UNIVERSITY OF CALIFORNIA, SAN DIEGO

Security of ADS-B Receivers

A thesis submitted in partial satisfaction of the
requirements for the degree
Master of Science

in

Computer Science

by

Devin Alec Lundberg

Committee in charge:

Stefan Savage, Chair
Kirill Levchenko
Hovav Shacham

2014

The Thesis of Devin Alec Lundberg is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

_____

_____

_____
Chair

University of California, San Diego

2014

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABSTRACT OF THE THESIS

Security of ADS-B Receivers

by

Devin Alec Lundberg

Master of Science in Computer Science

University of California, San Diego, 2014

Stefan Savage, Chair

Many modern pilots are now using tablet based Electronic Flight Bags (EFBs) in the cockpit where a tablet computer such as an Apple iPad is used to display charts and documents to the pilot. When this EFB is connected to a device known as an ADS-B receiver, EFBs can display not only static information, but relevant real time in flight data such as traffic and weather. The pilot can then use this information to make decisions while flying. This paper analyzes the security of these ADS-B receiver systems and creates threat models. Using these models, this paper finds attacks on existing systems including a malicious firmware update of the receiver. Lastly, security recommendations are given to fix these problems.

1 Introduction

Traditionally pilots have carried large bags, containing up to forty pounds of documents, called flight bags. These documents included charts, maps, approach plates, operator manuals, terminal procedures, and airport information. Electronic Flight Bags (EFBs) are the electronic version of these documents and with the recent advances in tablet technology, iPads are largely becoming the pilots choice over traditional methods [19].

Another trend in aviation technology is Automatic Dependent Surveillance-Broadcast (ADS-B). ADS-B is designed so aircraft can share their location data with air traffic control (ATC) and nearby planes. Nearly all planes will be required to broadcast ADS-B by 2020 [18]. To incentivize ADS-B's adoption, the FAA broadcasts live weather updates from towers located throughout the country. Unfortunately, pilots who want their on board systems to be able to read this traffic and weather information need to install expensive systems on their plane known as ADS-B In.

Instead of buying an ADS-B In system for their plane, many pilots are buying portable devices called ADS-B receivers that receive the ADS-B signal and send the information to their EFB. The EFB will then display the weather and traffic information to the pilot overlaid on the existing charts to give a pilot a more complete picture of their surroundings.

Neither the ADS-B receiver, the iPad, nor the application running on the iPad is required to be certified by the FAA (although they cannot be used on commercial planes without FAA authorization). This allows developers of these systems to quickly push application updates through the Apple App Store and focus on improving the pilot's experience rather than having to adhere to FAA

regulations and wait for approvals. As these systems are designed to provide the pilot with information to make in-flight decisions, it is reasonable to ask if these systems were designed with security in mind. We will discuss the security of the design of these systems and explore vulnerabilities in several current implementations.

In the first section of this paper we will discuss relevant background information. We will explain ADS-B, EFBs, and ADS-B receivers in general. The second section will discuss the attack surfaces and threat model of an ADS-B system. We will analyze each of the potential channels an attacker could use to maliciously affect this system. Next, we will show current implementations of the system through specific products and show examples of attacks from the channels we discussed in the previous section. Last, we will address future work that could be done to improve and better understand the vulnerabilities these new systems present.

2 Background

This section will describe background information on ADS-B, EFBs, and ADS-B receivers.

2.1 ADS-B

Automatic Dependent Surveillance-Broadcast (ADS-B) is a system for aircraft to broadcast position information. It is designed to replace radar as the primary means of tracking aircraft. Each aircraft equipped with ADS-B Out technology will obtain their position via GPS (or another GNSS-based system) and broadcast it over a data channel once every second. Other aircraft (those equipped with ADS-B In) and air traffic control (ATC) can then receive this information to create an accurate picture of the airspace. In the United States, most aircraft will be required to be equipped with some form of ADS-B Out capability by 2020. This is a part of FAA's NextGen, a program to update technology related to US aviation. To provide further incentive for this new technology, the FAA is providing several services through ADS-B broadcasts: rebroadcasting all traffic information available to ATC through Traffic Information Service-Broadcast (TIS-B), and broadcasting periodic weather information through Flight Information Services-Broadcast(FIS-B). In the US, there are two data links for transmitting and receiving ADS-B: 1090 MHz Mode S Extended Squitter (1090ES) and Universal Access Transceiver (UAT).

1090ES is the primary means of transmitting ADS-B data globally. 1090ES makes use of existing 1090 MHz transponders and an existing message type called extended squitter. Thus ATC and many aircraft can use existing hardware to

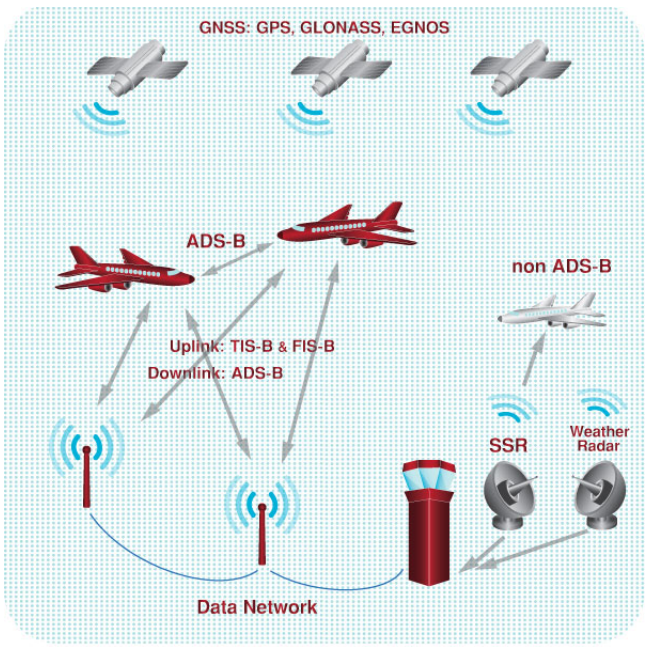

Figure 2.1.1: A simple diagram showing how aircraft communicate using ADS-B [5]

support 1090ES. Due to the use of an existing format, messages sent over 1090ES are limited to 112 bits of data per packet. This means that reports from aircraft are split into many short messages to transmit all of the necessary data. Because of this limitation, 1090ES is not used for FIS-B or TIS-B.

UAT is a major focus of FAA NextGen. UAT overcomes some of the limitations of 1090ES because it was designed specifically for ADS-B. UAT is capable of sending longer messages. This allows the FAA to send weather information via FIS-B and rebroadcast traffic via TIS-B. In order to send this data, the FAA has built ground based towers across the USA covering much of the airspace. For FIS-B, these towers send different types of updates periodically every 10-30 minutes. FIS-B updates include text based weather updates, graphical weather information (both local and national in different resolutions), relevant notices about in flight hazards or restrictions (NOTAMs), and information about current airport conditions (ATIS). TIS-B broadcasts all available radar and ADS-B traffic information within 15 nautical miles and within 3500 ft elevation for each aircraft with ADS-B Out in range of the ground station. In addition to weather and rebroadcast

traffic, UAT can be used to transmit traffic information via ADS-B for aircraft-to-aircraft or aircraft-to-ground communication and is recommended for general aviation aircraft. UAT data is sent over 978 MHz and requires the installation of new hardware.

2.2 Electronic Flight Bags

A flight bag is an aviation term referring to the document bag that pilots take on flights which contains necessary operation manuals, navigation charts, calculators, and other relevant pilot documentation. These flight bags can weigh up to 40 pounds [13]. The electronic flight bag (EFB) is a device that provides all of these documents digitally. These are preferred to traditional flight bags due to their ease of use and decreased size and weight [19].

The FAA has designated three different types of EFBs for the purpose of regulation. Class 3 EFBs are considered hardware installed on the aircraft and subject to the regulation normally provided to installed hardware. Class 2 EFBs are portable electronic devices that are mounted or attached to the aircraft in some way and that have not been certified by the FAA. Class 1 devices are non-certified portable electronic devices that are not attached to the aircraft. Besides being mounted or attached, the primary benefit of a class 2 EFB is that it can be used during all stages of flight where a class 1 needs to be stored during critical stages like takeoff and landing. Commercial airlines need to go through an FAA review process before adopting a new EFB [2, 3].

The FAA also has regulations corresponding to the applications installed on the EFB. There are three types of applications: A, B, and C. Type A applications only display static information, but not navigational charts. Type B applications may also include approach charts, show weather information, and perform weight and balance calculations. They are generally interactive. Type C applications must go through a software review process such as DO-178B or DO-178C and can overlay “own-ship” position on maps and charts. These application restrictions do not apply to non-commercial aircraft operators [2].

Figure 2.3.1: This image is an example ADS-B receiver, the Appareo Stratus 2 [24].

Apple iPads are increasingly popular as EFBs. Apple iPads can operate as class 1 or class 2 EFBs. American Airlines, Frontier, FedEx, UPS, Sky Leave I, Alaska Airlines, JetBlue, Centurion Air Cargo, and Mesa Airlines are among some of the many operators authorized to use iPads as class 2 EFBs (during all phases of flight) [13, 19, 9]. Other airlines like United are using iPads as class 1 EFBs [26]. Typical iPad EFB applications provide moving map charts, relevant documents, operator manuals, and flight planning tools. These applications generally keep these documents and charts up to date by downloading the latest version via the Internet while on the ground.

2.3 ADS-B Receivers

As a replacement to charts and documents, EFBs serve primarily as a static viewing device. Recently their usages is shifting to display real time data from ADS-B receivers.

ADS-B receivers are portable devices that collect data via internal sensors and share it directly with an EFB. An example ADS-B receiver is shown in Figure 2.3.1. One of the main purposes of these devices is to obtain weather information from FIS-B. Therefore all ADS-B receivers support UAT. A secondary purpose of ADS-B receivers is to display traffic. To obtain air-to-air traffic, a growing number of the receivers are also supporting 1090ES. Figure 2.3.2 shows how these devices interact in a system.

These devices are not equivalent to ADS-B In for several reasons. First, they are not permanently installed on the aircraft. This means that in contrast to ADS-B In systems they do not require FAA certification for general aviation pilots. Secondly they do not transmit data to the towers which means they will not receive TIS-B traffic unless there is another aircraft with ADS-B Out nearby. In that case, the ADS-B receiver will receive TIS-B traffic close to the transmitting aircraft. In this case the only way an ADS-B receiver could receive traffic like an ADS-B In system would be to have ADS-B Out installed on the aircraft with the ADS-B receiver.

Most ADS-B receivers have sensors other than ADS-B. GPS is the most common sensor. Since non commercial aircraft are permitted to display ownship position on a map, a GPS sensor allows for a more accurate display of this position. The most modern devices contain sensors for displaying heading, attitude, pitch, roll, and yaw of the aircraft using an attitude and heading reference system (AHRS). These applications can only be used on non-commercial aircraft and is not meant to replace on board instruments.

ADS-B receivers also connect to the EFB through some sort of data link. Some receivers act as a WiFi access point and broadcast their data from a specified port or range of ports. Other receivers use Bluetooth to pair with the EFB. Bluetooth receivers only support a limited number of pairings, but allow for the

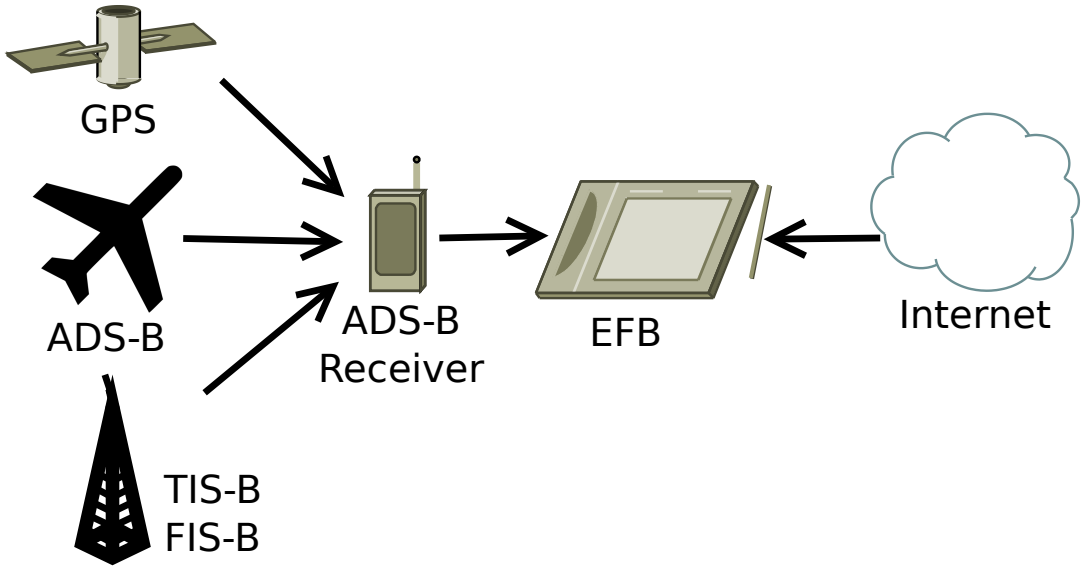

Figure 2.3.2: This image shows the communication between GPS, ADS-B, the ADS-B receiver, the EFB, and the Internet in the ADS-B receiver system.

EFB to be connected to WiFi and other Bluetooth devices.

3 Security Analysis

In this section, we will review the possible attack surfaces of an ADS-B receiver system. For each data channel and device presented in Figure 2.3.2, we will evaluate the attacker's capabilities if confidentiality, integrity, and availability are compromised. Confidentiality involves the ability to decipher the information traversing the channel. Integrity means the attacker is able to change data on the channel which is then accepted by one of the channel's legitimate participants. Attackers who control availability on a channel can prevent data from reaching the intended recipients.

In Table 3.0.1, we show the different types of attacks that can be used against an ADS-B receiver system. For each of these attacks, we discuss what the attacker can do with those capabilities on that channel or device and the requirements of an attacker performing such an attack. It is worthwhile to note that attacks on the channels communicating with external networks are considered previous work. These are presented for completeness. The rest of this paper will focus primarily on attacks against the EFB to ADS-B receiver channel and the ADS-B receiver device.

3.1 GPS to ADS-B Receiver

The GPS channel is most threatened by attacks related to integrity and availability. Confidentiality is not a problem because the planes position is not being transmitted over GPS, but calculated using the location and distance of satellites on the horizon which is public knowledge. Integrity can be compromised through GPS spoofing and availability through GPS jamming.

Table 3.0.1: The different types of attacks against channels and devices in an ADS-B system

Channels	**Integrity**	**Confidentiality**	**Availability**
GPS to ADS-B receiver	GPS spoofing	N/A	GPS jamming
ADS-B to ADS-B receiver	ADS-B spoofing	N/A	ADS-B jamming
Internet to EFB	Download spoofing	Compromise of personal pilot information	Prevention of document and firmware updates
EFB to ADS-B receiver	Man in the Middle	N/A	Attacks against pairing of EFB and ADS-B receiver
Devices	**Integrity**	**Confidentiality**	**Availability**
ADS-B receiver	Firmware update	N/A	Bricked ADS-B receiver
EFB	Direct control of EFB	Compromise of personal pilot information	Denial of EFB

3.1.1 GPS Spoofing

GPS spoofing is the act of simulating a GPS satellite to send false data to a GPS device. GPS spoofing is a problem for this system for several reasons. With the capability of GPS spoofing, an ADS-B receiver would pick up the wrong geolocation data and transmit it back to the EFB. This would interfere with a pilot who is using the EFB for ownship position, potentially making the aircraft appear at whatever latitude, longitude, or altitude that the attacker desires. A more serious threat that GPS spoofing could present is to undermine all ADS-B traffic. ADS-B relies on aircraft self reporting their location. If these aircraft are given an unreliable location through GPS spoofing, they will report that location to anyone receiving ADS-B.

The threat model for this attack involves an attacker who can operate a GPS spoofer within range of the aircraft. While a commercial GPS signal simulator can cost hundreds of thousands of dollars, researchers at UT Austin have shown how

to create a GPS spoofer for $1,500 [12]. This device then would need an antenna within the range of the aircraft. As these devices are generally not portable it may be difficult to hide on board an aircraft, but still could be attempted wirelessly. There is ongoing research in this area [25, 27].

3.1.2 GPS Jamming

Besides GPS spoofing, GPS jamming is also a threat to this system. GPS jamming prevents a GPS device from contacting the satellites. GPS jamming has been shown to affect aviation systems in the past, such as when a truck driver carrying a GPS jammer repeatedly took down a GPS system for assisting landing at Newark Airport [21]. GPS jammers would make it impossible for the receiver to communicate with a GPS satellite which would make the pilot unable to learn their position via GPS. This means that the ADS-B receiver would be unable to receive position information and if other aircraft were also being jammed, they would be unable to transmit their position. Pilots would have to fall back to other navigational tools.

To mount a GPS jamming attack, an attacker would need access to a GPS jamming device. These devices can be purchased for a cheaply as tens of dollars and are portable, so they could potentially be hidden on the aircraft. These devices could also be used in a longer range attack with some having a possible range of 8.7 km. These devices are also illegal in the United States which makes an attack more difficult. [16]

3.2 ADS-B to ADS-B Receiver

ADS-B is also vulnerable to threats against integrity and availability. Confidentiality is not an issue since the entire nature of ADS-B is to broadcast data so that any nearby receivers can read it. Integrity can be compromised through an ADS-B spoofing attack, and availability through a jamming attack.

3.2.1 ADS-B Spoofing

Neither the transport protocols nor the broadcast services provide message authentication, so ADS-B itself can be spoofed, compromising integrity. 1090ES or UAT spoofing would allow for an attacker to create false planes or sending conflicting information about ones already in the air. With UAT, FIS-B could also be spoofed. This type of attack is more severe than GPS spoofing alone as traffic can be created.

In order to spoof ADS-B, an attacker needs a device to transmit ADS-B data to the receiver. A 1090ES ADS-B transmitter has been constructed from a software defined radio (SDR) by researchers in France. The SDR devices used in their attack cost roughly a thousand dollars [7]. This device could spoof 1090ES if the attacker was within antenna range of the aircraft.

3.2.2 ADS-B Jamming

ADS-B jamming would prevent ADS-B receivers from receiving information. If ADS-B jamming was applied directly to the aircraft containing the ADS-B receiver, no signals would be found and the pilot could not receive traffic and weather through ADS-B. If the ADS-B jammer was applied to a ground station, there would be no TIS-B or FIS-B data received from that tower, in addition to the loss of data by ATC. This attack is less severe than ADS-B spoofing.

To mount such an in the air attack, a high power jamming device with a long range would be needed or an ADS-B jammer would need to be planted on the aircraft. High power ADS-B jamming devices are not readily available and this would only be effective while the target aircraft was in range [15]. An attack against a ground tower could use a device with less range.

3.3 Internet to EFB

The EFB communicates with the Internet to update documents and charts and it can also interact with payment and flight planning data. This means that this channel is vulnerable to attacks against integrity through download spoofing,

confidentiality through the compromise of pilot information, and availability in terms of denying a user the ability to update.

3.3.1 Download Spoofing

The EFB has to regularly update data to keep charts, documents, and firmware up to date. An attacker who has compromised the channel between the EFB and the update server can upload modified charts, incorrect approach plates, or modified documents to the EFB. Another target for a MITM attack is firmware updates. If the firmware update is downloaded over a network the attacker controls, they can replace the firmware update with different code leading to an attack against the ADS-B receiver.

To mount a man in the middle (MITM) attack, the attacker would need to have control or access to the network that the EFB is connected to. It is likely that an EFB user will have to update before flying at or nearby an airport where an attacker could set up a WiFi network to listen on. As many applications use unencrypted and unauthenticated HTTP, the attacker could easily modify the data requests and responses. Even if the application did not use HTTP, many mobile applications do not perform transport layer security (TLS) correctly so it is possible that an attacker would still be able to MITM on an HTTPS connection [10].

3.3.2 Compromise of Personal Pilot Information

If the attacker were able to undermine confidentiality of the Internet to EFB channel, it could reveal information about subscriber authentication and personal pilot data. This could potentially allow an attacker to log in as a target to circumvent paying for chart and document subscriptions. Payment information may also be sent over this channel. Also flight plans can be filed online through many of these applications which an attacker could read to figure out where the pilot is going.

The attacker needs to be in a position where he can listen to data on the

network through means we have already discussed in the download spoofing section. Also similar to download spoofing, if the application is using TLS correctly, the attacker will be unable to read this kind of private data.

3.3.3 Prevention of Document and Firmware Updates

If the attacker can prevent the EFB from connecting to the Internet, the pilot will not have the latest charts, documents, and firmware. Unless the pilot had not been connected to the Internet for a while, it is unlikely that documents and charts will become entirely irrelevant. This capability could possibly be used to prevent a vulnerable firmware version from being patched for a period of time. This attack is unlikely to pose a threat in most situations.

To prevent a pilot from accessing the update server, the attacker could use several different attacks depending on his capabilities. The most basic attack would be to disable infrastructure between the pilot and the update server. If the router the pilot uses to connect to WiFi is not working, the pilot would have to find another connection or simply use their existing software. Alternatively a web attacker could trigger a denial of service (DOS) attack against the update server. This would prevent any pilots from updating their EFB and could be launched remotely.

3.4 EFB to ADS-B Receiver

Integrity and availability are important on the ADS-B receiver to EFB channel. There is no private information transferred on this link so confidentiality is not an issue; the only data traveling over this channel is ADS-B, AHRS, and GPS. Attacks against integrity are man in the middle attacks between the EFB and ADS-B receiver. When the attacker controls availability, he is able to prevent the EFB from getting traffic and GPS position.

3.4.1 Man in the Middle

When the attacker controls the integrity of the EFB to ADS-B receiver, there are several attacks that can be performed. What kind of communication can happen over this channel determines what kinds of attacks can occur. Some common functionalities include changing the internal settings or performing a firmware update. By directly communicating to the ADS-B receiver, these tasks could be performed by an attacker to install fake firmware wirelessly or to change a user's hardware setting to consume more battery. An attacker can also send any data normally sent from the ADS-B receiver to the EFB. This could involve weather, traffic, GPS, or AHRS data. Since the attacker is sitting between the ADS-B receiver and the EFB, he could modify actual information to make the spoofed data seem more plausible to the pilot.

To perform an attack of this sort an attacker needs to be within range of the wireless device when it is turned on. With WiFi or Bluetooth, this attack could be performed at a distance using long range antenna. An alternative attack is to plant a device on the plane that is capable of communicating over the channel that the EFB and ADS-B receiver use. An example of this would be a mobile phone for Bluetooth and WiFi ADS-B receivers. These attacks require that the attacker know the message format and be able to connect to the receiver.

3.4.2 Attacks Preventing Pairing of EFB and ADS-B Receiver

If the attacker can make the channel between the EFB and the ADS-B receiver unusable, they would prevent the weather and traffic data from being used. This could cause frustration and may distract the pilot, but the information that the ADS-B receiver provides is not vital to flight operation so this is less serious than a man in the middle attack on the same channel. To perform this kind of attack, an attacker would need to be within range to jam the EFB and ADS-B receiver connection.

3.5 ADS-B Receiver

ADS-B receivers do not contain confidential information so only integrity and availability of the device are analyzed. The receiver's integrity is compromised if the attacker can execute code on the device, particularly in the case of a malicious firmware update. The receiver's availability is compromised if the attacker can prevent the device from functioning.

3.5.1 Firmware Update

The integrity of the receiver is lost when the attacker is able to execute code on that device or modify data. This could be used to trigger an attack at a later point in time, to make change the traffic or GPS data the pilot receives, or to launch a future attack against the EFB. The firmware update is a persistent threat as the attacker changes the code installed on the device. This is the second most serious threat to the system, after a compromise of the EFB. If the attacker is able to execute code without updating the firmware, this has similar although likely more limited consequences.

To compromise the firmware of the receiver an attacker must be able to modify it through one of the communication channels previously discussed. To only gain code execution capabilities, an attacker would need to find a vulnerability in the existing firmware like a buffer overflow that allowed for them to run code. Unless the ADS-B receiver is running a fully featured operating system, it may be difficult to take advantage of this kind of exploit.

3.5.2 Bricked ADS-B Receiver

If the attacker could prevent the ADS-B receiver from working, the pilot would be unable to access the device and the features it provides. This is similar to the previous attack.

The attacker may accomplish this by installing non functioning firmware or exploiting a vulnerability that temporarily disables the device. This attacker needs access to one of the channels that communicates with the device to launch

such an attack. Alternatively an attacker with access to the receiver can physically damage it to disable it from functioning.

3.6 EFB

EFBs are vulnerable to attacks against integrity, confidentiality, and availability. The confidentiality attack, a compromise of personal pilot information, is covered in subsection 3.3 as the results of the attack are very similar. Integrity attacks result in direct control of the EFB and availability causes a Denial of EFB to the pilot.

3.6.1 Direct control of EFB

This is the most serious vulnerability to the ADS-B receiver system as this is the device the pilot directly interacts with. With a compromised EFB, an attacker can emulate the results of any of the previous attacks and display arbitrary information to the pilot.

This attacker would have to be able to overwrite existing application code on the pilot's EFB. This would likely involve an OS vulnerability that allowed remote code execution. Also it is possible that a buffer overflow vulnerability exists within an EFB application that allows for the attacker to hijack control flow. It is likely that the vulnerability would be introduced by one of the existing channels or through installation of a malicious app. Research in the field of mobile OS security is a growing field and there are many possible types of vulnerabilities [14].

3.6.2 Denial of EFB

An attacker that controls the availability of the EFB would be able to disable access not only to weather and traffic information, but also the pilots primary source of charts and documents that may be necessary while in flight.

To perform this type of attack the attacker could use one of the previous

channels to introduce a vulnerability or trick the pilot into installing a malicious application to cause the EFB to crash.

4 Analysis of Existing Implementations

In this section, we will present the applications and devices and then demonstrate several attacks on these systems.

4.1 Applications

The three applications we will review are Foreflight, Garmin Pilot, and WingX Pro7. Each of these applications is a general aviation EFB application available in the Apple App Store. All apps uses a subscription model for payment where the app itself is free, but it costs money to keep the maps and charts up to date. All of these applications supports several kinds of VFR (visual flight rules) and IFR (instrument flight rules) as well as terrain and satellite maps. These maps can overlay data about airport conditions and weather. Each application also has a way to view airport data. There are many other applications, but according to a recent survey the three we discuss remain the most popular and highest grossing with Foreflight being by far the most [17]. We test these applications on a fourth generation iPad running iOS 7.0.3.

4.1.1 Foreflight

Foreflight is the most popular application for general aviation EFBs. Foreflight and iPad have also recently been approved by the FAA to be used as a class 2 EFB for all Frontier Airlines flights [9]. Foreflight can only connect to one ADS-B

receiver, the Appareo Stratus 2. Besides Appareo Stratus 2 weather, Foreflight also interacts with XM weather services and several other GPS only devices [8]. Foreflight requests updates over SSL and does not accept self signed certificates. It deals with subscriber information in the same manner. We use Foreflight version 5.6.

4.1.2 Garmin Pilot

Garmin Pilot is another popular EFB. Garmin Pilot is unique in that it also offers an Android app. Garmin Pilot interfaces with one ADS-B receiver, the Garmin GDL-39. Garmin Pilot updates its documents and charts over HTTP, but performs subscription based functionality through SSL and does not accept self signed certificates. We run our attacks using Garmin Pilot 6.0.1.

4.1.3 WingX Pro7

WingX Pro7 has won several awards and was ranked third in a survey for pilots using iPads as EFBs [17]. It supports data from 11 different ADS-B devices [11] including Sagetech Clarity. All data requests are done unencrypted over HTTP, except for monetary transactions which are done through the Apple App Store. We use WingX Pro7 version 7.1.2.5.

4.2 Devices

In this subsection we present the three ADS-B Receivers we will analyze: Appareo Stratus 2, Sagetech Clarity, and Garmin GDL-39.

4.2.1 Appareo Stratus 2

The Appareo Stratus 2 is one of the most popular ADS-B receivers. It is the only device that works with Foreflight. The device has won several awards such as Flying Magazine's editor choice award [1]. It's a small white rectangular

shaped device. The Appareo Stratus 2 has sensors for UAT, 1090ES, GPS, and AHRS.

Appareo Stratus 2 uses WiFi to communicate with Foreflight. Each Appareo Stratus 2 device operates as an access point broadcasting with an SSID that contains the name Stratus and the device's unique serial number. The Appareo Stratus 2 AP runs in infrastructure mode. To authenticate that Foreflight is connected to Appareo Stratus 2, Foreflight checks that the iPad has an IP in the subnet that the Appareo Stratus 2 transmits to. It sends UDP messages from 5 different ports signifying the message type: device status, GPS, UAT, AHRS, or 1090ES. Also messages can be sent to the Appareo Stratus 2 through another port.

Status messages contain information about the receiver hardware such as the battery level, serial number, internal temperature, firmware version, internal sensor errors, and sent message counts. This data has one message format that is sent at 1 Hz (one message per second). A Fletcher 16 checksum with modulus 255 is used for error correction [28].

GPS messages send latitude, longitude, altitude, velocity in three dimensions, accuracy, GPS fix, and relevant information about GPS satellites. Satellite data is sent at 1 Hz, while other GPS information is sent at 5 Hz. A Fletcher 16 checksum with modulus 256 is used for error correction [28].

AHRS messages contain information from internal gyroscopes. This information appears to be mostly ignored by Foreflight, but there is another application from Appareo for displaying a virtual flight instrument panel with that data. A Fletcher 16 checksum with modulus 256 is used for error correction [28].

UAT and 1090ES messages contain the raw bytes of the message with no added checksums. 1090ES messages are stripped of their last three bytes which contain parity information.

The Appareo Stratus 2 can also receive some messages. These messages can set options like WiFi power and LED brightness or initiate a firmware update.

The firmware update is bundled inside of the Foreflight application from the Apple App Store. The firmware update can also be triggered through the Appareo Stratus 2 updater app where the firmware update is downloaded over

HTTP. To install the update, Foreflight or the Appareo Stratus 2 updater app resets the receiver and then sends the update over WiFi.

4.2.2 Sagetech Clarity

Sagetech Clarity is a cube shaped ADS-B receiver. It supports UAT, 1090ES, GPS, and AHRS (if you get the more expensive version). Sagetech Clarity is designed to work with a number of different applications and the message format is available for developers willing to sign a NDA [22]. The Sagetech Clarity transmits data over WiFi. It sets up an ad-hoc WiFi network and the EFB authenticates the connection based on if it is receiving messages and the IP range of the EFB's current subnet. Messages sent from the Sagetech Clarity are broadcast to all connected IPs.

The Sagetech Clarity uses a message format very similar to the Garmin GDL 90 Data Interface Specification. In addition to this format, it includes messages for device status contains information about the current firmware, the serial number, battery status, and internal hardware problems.

The Sagetech Clarity is unique among the three devices looked at in that it does not receive any data from the EFB. This means that users cannot adjust any internal settings or trigger a firmware update from their device.

To update the firmware on Sagetech Clarity, the device must be connected to a windows machine where it can be put into Device Firmware Update (DFU) mode through a VCOM interface and then updated. The update mechanism does not guarantee that the device firmware version is greater than the version of the firmware to be installed so downgrading is possible.

4.2.3 Garmin GDL-39

The Garmin GDL-39 is another popular ADS-B receiver. It supports UAT, 1090ES, and GPS. Garmin GDL-39 is designed to only work with two applications, Garmin Pilot and the Garmin GDL-39 utility which displays the information from the receiver without requiring a subscription. Of the three devices tested, it is the

only one that uses Bluetooth to communicate with the EFB. This allows the EFB to be connected to the Internet and the receiver at the same time which is how it performs firmware updates. The Garmin GDL-39 can pair with a maximum of two devices at a time while a WiFi receiver could connect to however many the subnet supports. It will refuse to connect with additional devices. The Bluetooth protocol used by Garmin GDL-39 does not incorporate encryption so anyone with the MAC address of the receiver can connect. It communicates using RFCOMM (application layer protocol for Bluetooth) which emulates serial ports.

The way the Garmin GDL-39 receives and sends messages is very different from the other two devices. When an EFB connects to receiver's Bluetooth address, the two devices engage in a handshake. This handshake involves the ADS-B receiver sending data and a key to Garmin Pilot. The EFB then encrypts the data sent to it with a 16 round Blowfish cipher and the key and then encrypts a static message with the output of the first cipher as a key to an 11 round Blowfish cipher. This unusual algorithm is meant to be a shared secret to authenticate the Garmin GDL-39 as a valid device and Garmin Pilot as a valid application, but since this code is released in the firmware and in the app, an attacker can figure out the communication.

Once connected to Garmin GDL-39, Garmin Pilot can request GPS data be sent at 1 Hz or 5 Hz. This GPS data is in NMEA format sending GPGGA, GPRMC, and GPGSA sentences.

For other types of data, Garmin Pilot requests the data by filename and than Garmin GDL-39 sends it back over Bluetooth. The files include several types of text based and graphical weather data and traffic data.

4.3 Attacks

In this section we will discuss attacks on the implementations we just discussed. First we will discuss how the EFB to ADS-B channel can be compromised on each of the device combinations. Then we will discuss three attacks all based on this channel. Last we will compromise the link between the EFB and the Internet

Table 4.3.1: This shows attacks against ADS-B receivers. A ✓ means that the receiver is not vulnerable. An **X** means we demonstrated this attack. An X indicates we believe the receiver is vulnerable.

Attacks	**Stratus 2**	**Clarity**	**GDL-39**
EFB to Receiver Link	**X**	**X**	X
Status Packet Spoof	**X**	X	X
GPS Packet Spoof	**X**	X	X
Traffic Packet Spoof	**X**	X	X
Firmware Update	?	**X**	**X**

to change a firmware update of the device and run our own code. These attacks are summarized in Table 4.3.1.

4.3.1 Compromising the EFB to ADS-B Receiver Link

The Sagetech Clarity and Appareo Stratus 2 have a very similar receiver to EFB link. They both broadcast to the application over WiFi and are both susceptible to similar attacks. An attacker can simply create an access point with the same SSID in close proximity to the device leaving the user confused over which one to connect to. The attacker can then connect to the real receiver and forward traffic. This attack can be made more stealthy by taking advantage of the protocol used to initiate a connection [4]. Another simpler way to compromise the link is to connect to the ADS-B receiver and then send more packets then it. As the EFB only updates the UI at fixed intervals, this forces the device to ignore some of the packets which are likely the legitimate ones since they are sent at a smaller frequency. This attack did not cause any errors, but it could potentially cause a denial of service.

The Garmin Pilot is makes it more difficult to perform a MITM attack. First the address of the Bluetooth device is needed. This can be obtained listening to Bluetooth traffic using an Ubertooth [20]. Once the address is obtained a connection can be opened with the device using RFCOMM. We did not finish implementing the MITM attack, but the next step would be emulating the receiver using its Bluetooth address and a tool like SpoofTooph [23] and then forcing the EFB to connect with the attacker's spoofed device.

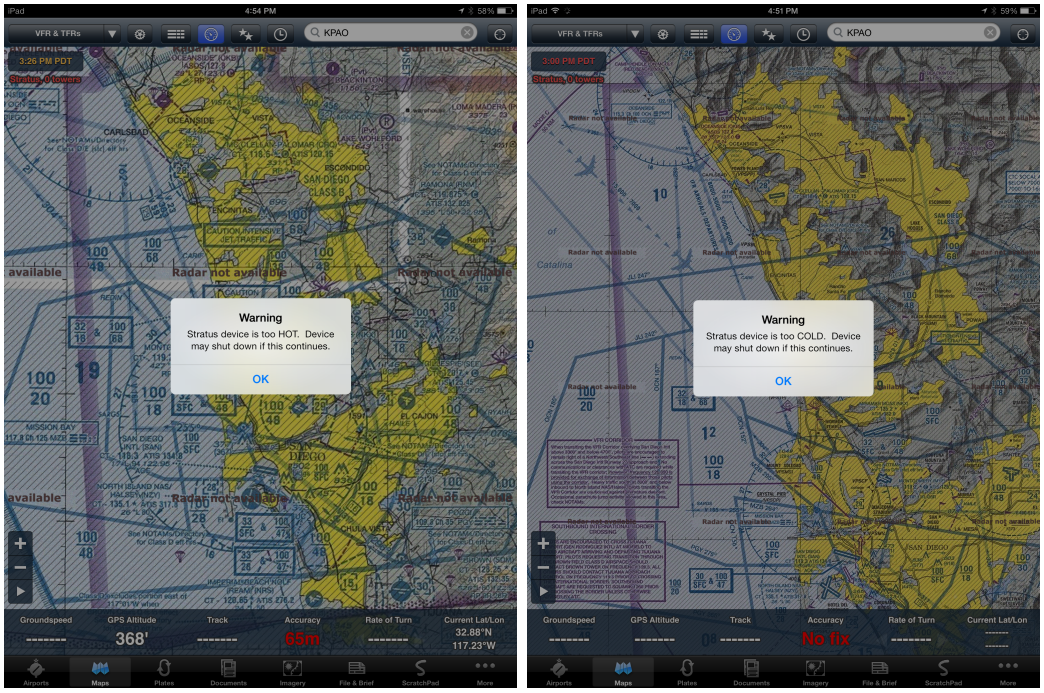

Figure 4.3.1: Warning messages that can be triggered using a spoofed status message from Appareo Stratus 2 to Foreflight

4.3.2 Status Packet Spoofing

In this attack we spoof the packets that send status information about the ADS-B receiver to the EFB. We chose to implement this attack against Foreflight. These status packets display error codes, battery status, internal temperature, serial numbers, and version numbers. These attacks could be used to distract the pilot from normal operation by displaying an error message and forcing the pilot to interact with the iPad. Figure 4.3.1 shows the warning error dialogs that are displayed when the temperature goes outside the acceptable range. Figure 4.3.2 shows some of the other information that can be spoofed using a status packet. Notice the serial number is longer than the 6 character value that it is normally restricted to due to a non-null character terminated strcpy(). We did not find a way to take further advantage of this overflow problem, but there may be other similar but more serious vulnerabilities that we missed. Also notice the Tap-to-Update flag is set even though the version number is higher than the current version 1.3.0.389. This is because only the last part of the version information is considered when

calculating if a version update is needed.

4.3.3 GPS Packet Spoofing

In this attack we spoof GPS data sent from the Appareo Stratus 2 to Foreflight. Appareo Stratus 2 packets for GPS contain latitude, longitude, horizontal accuracy, altitude, vertical accuracy, north groundspeed, east groundspeed, and satellite data. We are able to spoof all of these values. Figure 4.3.3 shows the ownship position at the White House with spoofed altitude and groundspeed data. In a real attack these values could deviate gradually from the actual GPS position causing the pilot to try to compensate by changing course.

4.3.4 Traffic Packet Spoofing

In this attack we spoof traffic information from the Appareo Stratus 2 to Foreflight. These packets are in the same format as ADS-B traffic. By parsing and altering this data, one can create, remove, or modify traffic. We changed the flight number and replayed existing flight paths as seen in 4.3.4. An attacker could use this kind of attack to make aircraft appear to be on a collision course and cause the pilot to react differently, perhaps increasing the likelihood of an actual collision.

4.3.5 Firmware Updates

Both the Sagetech Clarity and the Garmin Pilot can be maliciously updated. The Appareo Stratus 2 firmware appears to be encrypted. This does not mean an attack is not possible on Appareo Stratus 2. If the update is not signed and a key can be recovered from the device, the Appareo Stratus 2 firmware can be updated.

This attack takes advantage of the unencrypted, unsigned firmware updates used to update the Garmin Pilot. By intercepting and changing the responses to the HTTP requests sent by the application, we were able to send our own custom firmware. This image had several checksums to provide integrity in case the firmware was changed in transit, but no forms of authentication like a digital signature. Thus this firmware could potentially be modified to include any code.

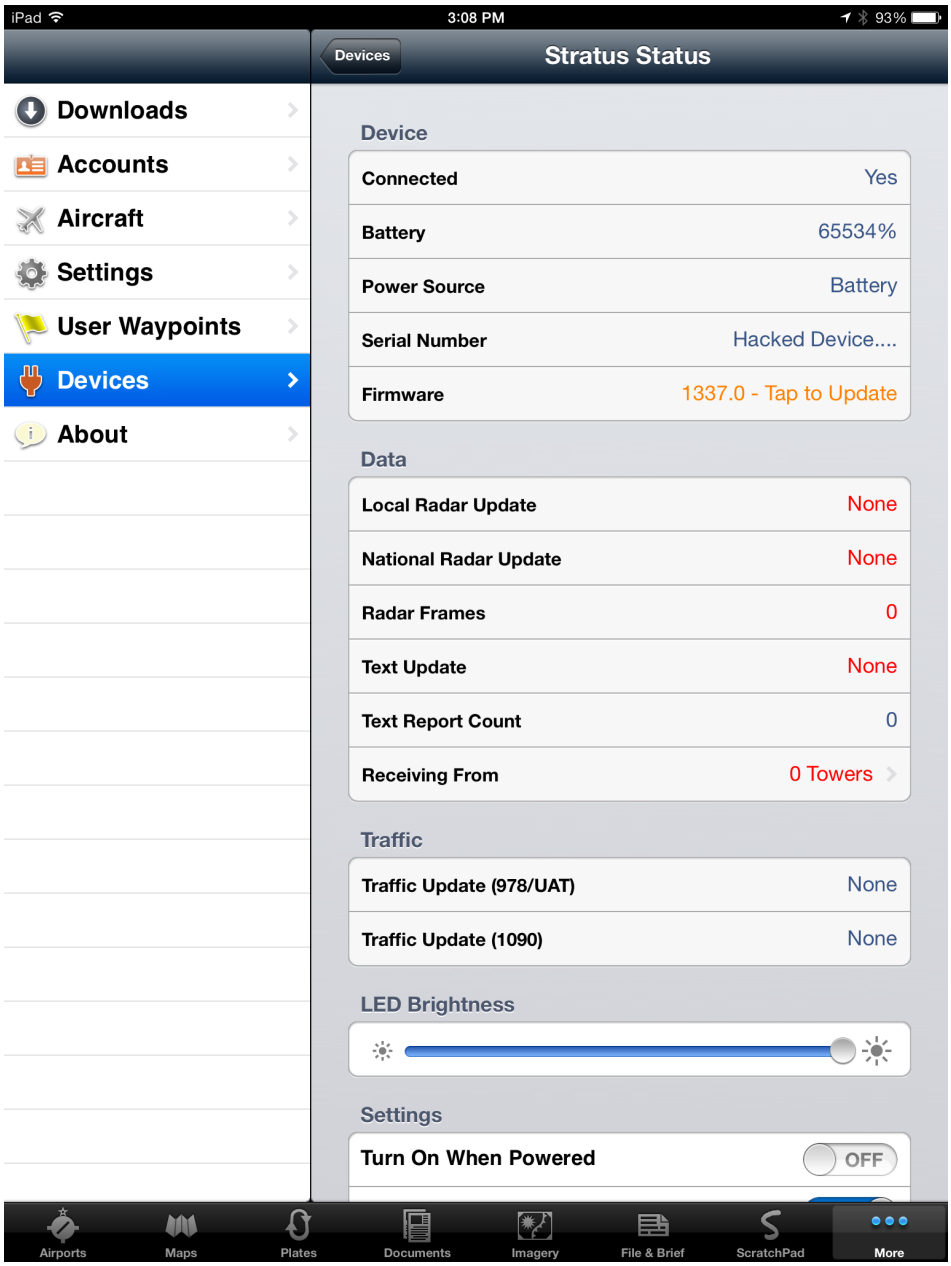

Figure 4.3.2: Example of some of the parameters that can be changed on the Foreflight status page from a spoofed Appareo Stratus 2

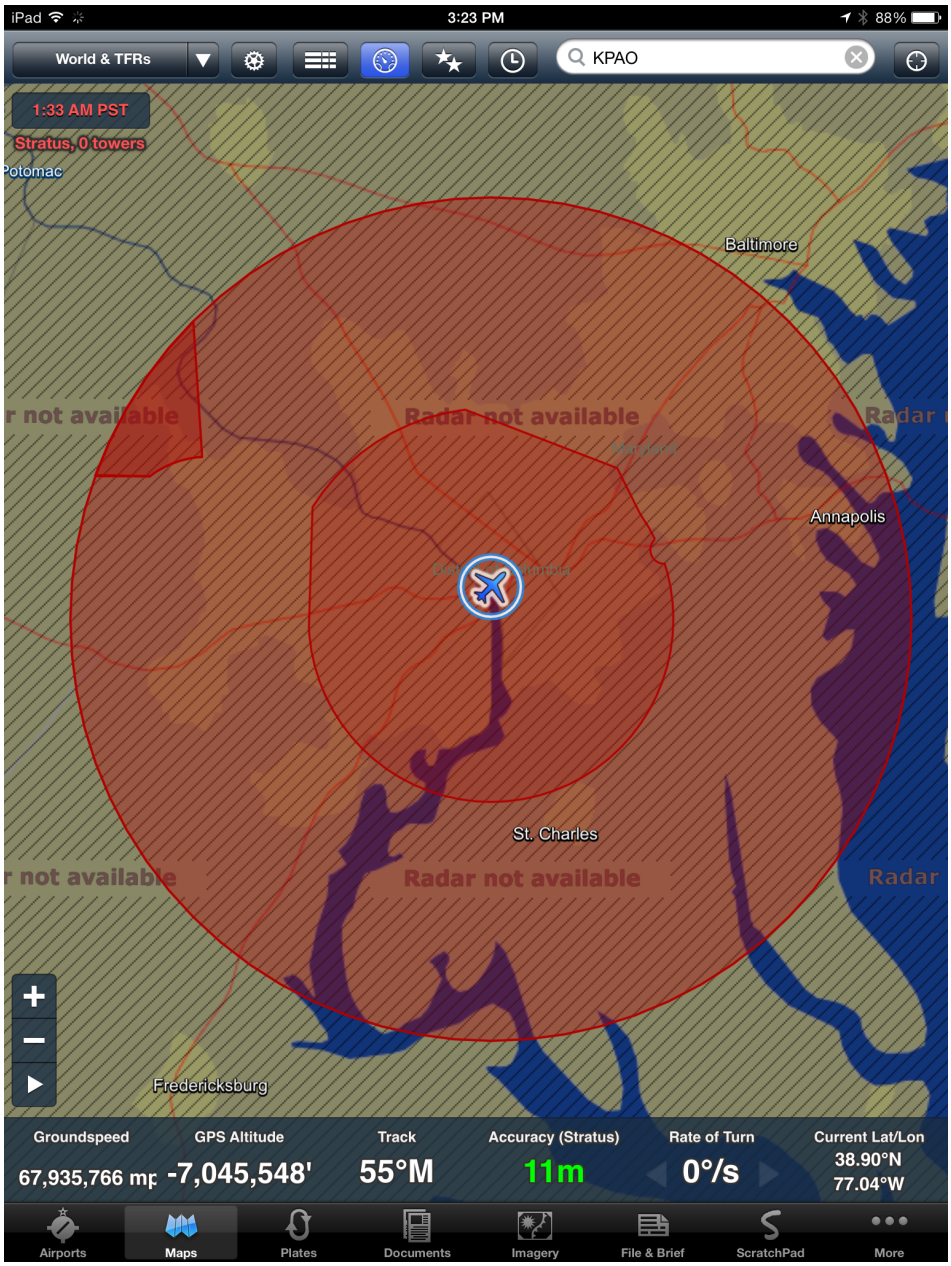

Figure 4.3.3: The result of spoofed GPS packets sent to Foreflight. This example contains a fake latitude, longitude, altitude, ground speed, and heading.

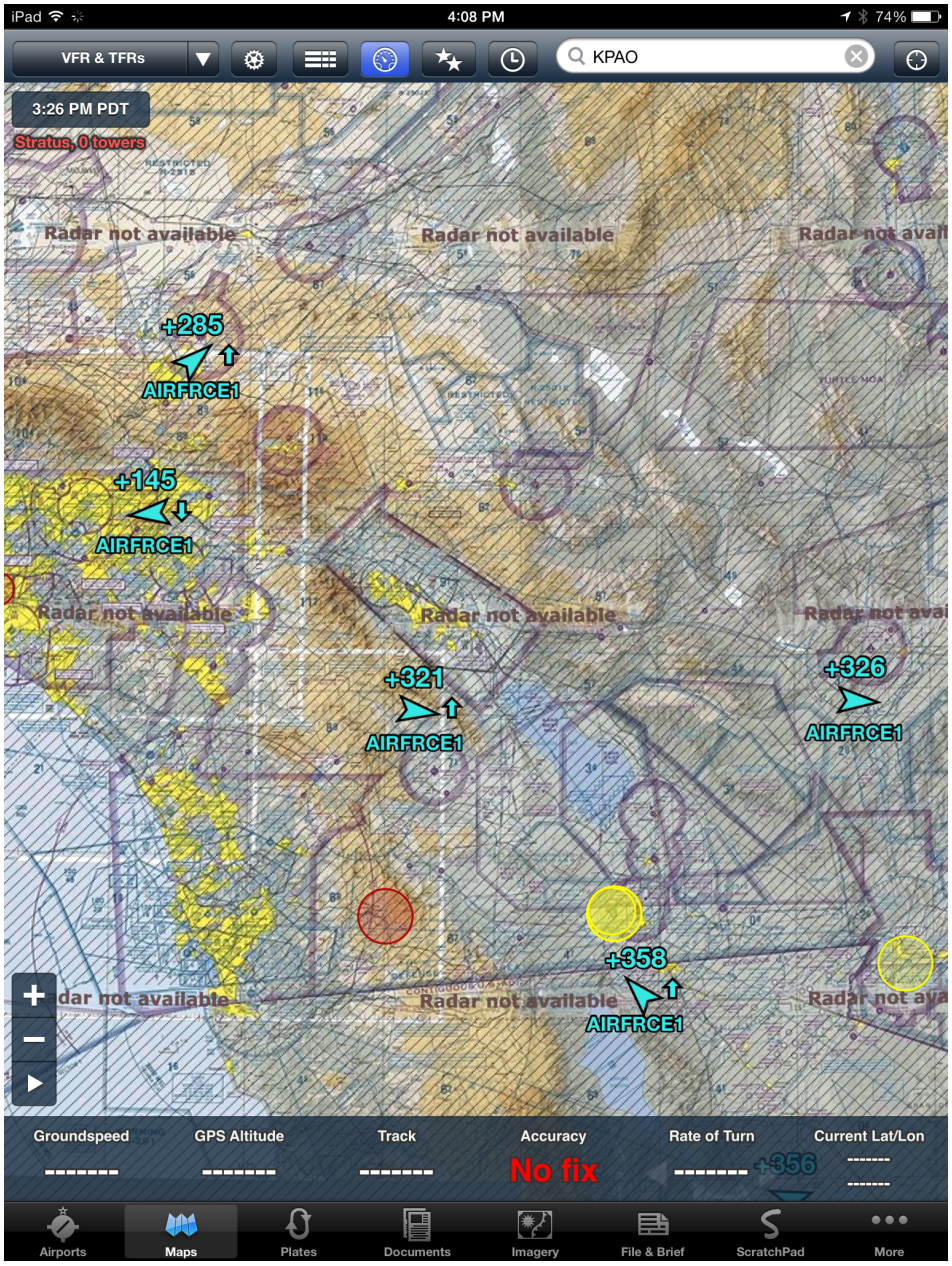

Figure 4.3.4: This is an example of spoofing traffic packets to Foreflight. We changed the flight number and used replayed position data from actual planes. The location data can be modified as well.

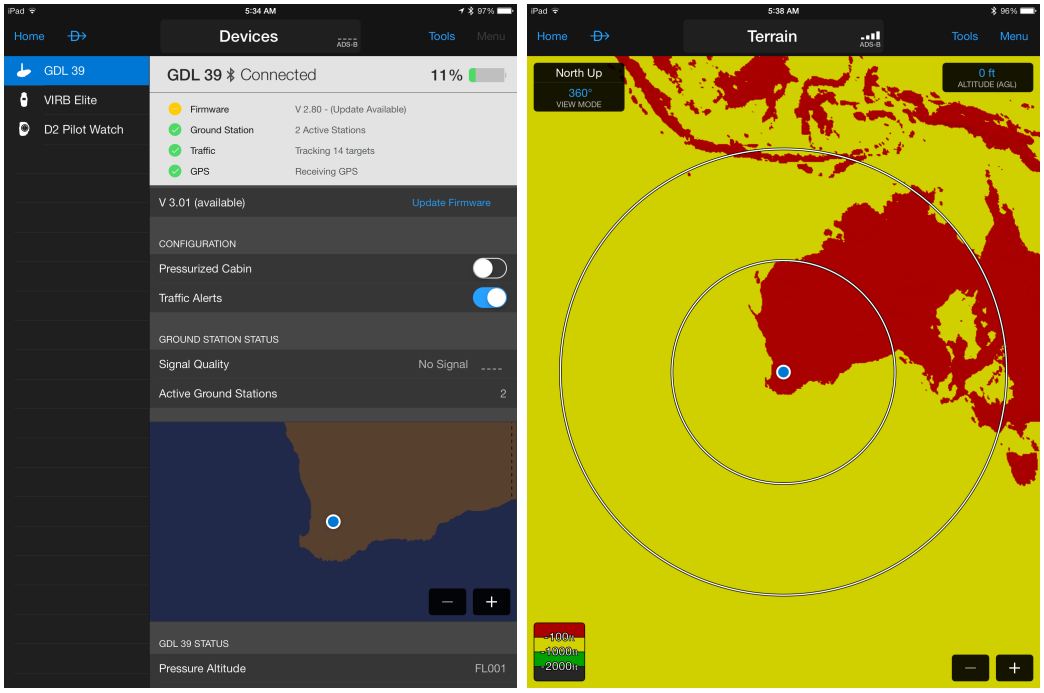

Figure 4.3.5: This point is the opposite end of the world from University of California, San Diego. This demonstrates an attack on the Garmin GDL-39 where the firmware was edited to flip north and south and east and west for GPS position data.

We modified the code to switch from north to south of latitude and east to west for longitude, making the user appear on the opposite end of the world as seen in Figure 4.3.5. Garmin Pilot downloaded the file and installed it on the Garmin GDL-39.

We successfully launched a similar attack against the Sagetech Clarity. We replaced the DFU image within the executable that runs the firmware update. This executable is downloaded via HTTP. The modified firmware image created ran code that overwrites all flight ids with a fixed string. Since the updates are triggered from a computer instead of a tablet, the target for the network attack changes, but the attack remains the same.

5 Security Recommendations

5.1 Firmware Updates

The property of non-repudiation should hold in firmware updates. This guarantees both the integrity and the authenticity of the update and guarantees that the software maker sent the update. Many of the firmware updates we looked at already have code for guaranteeing integrity, but as we showed, these integrity checks can be changed by a malicious party to match whatever changes the attacker wishes to make to the firmware updates. Another potentially useful guarantee these firmware updates could enforce is that the version is greater than or equal to the current version. In combination with non-repudiation, this prevents attackers from performing an attack by downgrading the firmware and taking advantage of previous vulnerabilities.

The most simple way to provide these guarantees is by using digital signatures. These signatures need to be verified by the ADS-B receiver otherwise an attacker who has the capability of compromising the channel between the EFB and the ADS-B receiver can still perform malicious updates. As the CPU is limited in power on these devices, RSA would be an example of a reasonable digital signature algorithm as verification is very efficient, it is viewed as secure by cryptographers when used with an appropriate key length and padding [6], and there exist many existing libraries implementing it. Overall the performance and speed of the verification algorithm should not have a huge impact as it would only be executed during a firmware update.

To update devices to use digital signatures via the existing model, a firmware update would have be released including a public key which would be used to verify

the signature of the next firmware update. There also should be a mechanism to update the key or algorithm in case the private key is compromised or as part of key rotation. As key or algorithm changes should not be happening very often, it would be reasonable to include a signature for each of the past used keys with each update to provide legacy support.

5.2 EFB Document Downloads

Non-repudiation is also important for EFB documents. These documents should come directly from the EFB servers to prevent compromise. Since the connection needs to be secured to the app. A simple way for the application creators to guarantee this is by using HTTPS for document downloads which Garmin Pilot already supports. Even if they didn't already implement TLS, it would likely be preferable to a custom solution because cryptography has many places for subtle errors and there are already existing libraries for TLS which have been tested and are considered secure.

5.3 More Secure EFB to ADS-B Receiver Links

This is a more difficult problem to solve then the previous two issues. To analyze possible solutions we will first look at improving the two links currently used: WiFi and Bluetooth. Then we will look at a the benefits of a wired solution.

5.3.1 WiFi

For WiFi connections, the current implementations simply broadcast on an unsecured network. Using WPA2 with a unique randomly generated key for each receiver could provide additional security in that an attacker would need to obtain the key in order to be able to spoof data on the channel. The same key should not be used across all devices even if it is a mutable default since then the attacker would still have access to every device that did not change the default. The downside of this scheme would be that the pilot might not like having to deal

with entering a key or may lose the key. Most devices like will remember the user's passwords so having to enter a password should not be an issue. A solution to loss of a key could be to print the key on the device, so an attacker would still need physical access to the device to connect wirelessly. A stronger solution would be to allow the password to be reset to some default value through a hardware reset button and then changed through the EFB.

5.3.2 Bluetooth

For Bluetooth connections, the pairing mechanism is the exact kind of defense to deter a wireless attacker. To pair with these receivers, a user must put the receiver into pairing mode. An attacker should be unable to connect unless he has correctly gone through the pairing process which requires physical access to the device.

To thwart attacks at periods outside of pairing, authenticated encryption should be used. Unfortunately Bluetooth 2.1 does this poorly. After pairing, the standard only supports encryption using a stream cipher widely considered broken. These devices should instead use Bluetooth 4.0, otherwise known as Bluetooth Low Energy (BLE). BLE uses AES-128-CCM for encryption and authentication which NIST estimates will still be secure past 2030 [6]. Also BLE has a shorter range than Bluetooth 2.1 and thus an attacker would potentially need a more powerful or focused antenna for long range attacks.

During pairing, attackers could potentially still set up a man in the middle attack. This is a more limited threat model as the attacker needs to be present during the pairing process. To prevent this threat, the Bluetooth standard has three solutions: displaying a passcode on both devices, requiring a user to enter a passkey on both devices, or using an out of band communication protocol such as Near Field Communications (NFC). To actually implement one of the first two solutions, the ADS-B receiver would have to have a display installed. Using NFC would be suitable to the use case of ADS-B receivers, but current iPads do not support NFC.

5.3.3 Wired

Wired connections should also be considered since it would not be possible to compromise that channel without physical access. The major downsides of using a wire is that it could clutter the cockpit and multiple devices cannot connect.

6 Future Work

One aspect that we did not study is how pilots actually use the information from iPad EFBs and ADS-B receivers. A pilot study investigating how pilots perceive this information and how they would react to various attacks would provide insight into the risks associated different attacks. As ADS-B receivers are not connected to the controls of the plane, it is only through the pilot that they would be able to do any real damage. Understanding which information is trusted and how pilots establish this trust is important to understanding the threat a compromised ADS-B receiver system could pose.

Many EFB apps have flight planning tools that allow pilots to file flight plans through the application. If these flight plans were compromised, they could present misinformation to ATC. This would be a different kind of attack then the ones we have presented in our paper in that they would misinform ATC instead of pilots.

We mentioned a compromise of the EFB's integrity (whether that being data or code) in our threat model, but we did not look in depth at what kind of attacks may exist. Doing a thorough analysis of the EFB software could find other areas that are weak. This also could include how other applications interact with the EFB or what kind of OS vulnerabilities would cause issues in EFB software.

7 Conclusion

Without strict FAA regulation, it is clear that security was not the first priority for ADS-B receivers. By laying out the threat model for ADS-B receiver systems, future versions of these systems can take security into account during the design phases. This will help prevent the kinds of attacks we presented in this paper. Existing systems can also benefit from the threat model and the security recommendations to help patch and prevent future threats.

Glossary

1090ES 1090 MHz Mode S Extended Squitter.

ADS-B Automatic Dependent Surveillance-Broadcast.

AHRS Altitude and Heading Reference System.

ATC Air Traffic Control.

ATIS Automatic Terminal Information Service.

BLE Bluetooth Low Energy.

EFB Electronic Flight Bag.

FAA Federal Aviation Administration.

FIS-B Flight Information Service-Broadcast.

GNSS Global Navigation Satellite System.

GPS Global Positioning System.

MITM Man in the Middle.

NOTAM Notice to Airmen.

SDR Software Defined Radio.

SSID Service Set Identification.

TIS-B Traffic Information Service-Broadcast.

UAT Universal Access Transceiver.

Bibliography

[1] *2013 Flying Editors Choice Awards*. 2013. URL: http://www.flyingmag.com/pilots-places/pilots-adventures-more/2013-flying-editors-choice-awards (visited on 03/06/2014).

[2] *AC 120-76B: Guidelines for the Certification, Airworthiness, and Operational Use of Electronic Flight Bags*. Federal Aviation Administration, 2012.

[3] *AC 20-173: Installation of Electronic Flight Bag Components*. Federal Aviation Administration, 2011.

[4] Marco Domenico Aime, Giogrio Calandriello, and Antonio Lioy. "Dependability in wireless networks: can we rely on WiFi?" In: *Security & Privacy, IEEE* 5.1 (2007), pp. 23–29.

[5] *Automatic Dependent Surveillance - Broadcast (ADS-B)*. 2012. URL: http://www.adaptaeronav.aero/technologies/adsb.htm (visited on 03/06/2014).

[6] Elaine Barker et al. *Recommendation for key management-part 1: General (revision 3)*. NIST, 2012.

[7] Andrei Costin and Aurélien Francillon. "Ghost in the Air (Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices". In: *Black Hat USA* (2012).

[8] *Foreflight*. 2014. URL: http://foreflight.com (visited on 03/06/2014).

[9] *ForeFlight and Frontier Airlines Announce Approval for ForeFlight Mobile in the Cockpit*. 2013. URL: http://blog.foreflight.com/2013/10/09/foreflight-and-frontier-airlines-announce-approval-for-foreflight-mobile-in-the-cockpit/ (visited on 03/06/2014).

[10] Martin Georgiev et al. "The most dangerous code in the world: validating SSL certificates in non-browser software". In: *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM. 2012, pp. 38–49.

[11] *Hilton Software*. 2014. URL: http://hiltonsoftware.com (visited on 03/06/2014).

[12] Todd E Humphreys et al. "Assessing the spoofing threat: Development of a portable GPS civilian spoofer". In: *Proceedings of the ION GNSS International Technical Meeting of the Satellite Division*. Vol. 55. 2008, p. 56.

[13] *JetBlue chooses Apple's iPad for its flight decks*. 2013. URL: http://appleinsider.com/articles/13/06/26/jetblue-chooses-apples-ipad-for-its-flight-decks (visited on 03/06/2014).

[14] Mariantonietta La Polla, Fabio Martinelli, and Daniele Sgandurra. "A survey on security for mobile devices". In: *Communications Surveys & Tutorials, IEEE* 15.1 (2013), pp. 446–471.

[15] Donald McCallie, Jonathan Butts, and Robert Mills. "Security analysis of the ADS-B implementation in the next generation air transportation system". In: *International Journal of Critical Infrastructure Protection* 4.2 (2011), pp. 78–87.

[16] Ryan H Mitch et al. "Signal characteristics of civil GPS jammers". In: *Proceedings of ION GNSS 2011* (2011), pp. 20–23.

[17] *Navigation App Showdown, round 2 - Foreflight vs. WingX vs. Garmin*. 2013. URL: http://ipadpilotnews.com/2013/08/navigation-app-showdown-round-2/ (visited on 03/06/2014).

[18] *Next Gen*. 2014. URL: http://www.faa.gov/nextgen/ (visited on 03/10/2014).

[19] *Product Focus: Electronic Flight Bags*. 2013. URL: http://www.aviationtoday.com/av/commercial/Product-Focus-Electronic-Flight-Bags_80135.html (visited on 03/06/2014).

[20] *Project Ubertooth*. 2013. URL: http://ubertooth.sourceforge.net/ (visited on 03/12/2014).

[21] Sam Pullen and G Xingxin Gao. "GNSS jamming in the name of privacy-potential threat to GPS aviation". In: *Inside GNSS* 7.2 (2012), pp. 34–43.

[22] *Sagetech Clarity*. 2014. URL: http://www.sagetechcorp.com/general-aviation-solutions/clarity-ads-b.cfm (visited on 03/06/2014).

[23] *SpoofTooph*. 2012. URL: http://www.hackfromacave.com/projects/spooftooph.html (visited on 03/12/2014).

[24] *Stratus ADS-B Receiver for iPad - Second generation*. 2014. URL: http://www.sportys.com/PilotShop/product/17996 (visited on 03/06/2014).

[25] Nils Ole Tippenhauer et al. “On the requirements for successful GPS spoofing attacks”. In: *Proceedings of the 18th ACM conference on Computer and communications security*. ACM. 2011, pp. 75–86.

[26] *United Airlines Launches Paperless Flight Deck With iPad*. 2011. URL: http://www.prnewswire.com/news-releases/united-airlines-launches-paperless-flight-deck-with-ipad-128240343.html (visited on 03/06/2014).

[27] Kyle Wesson, Mark Rothlisberger, and Todd Humphreys. “Practical cryptographic civil GPS signal authentication”. In: *Navigation* 59.3 (2012), pp. 177–193.

[28] Wikipedia. *Fletcher’s checksum — Wikipedia, The Free Encyclopedia*. 2013. URL: http://en.wikipedia.org/w/index.php?title=Fletcher%27s_checksum&oldid=587351903 (visited on 03/06/2014).