redundancy Check</td>
</tr>
<tr>
<td>DHS</td>
<td>Department of Homeland Security</td>
</tr>
<tr>
<td>DME</td>
<td>Distance Measuring Equipment</td>
</tr>
<tr>
<td>DO</td>
<td>Document</td>
</tr>
<tr>
<td>EFB</td>
<td>Electronic Flight Bag</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration</td>
</tr>
<tr>
<td>FIPS</td>
<td>Federal Information Processing Standards</td>
</tr>
<tr>
<td>FISMA</td>
<td>Federal Information System Management Act</td>
</tr>
<tr>
<td>FLS</td>
<td>Field-Loadable Software</td>
</tr>
<tr>
<td>FMCS</td>
<td>Flight Management Computer</td>
</tr>
<tr>
<td>GBAS</td>
<td>Ground Based Augmentation Systems</td>
</tr>
<tr>
<td>GNSS</td>
<td>Global Navigation Satellite Sensor</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSE</td>
<td>Ground Support Equipment</td>
</tr>
<tr>
<td>ICA</td>
<td>Instructions for Continued Airworthiness</td>
</tr>
<tr>
<td>ILS</td>
<td>Instrument Landing Systems</td>
</tr>
</tbody>
</table>
IMA  Integrated Modular Avionics
IT  Information Technology
NIST  National Institute of Standards and Technology
PED  Portable Electronic Devices
PIESD  Passenger Information and Entertainment Services Domain
SAE  Society of Automotive Engineers
SBAS  Satellite Based Navigation Systems
SC  Special Condition
TSA  Transportation and Security Administration
TSO  Technical Standard Order
UMS  User Modifiable Software
USB  Universal Serial Buss
VHF  Very High Frequency
VOR  VHF Omni directional Range

References
[1] IEEE 802.3 Ethernet Standard
[2] Internet Protocol (RFC 791)
[3] Internet Control Message Protocol (RFC 792/1122)
[9] ARINC 664 Avionics Full Duplex Switch (AFDX)
[12] IEEE 802.15 Wireless Personal Area Network (WPAN)
[16] Ford Sync powered by Microsoft
[17] Bluetooth Communications (IEEE 802.15)

Email Addresses
Raymond.W.Decerchio@faa.gov
Chris Riley riley@info-tools.com

30th Digital Avionics Systems Conference
October 16-20, 2011