CSFI ATC (Air Traffic Control) Cyber Security Project

July 16, 2015

www.csfi.us

OUR CSFI PROJECT TEAM

A team of diversified Information Security professionals, intelligence analysts, and engineers collaborated in a private portal towards this deliverable. CSFI believes in collaboration and sharing of knowledge as a way to shine light in the darkness of the cyber domain. Our goal is to minimize speculation through research and logical thinking. This is a preliminary foundational report from a Cyber Warfare perspective. Some of our volunteers have made the choice to serve in silence due to the sensitivity of their jobs. We thank them for their contribution and hard work.

Special thanks and credit to our CSFI volunteers:

Eva Frankenberger, CSFI ATC Cyber Security Project Manager.

Manager Global Cyber Security/Heightened Security (USA- Germany)

USAF Col (ret) Tim Evans (USA)

USAF Col (ret) Robert Morris (USA)

Anis Ben Othman, Information Security Specialist (Finland)

Arnold Webster, Founder and CEO, Cyber Research and Intelligent Solutions Provider (CRISP) (USA)

Arvin Verma, Senior Consultant (USA)

Bibi Hamid, Campus Services - IT Manager (USA)

Chia-Chi Teng, Information Techology - Associate Professor – BYU (USA)

Christos Ntrigkogias, PhD Candidate - UNI.PI. Security Lab (Greece)

Debajit Sarkar, Subject Matter Expert - Smart Weapons & Unmanned Vehicle Systems (India)

Eren Girgin, Sr.Manager, Cyber Defense & Technology Controls (Canada)

Gregory Digsby, Senior Network Engineer (USA)

Kristofer Mansson, CEO Silobreaker Ltd. (Sweden)

Mats Bjore, Consultant Intelligence Affairs, Infospehere AB (Sweden)

Michael Keith, Sr. IA Systems Engineer (USA)

Paul de Souza, CSFI Founder (USA)

ACRONYMS

ACARS	Aircraft Communications Addressing and Reporting System
ACL	Access Control List
ADS	Airborne Radio Systems
ADS-B	Automatic Dependent Surveillance-Broadcast
AFDX	Avionics Full-Duplex Switched Ethernet
ARINC	Aeronautical Radio, Incorporated
ATC	Air Traffic Control
BIA	Business Impact Analysis
CARTS	Common Automated Terminal System
CCTV	Closed Circuit Television
CDMA	Code Division Multiple Access
CERT	Computer Emergency Readiness Team
CPDLC	Controller Pilot Data Link Communications
CSPR	Closely Spaced Parallel Runways
DCL	Departure Clearances
DDoS	Distributed Denial of Service
DNS	Domain Name Service
DoS	Denial of Service
ECMA	European Computer Manufacturers Association
EFVS	Enhanced Flight Vision System
ERAM	En Route Automation Modernization
EU	European Union
EUROCAE	European Organization for Civil Aviation Equipment
FAA	Federal Aviation Administration
FANS	Future Air Navigation System
FTP	File Transfer Protocol
GA	General Aviation
GPO	Group Policy Object
GPS	Global Position System
FIS-B	Flight Information Service–Broadcast
FMS	Flight Management Systems
HTTP	HyperText Transfer Protocol
HVAC	Heating, Ventilation, and Air Conditioning
IATA	International Air Transportation Association
ICAO	International Civil Aviation Organization
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronic Engineers
IFR	Instrument Flight Rules
ILS	Instrument Landing System
IMRO	Improved Multiple Runway Operations
IOC	Initial Operating Capability
IP	Intellectual Property
IP	Internet Protocol
IPSec	IP Security
ISO	International Organization for Standardization

IT	Information Technology
ITU	International Telecommunication Union
MRO	Maintenance, Repair, and Operations
NAS	National Airspace System
NextGen ATS	Next Generation Air Transportation System
NIPRNet	Nonsecure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NVS	NAS Voice System
OPD	Optimized Profile Descent
ORD	Operational Readiness Demonstration
OSI	Open System Interface
RC	Radio-Controlled
RTCA	Radio Technical Commission for Aeronautics
SBU	Swift Broadband Unit
SCRM	Supply Chain Risk Management
SDR	Software-Defined Radio
SDU	Satellite Data Unit
SESAR	Single European Sky ATM Research
SIPRNet	Secret Internet Protocol Router Network
SNMP	Simple Network Management Protocol
SSL	Secure Socket Layer
STARS	Standard Terminal Automation Replacement System
SWIM	System Wide Information Management
TACS	Traffic Alert and Collision Avoidance System
TAMR	Terminal Automation Modernization and Replacement
TCP/IP	Transmission Control Protocol/Internet Protocol
TDLS	Tower Data Link System
TIS-B	Traffic Information Service–Broadcast
TRACON	Terminal Radar Approach Control
UAS	Unmanned Aircraft Systems
UAT	Universal Access Transceiver
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Air Vehicle
US	United States
V-LAN	Virtual Local Area Network
VDL	VHF Data Link
VoIP	Voice-over-IP
VPN	Virtual Private Network
WCDMA	Wideband Code Division Multiple Access

PROJECT SCOPE

1. Identify the top ATC Cyber vulnerabilities and offer countermeasures to remediate them and minimize the risk of such vulnerabilities as it pertains to ATC systems only.
2. Develop a scenario where a state actor would exploit an ATC systems vulnerability in a coordinated fashion against an American airport.

Table of Contents

Executive Summary

The goal of the project is to identify cyber vulnerabilities within the ATC systems and Airborne systems that is currently being upgraded. Several probable attack vectors have been outlined. The current ATC system is in an upgrade status. Because of the length of time and how funding is done the plan was implemented before the reality of the current cyber landscape had presented itself. The landscape has drastically changed in the last decade as the roll out of the NexGen ATC system has begun. The situation is further complicated by the fact that these are International changes. The changes are taking place on across the entire air space of the globe. Therefore it is not just convincing US air carriers but, convincing air carriers all over the world that there is a threat. That there are also threat actors willing to exploit these cyber vulnerabilities within the current upgrades.

The ATC system is responsible for controlling the National Air Space (NAS) in the United States. The system is responsible for tracking, identifying, landing and aircraft taking off. The ATC system is also part of the National Security architecture. By tracking all of the aircraft in the NAS the ATC system may be the earliest detection of a rogue aircraft within the borders of our country. The data from our NAS is shared throughout the North American continent to ensure a layered approach to identify threats. Many of the threat agents will be attacking these systems with minimal effort and minimal expenditure in capital.

This paper points out that there are exploits within the system as it is currently being deployed that will take little effort and little capital to exploit. Communications systems are vulnerable to attack with software defined radios that only cost a few thousand dollars to deploy. The identification systems that are being deployed are communicating through unauthenticated means that can be attacked from a laptop. Hackers at two different conferences have demonstrated how to introduce ghost aircraft into the system. Then there is the threat that Unmanned Arial Vehicles (UAV) can pose to the NAS. Rogue actors deploying UAV's into the NAS without proper authentication. Much of the communications systems are being deployed in a TCP/IP environment that is not properly secured and easily exploited. There is also the deployment of unencrypted wireless maintenance systems used to report back to aircraft manufacturers, the wiring of some Wi-Fi systems into the avionics cabling of older aircraft, and the introduction of fly-by-wireless systems that could allow an attacker direct access to the avionics systems.

Introduction

The purpose of this report is to identify the top ATC cyber vulnerabilities and offer countermeasures to remediate them and help minimize the risk of such vulnerabilities.

Scope

The scope of this report is limited to ATC vulnerabilities and the risks associated with ATC systems from a cyber warfare perspective.

Background Information

The current Air Traffic Control (ATC) system was designed and installed during the late 1950s and through the 1960s. Minimal upgrades have been made to the system over the past decades. Doppler weather radars and color monitors are the biggest steps forward that the system has made since its early inception in the 1960s. The system is obviously well maintained because of the limited outages it has suffered over the decades. The current system though is very susceptible to bad weather and does have limited ranges. The current system also has a number of radar blind spots because of the fixed radar tracks. An increase in the amount of planes in the National Air Space (NAS) has proven to a burden on the less dynamic system currently installed.

In an effort to create a safer flying experience the Federal Aviation Administration (FAA) along with other international agencies has started the process of upgrading the system. When the proposal was started almost 20 years ago, cyber threats were not even a concern. However, since the beginning of the installation of these systems, cyber threats have become the number one threat. The system being installed will be more dynamic and cover areas not previously covered by the fixed radar tracks.

The upgrades do not end with the ATC system. There are aircraft upgrades being installed as well. Some of these upgrade installations are on brand new airframes. Others are being retro fitted onto older airframes that may have not been meant for these types of systems. Again a major problem is that retro fitting aircraft that were not meant for networked systems introduces cyber threats to airframes that may not be able to defend against such threats. The aircraft themselves are very limited on space; in older aircraft some network systems may have to operate on the same bus as the avionics systems. All of these upgrades are setting up a dangerous scenario.

Ground Systems

Introduction

The upgrades for the current ground ATC systems are being done through the NexGen program. The NexGen system in the United States has a very aggressive install schedule. The NexGen program was initiated prior to the modern concern over cyberattacks, prior to any clear understanding of the ability of individuals and/or groups involved in attacking network systems of the present day. Much of the security of the ATC ground systems relied on the fact that these systems were not interconnected, as they now will be.

Vulnerability: Unauthenticated Inputs

All current aviation communications are unauthenticated and unencrypted whether sent by the aircraft or the ground ATC systems. Neither authentication nor encryption can be added to existing systems without modifications to all aircraft.

New global spectrum for new aviation communications have not been allocated or even placed on the agenda with the World Radio Congress which operates under the International Telecommunication Union (ITU).

All aircraft are identified only by their transponder code, which is actually its Open System Interface (OSI) network address allocated by the International Civil Aviation Organization (ICAO). There is no way to ensure that a transmitted address is not being spoofed by a threat agent.

An aircraft's transponder can be changed (mechanically) or turned off.

Using software-defined radio (SDR), components ordered off the Internet, and software and papers from the Internet, a transmitter/receiver unit can be built for a few hundred dollars for Aircraft Communications Addressing and Reporting System (ACARS), Future Air Navigation System (FANS), or Controller Pilot Data Link Communications (CPDLC). These are indistinguishable from real aircraft or ground system transmissions. The system sees a properly formatted signal and accepts it as authentic. The system has no process for interrupting between signals from an authorized transmitter as opposed to a threat agents systems. As long as the signal is on the correct frequency and transmits properly formatted information, then it is accepted. All of this information is available through open sources.

An Aeronautical Radio, Incorporated (ARINC) standard for encrypted ACARS was developed around 2002, but its use required some upgrades to the aircraft and was very difficult for the airlines to manage the keys on a fleet.

Iridium satellite is currently the only other spectrums or network type authorized for safety of flight uses. Inmarsat is working through the certification process to allow them to tunnel ACARS, FANS, and CPDLC over their satellite Internet protocol links. Once the first use is approved, it should not be long before the other satellite companies follow.

NextGEN/SESAR advanced flight communications have a limited set of options: 3/4/5G or satellite. As examples, GoGo is a 3G service. Row44 and OnAir are Ku-band satellite links. The good news is that all of these are becoming global and use IP networking, which can support both authentication and encryption. And the existing ACARS, FANS, and CPDLC can all be tunneled through them, thus authenticated and encrypted.

That bad news is two-fold. The connection opens Internet access to the aircraft, and they will share the links to the aircraft with passengers and airline operations uses. There is really no option to install a single use link/network. Costs, weight, drag, and power all preclude it, not mention just finding a spot on the aircraft for another antenna would by challenging as globally operating aircraft can have more than 50 antennae of various types on them.

There is precedent for this shared use; the higher capacity links to US command fleet is also a satellite IP based link. It ends up about triple encrypted (tunnels within tunnels) as voice, video, NIPRNet, SIPRNet, and Internet utilize the same link. This includes both presidential and the press corps, which are handled in isolated tunnels over the link. Communication traffic is highly prioritized, so press corps being the lowest can be very slow.

Automatic Dependent Surveillance-Broadcast (ADS-B) or any other sensors seems to be an easy target, compared with today's ground to air radio communications. But, a ghost flight is not a great problem for the ATC. Normally if they cannot identify it, then it will be transferred to a body that has primary radar or fighter aircraft to do the identification. More problematic are flights that exist but do not show on ADS-B or secondary radar such as can be found at the moment at the Baltic Sea where some state aircraft are not using transponders in civil international airspace.

These are carried over a small set of frequencies. Aeronautical VHF data links use the band 117.975–137 MHz assigned by the International Telecommunication Union to Aeronautical Mobile Services (Route). Mode 2 is the only one used for ATC; Mode 4 is being tested in Northern Europe, with one of the busiest being 131.550. It should be noted that ATC zones operate on different frequencies in particular airspaces in the US at least. In a few cases, ATC has transmitted an incorrect frequency for incoming aircraft to pick up. In such cases, the pilots will contact another nearby aircraft and request the correct frequencies. Conceivably a threat actor could with little effort get an aircraft to get on an incorrect frequency.

The trends in this area tend to follow a similar pattern that any business has when moving from company-wide, private networks to global systems using the Internet (in this case IPv6) as the main form of communication instead of private networks (mainly from X.25), and the means to fix the problems are more or less the same. As systems are becoming more automatic, and as self-services via the Internet are becoming more common, it creates possibilities for denial of service (DoS) attacks via those public services that can have an effect at the controller level.

Recommendations:

The main recommendation to counter this vulnerability is to cease making information like commercial ATC frequencies available to the public. Also, IPv6 should be used where possible because this version of TCP/IP has IPSec encryption as a default in the protocol stack.

The customer may always be right, but in this case, safety of flight trumps the customer. Networks should not be installed in any airframe where there is the potential to operate on the same bus as the avionics.

Further studies are needed to investigate authentication methods that can be instituted using systems currently available to all countries. The encryption type may have to be symmetric to start with, and possibly an asymmetric scheme may be developed later. However, this solution would require much more investigation. There are also other types of authentication other than encryption that can be investigated as viable candidates.

ADS-B could institute checks and counter-checks if there is suspicious activity or if transponder codes are being seen in undesignated areas. An encryption method for this system would be too costly, and the system is already deployed in some locations, which means it would have to be retro fitted.

Vulnerability: ATC Voice

As part of the NexGen overhaul of the ATC systems, tower voice systems are being upgraded. These voice systems operate in the Very High Frequency (VHF), Ultra High Frequency (UHF) and High Frequency (HF). There are many channels with these frequencies to prevent ground and airborne operators from talking over each other. A particular airspace has its designated set of frequencies. Many of the upgrades are designed to centralize the control of the radio systems.

The current radio system was developed long before the Internet came into viability. The system had to be hard wired to central control panels. The cabling was done using a multi-paired cable that was often connected through punch down blocks. The cabling and control system were maintained within the tower or in nearby facilities. These facilities had limited access with standard physical controls in place, including a key control program. Frequencies were publicly accessible, but the distribution was somewhat limited to hobbyists.

In the NexGen systems, the VHF, UHF, and HF systems will be integrated through an 802.11 connection. The networking of the radio systems is designed to allow for regional monitoring of the systems. Networking will also allow for airspaces to monitor each other's transmissions and hopefully be alerted to problems in a timelier manner. The current networking will be based on IPv4 standards. More weaknesses are introduced with the configuration as it is being installed.

All of the RF transmissions are made in what is known as the "clear." This means the transmissions do not use any type of encryption. The frequencies can be monitored very simply by any threat actor. The antennas are omni-directional, meaning the RF radiates in theory in all directions equally. So buying an antenna would not be very complex, neither would building an antenna be, if the threat actor were so inclined.

The frequencies used by a particular airspace are published on public websites that are accessible to anyone.

The technology used to make software radios has greatly advanced in the past few years. The ability of a threat actor to turn a laptop or desktop into a transceiver is currently much easier than ever before. For about $2,600 a threat actor can turn a home computer into a transceiver. With minimal understanding of radio operations, the threat actor could monitor frequencies and gather intelligence.

The spoofing of the IPs is somewhat more complex, but it can be an effective attack. The network the radio signals are be transmitted over is IPV4. IPv4 has no inherent encryption like IPv6, and transmissions again are in the clear and can be intercepted. Using a free program like Wireshark, a threat agent can learn a great deal about the network. It is not clear at this time if any other types of security are employed as the system is being installed.

Recommendations:

The newer radios are susceptible to Simple Network Management Protocol (SNMP), and voice-over-IP (VoIP) attacks. Ensure that measures are taken to mitigate SNMP and VoIP vulnerabilities.

A study needs to be conducted on the use of IPv6 as a medium for these types of links. Current effectiveness of IPv6 is limited to the 802.15.4 standard. Testing needs to be conducted on the 802.11 set of standards.

Authentication procedures need to be established for communications between ATC and aircraft.

Do not make frequencies available through open sources.

Research the ability of a system that uses a type of frequency hopping.

Use systems the implement signal encoding standards, i.e. Code Division Multiple Access (CDMA), Wideband Code Division Multiple Access (WCDMA), or similar.

Aircraft Systems

Introduction

There are multiple systems involved when operating an aircraft safely. This section will detail those specific systems and their relation with Air Traffic Control systems. Before getting in to the detail of the various systems, a brief history of the various aircraft manufactures will be provided. The most predominant manufactures of passenger aircraft in the world are Airbus and Boeing.

Boeing, headquartered in Chicago, IL, is the world's second largest aerospace company and leading manufacturer of both commercial jetliners and military aircraft. Boeing also designs and manufactures rotorcraft, electronic and defense systems, missiles, satellites, launch vehicles, and advanced information and communication systems. Some of its more popular products are the iconic 747, 737, 777, and the revolutionary 787. Its most recent military aircraft produced are the KC-46 Tanker and P-8 Poseidon.

Airbus, a derivative of the Airbus group (formerly known as the European Aeronautic Defense and Space Company), is headquartered in Blagnac, France, and is the creator of the first commercially viable fly-by-wire airliner – the A320 – and the largest passenger airliner ever created – the A380. Airbus also is a manufacturer of various military aircraft. One such fighter is the renowned Eurofighter. Revenues for 2013 are €33.7 billion or $37.8 billion. Their main competitor is Boeing.

Embraer is a Brazilian aerospace company, headquartered in São Jose dos Campos, Brazil, that produces commercial, military, executive, and agricultural aircraft. Embraer primarily competes in the small aircraft market (between 37 and 130 passengers). Embraer's military portfolio includes propeller and jet military aircraft as well as military cargo jets.

Bombardier is a multinational aerospace and transportation company, headquartered in Montreal, Quebec, Canada. Originally starting as a snowmobile manufacturer, it expanded to cover regional aircraft, mass transportation equipment, as well as recreational equipment. Bombardier Aerospace, headquartered in Dorval, Quebec, Canada, is the aerospace subsidy of Bombardier. Some of its aircraft are the CRJ 700, and it merged with Learjet in 1990.

Comac is the commercial aircraft corporation of China. Founded in May of 2008, Comac is headquartered in Shanghai, China, and is currently focusing their products in the >150 passenger market. They are planning on creating larger passenger aircraft to compete with Boeing and Airbus. Their two aircraft in production are the ARJ21 and C919. Comac and Bombardier signed a framework agreement in March of 2011 to go against the near-duopoly of Airbus and Boeing.

Textron Aviation is a general aviation business that manufactures the Cessna, Beechcraft, and Hawker brand aircraft.

The Dassault group is a French aviation company that creates various aircraft and aerospace solutions. The subsidiary, Dassult Aviation, is the primary manufacturing business of the company with 46% ownership by Airbus. Founded in 1929 by

Marcel Dassault, Dassault Aviation manufactures both military and regional jets. Some of the notable aircraft manufactured by this company is the Dassault falcon private jet line. Some of its military products are the Rafale, Mirage, and the new nEUROn Unmanned Combat Air Vehicle (UCAV).

The United Aircraft Corporation, headquartered in Moscow, Russia, is a group of Russian aircraft manufacturers focusing in military, civilian, transport/cargo, and unmanned aircraft. The corporation contains several aircraft manufacturers such as Ilyushin, Sukhoi, and Tupolev. A majority stake of the company is owned by the Russian government. Revenues for 2013 were $3.2 billion. Some of the notable aircraft to come out of the United Aircraft Corporation are the Su-34 fighter and the Tu-204 passenger jet.

Lockheed Martin is the largest global aerospace, security, advanced technology, and defense contractor in the world. It was formed by the merger of the Lockheed Corporation with Martin Marietta in 1995. Lockheed Martin is one of the world's largest defense contractors with about 74% of its revenue coming from military sales. Its most notable aircraft products are the F-22 Raptor, F-35 Lightning, C-130 Hercules, C-5 Galaxy, and the F-117 Nighthawk.

Northrop Grumman is a global aerospace and defense contractor formed by the merger of the Northrop Corporation with the Grumman Corporation. Listed as the fifth largest defense contractors as of 2013, some of its most notable products are the B-2 Spirit, EA-6 Prowler, and Growler.

General Dymanics is an American aerospace and defense contractor formed by many mergers, acquisitions, and divestures. It is listed as the sixth largest defense contractor as of 2013. General Dynamics gained much success with its F-16 Falcon fighter jet and F-111 Aardvark but left its aerospace business in the 1970s when the Cold War defense consolidation was occurring. However, as recently as 1999, General Dynamics has re-entered the airframe business by purchasing Gulfstream Aerospace, which mainly manufactures small to medium sized private civilian aircraft.

BAE Systems is a British, multinational aerospace, defense, and security company headquartered in London, England. It is ranked as the third largest defense contractor as of 2013. BAE Systems was formed in 1999 by the merger of Marconi Electronic Systems, General Electric Company PLC, and British Aerospace. Some of its most notable products in aerospace are the Typhoon and Tornado fighter/bomber aircraft and was a major partner in the F-35 Lightning program. BAE systems also holds shares in the Airbus Group.

While these manufactures create many different products, most of the systems are fairly common in principle. For all US airspace operations, the majority of aircraft brands are limited to Airbus, Beechcraft, Boeing, Bombardier, Cessna, Dassault, Embraer, and Lear. Many Russia, and Chinese built passenger aircraft as well as European military aircraft normally will not encounter US Airspace.

Vulnerability: Ground Maintenance Systems

The 787's development was not only to improve fuel economy and increase profitability to the airline. With the rise and advancement of aerospace technologies, the 787 was built with new, revolutionary diagnostic and maintenance systems that would reduce aircraft downtime due to faulty parts, engine and/or aircraft system issues, and general aircraft health.

While the traditional troubleshooting of manual inspection added computer diagnostics, the issue of connectivity arose. For older generation aircraft equipped with computer diagnostics, the general method of hooking up the aircraft via communication cable to a computer with the appropriate software was followed. With the expansion of wireless communication systems, diagnostic tracking became easier to conduct. Part of the new aircraft development process is working with airlines to identify requirements they may need in a new model. For example, the 777 was built with Boeing partnering with several large airlines such as American Airlines, by also understanding what the pilots, mechanics, and flight attendants wanted within an aircraft. Because of this, the success and popularity of the 777 is apparent in the current market. The next generation aircraft that Boeing (as well as Airbus) will be pushing out will have wired and wireless maintenance log systems as a way to streamline aircraft diagnostics for airlines. While the wired and onboard diagnostics will be standard, the wireless system will probably be sold as an add-on. As a matter of fact, the Boeing 777-9x and the 737 max will have this feature installed, and Boeing intends to create retrofit kits for airlines to install. Boeing and/or other manufactures could create this retrofit kit for older legacy aircraft, but when considering aircraft operating life-cycles, it may not make sense to create a kit for a 727 or 707. (Some examples of this maintenance technology can be seen in the Institute of Engineers article titled *Wireless Solutions for Aircraft Condition Based Maintenance Systems*, which was published in the Aerospace Conference Proceedings, Volume 6 in 2002.)

The potential vulnerability with these systems is that for those jets equipped with a wireless maintenance record system, attackers could use this technology to identify potential issues with an aircraft and run an exploit such as resetting the code without the repair being conducted and/or mechanics aware of the issue, thus creating a potentially unsafe aircraft. Additionally, this exploit could also result in false positives in terms of causing a notification of a system fault when there is no actual fault. This could result in potential economic damage to an airline as the aircraft will need to be pulled from service and evaluated for flight worthiness. Both these scenarios pose significant threat to airlines and customers, and since these diagnostic systems are somewhat linked to the systems that communicate with ATC systems, a risk is evident where if an ATC system was tampered with, an attacker could cause significant damage via the aircraft diagnostics system as detailed above.

Additionally, aircraft manufactures are now evaluating the use of wireless systems to communicate with flight control surfaces. This concept is called fly-by-wireless. Now this concept itself will pose an even bigger risk, as the flight controls can be directly accessed via wireless.

Fly-by-wireless systems are designed on the premise that by reducing the amount of wiring and various related systems, the weight of an aircraft can be dramatically reduced, which in effort will drive fuel efficiency, and/or more passenger/cargo revenue. Fly-by-wireless systems work very similarly to fly-by-wire systems except for a direct link, either cable or electronic wire, between the flight control and control surface. One can see this as using a wireless hotspot instead of directly wiring Cat 5 or Cat 6 cable to a router or switch. While this technology may be revolutionary and able to provide many benefits, it is not without risks and vulnerabilities.

Some of the risks that have occurred with this technology are seen in the use of drones, such as the RQ-170 Sentential intercepted by Iran. One can see the same increased potential risk through the implementation of fly-by-wireless systems.

The risks these systems provide is that the wireless transmission, although limited to a specific broadcast area as well as encrypted, can still be intercepted, and it would only take minutes before the signal is completely decrypted and for an attacker to take over the control surfaces. Additionally, these systems can be intercepted by sending signal transmissions to the aircraft itself. This would involve either sending a signal to interfere with the actual control of the flight controls or interfering with the aircraft computer to therefore change the trajectory of the aircraft itself.

In the article, *Fly-By-Wireless for Next Generation Aircraft: Challenges and Potential Solutions* (Dinh-Khanh,Mifdaoi, & Gayraud, 2012), potential options for successfully implementing a true fly-by-wireless system are detailed, including architecture and wireless protocols but also the potential risks of installing this type of system. The biggest risk the article mentioned was the susceptibility of interference of the actual communication signal. As a result, the following wireless technologies were evaluated: 802.11n, (ECMA-368) and IEEE 802.15.3c. ECMA and IEEE were classified with low interference levels, while 802.11n had high levels. The following table is referenced for additional detail of the wireless technologies:

Standard	**802.11n**	**HR-UWB**	**60 GHz**
Max Range (m)	30	10	10
Frequency Bands	2.4, 5GHz	3.10-10.6Ghz	60Ghz
Bandwidth	20/40Mhz	500Mhz-7.5Ghz	7GHz
Non-Overlap Channels	3	14	1
Modulation Technique	64QAM OFDM	QPSK MB-OFDM	QUSK, 64QAM ODFM or SC-FDE
LoS Requirements	No	No	Yes
Max Data Rate (Mbps)	600	110(10m)/ 200(6m)/480(2m)	3000
Encryption	RC4,AES	AES	N/A
Topology	Ad-Hoc,	Peer-to-Peer	N/A

	Infrastructure		
MAC Protocol	CSMA/CA DCF, PCF	TDMA or CSMA/CA HCF	TDMA

Figure 1: Wireless Technology Parameters

In addition to the wireless protocols, architecture was analyzed not only to be as efficient as possible but to also mitigate any potential risks that may occur due to signal interception. As a result, the architecture is built in a hybrid-cluster format (please see Figure 2 image below). By segmenting each control surface, this limits the possibility of control signals from the pilot's joystick being misinterpreted and operating the wrong flight surface. Additionally, if a signal is intercepted, odds are that only one flight control surface may be impacted (ex. one spoiler component vs the entire set of spoilers). This increases aircraft reliability, but once again poses a direct risk to the aircraft itself. Figures 3 and 4 detail the synchronization of signals and how the receiver transmission works with multiple clusters (as seen in the architecture diagram in Figure 2).

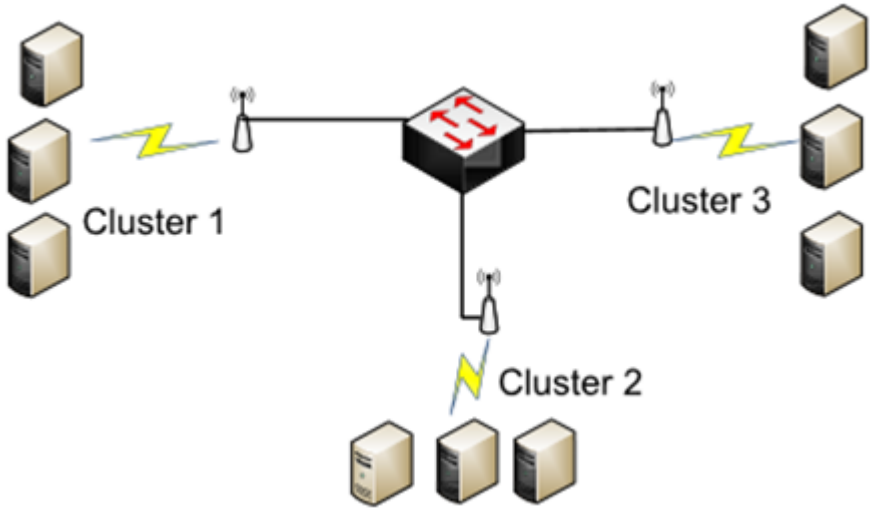


Figure 2: Network Architecture Structure for Fly-by-Wireless Systems

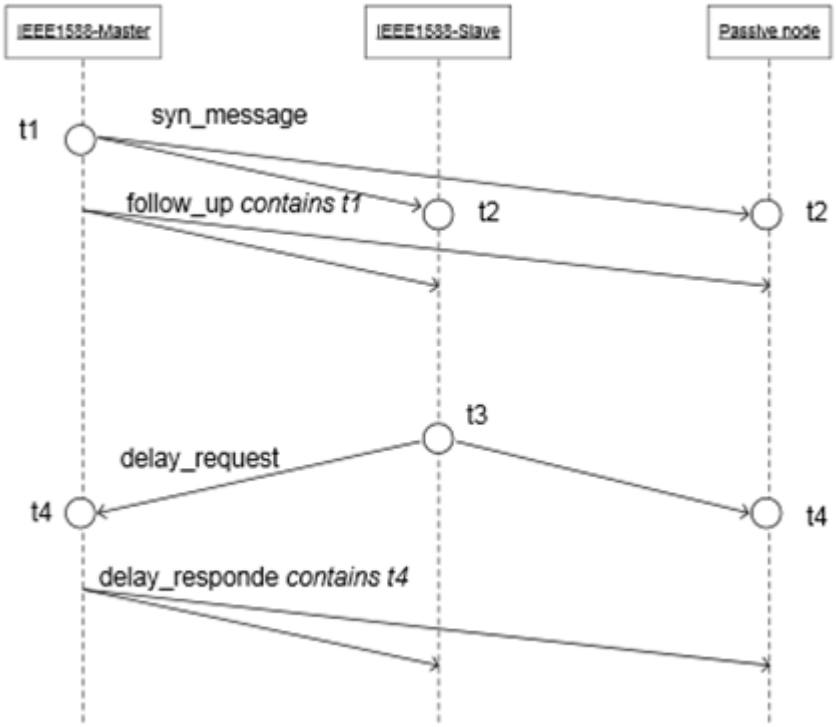


Figure 3: System syncronization flow chart

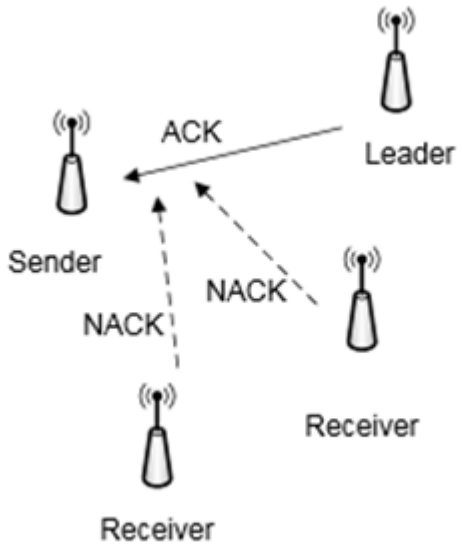


Figure 3: Reliable Wireless Transmission Flow

In the article's summary closing, the authors (Dinh-Khanh et al.) state the following:

> A Wireless Avionics Network (WAN) has been proposed based on hybrid architecture UWB/ Switched Ethernet to minimize communication latencies, reduce electromagnetic susceptibility and increase scalability. Communication predictability is enhanced due to TDMA-based protocol to guarantee a contention-free access. Furthermore, reliability mechanisms

> adequate to multicast communications are integrated to reduce overhead and guarantee reliable communications. The security risks like "man-in-the-middle" attacks are inherently reduced because of the low emission power and short range communications with UWB technology. (2012)

Although the likelihood of an attack occurring on a fly-by-wireless aircraft seems very unlikely, there still is a big chance that a direct attack may occur through the interception of ATC signal transmission that would put the aircraft and passengers at risk of a remote takeover with catastrophic events. While this may be the next generation, cutting edge technology with many numerous benefits for aircraft reliability, maintenance, and costs, the risk is simply too great (in the opinion of the authors of this report) for the technology to be implemented with the current state of security controls across the aviation industry.

With recent advancements and reduced costs with cloud computing and with the cloud being the new buzzword in technology, Boeing has begun pushing their cloud based solution called MyBoeingFleet (Boeing, 2015). Essentially, Boeing is taking ownership of collecting the data and allowing airlines to view the data via a thin client via a cloud solution subscription. A similar solution has been marketed by GE in terms of engine health. (GE Aviation, 2010).

This data being in a cloud environment poses its own set of problems with securing the information as well as providing it to a second or third party. The first issue that we see with cloud computing is that the risk increases on the individual holding the information. Attackers would like to use this information in malicious ways, so one would expect to see the rise in attacks against Boeing and any other cloud provider in this space to exponentially increase. In addition, one can expect that the airlines will be attacked as a way to not only obtain their information but also to monitor the data that they access/pull from these cloud systems. Perhaps they may conduct session hijacking attempts or username/password sniffing to access the data. Nevertheless, although as exciting as this new technology is, once can see these potential risks as a result of the damage they may cause.

Recommendations:

A complete Security Impact Assessment should be done per the National Institute of Standards and Technology (NIST) guidance. The assessment should include the cloud based solution and thin clients.

Encryption and encoding should be investigated for the end-to-end transmissions.

Implement two-factor authentication between thin client and cloud for logon.

Ensure that no interconnections of the maintenance and corporate networks are occurring.

Implement a Supply Chain Risk Management Plan.

Ensure computing systems have vulnerability and patch management plan in place. (This would not be for systems on board the aircraft.)

Vulnerability: Fly-By-Wire

The fly-by-wire system is a revolutionary system where flight controls are operated by electrical signals rather than cables attached to the yoke. Fly-by-wire was created primarily to drive more efficiency of not only operating an aircraft but to also increase aircraft reliability. The original flight system required mechanical and hydro-mechanical control systems, which added additional weight to the aircraft. In addition, the flight control cables had to be tightened to the right tension to ensure precise surface control movement. Multiple backup systems had to be in place to ensure that no failures impacted flight.

The concept of fly-by-wire was first tested on the Russian built Tupolev ANT-20, and the first pure electronic fly-by-wire aircraft with no mechanical or hydraulic pumps was the Apollo Lunar Landing Research Vehicle. More recently, the Boeing 777 was one such aircraft that was built purely on fly-by-wire technology, and Boeing adapted that technology to other various flight programs such as the 737 (only via thrust control) as well as the 787 program.

The development of fly-by-wire systems along with the advancement of flight technologies such as Global Positioning Systems (GPS) and radar, most aircraft are now essentially flying computers, with all flight controls running through a computer system prior to the flight controls making any movement. As a result, fly-by-wire systems need to be integrated to the automated flight controls for several reasons. Some systems that are linked to the flight controls that respond to the ATC systems are as follows, with a brief description of each:

- **Radio Altimeter** – The Radio Altimeter system essentially provides pilots and aircraft flight control systems the altitude information usually when the aircraft is operating between 0 and 2,500 feet. The system works with a series of transceivers that calculate radio altitude. This information is also transmitted to ATC systems for monitoring of aircraft actions. This system links with the ground proximity system, which prompts an alert to pilots if they are approaching the ground rapidly.
- **Air Traffic Control/Mode S System** – Possibly one of the most important system regarding this report, the ATC Mode S system's role is to let ground personnel monitor the aircraft as it moves across controlled airspace. The system reports back information such as if the transponders are communicating, altitude, and the aircraft's identification code.
- **Instrument Landing System** – The Instrument Landing System (ILS) supplies information required for approach, especially during instrument approaches. The flight computer uses ILS data to calculate aircraft position in accordance to the type of information required to make a safe approach and landing.
- **Traffic Alert and Collision Avoidance System** – The traffic alert and collision avoidance system works by utilizing data that is being communicated with the ATC/Mode S system. While most communication is done verbally, this computerized system that displays on the pilots screens

serves as additional safety. An aircraft cannot automatically adjust for a potential collision.

The integration between the autopilot, flight computer, display panels, and ATC systems works through a centralized, integrated communication system. The most popular system being used currently is manufactured by a company called ARINC, with the 429 series as the most widely used data bus standard in aviation. This system allows for the main fly-by-wire flight controls to be integrated to the flight computer flight management systems for smooth and precise operations, but this system also allows for the integration to autopilot systems so that the autopilot can make the necessary flight surface control movements to operate the aircraft as efficiently as possible. In addition, the data bus pulls in the data necessary for efficient action via some of the systems listed above via the autopilot flight director computer. As a result, all the various systems make an aircraft very well integrated and efficient, but this integration could also serve as a potential vulnerability to harm an aircraft's safe operation.

The following is an example of such vulnerability. With the revolution in aircraft technology, most ATC systems are now communicating with the aircraft via the flight computer. This flight computer contains all the necessary information for the flight to be successful. Details such as the various Instrument Flight Rules (IFR) points, flight plan, and navigation points are programmed into the computer, and the aircraft essentially follows these commands via the autopilot. The autopilot as such connects to the flight control systems in order to make the necessary movements of the aircraft to follow the commands set by the flight computer. Air traffic control systems come into play by working with the flight computer to ensure that commands are being followed by the flight plan. Obviously there is more to this than the ATC system sending commands to the aircraft, but essentially that is what happens most of the time, with pilots monitoring the aircraft to ensure that the commands are being followed. The risk identified asks if an ATC system is hijacked to send incorrect information, can the pilots make the necessary actions to mitigate the effects that the aircraft flight computer will make via the autopilot? This issue itself brings up Boeing and Airbus's philosophy of how the flight systems operate. Boeing believes that the pilots can override the computers actions in any case, while Airbus believes that the computer has the final say. As a result, there can be a potential scenario where the same attack may occur against two aircraft (one Boeing and one Airbus) where the Boeing aircraft may be able to recover from the false information while the Airbus may not. As a result of this cross integration, one can see this poses several risks, especially in the scope of this situation (ATC Hijacking).

Additionally, flight controls can be taken over by a hacker by simply using common devices and applications. As shared in hitbsecconf2013, an application was developed that can take control of various aircraft systems and ultimately, fly the aircraft with just the app (Teso, 2013). *More information can be seen in his Technology, Entertainment and Design Conference (TED) talk video: https://www.youtube.com/watch?v=wk1jIKQvMx8. In context to the ATC hijacking situation, this could result in several cases similar to this but also in communication issues, GPS/Radar tracking issues, and more. Because of the many various attack

options, this report will detail aircraft systems and the vulnerabilities they pose in conjunction to ATC systems.

Recommendations:

A complete Security Impact Assessment should be done per the National Institute of Standards and Technology (NIST) guidance on the entire system.

Ensure that some type of pilot intervention is capable if there is a failure event.

Investigate the operating systems used in the flight control computer.

Implement a Supply Chain Risk Management Plan.

Implement a Software Assurance Program.

Integrate cybersecurity into the Configuration Control Process.

Verify data paths and ensure there is proper separation.

Aircraft Identification

Commercial aircraft, business and general aviation, plus military aircraft that turn on their transponders as they enter commercial airspace, all use the ACARS and FANS VHF Data Link (VDL) Mode 2, which are standard worldwide for existing aviation navigation services. This spectrum was allocated in the 70s or 80s. It utilizes the 80s OSI network standards though slightly modified for aviation. This network is operated globally by only two providers; ARINC (now owned by Rockwell Collins) and SITA.

GPS is less a problem to commercial aviation as it is minimally used, originally due to the position "fuzzing" and potential shutoff in times of conflict. Fuzzing is no longer an issue but whose GPS to use for commercial aviation is. It is heavily used in business and general aviation (GA) aircraft now.

Radar identification may be carried out in several different ways:

- By use of Secondary Surveillance Radar (SSR). For example, by the following:
    - recognition of the aircraft identification in a radar label; or,
    - observing the setting of an assigned SSR code; or,
    - observing the selection of Squawk IDENT;
- By comparing the reported position of the aircraft with the radar response;
- By observing the response of the aircraft to a request to turn onto a specified heading;
- By transfer of radar identification.

An improved surveillance radar technology is Mode S, for Mode Select. Each Mode S-equipped aircraft has a unique, permanent identification number that remains during the life of the aircraft. It enables the air traffic control computer to tailor its interrogations, addressing only specified targets.

Once an air traffic control computer identifies an aircraft by its address, that aircraft goes into a "roll call." Subsequent interrogations are transmitted on a schedule. As a result, to track a target, Mode S needs far fewer interrogations than earlier radars, which translates into more accurate position reporting. A Mode S transponder does not have to wait until it is prompted from the ground to send out its address. It does so continually, and the unsolicited signals, or "squitters," can also include readings from the aircraft's altimeter, plus other flight information. This capability enables new kinds of air-to-air communication, such as the automatic signals of the Traffic Alert and Collision Avoidance System (TACS), which helps prevent midair collisions.

Recommendations:

A complete Security Impact Assessment should be done per the National Institute of Standards and Technology (NIST) guidance.

Verify manual procedures for verifying aircraft identification.

Aircraft Vulnerabilities

A more plausible Scenario could be the hacking of the Cobham AVIATOR, which is a system designed to meet the satellite communications needs of aircraft, including those related to safety operations.

International certification authorities provide a series of standards that represent the industry consensus opinion on the best way to ensure safe software, such as the Radio Technical Commission for Aeronautics (RTCA) specification DO-178B or the European Organization for Civil Aviation Equipment (EUROCAE) ED-12B. These regulatory standards define five levels of failure conditions, categorized by their effects on the aircraft, crew, and passengers:

- **Level A–Catastrophic** – Failure may cause multiple fatalities, usually with loss of the airplane.
- **Level B–Hazardous** – Failure has a large negative impact on safety or performance, reduces the ability of the crew to operate the aircraft due to physical distress or a higher workload, or causes serious or fatal injuries among the passengers.
- **Level C–Major** – Failure significantly reduces the safety margin or significantly increases crew workload. May result in passenger discomfort (or even minor injuries).
- **Level D–Minor** – Failure slightly reduces the safety margin or slightly increases crew workload. Examples might include causing passenger inconvenience or a routine flight plan.
- **Level E–No Effect** – Failure has no impact on safety, aircraft operation, or crew workload.

Software approved to levels A, B, or C require strong certification involving formal processes for verification and traceability. Software approved to levels D or E are subject to a more 'relaxed' control.

The vulnerabilities in the Cobham AVIATOR system could allow an attacker to take control of both the Swift Broadband Unit (SBU) and the Satellite Data Unit (SDU), which provides AeroH+ and Swift64 services. These vulnerabilities are (but not restricted to) the following:

- Hardcoded Credentials
- Undocumented Protocols
- Insecure Protocols
- Backdoors.

A successful attack could compromise control of the satellite link channel used by the FANS, CPDLC, or ACARS. A malfunction of these subsystems could pose a safety threat for the entire aircraft.

Threat description for Unmanned Aerial Vehicles (UAVs)

Small rouge UAVs at airport airspaces (B, C, D) have increasingly became a problem for ATC. While it is a more of a physical threat, the ATC information being broadcasted over the air can potentially make the threat more significant.

There have been many near-misses of mid-air collision between UAV and commercial jetliners reported all over the world. Whether they are accidental or malicious activities, a mid-air collision at takeoff or landing can be catastrophic. Even just the threat of having UAV targeting commercial aircrafts could seriously disrupt or halt air traffic.

The traditional radio-controlled (RC) drones have been sighted by airline pilots at altitudes between several hundred feet to 6,500 feet, and as close as 20 feet away. While the threats are real, it is still somewhat challenging to maneuver a RC drone to intercept a commercial aircraft at high altitude and velocity. However, with the NextGen system such as ADS-B, autonomous UAVs can be developed to utilize data from ADS-B In and calculate a mid-air collision course with an on-coming target aircraft with higher accuracy even at high altitude.

Security researchers have developed a Malware for ARDrone ARM Linux system, dubbed Maldrone (Malware Drone). According to the researcher, Maldrone can interact with the drone's device drivers and sensors silently and allow the hacker to control the drone remotely. As a result, Maldrone could be used to conduct remote surveillance (Estes, 2015).

Recommendations:

Possible countermeasures include the following:

Encrypted ADS-B – The discussion of ADS-B encryption has been brought up in the past. However, it has its challenges and will be difficult to implement anytime soon (Fink, Butts, & Mills, 2012).

Fuzzy ADS-B – The ADS-B protocol specifies levels of accuracy requirements. It is possible for ADS-B Out equipment to optionally introduce a randomized fuzziness in the velocity and position report within the margin of error allowed for the purpose of ATC. While this

does not completely eliminate the threat, it can potentially make it a little more difficult for malicious UAVs to track and intercept aircraft mid-air using ADS-B information. Such functionality can be built into the existing ADS-B software/hardware relatively easily.

GPS Spoofing – Researchers have shown that UAV can be spoofed by fake GPS data. Airport ATC can potentially use similar techniques to divert imminent threats from UAVs. The obvious downside for this countermeasure is that it interferes with systems like ADS-B and could potential impact the regular air traffic that relies on the GPS to function (Franceschi-Bicchierai, 2012). In practice however, the major commercial airlines do not solely depend on GPS for navigation, so they should still be able to operate normally without GPS (Charette, 2012).

Jamming – Jamming of WI-FI and radio frequency around the airports for targeted areas - technology to be implemented to block unauthorized UAVs approaching to the perimeter for both WI-FI (2.4 GHz and 5 GHz bands) as well as radio signals. This would result the remote control (ground unit) to lose signal to communicate to UAV immediately and drone to either return home or land based on its configuration. For more sensitive airports (i.e. military), a friendly discovery UAVs can be deployed to scan the perimeter and report back any hostile UAV's around the perimeter. This would be itself a detection control for any hostile UAV's approaching using the UAV technology itself.

Anti Aircraft Artillery – 20-25mm Anti Aircraft Artillery or Rifle chambered for the 25mm round mated to a state of the art sighting systems. The ideal system will be a modification of the airburst technology used in the OICW (Objective Individual Combat Weapon)and OCSW(Objective Crew Served Weapon). Modified AHEAD-type ammo, coupled with the laser rangefinder and ballistic computer can shoot down virtually all types of UAVs.

Threats and Attack Surfaces

Introduction

When thinking of a truly scary cyber attack scenario, one agree that it would deal less with the known capabilities that have been observed and more about the potential "unknowns" that slip by unnoticed but can have dramatic implications if gone unchecked. In this regard, one may find the subtle manipulation of data to be a potential effect as a result of a combination of cyber and physical activities working in tandem with one another. Therefore, for the purposes of the below scenario, the focus is more on that aspect of the cyber domain.

Scenario – Commercial Aviation and Economic Devastation

Iran, after suffering longstanding sanctions for pursuance of its nuclear program, decides to retaliate where it will hurt the US economy. Iran has supported proxy actors to conduct the ongoing distributed denial of services (DDoS) against US banks but has failed to inflict commensurate financial damage as Iran has suffered. This has prompted Iran to rethink its strategy and shift targeting to make a statement to the US government by impacting a critical transportation infrastructure and thereby causing immense financial losses.

Civil aviation represents a significant target for hostile actors. Civil aviation contributes substantially to the US economy. Among the notable financial statistics are the following:

- Commercial airline operations enabled $262.8 billion of visitor expenditures on goods and services (Federal Aviation Administration, 2014).
- Air travel hassles caused 38 million avoided trips, $35.7 billion in lost spending during 2013 (U.S. Travel Association, 2009).
- In 2012, the US economy generated $16.2 trillion in value-added economic activity and supported 143.3 million jobs in 2012. At the same time, the civil aviation industry supported 11.8 million jobs, accounted for $1.5 trillion in total economic activity, and contributed 5.4 percent to US GDP, or $15,826.8 billion (excluding R&D) (Federal Aviation Administration, 2014).

Commercial airports are often economic engines that drive the local, state, and national economies. Airports are valuable assets that contribute to the growth of jobs and economic output across the country. Using data from more than 90 state and individual airport economic impact studies, this analysis found that the 485 commercial airports in the US did the following:

- Supported 9.6 million jobs.
- Created an annual payroll of $358 billion.
- Produced an annual output of $1.1 trillion (CDM Smith, 2014).

After the 2001 terrorist attacks against the United States, the civil aviation industry suffered considerably. According to the International Air Transportation Association

(IATA), US airline revenues dropped from $130.2 billion to $107 billion in 2002. Losses for $19.6 billion were reported in 2001-2002, and between December 2002 and October 2005, United, Delta, Northwest, and UA Airways had filed for Chapter 11 bankruptcy reorganization (IATA, 2011). Hurting aviation appears to be a successful approach to hurting the US economy.

Scenario – Disruption

IEEE-USA Committee on Communications Policy indicated they wanted to take on UAVs communications policy this coming year. They are moving to a "Risk Based Safety Management" model which appears will now also encompass aviation cyber security and UAVs in their safety analysis processes for both aircraft and the national airspace.

For the following scenario, keep in mind that ground and aircraft response plans will be much different. Ground ATC response plans will look mostly like typical IT and other critical infrastructure systems. Aircraft systems will depend on which aircraft model and which systems and whether new protections can be added rapidly. The newer e-Enabled model have the beginning of a cyber perimeter, which may be able to accept new firewall rules or filters quickly without affecting certified onboard systems as NextGEN and SESAR develop. If the affected system is not protectable, patching the system software, testing, and re-certification will likely take 90 days, during which time the entire set of affected aircraft might grounded or at least have reduced operational capabilities as appropriate.

Also, the Avionics Full-Duplex Switched Ethernet (AFDX) bus used on the new E-enabled aircraft models (based on ARINC 664) is essentially a deterministic ethernet on which to run IP traffic (simplified but generally accurate). At the gate, via an ethernet gateway maintenance traffic can be sent to it, and during flight there is the capability to send aircraft health information out from the AFDX bus via a transmit only interface (one way diode) to onboard servers in non-critical areas for storage or transmission offboard. The core AFDX systems have no idea whether it was received or not; they simply stream data out. The ethernet gateways to AFDX need to have a robust cyber perimeter architecture and capability to control all communication to the aircraft as NextGEN/SESAR deploy.

This scenario focuses on causing disruption rather than destruction by targeting the confidence of the American people to take civil aviation for transportation. This will be done in two ways:

1. **Recruited Insiders** – Using standard tactics (money, extortion, ideology, ego, etc.), a person or persons with access to the air traffic control tower will be recruited. The recruitment of these individuals is critical because they will have direct access to the information to be manipulated. Flight information is provided by the pilot to the air traffic control. Flight data persons are the individuals responsible to review this information and enter it into the FAA host computer. The types of information inputted includes airline name and flight number, type of aircraft, intended airspeed and cruising altitude, and route of flight. Recruited flight data persons can input fake information into the FAA host computer. The FAA computer generates the flight progress strip

that will be passed from controller to controller throughout the flight. While this information is updated throughout the flight, it should not initially be discovered as the flight data person will be interfacing with the updates and is the same individual to give the pilot initial clearance to take off.

2. **Hacker Group** – A group of nation state proxy actors will "spoof" radio signals equipment and create "ghost" planes on the air traffic controller screens, as well as spoof GPS information back to the pilots. These acts should be done in a coordinated manner and would build off one another. This is done to confuse the two primary sources of information affecting air travel: the pilots and the air traffic controllers. Making both sources of this information questionable will cause major segments of the air traffic to be halted, cancelled, or redirected until the integrity of the information can be guaranteed. Based on previous information cited above, this quickly can become very costly.

The target airport is Chicago O'Hare, the word's second busiest airport. In 2011, the FAA published a study determining that O'Hare was one of the most dangerous airports with the most near collisions. Furthermore a recent incident occurred at O'Hare, where an FAA contractor purposefully set an air traffic control center on fire, forcing flight groundings and cancellations.

Goals

The goal of the above scenario is to ground, cancel, or delay flights.

A 2010 FAA report found that flight delays generally cost $32.5 billion dollars (Guy, 2010). Given the potential extensive ramifications of delayed/cancelled flights, especially for key airports, this could become very costly. For the 2014 Chicago O'Hare fire, every delayed flight cost $50,000 (Charisse, 2014).

- Other major airports will have to confirm they do not have similar occurrences; this will cause flights to be delayed, grounded, or cancelled for a period of time.
- After understanding that a percentage of the input information at O'Hare may be contaminated, flights to and from O'Hare will be stopped, cancelled, or re-routed.
- Air traffic controllers may be forced to transfer flight data manually rather than by computer, further adding to flight delays.

A further catalyst will be media exposure, which will target the fears of the American people. As the story breaks over the news, this will undoubtedly cause a minor panic in the population at large who may cancel their own trips. As evidenced after 9/11, people did not want to fly due to the unknown. Here, a similar impact can occur, which will last some period of time even after issues have been resolved.

Mitigations

Introduction

Because of the highly destructive functionality of the malware, an organization infected with the malware could experience operational impacts including loss of intellectual property (IP) and disruption of critical systems. Actual impact to organizations may vary depending on the type and number of systems impacted.

The following best practices, which are provided by the United States Computer Emergency Readiness Team (US-CERT), are recommended for tactical and strategic mitigations.

Tactical Mitigations

- Implement the indicators of compromise within your systems for detection and mitigation purposes.
- Encourage users to transfer critical files to network shares, to allow for central backed up.
- Execute daily backups of all critical systems.
- Periodically execute an “offline” backup of critical files to removable media.
- Establish emergency communications plans should network resources become unavailable.
- Isolate any critical networks (including operations networks) from business systems.
- Identify critical systems and evaluate the need for having on-hand spares to quickly restore service.
- Ensure antivirus is up to date.
- Disable credential caching for all desktop devices with particular importance on critical systems such as servers and restrict the number of cached credential for all portable devices to no more than three if possible. This can be accomplished through a Group Policy Object (GPO).
- Disable AutoRun and Autoplay for any removable media device.
- Prevent or limit the use of all removable media devices on systems to limit the spread or introduction of malicious software and possible exfiltration data, except where there is a valid business case for use. This business case must be approved by the organization Chief Information Technology (IT) Security Officer, with policy/guidance on how such media should be used.
- Consider restricting account privileges. It is recommended that all daily operations should be executed using standard user accounts unless administrative privileges are required for that specific function. Configure all standard user accounts to prevent the execution and installation of any unknown or unauthorized software. Both standard and administrative

accounts should have access only to services required for nominal daily duties, enforcing the concept of separation of duties. Lastly, disable web and email capabilities on administrative accounts. Compromise of admin accounts is one vector that allows malicious activity to become truly persistent in a network environment.

- Ensure that password policy rules are enforced and admin password values are changed periodically.
- Consider prohibiting hosts within the production environment or DMZ from sharing an Active Directory enterprise with hosts on other networks. Each environment should have separate forests within Active Directory, with no trust relationships allowed between the forests if at all possible. If necessary, the trust relationships should be one-way with the low integrity environment trusting the higher integrity environment.
- Consider deployment of a coaching page with click through acceptance; these are traditionally deployed in an environment to log the acceptance of network acceptable use policy or to notify users of monitoring. Coaching pages also provide some measure of protection from automated malicious activity. This occurs because automated malware is normally incapable of physically clicking an acceptance radial button. Automated malware is traditionally hardcoded to execute and then retrieve commands or additional executables from the Internet. If the malware is unable to initiate an active connection, the full train of infection is potentially halted. The danger still exists that the physical user will authorize access, but through the use of coaching pages, infections can be limited (or at least the rate of infection can be reduced).
- Monitor logs – Maintain and actively monitor a centralized logging solution that keeps track of all anomalous and potentially malicious activity.
- Ensure that all network operating systems, web browsers, and other related network hardware and software remain updated with all current patches and fixes.

Strategic Mitigations

- Organizations should review *Security Tip Handling Destructive Malware #ST13-003* and evaluate their capabilities encompassing planning, preparation, detection, and response for such an event.
- Always keep patch levels up to date, especially on computers that host public services accessible through the firewall, such as HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), mail, and Domain Name Service (DNS) services.
- Build host systems, especially critical systems such as servers, with only essential applications and components required to perform the intended

function. Any unused applications or functions should be removed or disabled, if possible, to limit the attack surface of the host.

- Implement network segmentation through virtual local area networks (V-LANs) to limit the spread of malware.
- Consider the deployment of a Software Restriction Policy set to only allow the execution of approved software (application whitelisting).
- Recommend the whitelisting of legitimate executable directories to prevent the execution of potentially malicious binaries.
- Consider the use of two-factor authentication methods for accessing privileged root level accounts or systems.
- Consider deploying a two-factor authentication through a hardened IPsec/VPN gateway with split-tunneling prohibited for secure remote access.
- Deny direct Internet access, except through the use of proxies for Enterprise servers and workstations. Perform regular content filtering at the proxies or external firewall points of presence. Also consider the deployment of an explicit versus transparent proxy policy.
- Implement a Secure Socket Layer (SSL) inspection capability to inspect both ingress and egress encrypted network traffic for potential malicious activity.
- Isolate network services, such as email and Web application servers by utilizing a secure multi-tenant virtualization technology. This will limit the damage sustained from a compromise or attack of a single network component.
- Implement best practice guidance and policy to restrict the use of non-Foundation assets for processing or accessing Foundation-controlled data or systems (e.g., working from home, or using a personal device while at the office). It is difficult to enforce corporate policies, detect intrusions, and conduct forensic analysis or remediate compromises on non-corporate owned devices.
- Minimize network exposure for all control system devices. Control system devices should not directly face the Internet.
- Place control system networks behind firewalls and isolate or air gap them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.
- Industrial Control System (ICS)-CERT and US-CERT remind organizations to perform proper impact analysis and risk assessment prior to taking defensive measures (US-CERT, 2014).

Process for Implementation

Introduction

When wondering where to start in the implementation of any advanced technological solution, one of the most efficient answers is to turn to the industry best practices and current guidance.

Best Practices and Planning Strategies

Common strategies can be followed to strengthen an organization's resilience against destructive malware. Targeted assessment and enforcement of best practices should be employed for enterprise components susceptible to destructive malware. The following implementation guidelines are provided by US-CERT:

Communication Flow

- Ensure proper network segmentation.
- Ensure that network-based access control lists (ACLs) are configured to permit server-to-host and host-to-host connectivity via the minimum scope of ports and protocols and that directional flows for connectivity are represented appropriately.
    - Communication flow paths should be fully defined, documented, and authorized.
- Increase awareness of systems that can be utilized as a gateway to pivot (lateral movement) or directly connect to additional endpoints throughout the enterprise.
    - Ensure that these systems are contained within restrictive VLANs, with additional segmentation and network access-controls.
- Ensure that centralized network and storage devices' management interfaces are resident on restrictive VLANs.
    - Layered access-control, and
    - Device-level access-control enforcement – restricting access from only pre-defined VLANs and trusted IP ranges.

Access Control

- For Enterprise systems that can directly interface with multiple endpoints:
    - Require two-factor authentication for interactive logons.
    - Ensure that authorized users are mapped to a specific subset of enterprise personnel.
- If possible, the "Everyone," "Domain Users," or the "Authenticated Users" groups should not be permitted the capability to directly access or authenticate to these systems.

    - Ensure that unique domain accounts are utilized and documented for each Enterprise application service.
    - Context of permissions assigned to these accounts should be fully documented and configured based upon the concept of least privilege.
- Provide an enterprise with the capability to track and monitor specific actions correlating to an application's assigned service account.
    - If possible, do not grant a service account with local or interactive logon permissions.
- Service accounts should be explicitly denied permissions to access network shares and critical data locations.
    - Accounts that are utilized to authenticate to centralized enterprise application servers or devices should not contain elevated permissions on downstream systems and resources throughout the enterprise.
- Continuously review centralized file share access control lists and assigned permissions.
    - Restrict Write/Modify/Full Control permissions when possible.

Monitoring

- Audit and review security logs for anomalous references to enterprise-level administrative (privileged) and service accounts.
    - Failed logon attempts,
    - File share access, and
    - Interactive logons via a remote session.
- Review network flow data for signs of anomalous activity.
    - Connections utilizing ports that do not correlate to the standard communication flow associated with an application,
    - Activity correlating to port scanning or enumeration, and
    - Repeated connections utilizing ports that can be utilized for command and control purposes.
- Ensure that network devices log and audit all configuration changes.
    - Continually review network device configurations and rule sets, to ensure that communication flows are restricted to the authorized subset of rules.

File Distribution

- When deploying patches or AV signatures throughout an enterprise, stage the distributions to include a specific grouping of systems (staggered over a pre-defined time period).
    - This action can minimize the overall impact in the event that an enterprise patch management or AV system is leveraged as a distribution vector for a malicious payload.
- Monitor and assess the integrity of patches and AV signatures that are distributed throughout the enterprise.

- Ensure updates are received only from trusted sources,
- Perform file and data integrity checks, and
- Monitor and audit – as related to the data that is distributed from an enterprise application.

System and Application Hardening

- Ensure that the underlying Operating System (OS) and dependencies (ex. IIS, Apache, SQL) supporting an application are configured and hardened based upon industry-standard best practice recommendations. Implement application-level security controls based upon best practice guidance provided by the vendor. Common recommendations include:
    - Utilize role-based access control,
    - Prevent end-user capabilities to bypass application-level security controls,
        - Example – disabling Antivirus on a local workstation
    - Disable un-necessary or un-utilized features or packages, and
    - Implement robust application logging and auditing
- Thoroughly test and implement vendor patches in a timely manner.

Recovery and Reconstitution Planning

A Business Impact Analysis (BIA) is a key component of contingency planning and preparation. The overall output of a BIA will provide an organization with two key components (as related to critical mission/business operations):

- Characterization and classification of system components and
- Interdependencies.

Based on the identification of an organization's mission critical assets (and their associated interdependencies), in the event that an organization is impacted by a potentially destructive condition, recovery and reconstitution efforts should be considered.

To plan for this scenario, an organization should address the availability and accessibility for the following resources (and should include the scope of these items within Incident Response exercises and scenarios):

- Comprehensive inventory of all mission critical systems and applications:
    - Versioning information,
    - System / application dependencies,
    - System partitioning/ storage configuration and connectivity, and
    - Asset Owners / Points of Contact.
- Contact information for all essential personnel within the organization,
- Secure communications channel for recovery teams,
- Contact information for external organizational-dependent resources:
    - Communication Providers,
    - Vendors (hardware/software), and

    - Outreach partners/external Stakeholders
- Service Contract Numbers – for engaging vendor support,
- Organizational Procurement Points of Contact,
- International Organization for Standardization (ISO) image files for baseline restoration of critical systems and applications:
    - Operating System installation media,
    - Service Packs/Patches,
    - Firmware, and
    - Application software installation packages.
- Licensing/activation keys for Operating Systems (OS) and dependent applications,
- Enterprise Network Topology and Architecture diagrams,
- System and application documentation,
- Hard copies of operational checklists and playbooks,
- System and application configuration backup files,
- Data backup files (full/differential),
- System and application security baseline and hardening checklists/guidelines, and
- System and application integrity test and acceptance checklists.

Containment

In the event that an organization observes a large-scale outbreak that may be reflective of a destructive malware attack, in accordance with Incident Response best practices, the immediate focus should be to contain the outbreak and reduce the scope of additional systems which could be further impacted.

Strategies for containment include the following:

- Determining a vector common to all systems experiencing anomalous behavior (or having been rendered unavailable) – from which a malicious payload could have been delivered:
    - Centralized Enterprise Application,
    - Centralized File Share (for which the identified systems were mapped or had access),
    - Privileged User Account common to the identified systems,
    - Network Segment or Boundary, and
    - Common DNS Server for name resolution.
- Based on the determination of a likely distribution vector, additional mitigation controls can be enforced to further minimize impact:
    - Implement network-based access-control lists to deny the identified application(s) the capability to directly communicate with additional systems.
- Provides an immediate capability to isolate and sandbox specific systems or resources.

- Implement null network routes for specific IP addresses (or IP ranges) – from which the payload may be distributed.
- An organization's internal DNS can also be leveraged for this task – as a null pointer record could be added within a DNS zone for an identified server or application.
    - Readily disable access for suspected user or service account(s), and
    - For suspect file shares (which may be hosting the infection vector), remove access or disable the share path from being accessed by additional systems.

As related to incident response and incident handling, organizations are reminded to do the following:

- Report the incident to US-CERT and/or ICS-CERT for tracking and correlation purposes, and
- Preserve forensic data for use in internal investigation of the incident or for possible law enforcement purposes.

Perimeter Security

Introduction

Perimeter security controls are the First Line of Defense and are usually located as far as possible from the main buildings. They should delay an intruder long enough for security personnel to reach appropriately. Protective barriers can be either natural or structural (e.g. fences, gates, bollards, and facility walls).

Threat	**Controls**
Theft	Locks
Espionage	Background Checks
Dumpster Diving	Disposal Procedures
Social Engineering	Awareness
Shoulder Surfing	Screen Filters
HVAC Access	Motion sensors in ventilation ducts

Perimeter Protection

Perimeter intrusion detection systems can be external to the facility, manually operated, electronic, unmanned, etc. Some perimeter sensors can detect intrusion across or under a land boundary or through a physical barrier such as chain link fencing.

The following examples are various types of perimeter protection, which can be preventative or detective:

- **Lighting** – various types of lighting should be in place:
  - Continuous lighting
  - Trip Lighting
  - Standby Lighting
  - Emergency Exit Lighting
  - Emergency Egress lighting.
- **Closed Circuit Television (CCTV)** – should have total surveillance:
  - Size
  - Depth
  - Height
  - Width
  - Lighting and contrast
  - Capability requirements:

        - Detection
        - Recognition
        - Identification
        - Mixing capabilities
        - Virtual CCTV System.

- **Doors** – Doors play a key role in a physical security program:
    - Isolation of critical areas
    - Lighting of doorways
    - Contact devices (switches)
    - Facility construction considerations
    - Protection of human life is the top priority.

- **Lock and Key Control** – Lock and key control system should have a proper procedure in place to accurately account for records:
    - Who has access to keys
    - To whom the keys are issued
    - Key inventory (sign out, destruction)
    - Access logs
    - Equipment Room should have adequate access controls and intrusion detection in place.

- **Data Processing Facility**
    - Small devices threat
    - Server room
    - Mainframes
    - Storage

- **Communication and Power**
    - Wireless Access Points
    - Network Access Control
    - Utility and Power Rooms

- **Work Area**
    - Operators
    - System administrators
    - Restricted work areas

The following are key threats to Support Systems:

- **Power Loss** – disruption/stoppage of operations

- **Heating, Ventilation, and Air Conditioning (HVAC) Failure** – overheating/overcooling
    - Water – flooding/dripping
    - Gas leaks – explosion
    - Fire – damage and destruction of facilities/equipment

- Sewage backup/breakage

Incident Response Plan for Aviation Exploits

Introduction

A well prepared Incident Response Plan could give the ATC, the crew an action plan how to:

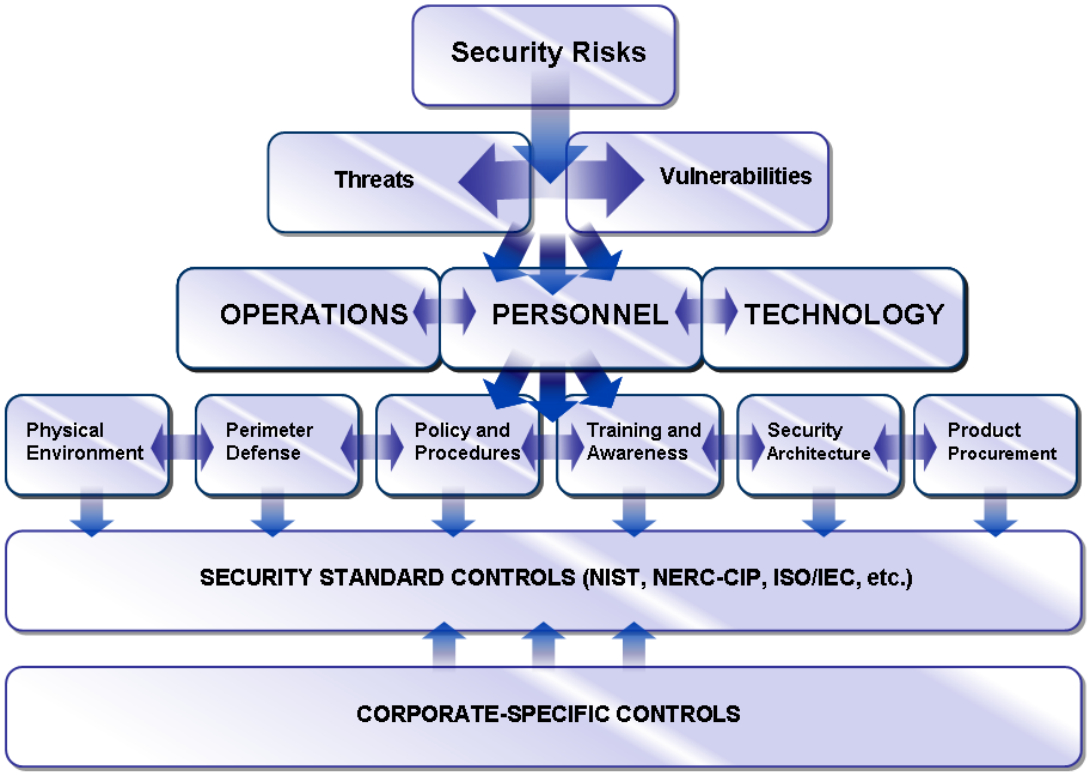
1. Identify an exploit (e.g. is it a physical fuel leakage issue or an exploit, truly issue of a too low altitude or an exploit, issues in autopilot?);
2. Immediately stop an exploit/ verify actions before reacting to situations (shut off the autopilot, do not correct altitude etc.); and
3. Mitigate issues caused by the exploit and further steps a regular Incident Response Plan practice suggests.

Activities for Incident Response Planning for Aviation Exploits

- Create a national Incident Response team
  - Create cross-functional, pre-cleared rapid ready teams. They need to be able to be assembled on-line within 15 minutes as there will not be much time to decide on a course of action. (Sorry if management wants to "appoint" members as the incident occurs; by then it is too late!)
  - Create incident response templates for different scenarios and different groups, but ensure responses are coordinated so that the different groups do not put out information or take conflicting courses of action.
- Define Roles
- Conduct Risk Analysis
- Generate Expected Activities, Test, and Document based on application system:
  - Air Systems/Aircraft
    - Distinguish between different type of A/C model and used systems
    - Generation of the A/C: legacy A/C OR E-enabled A/C
  - Ground System
- Perform Training with applicable personnel:
  - Pilot
  - Crew
  - Ground systems staff
  - Air framers
  - Engine manufacturers
  - Major onboard flight critical system suppliers (Honeywell, Thales, GE, etc.)
  - Airline ops staff

- Maintenance, Repair, and Operations (MRO)
- ATC staff
- FAA staff

Deciding who is "in charge" of incident response activities depends on each situation and what is being exploited. The airline, the air framer, the supplier, or any link in the aviation chain may need to take the lead. However, in particularly devastating incidents, it may be wise for the FAA to be in control, as they likely have the most complete view and can call in national resources.



Conclusion

The above research has indicated that there are many areas within the NexGen ATC system that will require a second look from a Cybersecurity perspective. The FAA needs to examine their ability to respond to incidents. The FAA needs to identify critical systems and then develop an incident response plan to keep those systems operating during outages caused by a cyber-attack. The response needs to be a coordinated response between the Airlines, Airline manufactures, and Government agencies to ensure the most effective response. The incident response is just not the responsibility of the FAA. While the FAA should be the lead agency each of the Airlines and Airline manufactures should also have their own incident response plans that can be implemented in coordination with the FAA.

A second point of entry that is critical to protect is the area of software and electronic maintenance. Maintenance systems should be subject to the same protection measures as a wired network under the FISMA guidance. The airborne systems of today are subject to updates through software loads from maintenance systems. The maintenance systems are also capable of monitoring airborne systems in flight. Currently these systems have very minimal protections that are employed. Two simple fixes for this would be to encrypt wireless maintenance transmissions. A second would be to employ digital software signatures. The signatures would have to be verified prior to upload of any updates. If a valid signature was not present then the software upload would fail with an alert message. This would ensure that at least the code being loaded was from a verifiable source.

Another identified weakness is the processes currently used for air-to-ground communications. There needs to be extensive testing of the current communications and data systems that communicate between the airborne platform and the ground. The testing should identify the weaknesses in the system. There should be discussion on a process forward to mitigate these weaknesses. Testing should be done at vendor facilities prior to system implementation to ensure that weaknesses are discovered and mitigated well before the system goes into operation. The effort has to be coordinated on an international level through the FAA and other like agencies. This ensures that there is a standard of security maintained across all communications and data systems being fielded.

There needs to be consideration given to current configuration of direct two-way Internet communications to the aircraft control domain in the NexGen systems. As identified in this report there are currently several notable weaknesses with the current configuration. These weaknesses should be thoroughly examined and mitigated before any further two-way Internet connections are allowed to be established. The current two-way Internet connections should be limited even more their transmissions to required messaging only. Airframe kits that retrofit these two-way Internet transmissions need to be built using an ICS standard. There needs to be consideration given to only retrofitting airframes that will provide sufficient air gap. No retrofitting should be done where the two-way Internet connections shares cabling with avionics systems.

It is not enough just to upgrade the current NAS systems there has to be consideration given to cybersecurity. There has to be an in depth review of the current systems with the objective of discovering weaknesses. State level threat agents need to be considered during any discussion of weaknesses within the NexGen system and the ability to exploit these weaknesses by these actors. The interconnectedness of the NexGen systems require that threats such as these be examined. The NexGen system also requires that a long examination of weaknesses and how to mitigate them is completed to ensure the NAS remains safe.

References

Boeing. (2015). *MyBoeingFleet*. BoeingEdge. Retrieved from https://www.myboeingfleet.com.

CDM Smith. (September 2014). *The Economic Impact of Commercial Airports in 2013*. Airports Council International – North America. Retrieved from http://airportsforthefuture.org/files/2014/09/Economic-Impact-of-Commercial-Aviation-2013.pdf.

Charette, Robert. (July 6, 2012). *Drones and GPS Spoofing Redux*. IEEE Spectrum. Retrieved from http://spectrum.ieee.org/riskfactor/aerospace/aviation/-drones-and-gps-spoofing-redux.

Dinh-Khanh, Dang, Ahlem Mifdaoi, and Thierry Gayraud. (2012). *Fly-By-Wireless for Next Generation Aircraft: Challenges and Potential Solutions*. University of Toulouse-ISAE. Retrieved from http://www.gta.ufrj.br/ftp/gta/TechReports/wd2012/1569654179.pdf.

Estes, Adam Clark. (January, 27, 2015). *New Malware Can Bring Down Drones Mid-Flight*. Gizmodo. Retrieved from http://gizmodo.com/new-malware-can-bring-down-drones-mid-flight-1682100201.

Federal Aviation Administration. (June 2014). *The Economic Impact of Civil Aviation on the U.S. Economy*. U.S. Department of Transportation. Retrieved from https://www.faa.gov/air_traffic/publications/media/2014-economic-impact-report.pdf.

Finke, Cindy, Jonathan Butts, and Robert Mills. (2012). *ADS-B Encryption: Confidentiality in the Friendly Skies*. Air Force Institute of Technology. Retrieved from http://www.usafa.edu/df/dfe/dfer/centers/accr/docs/CSIIRW.pdf.

Franceschi-Biccierai, Lorenzo. (July 19, 2012). *GPS Hijacking Catches Feds, Drone Makers Off Guard*. Wired. Retrieved from http://www.wired.com/2012/07/drone-gps-spoof/.

GE Aviation. (2010). *Integrated Vehicle Health Management: Connecting You with Your Aircraft*. General Electric Company. Retrieved from http://www.ge.com/thegeshow/docs/ge_ivhm_brochure.pdf.

Guy, Ann Brody. (October 18, 2010). *Flight Delays Cost $32.9 Billion, Passengers Foot Half the Bill*. UC Berkeley News Center. Retrieved from http://newscenter.berkeley.edu/2010/10/18/flight_delays/.

IATA. (June, 2011). *The Impact of September 11 2001 on Aviation*. Retrieved from http://www.iata.org/pressroom/documents/impact-9-11-aviation.pdf.

Jones, Charisse. (September 26, 2014). *Snarl in Chicago May Cost Airlines Millions*. USA Today. Retrieved from http://www.usatoday.com/story/money/business/2014/09/26/chicago-flights-grounded-airlines-impact/16268699/.

Teso, Hugo. (April, 2013). *Aircraft Hacking: Practical Aero Series*. N.runs Professionals. Retrieved from https://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf.

US-CERT. (December 19, 2014). *Targeted Destructive Malware*. Department of Homeland Security. Retrieved from https://www.us-cert.gov/ncas/alerts/TA14-353A.
U.S. Travel Association. (September 2009). *Key Findings from the Air Travel Summary*. Retrieved from https://www.ustravel.org/sites/default/files/page/2009/09/Key_Findings_Summary_D7.pdf.