
# EXPLORING POTENTIAL ADS-B VULNERABILITES IN THE FAA'S NEXTGEN AIR TRANSPORTATION SYSTEM

GRADUATE RESEARCH PROJECT

Donald L. McCallie, Major, USAF

AFIT/ICW/ENG/11-09

**DEPARTMENT OF THE AIR FORCE**
**AIR UNIVERSITY**

***AIR FORCE INSTITUTE OF TECHNOLOGY***

**Wright-Patterson Air Force Base, Ohio**

AFIT/ICW/ENG/11-09

# EXPLORING POTENTIAL ADS-B VULNERABILITIES IN THE FAA's NEXTGEN AIR TRANSPORTATION SYSTEM

GRADUATE RESEARCH PROJECT

Presented to the Faculty

Department of Electrical & Computer Engineering

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Cyber Warfare

Donald L. McCallie, BS, MS

Major, USAF

June 2011

AFIT/ICW/ENG/11-09

# EXPLORING POTENTIAL ADS-B VULNERABILITIES IN THE FAA's NEXTGEN AIR TRANSPORTATION SYSTEM

Donald L. McCallie, BS, MS
Major, USAF

Approved:

| | |
|---|---|
| _____/SIGNED/_____ | 23 May 2011 |
| Jonathan W. Butts, Capt, PhD (Chairman) | Date |
| _____/SIGNED/_____ | 23 May 2011 |
| Robert F. Mills, PhD (Member) | Date |

## Abstract

The Federal Aviation Administration's (FAA) Next Generation upgrade proposes a fundamental transformation to the national airspace system (NAS) that aims to reduce dependence on outdated radar infrastructure, increase airline safety and condense required aircraft spatial separation. A key component of the upgrade is the Automatic Dependent Surveillance-Broadcast (ADS-B) system. ADS-B provides continual broadcast of aircraft position, identity, velocity and other information over unencrypted data links to generate a precise air picture for air traffic management. Official documents claim operational requirements necessitate unencrypted data links while maintaining that there is a low likelihood for malicious exploitation. This paper studies the security vulnerabilities associated with the ADS-B implementation plan and develops a taxonomy to classify attacks and examine potential impacts the attacks have on overall NAS operations. The taxonomy helps provide a comprehensive understanding of the threats associated with ADS-B implementation and facilitates risk analysis and risk management. For demonstration purposes, three vignettes are presented to highlight how ADS-B attacks could impact military operations and homeland defense. Finally a series of recommendations for consideration in the implementation plan going forward is provided.

**Acknowledgements**

First and foremost, I want to thank my wife for her support throughout my Air Force career, and especially during my time at AFIT. Without her encouragement and patience many of the challenges we've faced would seem impossible!

I would also like to thank my research advisor, Capt. Jonathan Butts, for allowing and encouraging me to conduct this research project based on my personal experience and interests in aviation, computer automation and perceived vulnerabilities in the FAA's NextGen upgrade to the U.S. National Airspace System.

.

## Table of Contents

Page

## List of Figures

## List of Tables

# Exploiting ADS-B Implementation In The FAA's Next Generation Air Transportation System

## I. Introduction

*The question that's out there goes something like this: Is NextGen real? Yes, NextGen is quite real. It really can happen. It really is happening. NextGen is good for the passenger, the pilot and everybody whose paycheck is touched by an airplane. And when we're talking aviation, we're talking 5.6% of America's GDP. In a time of economic turbulence, American can ill afford turbulence in the national airspace system* [1].

### 1.1 Background

The United States–indeed the global economy–is dependent on safe and reliable air transportation. With an exponential increase in aviation expected over the next decade and the reliance on aviation for transportation of people and goods, even a temporary loss could have devastating impacts.

Consider the recent Iceland volcano eruption in April 2010. Due to volcanic ash, flights throughout Europe were canceled because of safety concerns. During a week-long period over 95,000 flights were canceled and 1.2 million passengers a day were impacted–affecting approximately 29 percent of global aviation [2]. International Air Transport Association chief executive Giovanni Bisignani estimated that airlines lost revenues of $80 million each day during the first three days of groundings.

Impacts to air transportation are not limited to acts of nature. Indeed, "Operation Hemorrhage" is one of the latest plots by terrorist extremists designed to cripple the U.S. economy [3]. Intended to bring down UPS and FedEx cargo planes via printer bombs, Operation Hemorrhage cost only $4,200 to fund and three months to plan and execute [3]. A similar plot was carried out in December 2009, when an al Qaeda member attempted to bring down a

commercial airliner over Detroit by smuggling explosives onboard that were stowed in his underwear [4]. The results of the two failed attempts were felt by passengers in longer check point lines and increased security regulations.

The current national airspace system (NAS) relies on a systematic framework that dates primarily back to the 1970s [5]. In an attempt to increase safety and capacity of air transportation operations, the Federal Aviation Administration (FAA) is moving forward with a fundamental overhaul. The new framework, called Next Generation (NextGen), will drastically change the current infrastructure and operations [6]. A key component of the NextGen upgrade is the Automatic Dependent Surveillance-Broadcast (ADS-B) system. When fully operational, NextGen will rely on ADS-B for air traffic management.

### 1.2 Motivation

Historically, new technology is deployed with the primary focus on functionality as opposed to examining security implications; ADS-B is no exception. ADS-B provides continual broadcast of aircraft position, identity, velocity and other information over unencrypted data links [7]. There are no apparent security mechanisms to protect the confidentiality, integrity or availability of the data transmitted between aircraft and air traffic controllers. As a result, a motivated attacker could inject false targets into the system or prevent legitimate targets from being properly displayed. Such actions could have devastating effects on the entire NAS infrastructure.

This paper examines security vulnerabilities associated with the ADS-B implementation plan. A taxonomy to classify attacks and examine potential impacts the attacks have on overall NAS operations is provided. This taxonomy helps provide a comprehensive understanding of the threats associated with ADS-B implementation, which supports risk analysis and risk

management. Finally a series of generalized recommendations for addressing the complex security issues relating to NextGen and ADS-B is discussed. These recommendations not only apply to commercial aviation but also to military aviation and DoD operations. Military aircraft will be forced to upgrade avionics to comply with the FAA's ADS-B mandates which will expose military aircraft and operators to the same vulnerabilities as commercial aviation.

### 1.3 Organization

The remainder of the paper is organized as follows. Chapter II examines the history and progression of the national airspace system. Chapter III details ADS-B technology. Chapter IV examines the security principles of ADS-B. Chapter V introduces the taxonomy, provides example attacks and presents vignettes that demonstrate ADS-B messaging attacks that effect DoD and DHS operations. Chapter VI discusses recommendations and Chapter VII provides conclusions.

### 1.4 Scope

The FAA's NextGen upgrade to the U.S. NAS includes many systems and subsystems; overall it is often referred to as a system of systems. This paper, however, examines only one component of the upgrade, the linchpin, ADS-B. Furthermore, the discussion of ADS-B is restricted specifically to the ADS-B 1090MHz frequency; although the analysis readily translates to the General Aviations (GA) 978MHz Universal Access Transceiver (UAT) and ADS-R (rebroadcast) technologies. The taxonomy and attack examples focus on commercial operations, but as demonstrated by the vignettes, they could readily translate to military operations.

## II. Overview of the National Airspace System

Chapter II focuses primarily on the history of the U.S. NAS, the upgrades over the past 70 years that have led to today's ATC systems and the FAA's proposed NextGen upgrade to the system.

### 2.1 History

The advent of air traffic control (ATC) and navigation aids date back to the 1920s when the Post Office Department maintained bonfires at night to help aviators navigate [5]. These bonfires later transitioned to beacon lights maintained by the Department of Commerce Lighthouse Division; by 1930 the beacons were replaced by a non-directional radio navigation system that emitted beams of electromagnetic energy modulated with Morse code. During this period, aviation was still in its infancy and the need for an overarching air traffic control system was not fully recognized.

As beacons were being employed to aid in navigation, the airlines created an internal system of radio stations to monitor their en route traffic [5]. The stations were located in Chicago, Newark and Cleveland–each with distinct radio frequencies for the individual airlines. In 1936, the Bureau of Air Commerce acquired the radio stations, introducing the skeletal beginnings of a federal air traffic control system [5]. The Chicago, Newark and Cleveland airline radio stations constituted what is considered the first generation of ATC. The first generation of ATC consisted of no automation and little to no radar coverage; the system predominantly employed manual methods of tracking aircraft using progress strips [5]. Thirty-three years later, in 1959, automation transitioned ATC into the second generation with en route computers for processing flight data and ground based radar to track aircraft.

In 1961, ATC transitioned once again when the FAA's "Project Beacon" incorporated ground based equipment to interrogate a transponder located on the aircraft [5]. Project Beacon evolved from the Identification Friend or Foe (IFF) concept of World War II that allowed British Radar operators to identify German aircraft trying to fly undetected into England.

Ultimately, it was computer technology that allowed aviation to enter a new era with the upgraded third generation development (UG3d) in the 1970s [5]. UG3d provided the FAA advanced equipment upgrades in both the terminal and en route environments. The upgrades enabled automation of controller tasks and the capability for the controller to have an instant picture of aircraft location, identity, altitude, direction and speed.

### 2.2 Current National Airspace System Infrastructure

With the exception of GPS technologies, the current NAS infrastructure has undergone few changes since the UG3d of the 1970s [5]. Computer automation, computer networks, unique four digit IFF aircraft transponder codes, radio communication and radar integration are still the major components and backbone today's NAS.

The NAS consists of more than 750 ATC facilities, 18,000+ airports, 4,500 air navigation facilities and 13,000 instrument flight procedures with approximately 2,153,326 instrument approaches executed annually [8]. The 750 ATC facilities are comprised of 21 Air Route Traffic Control Centers (ARTCCs), 197 Terminal Radar Approach Control (TRACON) facilities, 460+ airport control towers and 75 flight service station (FSS) facilities [8]. ARTCCs are responsible for controlling en route traffic within designated control sectors, some of which cover more than 100,000 square miles and traverse multiple states. ARTCCs accept air traffic from and pass air traffic to TRACON facilities that control aircraft within an approximate 30 nautical mile radius of the airport. FSS facilities provide general information to pilots such as

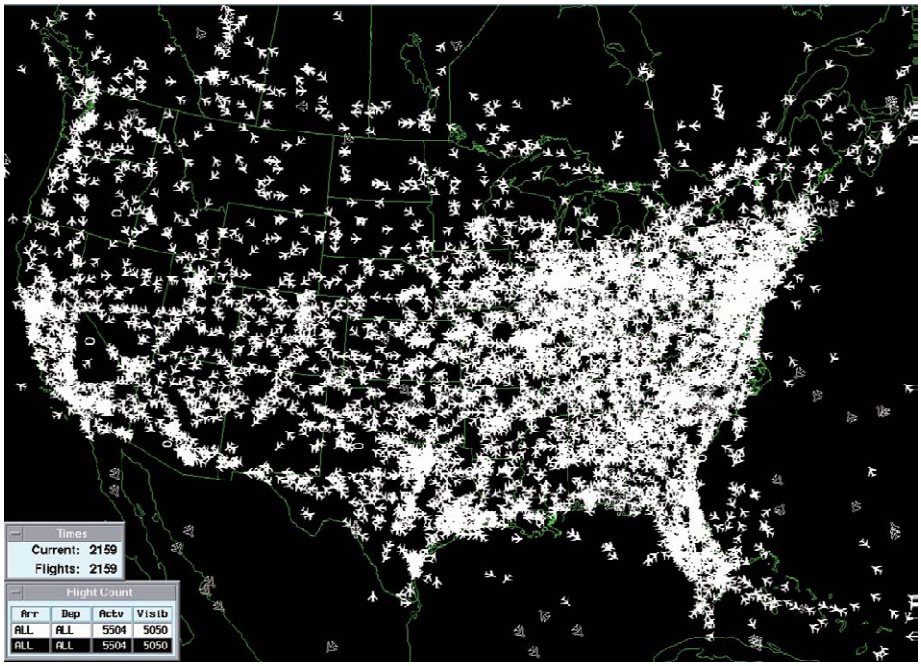


**Figure 1: Screen capture from an ARTCC monitor [8].**

weather and traffic advisories. Figure 1, from an Air Traffic Control System Command Center monitor, shows how busy this complex system of facilities, systems, equipment, procedures, airports and people are with over 5,000 aircraft operating during a peak period. Increased air traffic, aging equipment and a desire to leverage technological advancements necessitate a comprehensive overhaul to the NAS.

### 2.3 Next Generation National Airspace System Upgrade

The current air transportation system performs well but is susceptible to disturbances that can cause long delays (e.g., weather) and is approaching its capacity limits [9]. Without a transformation, the expected growth in air traffic will likely create costly flight delays and increased flight safety hazards. In response to growing concerns, the U.S. Congress established the Joint Planning and Development Office to manage the development of NextGen [10]. The primary goal of NextGen is to significantly increase the safety and capacity of air transportation operations [6]. The upgrade requires a fundamental transformation of the entire NAS, including

incorporation of satellite-based technologies for surveillance operations to replace legacy ground-based systems currently in use.

## III. Automatic Dependent Surveillance-Broadcast

Automatic Dependent Surveillance-Broadcast (ADS-B) is a crucial component of the FAA's NextGen upgrade. It comprises surveillance techniques for precise aircraft tracking that replaces antiquated capabilities. Indeed, the operational plans claim significant advancements in safety, efficiency and flexibility over the current NAS infrastructure [9]. This chapter discusses ADS-B functionality and system details concluding with a discussion on how NextGen will impact military operations.

### 3.1 Overview

For safety, ADS-B will enhance ATC situational awareness, collision avoidance, surface runway incursion avoidance, and the ability to implement ATC in non-radar environments (e.g., oceanic surveillance). Increased accuracy will allow condensed aircraft separation standards, higher probability of clearance requests, and enhanced visual approaches. Additionally, ADS-B will contribute to more direct routings and optimized departures and approaches, which will increase capacity, while saving time and fuel. Finally, the infrastructure relies on simple radio stations that are significantly cheaper to install and maintain than the mechanical infrastructure associated with traditional radar ground stations [11]. A general comparison of current surveillance and ADS-B attributes are summarized in Table 1.

Current NAS surveillance techniques rely on Procedural ATC, Primary Surveillance Radar (PSR) and Secondary Surveillance Radar (SSR). Procedural ATC is a dependent surveillance technique that requires pilots to report their position using voice channels (e.g., HF and VHF). This technique is slow, cumbersome and prone to human error. PSR is an independent and non-cooperative technique typically used in busy terminal areas. These ground-based radars measure aircraft position (i.e., range and azimuth); the aircraft does not require any

**Table 1: Comparison of surveillance attributes (derived from [11]).**

| Ground based radar system | ADS-B system |
|---|---|
| Ground based infrastructure only, requires challenge and response and pilot-to-controller voice comm. | Aircraft, ground and space based infrastructure, provides constant flow of more precise position data, reduces required voice comm. |
| Coverage gaps exist in some areas | ADS-B ground stations can be placed virtually anywhere |
| Position updates every 12 seconds | Position updates every second |
| Costly to install and maintain | Significantly less costly to install and maintain |
| Air Traffic Control | Air Traffic Management |

on-board equipment. SSR is a partly-independent and cooperative technique typically used for en route tracking. Ground-based radars measure aircraft position but rely on aircraft to provide altitude and identity. Aircraft are required to carry a transponder that only responds when interrogated by a ground station.

ADS-B is designed to overhaul current surveillance techniques, with the new capabilities intended to enhance air traffic management. It is automatic because it requires no pilot or controller intervention; it is dependent surveillance because the aircraft derives its own position from the global navigation satellite system; and it continually broadcasts the position and other data to nearby ground stations, aircraft and surface vehicles (e.g., taxiing aircraft) [11]. ADS-B affords improved accuracy over conventional radar–20 meters of precision compared to 300 meters at 60 nautical miles–and does not deteriorate as receiver range increases [12].

### 3.2 ADS-B Operations

ADS-B will play a key role for NextGen. System capabilities will be integral in all phases of flight: push back, taxi and departure; climb and cruise; descent and approach; and

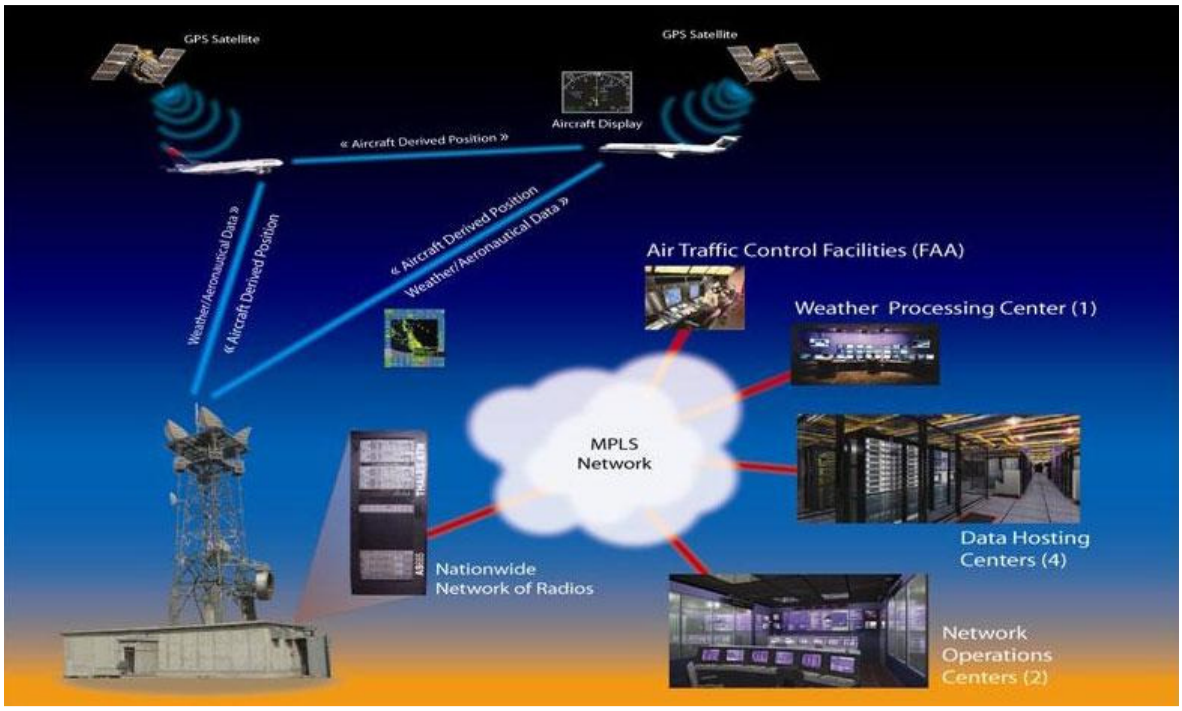


**Figure 2: Depiction of ADS-B operations [11].**

landing, taxi and arrival [9]. Figure 2 provides a generalized depiction of ADS-B operations. An aircraft first determines its position via GPS. The position data along with identity, altitude, velocity vector and vertical rate are then broadcast using the aircraft's Mode S transponder. ADS-B ground stations within range receive the broadcast and relay the information via a networked backbone to air traffic control. Properly equipped aircraft within range also receive the broadcast.

ADS-B is separated into two functional operations: (i) ADS-B OUT and (ii) ADS-B IN. ADS-B OUT allows aircraft or surface vehicles to continually generate ADS-B broadcasts; this functionality provides ATC with real-time position data. ADS-B IN allow aircraft to receive and display another aircraft's ADS-B OUT information (e.g., graphical display of relative horizontal and vertical positions of aircraft, surface indicators/alerts, airborne conflict detection, along-track guidance, and deconfliction guidance). ADS-B IN will also allow aircraft to receive services

provided by the ground stations (e.g., weather updates). Aircraft can be equipped with ADS-B OUT without having ADS-B IN capability.

The FAA is proposing a series of approximately 800 ADS-B ground stations, placed approximately 150 to 200 miles apart [13]. Currently, the NAS has over 315 active ground stations reporting on the Surveillance and Broadcast Services (SBS) network with 400 stations planned by year-end 2011 [14]. Although data from the March 2011 NextGen Implementation Plan shows current equipage levels of ADS-B OUT at "0%", companies such as UPS have equipped their entire fleet (i.e., 211 airplanes) for ADS-B OUT and 107 aircraft have been equipped with ADS-B IN [15].

Because the NAS is in a transition period, the current ATC sectors leveraging ADS-B are still augmented by traditional surveillance tracking (e.g., Secondary Surveillance Radar). However, on May 28, 2010, the FAA released a Final Ruling that specifies aircraft must be equipped with ADS-B OUT by 2020; equipage of ADS-B IN for aircraft is to remain optional [7]. At that point, Secondary Surveillance Radar will become obsolete, although it is expected that Primary Radar Surveillance will remain as a compliment to ADS-B.

### 3.3 System Details

Figure 3 shows the functional components and modules of the ADS-B system. Data exchange between the three primary components (i.e., transmitter aircraft, receiver aircraft and ground station) requires standard message formats and transmission protocols.

ADS-B messages are to be transmitted on the 1090MHz data links that currently facilitate transmission of Mode S. To support ADS-B, Mode S transponders will incorporate a feature called extended squitter (ES). The Mode S extended squitter is intended to provide a smooth upgrade from traditional Mode S; the notion is to ensure seamless integration with

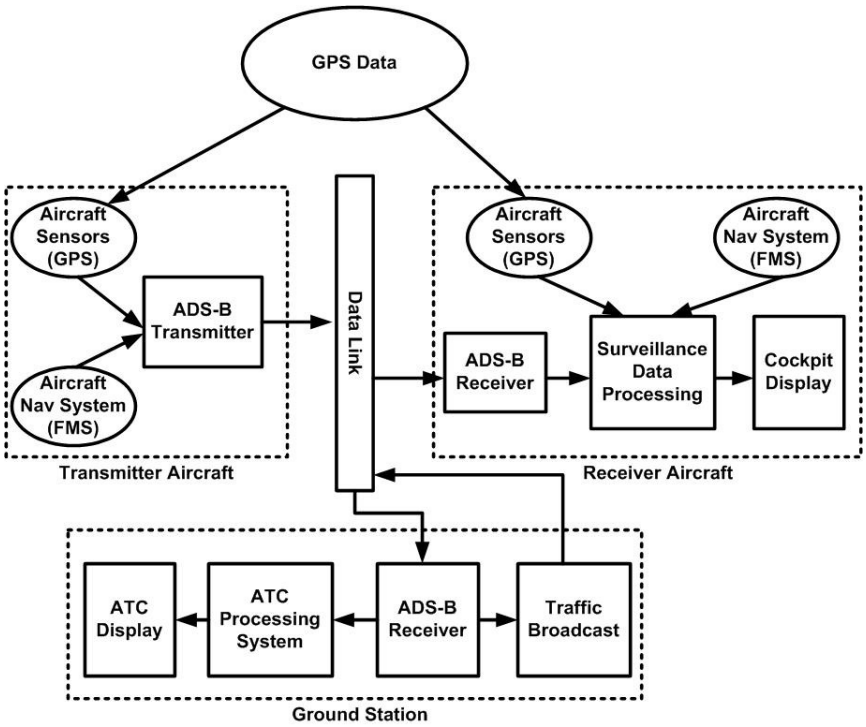


**Figure 3: Functional components of ADS-B system (modified from [12]).**

existing systems during the upgrade transition period. Figure 4 depicts the 1090MHz ES message format which is 112 bits long and contains 56 bits of ADS-B information. The preamble contains a special sequence of bits used for synchronization. The downlink format field is 5 bits and indicates the type of message–this field is set to 17 for ES messages. Capability is a 3 bit field and indicates the capability of the Mode S transponder. The aircraft address is a unique 24 bit identifier assigned for the life of the transponder; it is intended that no two aircraft should ever have the same identifier.

Military and special government flights will have the ability to change this 24 bit identifier to increase operational security. The ADS-B data field is 56 bits long and contains corresponding surveillance data (e.g., identification, position, velocity, urgency code and level of quality). The parity check is a 24 bit field used by receivers to detect and correct transmission errors in the received message. Pulse Position Modulation (PPM) is the signal modulation


**Figure 4: 1090 ES Message Format**

scheme used for message encoding, decoding and transmission.

As mentioned previously, ADS-B uses a broadcast communication paradigm. Aircraft transmit messages with no awareness of what entities might receive the information; any entity within range can receive and decode the transmission. Further, the transmission protocol does not require an acknowledgement of message receipt or implement any keep alive functionality (i.e., if an aircraft is not 'heard from' within a specified time period the system will not query the aircraft to determine current status).

As a final note, the 1090MHz ES is designed for commercial aircraft aviation and is the international standard for ADS-B OUT. However, the FAA has approved the Universal Access Transceiver (UAT) link for use by general aviation aircraft flying at lower altitudes [7]. UAT transceivers operate in the 978MHz range and are specific to U.S. airspace–UAT operations are not used internationally. To facilitate interoperability, the support component called Data Surveillance-Rebroadcast (ADS-R) will be deployed in all areas where ADS-B ATC exists. ADS-R receives the traffic information broadcasts on the 1090MHz ES or UAT links and rebroadcasts the information to the opposite data link user.

### 3.4 Military Aviation and ADS-B

Military aviation will benefit from enhanced ATC situational awareness, collision avoidance, surface runway incursion avoidance, and the ability to operate in non-radar environments. However, this free flow of unencrypted information could be an Operational Security (OPSEC) issue for the DoD [16].

Military aviation mission sets can typically be classified into three types: Training/Overt, Sensitive and Covert/Classified [17]. ADS-B can and should be employed to its full capabilities during training or overt missions such as air refueling operations, oceanic crossings and daily pilot training operations. During sensitive operations (e.g., combat operations) use of ADS-B will need to be evaluated on an individual basis. Some missions may dictate that ADS-B OUT be turned off completely. Another option is the continued development of an encrypted channel such as Mode5 Level2-B (Broadcast), which encrypts ADS-B data and relays it via Mode5 Level2 transmissions to other military aircraft and ground stations; the aircraft only receives ADS-B IN but does not transmit an ADS-B OUT signal. Covert/Classified missions will require that ADS-B be turned off completely; however, these missions may still be able to enjoy some benefits of ADS-B via encrypted channels such as Mode5 Level2 Broadcasts.

If proper employment procedures are developed, tested and coupled with new avionics systems such as Mode5 Level2, ADS-B can be a force enhancer for the military. However, the security implications of using ADS-B should be considered for each specific mission.

# IV. Security Assessment of ADS-B

This chapter examines the security principles of the ADS-B implementation plan. The vulnerabilities stem primarily from the opposing goals of open information sharing and security.

## 4.1 ADS-B Vulnerabilities

In October 2009 the FAA released findings from the Security Certification and Accreditation Procedures (SCAP) [7]. The report included comments from various entities, including the Department of Defense, expressing concerns that malicious parties could monitor transmissions, broadcasts could be used to target and harm aircraft, and position/timing signals could be subject to interruption. Some recommended oversight that requires licensing of ground receivers.

According to the report, the FAA conducted several analyses on the security aspects of ADS-B. The system was subject to certification and accreditation under National Institute of Standards and Technology (NIST) guidelines conforming to confidentiality, integrity and availability security principles. Findings from the analyses are summarized as:

> "...the FAA specifically assessed the vulnerability risk of ADS-B broadcast messages being used to target air carrier aircraft. This assessment contains Sensitive Security Information that is controlled under 49 CFR parts 1 and 1520, and its content is otherwise protected from public disclosure. While the agency cannot comment on the data in this study, it can confirm, for the purpose of responding to the comments in this rulemaking proceeding, that using ADS-B data does not subject an aircraft to any increased risk compared to the risk that is experienced today [7]."

The FAA concluded that the ADS-B transmissions are no more susceptible to intentional introduction of false targets than the current SSR transmissions. Additionally, the FAA claims they do not expect spoofing or jamming to occur because ADS-B surveillance data will be fused with PSR returns before it is displayed for ATC. Finally, encryption would unnecessarily limit its use internationally.

From a security standpoint, there are some major concerns relating to this report. First is the comparison of security principles for current operating technologies with ADS-B. Current SSR transmissions (e.g., Mode A, C, and S) are cooperative and respond when interrogated by ground stations; ADS-B provides continuous broadcast of data. The systems, no doubt, share some common security characteristics; however, it should not be assumed that they share the same susceptibility to exploitation and should be researched further. One does not claim that a house protected by dogs and a house protected by an alarm system have the same susceptibility to burglary; indeed, both instances have unique vulnerabilities that may be exploited differently.

The second concern is the accuracy and validity of the data being transmitted. The report claims the fusion of data along with automation will reveal any discrepancies between a spoofed or jammed ADS-B target and the target reported by the radar. Given the commonality of position errors in radar returns from natural and manmade structures, how will the system determine the correct target? Will ADS-B data be considered more precise than radar data for determining position errors in ADS-B message traffic? Has operational testing been considered to validate that the system displays the correct target when confronted with malicious traffic injections? It is important to note that the actual operating characteristics of ADS-B are not yet defined. Indeed, the FAA Final Ruling discusses data fusion for security while in the same document alluding to the discontinuation of primary radar systems once ADS-B is fully

operational [7]. Additionally, the NextGen implementation plan claims that ADS-B will become the primary source of surveillance [9].

Finally, historical precedence has demonstrated how unencrypted data links can be exploited by a motivated adversary. In 2009, the U.S. military captured a Shiite militant whose laptop contained video files from Predator unmanned aircraft system (UAS) video feeds [18]. The communications link between the Predator and the local ground forces is not encrypted. It was determined that the militants had used a $26 off-the-shelf program called SkyGrabber to intercept the unencrypted Predator video [18]. The same vulnerability is attributed to the ambush and killing of Israeli commandos by Hezbollah forces during a 1997 military raid in Lebanon [19]. Hezbollah forces used intercepted Israeli UAS video footage from surveillance operations to target and plan their attack. The interception of unencrypted UAS communications is thought to have been due to a miscalculation by Israeli intelligence of the technological capabilities of Hezbollah.

### 4.2 Exploiting ADS-B

As early as 2006, concerns were raised about the ability of hackers to introduce as many as 50 false targets onto controllers' radar screens [20]. Dick Smith, former chairman of Australia's Civil Aviation Administration, reported this was possible with the use of a general aviation transponder, a laptop computer and a $5 antenna. Smith also warned that real-time positioning broadcasts allow adversaries to track military flights and criminal elements to monitor the movements of law enforcement.

Additionally, in 2010, an iPhone and Android application called Plane Finder AR was released that allows near real-time tracking of aircraft via reception of ADS-B transmissions [21]. An individual points their phone at the sky to obtain the identity, position, height,

departure point, destination and likely course of nearby aircraft. The phone uses its location to query an online database of aircraft and the camera is used to filter the data, based on field of view, for display on the phone's screen. The developers claim that over 2,000 people downloaded the application within the first month of its launch.

The two primary system access points for ADS-B are the network backbone and the data link. The network backbone comprises the interconnection of the various ground elements (see Figure 2). The infrastructure will rely on AT&T's multiprotocol labeled switching (MPLS) network for routing of data (e.g., from ground station to the ATC) [22]. Although the security of the network backbone is a critical component for ADS-B implementation, the focus for this research is on the data link infrastructure. Readers interested in security concerns of MPLS should refer to [23, 24, 25]

In security assessments, systems are typically analyzed for confidentiality, integrity and availability. Although the SCAP claims these principles were examined, the lack of actual data makes it difficult to refute what appear to be obvious vulnerabilities. With open broadcast and no encryption there is no confidentiality; a lack of any authentication provides no integrity; and the ability to jam signals brings into question availability. The ADS-B infrastructure requires that all surveillance be open and therefore, non-secure communications. As ADS-B is implemented, the potential exists for an attacker to exploit the inherent vulnerabilities of such an open system.

# V. Classifying Attacks on ADS-B

This chapter discusses potential attacks on the ADS-B implementation. The proposed taxonomy provides a systematic way to classify attacks and a means to logically reason how ADS-B vulnerabilities impact the overall NAS. The goal is to highlight the important characteristics of attacks and to stimulate discussions that lead to a better awareness of the potential security/safety implications.

## 5.1 Taxonomy

In order to devise a taxonomy, *attack techniques* associated with exploiting the ADS-B vulnerability, the specific component(s) that comprise the *target of the attack* and the *difficulty* associated with preparing/performing the attack have been identified. The discussion here is limited to the 1090MHz ES data link; although, the taxonomy readily extends to UAT (978MHz) and ADS-R.

The proposed taxonomy focuses on creating adverse effects in the NAS via messaging attacks on the ADS-B system. Attack techniques are specified by the primitive operations that can be used to construct complex messaging attacks. These consist of interception of ADS-B transmissions, jamming transmissions to prevent a recipient from receiving ADS-B messages, and injecting ADS-B messages into the data link. Indeed, the ability to intercept, jam and/or inject messages enables an attacker to launch a variety of messaging attacks.

The ADS-B system consists of two primary components an attacker may choose to target: aircraft or ground stations. Although the implications of an attack may have far-reaching consequences, the specific messaging attack is targeted to create an effect on one of the two end systems. To help distinguish attack classifications the target is specified based on the intent of the attack; unintended effects on a secondary target are considered collateral.

Difficulty is associated with the level of expertise required to carry out the attack. Attack difficulty is specified via a range of low, medium and high levels. *Low* constitutes attacks that can be accomplished via readily available hardware and/or software with minimal or no adaptation and minimal knowledge of NAS details (e.g., purchase of equipment through avionics/electronics stores and downloading software from the Internet). *Medium* attacks require modification of capabilities in order to achieve desired effects and assume increased knowledge of NAS operations. *High* attacks are complex in nature and require development/implementation of capabilities. These attacks require an extensive comprehension of NAS infrastructure and operations.

### 5.2 Examples

This section discusses attacks that exploit vulnerabilities in the ADS-B operations. For demonstration purposes, we discuss six attack examples. Each example includes a short synopsis of the attack followed by characterizations associated with the taxonomy. Note that different attack techniques can be combined to produce more complex attacks. Understandably, combining attacks creates a more complex attack that will likely result in a higher degree of difficulty.

- **Aircraft Reconnaissance**: An Aircraft Reconnaissance attack intercepts and decodes ADS-B transmissions. When used for information gathering, Aircraft Reconnaissance may be used to target specific aircraft or gain knowledge about movement of assets. Aircraft Reconnaissance may be used to track corporate executive movements or allow potentially allow other countries to track aircraft and build an air order of battle (AOB) for the U.S. Military. It is likely, however, that Aircraft Reconnaissance is the first step of a more insidious attack. The difficulty of a Reconnaissance attack is Low due to the

existence of technology which can use ADS-B signals to track aircraft in near real-time, such as Plane Finder AR or real-time via applications for General Aviation such as SkyRadar.

  - **Target**: Aircraft
  - **Attack Technique**: Interception of ADS-B OUT signals
  - **Difficulty**: Low

- **Ground Station Flood Denial**: The Ground Station Flood Denial is an attack that disrupts the 1090MHz frequency at the ground station. Typically, gaining close proximity to a ground station is relatively simple. As a result, a low power jamming device will suffice for overpowering (i.e., blocking) legitimate ADS-B signals that originate from aircraft miles away. Note that this attack is not targeted and blocks all ADS-B signals intended for the ground station. The impact is localized to a small area determined by the range and proximity of the jamming signal to the ground station. A Ground Station Flood Denial is categorized as a Low difficulty attack because of the readily available equipment that can jam GPS signals.
  - **Target**: Aircraft and FAA Controllers
  - **Attack Technique**: Jamming signal capable of disrupting the 1090MHz frequency range or GPS frequency
  - **Difficulty**: Low

- **Ground Station Target Ghost Inject**: A Ground Station Target Ghost Inject is an attack that injects an ADS-B signal into a ground station. This attack requires an adversary to craft and encode a 112 bit message that conforms to the ADS-B messaging protocol. As a result, the adversary can cause illegitimate (i.e., ghost) aircraft to appear on the ground

controller's console. A Targeted Ghost Inject attack is categorized as a Medium-High difficulty because it requires the ability to craft and transmit an ADS-B message that mirrors legitimate traffic. The impact of this type of attack can range from annoyance to high safety implications.

  - **Target**: Ground Station
  - **Attack Technique**: Inject message that conforms to ADS-B message protocol and mirrors legitimate traffic
  - **Difficulty**: Medium-High

- **Aircraft Flood Denial**: The Aircraft Flood Denial is similar to the Ground Station Flood Denial, with the exception that the target for the attack is an aircraft. The primary difference is the ability to gain close proximity to the target. The adversary can obtain a high power jamming device; however, these are not readily available and once the aircraft moves out of range the attack will no longer be effective. An alternative is for the adversary to carry out the attack from on-board the aircraft; however, this option is also somewhat constrained due to the bulk and irregularity of the equipment. The most significant impact involving this attack likely stems from gaining close proximity to an airport and affecting landing or taxi operations. A final consideration is that an aircraft must be equipped with ADS-B IN for the attack to be successful. The Aircraft Flood Denial is categorized as a Medium difficulty.
  - **Target**: Aircraft
  - **Attack Technique**: Jamming signal capable of disrupting 1090MHz
  - **Difficulty**: Medium

- **Aircraft Target Ghost Inject**: The Aircraft Target Ghost Inject is similar to the Ground Station Target Ghost Inject, with the exception that the target for the attack is an aircraft. Because there is no data correlation like that which may occur in a ground station, it may be somewhat easier to inject a ghost target into an aircraft; although, physical access may offset that advantage. The Aircraft Target Ghost Inject is categorized as a Medium-High difficulty based on the associated attack attributes. The impacts of the attack are consistent with the Aircraft Flood Denial attack.
  - **Target**: Ground Station
  - **Attack Technique**: Inject message that conforms to ADS-B message protocol and mirrors legitimate traffic
  - **Difficulty**: Medium-High

- **Ground Station Multiple Ghost Inject**: A Ground Station Multiple Ghost Inject is an attack that injects ADS-B signals into a ground station. The attack is similar to the Ground Station Target Ghost Inject, with the exception that multiple targets are injected into the system. An adversary can use this type of attack to overwhelm the surveillance system and create mass confusion for the ground controller. The Ground Station Multiple Ghost Inject attack is categorized as a Medium-High difficulty because it requires the ability to automate the transmission of crafted messages, multiple transmitters and coordination of message transmissions.
  - **Target**: Ground Station
  - **Attack Technique**: Inject multiple messages that conform to ADS-B message protocol and mirrors legitimate traffic
  - **Difficulty**: Medium-High

### 5.3 Dynamic Attack Analysis

The proposed taxonomy provides a clear method for classifying attacks and helps formulate a generalized threat picture. Table 2 lists the tendencies discerned through initial classification of attacks. Attacks that are characterized with a rank order of difficulty 1 are the most difficult, with 5 being the least difficult. Not surprisingly, preliminary findings demonstrate that targeting a ground station for message injection generally proves most difficult. This is primarily due to expected data correlation at a ground station that would not be performed by an aircraft. Message jamming for an aircraft is generally more difficult than a ground station based on access ability. The attacks associated with intercepting aircraft messages comprise the lowest difficulty. Note that the table provides a general characterization based on preliminary static analysis.

Although attack generalizations are informative, strict static analysis of attacks is sufficient only in the general case. To examine the impact of attacks, the dynamic nature of the overall NAS must be considered. Commercial aviation is a very complex medium with multiple aircraft in takeoff, arrival, landing and taxi phases at any given time. Aircraft routinely transit airport terminal airspace at airspeeds in excessive of 250 miles per hour–dealing with multiple controllers, arrival and departure corridors, weather and varying levels of traffic.

For dynamic analysis, the taxonomy must be examined using a scenario-based approach. For example, a Ground Station Target Ghost Inject attack on a clear weather day in the Midwest may have minimal impact on airport operations. However, the same attack perpetrated against an East Coast airport during a busy travel day (e.g., Thanksgiving holiday), coupled with marginal weather conditions could have a dramatically different impact. This notion is

**Table 2: General characterization of attack difficulty**

| Rank Order of Difficulty | Attack Technique | Target |
|---|---|---|
| 1 | Message injection | Ground station |
| 2 | Message injection | Aircraft |
| 3 | Message jamming | Aircraft |
| 4 | Message jamming | Ground station |
| 5 | Message interception | Aircraft |

somewhat different from traditional attack analysis. Attack analysis involving general information management systems are typically static in nature. Although threats may be dynamic and attacks may manifest through a multitude of avenues, the general environment does not fluctuate in the same manner as air travel. Similarly, attacks associated with NextGen may have far reaching consequences. Attacks that covertly target a specific aircraft type may result in the grounding of an entire fleet; attacks that create delays at a local airport can quickly impact air travel on a national scale.

To clarify the impact of attacks and facilitate formal risk analysis, it is useful to categorize the attack instances based on their effects with respect to three high-level system objectives: confidentiality of data, situational awareness and the ability to control assets. Loss of confidentiality occurs when an attack reveals information about NAS operations (e.g., aircraft altitude, vector or identification number). Based on current implementation plans, it should be assumed that loss of confidentiality is universal. Loss of situational awareness occurs when the pilot or ground controller is unable to obtain accurate and timely information. For an adversary, it may be sufficient to simply diminish trust in the system. Indeed, a carefully crafted attack could create multiple indications such that a pilot or ground controller is unsure of which data to trust. Perhaps the most dangerous attacks result in the loss of control. In this situation, actions of ground controllers or pilots are dictated by the adversary. Consider an attack that causes a

pilot to perform course corrections due to a ghost inject or, alternatively, jams the signal of an approaching aircraft resulting in a taxiing aircraft assuming it is clear to cross an active runway.

## 5.4. Vignettes – DoD and DHS

This section discusses three hypothetical scenarios in which the ADS-B messaging attack examples are applied to military and homeland defense events. The vignettes are designed to educate the reader and increase awareness on how state-sponsored and non-state actors potentially could exploit ADS-B and impact military and DHS assets.

### 5.4.1 Reconnaissance of the F-35 JSF

Every year aviation enthusiasts flock to air shows to watch the newest civilian and military aircraft demonstrations. A small subset of these enthusiasts, called Plane Watchers, sit outside local airports or use new computer technology from abroad to track aircraft movement. The following vignette highlights how computers, ADS-B and Plane Watchers can easily piece together data that could pose an OPSEC issue for the military.

It is a sunny day at Eglin AFB in Florida, home of the 33rd Fighter Wing and the F-35 Integrated Training Center, tasked with training future pilots from across the services to fly the 5th generation fighter. The recent delivery of the first Joint Strike Fighters (JSF) to the 33rd FW has garnered interest from opposing countries. Indeed, several of their embedded Human Intelligence (HUMINT) assets have been relocated to the Eglin area to collect performance data on the JSF.

On this day, two of the HUMINT assets are sitting in the parking lot of Northwest Florida Regional Airport monitoring ATC frequencies in the hopes of picking up an F-35's transponder code to correlate the ADS-B OUT signal. Today their patience has paid off as they hear SABLE01 flight, a flight of two F-35s, instructed to squawk a transponder code of 0154 and

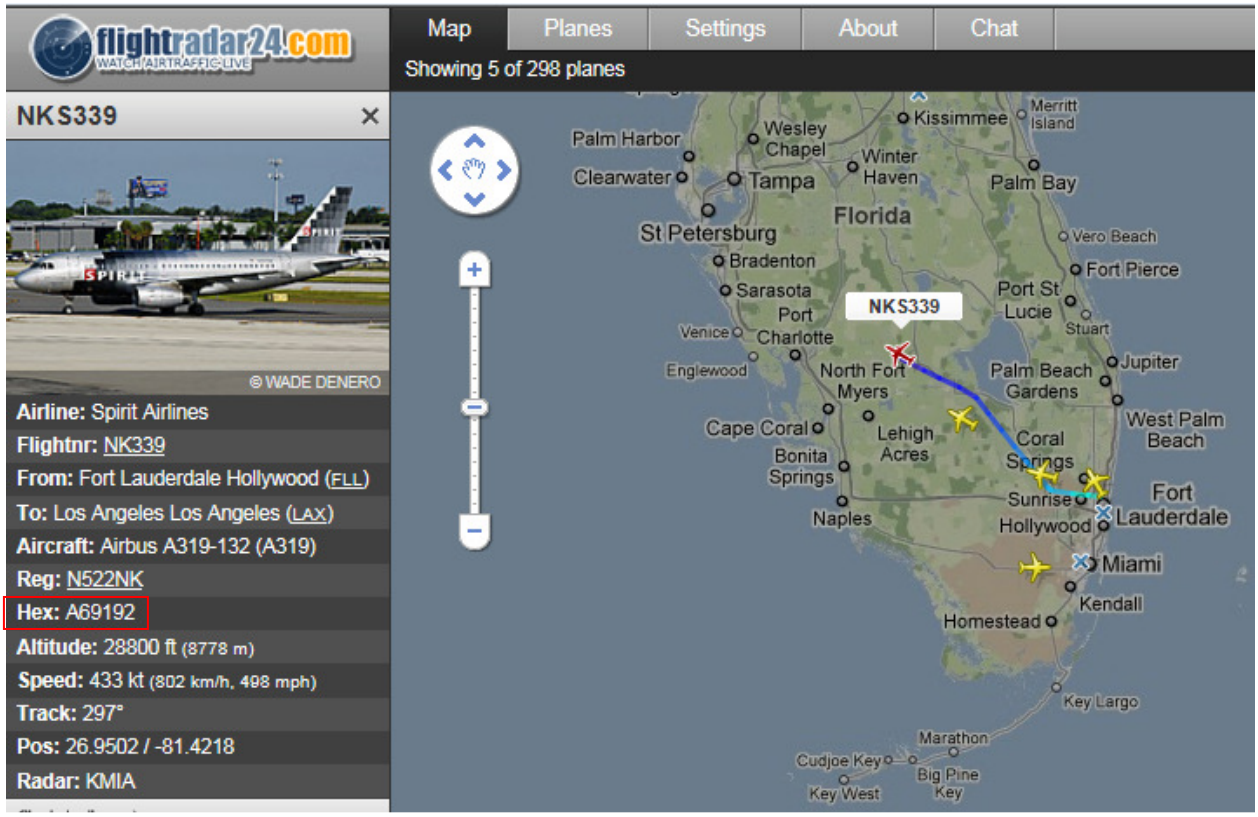


**Figure 5: Screen capture from FlightRadar24.com [26].**

cleared to taxi to RWY12. As SABLE01 flight approaches the hold short for RWY12 and receives clearance for takeoff, the two "Plane Watcher's" IPhone application starts to receive ADS-R broadcasts from SABLE01 flight. Today they are using the SkyRadar Remote ADS-B Antenna and associated SkyRadar application, much like the screenshot shown in Figure 5, to receive 1090MHz ADS-B OUT transmissions converted and rebroadcast in ADS-R as 978MHZ (UAT) transmissions. This application, combined with an easily developed software program, allows them to view the unique 24 bit ICAO address that the FAA requires to fly in the U.S. In the FlightRader24.com example, this 24 bit address is shown in its Hexadecimal equivalent (i.e., A69192). Provided SABLE01 flight does not turn off their ADS-B OUT transmitter, all flight data can be accessed and recorded for later review. Indeed, this data

provides valuable insight into F-35 Tactics, Techniques and Procedures (TTPs) as well as potential performance characteristics not yet known by opposing countries.

As the two Plane Watcher's drive away from the airport, they transmit the 24 bit ICAO address via encrypted email back to their superiors. The country's Cyber Warfare detachment in charge of attacking and exploiting the FAA's NextGen ATM can pinpoint this target to filter from the mass amount of data extracted daily from the recently exploited NextGen computer systems. Using Computer Network Attack (CNA) exploits the Cyber Warfare detachment gains access to the FAA's East Coast Control Center's ADS-B data streams. Coupled with the 24 bit ICAO addresses from SABLE01 flight, they have access to a "god's eye" view of the entire flight of SABLE01. Using simulation software, they will be able to recreate and playback the two F-35s dogfights over the Gulf of Mexico, much like the Air Force Weapon School does after a Red Flag engagement, but in much higher fidelity.

### 5.4.2 Air Order of Battle

Since early warfare, opposing forces have tried to track and maintain an accurate count of one another's forces. As technology has advanced, this complex task has become easier. Indeed, ADS-B and computer technology have made it possible for someone across the globe to monitor ATC VHF/UHF frequencies, radar feeds and ADS-B tracking from the comfort of their home.

For example, consider the recent U.S. and NATO attacks on Libya. A Dutch radio operator, known as Huub, employed aircraft transponder data, IRC chatrooms, data mining, general knowledge of ATC procedures, communication, encryption, call signs and unencrypted VHF, UHF and HF frequencies to report on aircraft attacking or supporting the attacks on Libya [27]. Using off the shelf electronics, the Internet and some basic knowledge, Huub was able to

| | Serial | Callsign | GMT | Type | Country | Operator | Squawk | Altitude |
|---|---|---|---|---|---|---|---|---|
| | 59-1500 | --- | 2011-04-10 20:45:37 | KC-135R | United States | IL ANG \| 126ARW \| 108ARS [KBLV] | 1633 | 35000 |
| | TK17-1 | --- | 2011-04-10 20:38:59 | B-707 | Spain | 471ESC | 1561 | 19000 |
| | 63-7993 | MOBIL32 | 2011-04-10 20:27:53 | KC-135R | United States | OH ANG \| 121ARW [KLCK] | 4420 | 40000 |
| | 58-0072 | MOBIL35 | 2011-04-10 20:19:26 | KC-135T | United States | PA ANG \| 171ARW [KPIT] | 6764 | 30000 |
| | ZZ175 | RRR6753 | 2011-04-10 20:16:31 | C-17A | United Kingdom | RAF \| 99SQ | 6767 | 34000 |
| | 62-3519 | EXXON22 | 2011-04-10 20:10:20 | KC-135R | United States | USAFE \| 100ARW \| 351ARS [EGUN] | 0342 | 40000 |
| | ZH865 | RRR5761 | 2011-04-10 20:06:31 | C-130C4 | United Kingdom | RAF \| LTW | 1227 | 28000 |
| | TC-GAP | TCGAP | 2011-04-10 20:03:41 | Gulfstream Aerospace G-IV | Turkey | Turkey-AirForce | 5547 | 9275 |
| | 2590 | BRS2591 | 2011-04-10 19:42:05 | VC-2B | Brazil | BRAZILIANAIRFORCE | 2076 | 35000 |
| | 63-7993 | MOBIL32 | 2011-04-10 19:40:31 | KC-135R | United States | OH ANG \| 121ARW [KLCK] | 4420 | 40000 |
| | ZZ175 | RRR6753 | 2011-04-10 19:39:50 | C-17A | United Kingdom | RAF \| 99SQ | 6767 | 34000 |
| | ZH865 | RRR5761 | 2011-04-10 19:38:28 | C-130C4 | United Kingdom | RAF \| LTW | 1227 | 28000 |

**Figure 6: Mode-S Tracking of Aircraft flying in Support of Operation Odyssey Dawn [28].**

track, record and report on transmissions from an Air Force EC-130J "Commando Solo" operating off the coast of Libya [27]. Figure 6, from *www.live-mode-s.info*, shows Mode-S logs that provide specific details on aircraft serial number, call signs (for use in monitoring radio chatter), aircraft type and country of origin. This example demonstrates the efforts of only one individual; consider what a motivated, funded adversary could achieve. ADS-B implementation will only make it cheaper, easier and faster to accomplish what once took many assets to achieve.

### 5.4.3 The Fog of a "Cyber" War

It has been well documented in the news that Islamic terrorists now plan a slow bleed of the "Great Satan" by systematically targeting the U.S. economy [3]. They took note on 9/11 of the impacts of stopping commercial air traffic, if only for a few days. Their new attack plan is not likely to kill as many as the attacks on 9/11, but rather, its target is the hearts and minds of the traveling public.

It is late fall 2025; Al Qaeda sleeper cells target the disruption of airline traffic into multiple East coast airports during the busy travel season from Thanksgiving through Christmas. ADS-B IN/OUT has been fully implemented by the FAA; all commercial airlines have invested heavily to comply with the mandate. Oil prices are at an all time high and flights are carrying minimal fuel loads to save money and offset the cost of avionics. The goal: force multiple airplanes to divert; pilots, FAA controllers and passengers to lose faith in the system; and possibly cause enough chaos to the NAS system that a few lives are lost. The plan: exploit the U.S. dependency on ADS-B IN/OUT and GPS for arrivals into busy airports, especially during low visibility conditions.

The teams: five two man teams have been put into play for the mission. They are provided with all the commercially available technology they will need, along with a few modified laptop computers, antennas and transmitters.

The targets: Regan National, Dulles, La Guardia, JFK and Philadelphia International airports. The terrorists have been tasked to park minivans with computers containing modified software that are coupled to ADS-B OUT transmitters. The software is designed to be remotely activated and controlled over an Internet connection. Each computer is programmed specifically for the targeted airport, and transmits 978MHz and 1090MHz signals out a boosted transmitter. As a result, airlines on final approach will receive false targets on their displays. The terrorists ghost target injects also propagate to the FAA controller's screens. The terrorists intended these spoofed targets, programmed at conflicting arrival and departure corridors as well as in runway incursion situations, to cause multiple airports to become temporarily unusable. The resulting domino effect causes aircraft diversions and delays that will lead to chaos.

### 5.4.4 Vignette Summary

These vignettes highlight how the taxonomy of ADS-B messaging attacks, specifically Aircraft Reconnaissance and Target Ghost Inject, could be used against the military and ATC systems. They were designed for the reader to consider the security implications of open architecture systems, such as ADS-B, and the security implications it could have on military and commercial aviation.

# VI. Recommendations and Future Research

Securing a large-scale system that is designed for openness and information sharing is not a trivial task–one needs to look no further than the Internet to get a sampling of the associated difficulties. As highlighted by security expert Bruce Schneier, security is a trade-off between functionality and security [29]. To increase security for ADS-B, some level of functionality must be diminished. The immediate question that follows is, does the decreased functionality have a negative impact on safety? For ADS-B and the NAS, a contradiction arises in that increased security appears to negatively impact safety; however, decreased security appears to negatively impact safety as well. Determining the correct trade-offs and to what degree will by key to ensuring secure and safe operations.

## 6.1 Recommendations

In this section some generalized recommendations for addressing the complex security issues relating to NextGen and ADS-B are provided. The first recommendation is to release the FAA SCAP data. Time and again, it has been demonstrated that security through obscurity does not work. If the system is indeed secure, then releasing the data or, at a minimum, the specific tests and results should carry minimal risk. This data alone will aid security researchers in the formulation of mitigation strategies and techniques.

The second recommendation is a complete and holistic security analysis of the NextGen implementation plan. In the current 84-page implementation plan document, safety is referenced over 100 times; efficiency is referenced over 50 times [9]. There are less than four references, however, that encompass security principles. The most notable reference relates to the security integrated tool set (SITS). SITS is intended to support automated threat detection and tracking, data correlation, and NAS impact analysis of security or emergency actions [30]. Indeed, SITS

is intended to encompass air threats; system-level analysis is not considered. It is critical that security is integrated throughout the system development and implementation life cycle–a bolt-on security mentality could prove devastating.

The third recommendation calls for operational security assessments of NextGen components to include ADS-B infrastructure, aircraft avionics upgrades, ground station security and effects of RF interference on the reliability of the system. The assessments should leverage Red Teams and penetration testing to identify vulnerabilities in system design and implementation. It is important that guidelines for security assessments, as well as the aforementioned security analysis, are explicitly detailed in an updated NextGen implementation plan.

The fourth recommendation is user education. The aviation community must be properly educated on the capabilities as well as vulnerabilities that exist in the system. Without appropriate knowledge of the risks, operators may blindly follow flawed technology into a situation that ends in a loss of property or life.

A fifth recommendation relates specifically to military operations. Military aircraft will be required to upgrade transponders to comply with FAA mandates for ADS-B. As the military completes these upgrades, in depth security testing specific to military operations need to be considered. The ADS-B security concerns for commercial aviation and military aviation may not always run in parallel. The results of security tests pertaining to military operations should be used to develop procedure guidance related to the use of ADS-B by military aircraft and personnel during CONUS, OCONUS, peacetime and wartime flights.

Finally, it is important to explore technological solutions. For example, ADS-B is susceptible to messaging attacks primarily due to a lack of message encryption. If, however, a

viable encryption solution could be introduced, many of the messaging attacks could be mitigated. The ability to inject messages could be eliminated through authentication schemes and interception could be minimized by using channel encryption. Note that encryption alone would not preclude attacks that jam transmissions. Developing adequate technical solutions in this complex environment is not an easy task and will likely require non-traditional security measures. For example, the implementation of an encryption scheme is non-trivial. The key distribution and management would be overwhelming in the global aviation industry. Although this security mechanism may be inadequate, it is nevertheless critical that open dialogue and research occur so that the appropriate balance between security and safety can be determined.

## 6.2 Future Research

A goal of this research is to enlighten the reader to perceived security issues in the NextGen upgrade and ADS-B architecture. While researching these topics, several other research areas were identified. This section highlights those areas in the hopes that further research can help address these potential problems before the reprecussions impact DoD and commercial aviation.

### 6.2.1 LightSquared Broadband Internet

LightSquared is a proposed 4G-LTE open wireless broadband network that is designed to use a combination of satellite and terrestrial technology. By 2015, LightSquared plans to cover 92% of the U.S. population by installing 40,000 high-power transmitters across the country [31]. However, this coverage comes at a potential cost. Interference to GPS receivers operating in the L-band (1.5 – 1.6GHz frequency range) will indirectly impact ADS-B [31].

Over the past 20 years the military and commercial aviation has become heavily dependent on GPS for navigation, ISR, timing signals and for putting bombs on target. Now it is

the cornerstone of the FAA's NextGen upgrade. Any interference in the GPS L-band, even sporadic, could wreak havoc on commercial air traffic and military operations [31].

Given that LightSquared is targeted to increase Internet availability and speeds in rural communities; the military is likely to experience more issues than commercial aviation. Indeed with many of the Air Force's bases and training ranges located in rural areas, LightSquared interference will more likely have a greater impact around these areas than in populated areas or bases on the East Coast. Further military implications as well as impact to ADS-B reliability should be explored prior to Initial Operational Capability (IOC) of LightSquared Broadband.

### 6.2.2 Using ADS-B Signals to recreate Red Flag in a Simulated Environment

One of the major goals of Red Flag is to gather and disseminate lessons learned. This is accomplished via data collection with sufficient detail to evaluate Tactics, Techniques and Procedures (TTPs) for all Red Flag events. Mission aircraft and ground players carry multiple sensors, pods and receivers to facilitate transmission and collection of the required data.

ADS-B, more specifically Mode5 Level2-B encrypted ADS-B data transmissions, could be employed to reduce the number of required sensors and increase fidelity of the recreation of air-to-air and air-to-ground events for post exercise debriefs during Red Flag. All players would transmit their position via encrypted RF signals to be used real time and during recreation. Given all military aircraft will be required to have ADS-B OUT capability, research into the viability of employment in military exercises as a replacement for current sensors should be explored.

### 6.2.3 Controlling uncontested airspace using Mode5L2-B

ADS-B technology alone is not secure enough for controlling military aircraft over hostile ground. However, feeding ADS-B data streams into an encrypted channel such as Mode5

Level2-B could allow more precise control of military aircraft in environments lacking radar coverage.

Predator aircraft could be used in stationary orbits as ADS-B transceivers relaying to ground based controllers either behind the forward lines or over-the-horizon via satellite uplinks. These airborne relays would operate as pseudo radar and could provide both encrypted and unencrypted data streams, ultimately reducing the need for E-3 AWACS aircraft to control uncontested airspace.

Research in these areas could consist of the optimum number of UAVs required for coverage and relay to ground control stations; bandwidth requirements, RF spectrum issues related to Mode5 Level2-B and ADS-B transmissions; and security implications of controlling aircraft only using ADS-B.

### 6.2.4 Impact of duplicate 24 bit ICAO addresses

To increase security, DoD and government aircraft transponders are not required to have fixed 24 bit ICAO addresses. This exception to policy has introduced human error into the ADS-B technology. It has been noted in European airspace, where ADS-B is already being used that U.S. military aircraft are routinely flying with duplicate 24 bit ICAO codes.

As the FAA brings ADS-B and NextGen upgrades online in the U.S. it is likely that we will see these same conflicts occur here. Research in this area should explore how FAA controllers and the NextGen system will handle duplicate codes and if this exception could be used by an attacker to further exploit the system.

### 6.2.5 Using ADS-B Technology to Reduce AETC Training Costs

U.S. Air Force pilot training bases represent some of the busiest airspace in the NAS. During periods of inclement weather, arrival, departure and ground traffic becomes congested.

This ultimately means more fuel is burned waiting to takeoff and recover due to ATC spacing requirements.

ADS-B technology has been envisioned as the savior to arrival and departure congestion at commercial airports. If employed correctly it could save the U.S. Air Force millions of dollars a year in fuel savings. As airspace becomes more congested and military airspace begins to encroach on commercial air routes, ADS-B could also be used to reduce the required separation between military and commercial aircraft.

As the Air Force goes forward with transponder upgrades for its fleet of T-38C, T-1A and T-6A trainer aircraft, research should be performed to explore upgrading base infrastructure to exploit the capabilities ADS-B affords. ADS-B technology could ultimately provide fuels savings and increase efficient use of military airspace.

## VII. Conclusions

One of the biggest security challenges faced today relates to control systems associated with the critical infrastructure (e.g., oil and gas, electrical and water sectors). These systems are inherently insecure because they were designed and implemented decades ago with little emphasis on security implications. These once isolated systems are now interconnected via the Internet and security professionals are struggling with how best to secure them. With the NextGen and ADS-B implementation plan, it appears we may be on a collision course with history.

This paper highlighted security risks associated with ADS-B and proposed a taxonomy for classifying attacks. The taxonomy introduces clarity into the myriad attacks that extend from the inherent vulnerabilities of the ADS-B implementation plan and supports formal risk analysis and risk management. Three vignettes demonstrating the dynamic nature of ADS-B messaging attacks were provided to give the reader a perspective on how ADS-B might be exploited if the security of NextGen is not addressed. Additionally, the paper provided recommendations for addressing the complex security issues and listed future considerations for research.

The majority of the paper's discussion on ADS-B and security issues related to commercial aviation, as this is where ADS-B has primarily been developed and will be implemented ahead of military applications. However, military aviation must follow in the footsteps of commercial aviation and implement ADS-B upgrades or be forced to operate under restrictions which could impact CONUS and OCONUS operations. Thus, just as commercial aviation must incorporate security testing into the planning phases of development, the DoD must implement the required avionics upgrades in a cost effective manner that will leverage ADS-B benefits, while managing the security impacts on operations.

The intention of this research is to provide awareness about the vulnerabilities that exist with the current ADS-B implementation plan. The intent is not to advocate a complete dismissal of the upgrade efforts. Indeed, with the increase in air travel and dependence on outdated technologies, an upgrade to the current NAS framework is necessary and warranted. The papers ultimate position, however, is that security must be infused throughout the planning, implementation and operation life-cycle. Security as an afterthought will not suffice.

## Appendix A: Acronyms

AETC: Air Education and Training Command

ATC: Air Traffic Control

ADS-B: Automatic Dependent Surveillance – Broadcast

ADS-R: Automatic Dependent Surveillance – Rebroadcast

ATM: Air Traffic Management

AWACS: Airborne Warning and Control System

CFR: Code of Federal Regulations

CNA: Computer Network Attack

CONUS: Contiguous United States

DoD: Department of Defense

DHS: Department of Homeland Security

ES: Extended Squitter

FAA: Federal Aviation Administration

FW: Fighter Wing

GNSS: Global Navigation Satellite System

GPS: Global Position System

HF: High Frequency radio

HUMINT: Human Intelligence

ICAO: International Civil Aviation Organization

IFF: Identify Friend or Foe

IOC: Initial Operational Capability

MHz: Megahertz

Mode5L2-B: Mode5 Level2-Broadcast

MPLS: Multiprotocol Label Switching

NAS: National Airspace System

NIST: National Institute of Standards and Technology

NM: Nautical Miles

OCONUS: Outside Contiguous United States

OPSEC: Operational Security

PPM: Pulse Position Modulation

PSR: Primary Surveillance Radar

RF: Radio Frequency

SCAP: Security Certification and Accreditation Procedures

SITS: Security Integrated Tool Set

SM: Statutory Miles

SSR: Secondary Surveillance Radar

TTP: Tactic, Technique or Procedure

UAS: Unmanned Aircraft System

UAT: Universal Access Transceiver

UAV: Unmanned Aerial Vehicle

VHF: Very High Frequency

## References


[1] J. Randolph Babbit, "NextGen is Happening," *Aviation Week and Space Technology NextGen Forum*, May 20, 2010.

[2] M. Moore, S. Likic, A. Charlton, F. Jordons and C. Piovano, "Iceland volcano costs airlines at least $1.7 billion due to travel disruptions," *The Huffington Post*, June 21, 2010.

[3] M. Krebs, "Al Qaeda magazine: Printer bombs designed to bleed U.S. economy," *Digital Journal*, (www.digitaljournal.com/article/3005/30), November 23, 2010.

[4] R. Esposito and B. Ross, "Exclusive: Photos of the Northwest Airlines FLight 253 Bomb," December 28, 2009. [Online]. abcnews.go.com

[5] P. Dempsey and L. Gesell, *Air Transportation: Foundations for the 21st Century*. Arizona: Coast Aire Publications, Arizona, 1997.

[6] Joint Planning and Development Office, "Concept of Operations for the Next Generation Air Transport System, Version 2.0," Washington DC, June 13, 2007.

[7] Federal Aviation Administration, "Automatic Dependent Surveillance-Broadcast (ADS-B) Out Performance Requirements to Support Air Traffic Control (ATC) Service; Final Rule, 14 CFR Part 91," *Federal Register*, vol. 75(103), May 28, 2010.

[8] Federal Aviation Administration, "Instrument Procedures Handbook, FAA-H-8261-1A," 2007. [Online]. http://www.faa.gov/library/manuals/aviation/

[9] Federal Aviation Administration, "FAA's NextGen Implementation Plan," Washington, DC, March 2011.

[10] U.S. Congress, "Vision 100-Century of aviation reauthorization act, Public Law 108-176, Sec. 709," December 12, 2003.

[11] ITT, ADS-B Explained, Herndon, Virginia, (http://www.itt.com/adsb/adbs-explained.html), 2009.

[12] L. Purton, H. Abbass and S. Alam, "Identification of ADS-B system vulnerabilities and threat," *Proceedings of the 2010 Australasian Transport Research Forum* , 2010.

[13] Federal Aviation Administration, "Automatic Dependent Surveillance Broadcast (ADS-B) Out Performance Requirements To Support Air Traffic Control (ATC) Service; OMB approval of information collection, 14 CFR Part 91," *Federal Register*, vol. 75(154), August 11, 2011.

[14] Federal Aviation Administration, "Surveillance and Broadcast Services: ADS-B Status Briefing," March 15, 2011.

[15] C. Kast (Capt), "NextGen & ADS-B at UPS," UPS Advanced Flight Systems, Louisville, Kentucky, March 15, 2011.

[16] K. Sampigethaya and R. Poovendran, "Visualization & assessment of ADS-B security for green ATM," *Proceedings of the 29th IEEE Digital Avionics Systems Conference*, 2010.

[17] P. Rivas, Lt Col, Headquarters U.S. Air Force, USAF XOR-GANS, "Military Unique Applications for ADS-B," April 3, 2001.

[18] S. Gorman, Y. Dreazen and A. Cole, "Insurgents hack U.S. drones," *The Wall Street Journal*, December 17, 2009.

[19] Y. Katz, "IDF encrypting drones after Hezbollah accessed footage," *The Jerusalem Post*, October 27, 2010.

[20] A. Wood, "After ADS-B launch, security concerns raised," *Aviation International News*, July, 2006.

[21] NDTV, "A phone application that threatens security," *Press Trust of India*, October 4, 2010.

[22] M. Unnikrishnan, "ITT Calls on AT&T for ADS-B infrastructure," *Aviation Week*, September 4, 2007.

[23] D. Grayson, D. Guernese, J. Butts, M. Spainhower and S. Shenoi, "Analysis of security threats to MPLS virtual private networks," *Internatinal Journal of Critical Infrastructure Protection*, vol. 2(4), pp. 146-153, 2009.

[24] D. Guernesy, A. Engel, J. Butts and S. Shenoi, "Security analysis of the MPLS label distribution protocol," in *Critical Infrastructure Protection IV*, T. Moore and S. Shenoi (Eds.), Springer, Heidelberg, Germany, 2010, pp. 127-139.

[25] M. Spainhower, J. Butts, D. Guernsey and S. Shenoi, "Security analysis of RSVP-TE signaling in MPLS networks," *International Journal of Critical Infrastructure Protection*, vol. 1, pp. 74-88, 2008.

[26] FlightRadar24.com, (http://www.flightradar24.com), April 26, 2011.

[27] N. Shachtman, "Listen: Secret Libya Psyops, Caught by Online Sleuths", March 20, 2011. [Online]. http://www.wired.com/dangerroom/2011/03/secret-libya-psyops/

[28] Coalition of the Willing Mil Mode-s Logs, (http://www.live-mode-s.info/PublicArea/MilLogsCoalitionoftheWilling.php), April 22, 2011.

[29] B. Schneier, *Beyond Fear*. Springer-Verlag, New York, 2003.

[30] FedBizOps, Security integrated tool suite (SITS) industry day, Solicitation Number 8734, Federal Aviation Administration, Washington, DC, October 13, 2009.

[31] GPS World, Data Shows Disastrous GPS Jamming from FCC-Approved Broadcaster, (data-shows-disastrous-gps-jamming-fcc-approved-broadcaster-11029), February 1, 2011.

## Vita

Major Donald L. McCallie entered the Air Force through the Reserve Officer Training Corps program at Texas Christian University where he was awarded a B.S. in Computer Science.

Major McCallie is a senior pilot with over 3700 hours in multiple airframes. He has accumulated over 1300 combat hours in RC-135 U/V/W/S and MC-12W aircraft, as well as having experience in training future AF pilots with an assignment in the T-1A as a UPT instructor pilot. He was selected to attend AFIT in 2010 and is currently completing the Cyber Warfare Intermediate Developmental Education program. Upon graduation he will be assigned to the Air Force Personnel Center, Randolph AFB, TX as a Rated Assignments Officer.

| REPORT DOCUMENTATION PAGE | | | Form Approved OMB No. 074-0188 |
|---|---|---|---|



| 1. REPORT DATE *(DD-MM-YYYY)* | 2. REPORT TYPE | 3. DATES COVERED *(From – To)* |
|---|---|---|
| 16-06-2011 | Graduate Research Project | 14 May 2010 - 16 Jun 2011 |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| Exploring Potential ADS-B Vulnerabilites in the FAA's NextGen Air Transportation System | N/A |
| | **5b. GRANT NUMBER** N/A |
| | **5c. PROGRAM ELEMENT NUMBER** N/A |
| **6. AUTHOR(S)** | **5d. PROJECT NUMBER** N/A |
| Donald L. McCallie, Major, USAF | **5e. TASK NUMBER** N/A |
| | **5f. WORK UNIT NUMBER** N/A |

| 7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) | 8. PERFORMING ORGANIZATION REPORT NUMBER |
|---|---|
| Air Force Institute of Technology - Graduate School of Engineering and Management<br>2950 Hobson Way<br>Wright Patterson Air Force Base, OH 45433-7765 | AFIT/ICW/ENG/11-09 |
| **9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)** N/A | **10. SPONSOR/MONITOR'S ACRONYM(S)** N/A |
| | **11. SPONSOR/MONITOR'S REPORT NUMBER(S)** N/A |

**12. DISTRIBUTION/AVAILABILITY STATEMENT**
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

**13. SUPPLEMENTARY NOTES**
This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

**14. ABSTRACT**
The Federal Aviation Administration's (FAA) Next Generation upgrade proposes a fundamental transformation to the national airspace system (NAS) that aims to reduce dependence on outdated radar infrastructure, increase airline safety and condense required aircraft spatial separation. A key component of the upgrade is the Automatic Dependent Surveillance-Broadcast (ADS-B) system. ADS-B provides continual broadcast of aircraft position, identity, velocity and other information over unencrypted data links to generate a precise air picture for air traffic management. Official documents claim operational requirements necessitate unencrypted data links while maintaining that there is a low likelihood for malicious exploitation. This paper studies the security vulnerabilities associated with the ADS-B implementation plan and develops a taxonomy to classify attacks and examine potential impacts the attacks have on overall NAS operations. The taxonomy helps provide a comprehensive understanding of the threats associated with ADS-B implementation and facilitates risk analysis and risk management. For demonstration purposes, three vignettes are presented to highlight how ADS-B attacks could impact military operations and homeland defense. Finally a series of recommendations for consideration in the implementation plan going forward is provided.

**15. SUBJECT TERMS**
ADS-B, Mode5L2, NEXTGEN, FAA, Exploitation, Airspace, Vulnerabilities

| 16. SECURITY CLASSIFICATION OF: U | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| REPORT | ABSTRACT | c. THIS PAGE | | | Capt Jonathan Butts, PhD (ENG) |
| U | U | U | UU | 56 | **19b. TELEPHONE NUMBER** *(Include area code)* (937)-257-3636x4527 jonathan.butts@afit.edu |

**Standard Form 298 (Rev: 8-98)**
Prescribed by ANSI Std. Z39-18