On The Security of Mobile Cockpit Information Systems

Devin Lundberg,* Brown Farinholt,* Edward Sullivan,* Ryan Mast,*
Stephen Checkoway,† Stefan Savage,* Alex C. Snoeren,* and Kirill Levchenko*
*UC San Diego, 9500 Gilman Drive, La Jolla, CA 92093-0404
†Johns Hopkins University, 3400 N. Charles Street, Baltimore, MD 21218
{dlundber, bfarinho, elsulliv, rmast, savage, snoeren, klevchen}@cs.ucsd.edu, s@cs.jhu.edu

ABSTRACT

Recent trends in aviation have led many general aviation pilots to adopt the use of iPads (or other tablets) in the cockpit. While initially used to display static charts and documents, uses have expanded to include live data such as weather and traffic information that is used to make flight decisions. Because the tablet and any connected devices are not a part of the onboard systems, they are not currently subject to the software reliability standards applied to avionics. In this paper, we create a risk model for electronic threats against mobile cockpit information systems and evaluate three such systems popular with general aviation pilots today: The Appareo Stratus 2 receiver with the ForeFlight app, the Garmin GDL 39 receiver with the Garmin Pilot app, and the SageTech Clarity CL01 with the WingX Pro7 app. We found all three to be vulnerable, allowing an attacker to manipulate information presented to the pilot, which in some scenarios would lead to catastrophic outcomes. Finally, we provide recommendations for securing such systems.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protections

General Terms

Security, Aviation, Human Factors, Mobile Cockpit Information Systems

1. INTRODUCTION

Modern tablet PCs and smart phones offer a capable low-cost platform for many applications that have until recently required special-purpose hardware. In most cases—point-of-sale terminals, information kiosks, home automation controls, and so on—our expectations of security and reliability are on par with everyday consumer electronics. There are domains, however, where we expect near-absolute security and reliability. Among them is aviation, where a malfunctioning safety-critical system can lead to loss of life. The use of consumer mobile electronics in a capacity where they can affect flight safety thus warrants closer scrutiny.

In this paper we examine a particular use of mobile devices in general aviation, in which an iPad (or similar tablet) supplements conventional flight and navigation instruments. An app running on the iPad communicates with a separate handheld device, which combines a GPS receiver with additional aeronautical information receivers into a single unit. We term this combination of tablet, app, and receiver a *Mobile Cockpit Information System (MCIS)*. A state-of-the-art MCIS presents the pilot with a unified moving map display showing aircraft position overlaid on an aeronautical chart. Depending on the aeronautical information services supported by the receiver, the display may also include a graphical weather overlay (FIS-B service) and may display nearby aircraft (ADS-B and TIS-B service). Some receivers also include solid-state magnetometers and accelerometers, which provides the app with aircraft magnetic heading and attitude (pitch and roll).

The iPad is often mounted alongside conventional instruments (Figure 1), mimicking the glass cockpit found on modern high-end aircraft. In this configuration, the iPad effectively becomes part of the cockpit instrument panel. However, because it is a pilot's portable electronic device, and not part of the aircraft, it is not subject to aviation electronics (avionics) airworthiness requirements. This regulatory exemption allows MCISes to be developed at the cost and pace of modern mobile apps and consumer electronics. At issue is whether this rapid growth in features and capabilities comes at the cost of security, and this is the first question we address in this paper:

✻ **Do mobile cockpit information systems provide the security guarantees expected of similar avionics systems?**

Answering this question requires an agreed upon notion of the security we expect of such systems. In the computer security community, we formulate security properties as hypotheses subject to refutation by an attack that causes the target system to exhibit some undesired behavior or reveal some secret information. Whether an attack succeeds or fails is well defined, and depends only on the target itself. In this setting, the most natural MCIS security property concerns the authenticity of information presented to the pilot. In other words, in this setting, an MCIS is secure if an attacker cannot cause it to present false information to the pilot.

By this measure, current mobile cockpit information systems are not secure against a variety of attacks. In addition to the already-known attacks on GPS and the underlying aeronautical information services (ADS-B, TIS-B, and FIS-B), the systems we examined are also vulnerable to MCIS-specific attacks, the most severe of which allows an attacker to reflash receiver firmware, giving him complete control over when and what information is presented to the pilot.

In the aviation community, security of avionics systems is viewed as a matter of reliability, which is itself part of the overall airworthiness determination for an avionics system. Reliability differs

CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA.
Copyright is held by the authors. Publication rights licensed to ACM.
2014 ACM 978-1-4503-2957-6/14/11 ...$15.00.
http://dx.doi.org/10.1145/2660267.2660375.

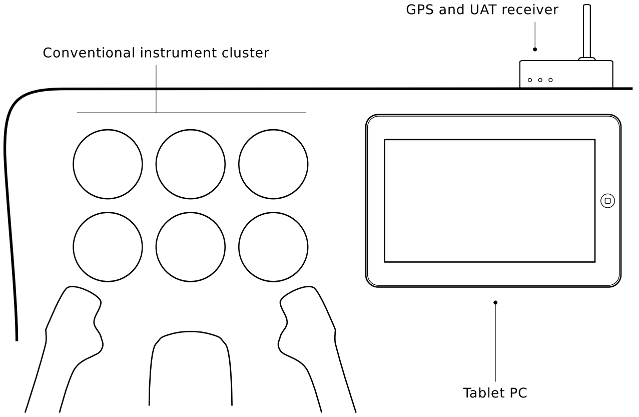


Figure 1: A modern cockpit mobile arrangement consisting of a mobile computing device (e.g. iPad) and a GPS and UAT receiver.

from security in its adversary: the adversary of reliability is Nature, while the adversary of security is a motivated attacker. In reliability analysis, Nature is a stochastic process that can be tamed by driving the probability of a system failure to an acceptable level. However, unless a system is absolutely reliable, a determined attacker can exploit the tiniest sliver of vulnerability. These were lessons learned two decades ago by the computer security community. The inherited wisdom of that experience is that security requires separate explicit consideration.

Reliability as considered in airworthiness determination differs from computer security in another important way. The airworthiness of a system is considered in terms of its effect on overall flight outcome should the system fail. By way of example, FAA Advisory Circular (AC) No. 20–149A, which describes one means of gaining airworthiness approval for FIS-B avionics installed on aircraft, mandates that, "the effect of undetected errors in FIS-B products ... is no greater than a minor failure condition." A "minor failure condition" is one which does not significantly reduce aircraft safety and which involves crew actions well within their capabilities [16, Ch. 3]. Thus, airworthiness depends not only on the component itself, but also on the severity of the overall outcome *taking into account crew actions*.

For computer security analysis to be practically useful in determining airworthiness, we must reason about possible crew actions in response to (detected or undetected) attacks. In other words, to connect security results to airworthiness, we must connect MCIS output to pilot actions to overall flight safety. This is the second question we consider:

✻ **How does the security of mobile cockpit information systems affect flight safety?**

There are two ways to go about answering this question. The first is empirical, using experiments with pilots in a controlled setting. While this approach is the most reliable, it is cost-prohibitive and unlikely to be adopted by manufacturers or regulators.

The second approach is to work with a model of pilot decision-making. The simplest such model assumes, pessimistically, that a pilot will accept as correct all information presented to her by a compromised MCIS and act accordingly. Unfortunately, this line of reasoning leads one to conclude, for example, that nearly all navigation systems (GPS, VOR/DME, ILS) should not be used because they all are easily spoofed. The way out of this conundrum is to insist that the pilot rely on multiple sources of information to determine the true state of affairs. This point is worth emphasizing: modern aviation safety depends on pilots successfully reconciling possibly conflicting information presented by multiple sources. In this regime, the FAA considers current aeronautical information services (ADS-B, TIS-B, and FIS-B) supplementary in nature.

For example, AC 20–172A states, "The installation of ADS-B in avionics provides the pilot(s) with supplemental information." In this view, there is no harm in additional information, because pilots can optimally reconcile all information presented to them. By necessity, this must hold even when some sources are manipulated by an attacker. We believe this view is too optimistic: it is unreasonable to expect pilots to always correctly reconcile conflicting information presented by multiple systems. It becomes necessary, therefore, to consider pilot decision-making in order to assign potential outcomes to attacks on information systems.

We propose one way of modeling this decision-making process when an information system is under attacker control. We believe our approach may be useful in the analysis of similar systems. It is not a replacement, however, for empirical evaluation. Thus, our answer to the above question is only partial; however, we believe that it is a fruitful first step.

In Section 6 we evaluate several MCISes on the market today. Our analysis finds that under several scenarios an attacker with modest capabilities can exploit the weak security of these systems to cause catastrophic outcomes. The situation need not be hopeless, however. The third question we investigate is:

✻ **Can consumer mobile cockpit information systems be redesigned to satisfy the airworthiness requirements of comparable avionics systems?**

Our answer is a guarded yes, although concerns about the integrity of GPS and aeronautical information service signals themselves still remain. We make several recommendations for securing such systems, and we believe the proposals do not impose an undue burden on developers.

In summary, our contributions are:

- ❖ We define the security threats facing Mobile Cockpit Information Systems (MCISes) and develop a model for evaluating information systems where assessing the severity of potential attacks requires modeling a human operator.
- ❖ We analyze three existing MCISes. We find that all three allow an attacker to provide false information to the pilot; two of these systems allow an attacker to carry out a delayed or situation-triggered attack by replacing receiver firmware; all three are vulnerable to a malicious app installed on the tablet device.
- ❖ We provide recommendations for securing MCISes that would protect against the MCIS-specific vulnerabilities we identified. We believe our recommendations do not impose an undue burden on developers.

2. BACKGROUND

This work is about mobile cockpit information systems (MCISes) used by pilots as an aid to situation awareness during flight. MCISes are targeted at pilots in small general aviation aircraft that lack the sophisticated cockpit information systems found on larger and newer aircraft. Physically, an MCIS consists of two devices: an aeronautical information service receiver and a general-purpose tablet PC—most commonly an iPad. The receiver relays broadcasts from multiple aeronautical information services to the app, which presents the information to the pilot. Figure 3 illustrates these components, which we describe next.

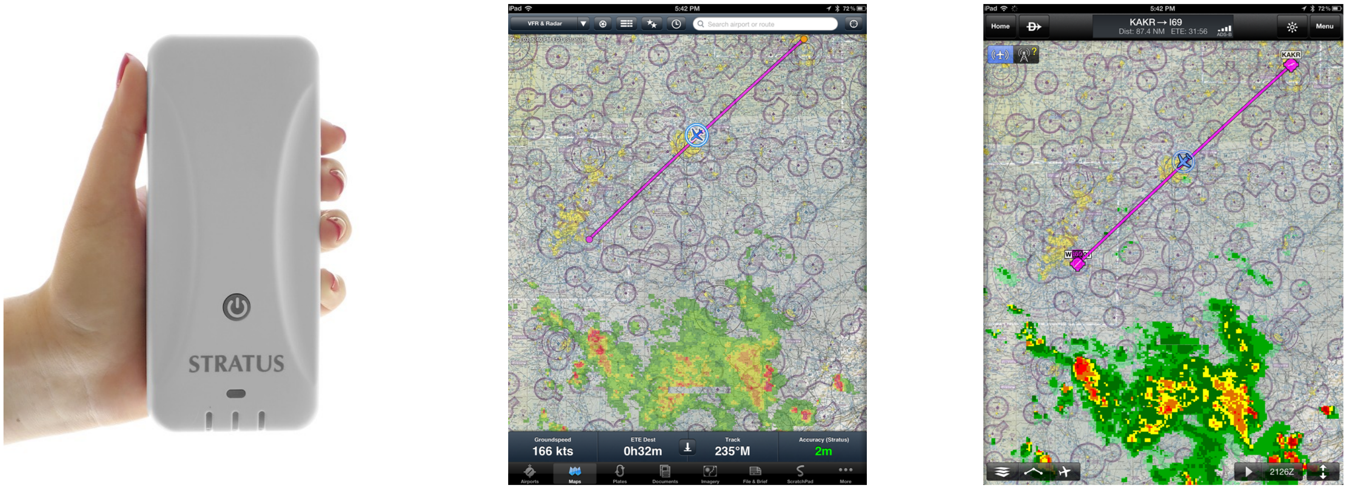


Figure 2: The Stratus 2 receiver (left), ForeFlight iOS App (center), and Garmin Pilot iOS app (right). The app is showing real-time weather against a US sectional aeronautical chart. The aircraft's position is shown as a blue plane along the magenta planned route. App screenshots Copyright 2012 Sporty's Pilot Shop, used with permission.

2.1 Aeronautical Information Services

Mobile cockpit information systems are built around three aeronautical information services.

2.1.1 GPS

Most readers are already familiar with the *Global Positioning System* (GPS), a satellite-based positioning system. GPS receivers are entirely passive, allowing the 32-satellite constellation to support an arbitrary number of users. GPS receivers provide horizontal accuracy down to one meter [25], making GPS an attractive alternative to the system of ground-based navigation aids still in wide use today.

Known vulnerabilities. The non-interactive (passive) nature of GPS makes it vulnerable to replay attacks. Moreover, the non-military navigation signal is unauthenticated, making spoofing possible. These shortcomings of GPS are well known, with results on GPS spoofing [27, 28, 38, 46, 51, 57, 59], software attacks on GPS [41], GPS cryptography [60], and more [3, 9, 11, 29, 31, 43, 47, 48, 52, 55, 61]. In this work, we do not address these attacks and proposed fixes. We note, however, that attacks on GPS require the attacker to transmit a GPS signal. Ground-based attacks against an airborne target would be detectable by nearby receivers.

2.1.2 ADS-B and TIS-B

Automatic Dependent Surveillance–Broadcast (ADS-B) is an aircraft position self-reporting system. An aircraft equipped with an ADS-B transmitter broadcasts its own position (obtained from a source such as GPS); aircraft equipped with an ADS-B receiver can display other aircraft to the pilot and issue collision avoidance warnings if necessary. The United States Federal Aviation Administration (FAA) has mandated that by 2020, all aircraft operating in airspace that today requires a transponder will be required to broadcast their position via ADS-B. The receivers considered in this work *do not* transmit ADS-B data; they only receive ADS-B from aircraft equipped to do so.

Traffic Information Service–Broadcast (TIS-B) is an aircraft position reporting system. TIS-B uses the same data format as ADS-B; however, TIS-B position information is broadcast by FAA ground stations in the United States and includes aircraft positions from radar-based aircraft tracking systems. As such, it provides a transition to ADS-B by allowing aircraft equipped with ADS-B to know about aircraft using a transponder only.

There are two data links used to disseminate ADS-B and TIS-B: Mode S Extended Squitter on 1090 MHz (1090ES) and Universal Access Transceiver protocol on 978 MHz (UAT). Both data links have a data rate of 1 Mbit/sec; however, 1090ES uses 112-bit packets while the UAT data link supports larger packet sizes, making it more suitable for larger messages. UAT is only used in the United States.

Known vulnerabilities. ADS-B and TIS-B services are provided over the 1090ES and UAT data links, neither of which is authenticated. Attacks on these services have been considered in the research community [7, 50, 54, 56]; Strohmeier et al. [54] provide an overview of this problem and propose a number of solutions. Like GPS attacks, these require a transmitter and may be detected by other receivers near the victim.

2.1.3 FIS-B

Flight Information Service–Broadcast (FIS-B) provides several kinds of real-time information, most notably graphical weather data. Like TIS-B, FIS-B is a free broadcast service provided by the FAA. Figure 2 (center and right) shows TIS-B weather data overlaid on an aeronautical chart. FIS-B also provides textual weather and time-sensitive pilot advisories.

Known vulnerabilities. Like ADS-B and TIS-B, FIS-B is transmitted over the unauthenticated UAT data link; it is, therefore, also vulnerable to spoofing.

2.2 Aeronautical Information Receivers

Availability of the services described above has created a market for devices capable of receiving and displaying this information. While it is possible to equip an aircraft with avionics capable of receiving and presenting this information on a cockpit display, an MCIS is a far cheaper alternative for doing so.

The portable aeronautical information receivers that are the subject of this work combine a GPS receiver and UAT receiver into a compact, battery-operated device. Many also incorporate a 1090ES receiver—all three receivers we examined do.

Some receivers also include an Attitude and Heading Reference System (AHRS) module, which provides aircraft attitude (pitch and roll) as well as magnetic heading using solid-state accelerometers and magnetometers. AHRS information is displayed in the style of a modern Primary Flight Display (PFD) and is marketed as a backup to primary flight instruments. The Stratus 2 unit shown in Figure 2 (left) is a battery-powered receiver incorporating a GPS, UAT, and 1090ES receiver and an AHRS module.

Nearly all receivers communicate with the tablet using either WiFi or Bluetooth. A wireless link reduces clutter and allows the receiver to be placed more conveniently inside the cockpit.

2.3 Aeronautical Information Apps

The receiver provides all information to an aeronautical information app running on the tablet. Modern aeronautical information apps evolved from *Electronic Flight Bags* (EFBs), electronic replacements for paper documents carried by pilots. An EFB includes aeronautical charts, approach plates, aircraft manuals, and checklists. EFBs replace several pounds of paper and provide an efficient interface to these documents. The simplest EFBs are nothing more than PDF viewers, while more sophisticated EFBs provide features such as interactive checklists.

Because they were already familiar to pilots, EFBs provided a natural place to add real-time data from aeronautical information services. The emergence of low-cost GPS receivers and the introduction of services such as ADS-B and FIS-B brought more kinds of information to what are now known by the general term *aviation apps*. Such applications promise to improve general aviation safety by providing pilots with more information to aid in-flight decision-making. There is a real danger, however, that pilots will come to rely on these apps while neglecting more basic skills. Such apps may also engender a false sense of security, leading pilots to cut corners in pre-flight preparation or to be less vigilant in flight [4, 15].

The problem of over-reliance on automation has garnered considerable attention in the aviation safety community. In this work, we take pilot reliance on an MCIS, to a greater or lesser degree, as given. From a computer security point of view, we would prefer to make these systems more secure rather than rely solely on a pilot's ability to make critical decisions under pressure.

2.4 Mobile Computing Environment

Aeronautical information apps run on ordinary consumer tablet PCs. By far the most popular choice is an iPad, although several aviation apps are available for Android also. Of the apps we examined, only Garmin Pilot has an Android version with the same functionality as the iOS version.

2.5 Government Regulations

In the United States, use of mobile computing devices in the cockpit is regulated by the FAA. The FAA has been open to the use of EFBs and has issued detailed guidance on their use [17–19]. Broadly speaking, portable EFBs, that is, EFB systems not integrated into the aircraft, do not require software certification. (Airborne software systems are normally certified to the RTCA DO-178B standard.) However, air carrier use of such EFBs requires FAA approval—use in general aviation does not.

Furthermore, EFBs used by air carriers are prohibited from showing "own-ship position." That is, they may not display the location of the aircraft on an aeronautical chart or procedure plate. General aviation use carries no such restriction, and indeed, all of the apps we examine provide "own-ship position." See Figure 2 (center and right). Regarding such use, the FAA only warns, "The EFB system does not replace any system or equipment (e.g. navigation, communication, or surveillance system) that is required by 14 CFR part 91" [17].

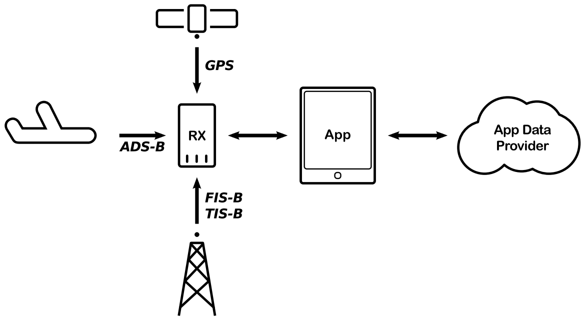


Figure 3: Components of a mobile cockpit information system.

3. RELATED WORK

To our knowledge, we are the first to consider the security of mobile cockpit information systems. With the rise of mobile computing devices, there has been considerable work on mobile security [2, 42], most of which has focused on security issues internal to the platform. In our security analysis, we lean on the numerous studies of mobile malware [22, 58, 65, 66] to motivate our malicious app attacker model (Section 4.2). The technique of using the mobile device itself to attack a peripheral was used by Frisby et al. [24] to attack mobile point-of-sale terminals.

Firmware update attacks have been used on printers [8], medical devices [26], batteries [35], voting machines [1], among others.

Attacks on Bluetooth and WiFi are too numerous to mention. Integrity attacks on GPS and ADS-B have already been discussed in Section 2.1.

4. SECURITY MODEL

In this section, we describe the MCIS threat model. Our motivation is an attacker intent on disrupting the flight of a particular aircraft. An attacker can attack a target *directly* by manipulating information presented by the MCIS to the pilot of the target aircraft. This is the mode of attack implicit in most of the scenarios we describe in Section 5. An attacker can also attack the target indirectly by manipulating information presented to pilots of nearby aircraft. In this regime, the aircraft with the compromised MCIS becomes a guided weapon used to attack another aircraft.

We begin our security analysis with a description of the attack surfaces of an MCIS.

4.1 Attack Targets

An MCIS is made up of several discrete components linked by communication channels, illustrated in Figure 3. The receiver, app, tablet, and aeronautical information services have already been described in Section 2. The remaining service, the App Data Provider, is a subscription service providing up-to-date information not disseminated via the aforementioned aeronautical information services. (In all cases we examined, the App Data Provider is the same as the app developer.) This additional information, which includes the aeronautical charts and procedure plates displayed to the pilot, is updated on the ground, over a normal Internet connection.

An attack on an MCIS entails attacking one or more of the components or channels shown in Figure 3. We describe possible attacks against each channel or against the receiver or app directly, what an attacker might gain from each, and the steps necessary to protect it. We do not discuss attacks on the information services (GPS, ADS-B, TIS-B, FIS-B) themselves, which have been considered in prior work (see Section 2.1). Instead, we focus on attacks unique to the MCIS platform.

Table 1 lists the information provided by an MCIS, along with the conventional source of each piece of information. A successful attack would allow an attacker to control or deny access to one or more of these variables. Our next task is to define how a successful attack on a component or channel would affect these variables. In Section 5 we consider scenarios in which an attacker controls one or more of these variables, and the potential outcome of such attacks.

We consider only attacks on the *integrity* and availability of a component or communication channel. Attacks on *secrecy/privacy* are less of a concern, because most of the information involved is not confidential in nature. We also note that we do not consider issues of receiver or app *reliability*, a distinct but separate concern in an environment like an aircraft cockpit.

Receiver to App channel. In all three of the MCISes we examined, the receiver communicates with the app on the mobile computer wirelessly, using either Bluetooth or WiFi. With the exception of EFB data, which is preloaded before flight, all information presented to the pilot must be sent over this channel. The channel may also be used to control some functions of the receiver and to send firmware updates to the device.

The simplest class of attacks involves denying access to the channel (e.g., by jamming). This would deny the pilot access to everything except EFB data. However, such an attack is easily detected, although it may be misattributed to receiver failure. A more subtle attack would be to *selectively* deny access to specific information; this attack would require the channel to be unencrypted or vulnerable to packet timing/size attacks. In the absence of proper authentication, an attacker could tamper with all information sent over this channel. Finally, in the absence of replay protection, the channel would be vulnerable to selective replay of old information.

App to Internet channel. This channel is used to retrieve EFB information as well as app updates and receiver firmware updates.

By denying access to this channel, an attacker would be able to prevent EFB updates and potential security-related firmware updates. If a failure to update EFB data is not properly indicated, the pilot may be unaware she is lacking important flight information.[1] In the absence of proper authentication, an attacker could tamper with EFB data.

Receiver. The receiver provides the app with non-EFB information shown in Table 1. Attacks on receiver availability are similar to attacks on the receiver to app channel availability; however, in some cases, they may be easier to carry out (e.g., via battery drain attacks).

A successful attack on receiver integrity is much more serious. An attacker would be able to impersonate the receiver, and thus provide arbitrary non-EFB data to the app. Reflashing device firmware is the most common means of compromising device integrity, and this is the most serious attack we consider in Section 6. However, reflashing alone does not automatically imply integrity compromise, if the app *validates the authenticity of the data from the receiver*. Unless the attacker can also learn the keying material used by the legitimate firmware to sign updates, reflashing alone will only result in a denial of device availability.

App and tablet PC. The tablet is the sole MCIS interface to the user. A successful attack on app availability would deprive the pilot of all MCIS information. Compromising app or tablet PC integrity would give an attacker complete control over information presented to the pilot. This is the most serious attack on an MCIS. Fortunately, recent progress in mobile platform security, most notably code signing, has made such attacks difficult. Nevertheless, security problems still remain. Compounding the problem is that in many cases, the tablet PC may be used for non-aviation purposes, exposing it to additional malware risks.

4.2 Attacker Model

An attacker's ability to carry out attacks on parts of the MCIS described above depend on the attacker's technical capabilities. We consider five classes of attacker defined by the level of access to the MCIS under attack. We assume that an attacker has the technical skills and equipment of a properly motivated graduate student, and is only limited by his access to the target MCIS. These five types of access are:

Brief proximity. Brief proximity is the weakest class, granting an attacker brief physical proximity to the receiver for a few minutes while the receiver is powered. This allows the attacker access to the wireless communication channels, which he may use to gain lasting control over the MCIS. Such access might be arranged while the pilot is preparing for flight on the ground. A properly secured receiver to app communication channel and properly implemented aeronautical information service receiver components can protect against such an attack.

Brief access. Brief access grants an attacker physical access to the receiver for a few minutes. Brief access implies brief proximity. Physical access is a fairly powerful capability that includes the ability to replace the device with an attacker-controlled facsimile or render the MCIS inoperable. To defend against such an attack, the app must be able to detect receiver tampering. (See discussion of receiver integrity in Section 4.1.) The pilot should also have a way of detecting tablet PC tampering or replacement.

Time-of-use proximity. Time-of-use proximity grants an attacker physical proximity to the MCIS while it is in use. Practically, this requires either a tracking directional antenna or the ability to plant a device on the aircraft. Time-of-use proximity implies brief proximity. At a minimum, an attacker with time-of-use proximity can jam all communication links, denying access to all real-time information.

Update man-in-the-middle. An attacker with update man-in-the-middle capability has control over the Internet connection between the tablet and the app data provider. Such access might be arranged by enticing the user to use an attacker-controlled WiFi access point. At a minimum, a man-in-the-middle attacker can deny the app access to the app data provider. A properly secured channel between app and app data provider would prevent tampering with EFB data and any receiver firmware updates sent to the app.

Collocated app. The collocated app capability allows an attacker to install an app on the tablet device. We assume the attacker can arrange for the app to be executing when the device is in use. (See Section 6.5 for a description of the demonstration attack app we developed.) An attacker might gain such a capability through social engineering, by exploiting a vulnerability in the tablet operating system, or by gaining control of an already installed app.

In the ideal case, any combination of the above capabilities would allow an attacker no more than the ability to deny use of the MCIS. If the necessary security measures are absent or are not implemented properly, an attacker could gain the ability to tamper with MCIS data presented to the pilot.

[1] At least one incident in the Aviation Safety Reporting System (ASRS) database describes a pilot violating airspace flight restrictions because of a silent update failure (ACN 1091530).

Variable	*MCIS source*	*Conventional source*
Altitude	GPS	**Altimeter**, ATC, visual
Attitude	AHRS	**Attitude indicator**, visual
Heading	AHRS	**Heading indicator**, compass
Position	GPS	VOR/ILS/DME ind., ATC, visual
Alt. setting	FIS-B	ATIS/ASOS/AWOS, ATC, brief
Wx (general)	FIS-B	ATIS/ASOS/AWOS, ATC, brief
Wx (spatial)	FIS-B	Visual, brief
Other aircraft	ADS-B/TIS-B	Visual, ATC
Procedures	EFB	Printed procedures
Terrain	EFB	Printed charts

Table 1: Elements of situation awareness provided by an MCIS and conventional sources of the same information. Sources that are both continuous and direct are shown in boldface.

5. RISK ASSESSMENT

What happens when an attack against an MCIS succeeds? In this section, we consider the impact of a successful attack on flight safety. Most attacks on safety-critical systems considered by the research community have attacked a control system, which give an attacker direct control over the controlled process. Our case is different. An MCIS is an *information* system without direct control of the aircraft. By gaining control over an MCIS, an attacker gains control over the information presented to the pilot; it is up to the pilot to act on that information.

We reason about the effect of such attacks in the framework of *Hazard Analysis*. The flavor we use is most closely aligned with the FAA's usage [20, Appendix C]. (Stamatis [53] provides a more general introduction to Risk Analysis and the elements used here.)

In our context, a *hazard* is a successful attack resulting in attacker-controlled information being presented to the pilot by the MCIS. A hazard *scenario* is a sequence of events leading from the hazard to an undesirable system outcome. With each scenario, we associate a *likelihood* and a *severity*; the combination of the two is often termed the *risk* associated with the scenario. Likelihood, which may be quantitative (e.g., a probability) or qualitative, is the likelihood of the undesirable outcome *given* the hazard. That is, the attack on the MCIS is assumed to succeed, allowing the attacker to control some of the information displayed by the MCIS. The environmental conditions are fixed by the scenario. The likelihood is understood to be over all general aviation pilots and their preferred aircraft.

An alternative approach, described in NIST's *Guide for Conducting Risk Assessments: Information Security* is to include the likelihood of attack initiation in an overall information security risk assessment of an organization or system. This requires "taking into consideration capability, intent, and targeting" [39]. We know of no way to meaningfully assign a likelihood to an attacker initiating an attack in the general case. Our analysis is, therefore, concerned only with the likely outcome of an attack, and not the likelihood of the attack itself. We use a likelihood scale with five discrete levels denoted, from most to least likely: *frequent* (expected to occur routinely), *probable* (expected to occur often), *remote* (expected to occur infrequently), *extremely remote* (expected to occur rarely), and *extremely improbable* (not expected to occur, but not impossible). Severity is also classified into five discrete levels, denoted, from most to least severe: *catastrophic* (multiple fatalities), *hazardous* (multiple serious injuries or fatal injuries to a small number of persons, or a hull loss without fatalities), *major* (physical distress or injuries, substantial damage to aircraft), *minor* (physical discomfort, slight damage to aircraft), *minimal* (negligible safety effect).

In the following, we consider several scenarios attacking the information presented by an MCIS. For each, our goal is to assign a likelihood and severity score. The ideal means of determining likelihood and severity is empirical through high-fidelity controlled experiments measuring pilot response to data tampering scenarios. Unfortunately, such experiments are beyond the capabilities of most computer security researchers. The alternative is a qualitative assessment based on our own judgement. This is the approach we take here. Our assessment of likelihood is subject to disagreement, which an aviation safety expert may judge to be greater or lesser than what we determine.

The scenarios are structured around two critical events we term *detection* and *selection*. In each scenario, an attacker manipulates some subset of variables presented by the MCIS to the pilot. Detection occurs if a pilot notices a discrepancy between the MCIS-reported datum and the same datum obtained from another source. Having noticed the discrepancy, a pilot is faced with a choice of which source to trust. At this point, the pilot must reject either the MCIS-supplied information controlled by the attacker or the refuting source providing accurate information. We call this decision point the *selection* of one or the other data source.

5.1 Detection and Selection Factors

Detection and selection are influenced by a number of factors. These factors form the basis of our likelihood assessments. Throughout, we refer to the (correct) information that contradicts MCIS-supplied information as *refuting information* and its source as the *refuting source*.

Exposure. The first, and probably most important, factor affecting detection is operator exposure to refuting information. We classify exposure as *continuous* or *request-driven*. Continuous information is presented to the operator at all times; it includes altitude (via altimeter), attitude (via attitude indicator), and heading (via heading indicator and compass). Request-driven information requires an explicit, discrete acquisition action. This includes information such as the local altimeter setting, which is obtained from air traffic control (ATC) or an automated station (ATIS/ASOS/AWOS). A discrepancy in continuously available information is significantly more likely to be detected than a discrepancy in information that requires operator action to obtain.

Cognitive complexity. Refuting information may be *direct* or *indirect*. Direct information is information that, once available, requires no additional cognitive processing to detect a discrepancy. An altitude obtained from an MCIS and from the altimeter can be readily compared. The same is true for attitude, heading, altimeter setting, general weather information, presence of other aircraft, approach procedures, terrain and obstacle information.

Conventional sources of aircraft position may be direct or indirect. In familiar terrain and good visibility, a pilot can directly observe her position. When radar service is available, ATC is another direct source of position information, as long as the pilot is in communication with the controller. The instrument landing system (ILS) also provides direct position information in the form of course deviation, however, it is only available on final approach. Terrestrial navigation aids, such as VOR and DME, when used to navigate along airways, provide direct position information in the form of a course deviation. However, when not configured to follow a pre-determined course, these instruments do not directly indicate aircraft position.

Weather data comes in many forms. Simple variables, such as cloud ceiling and visibility, can be directly compared between those reported by an MCIS and those obtained from a weather observation recording. On the other hand, spatial weather information, as obtained from a graphical weather overlay, cannot be directly compared to information received during a pre-flight briefing or from direct visual observation.

The presence of another aircraft reported by an MCIS can be confirmed visually, however the absence of an aircraft cannot be directly established with certainty.

Workload. Operator workload has been found to adversely affect fault detection and mitigation in many domains [13, 14, 62]. Attacks during high-workload stages of flight (take-off and landing) significantly increase risk.

Trust and preference. A operator's trust of automation, and the MCIS in particular, plays an important role in both detection and selection phases. In the detection phase, trust will determine how often a pilot will check MCIS-reported information against conventional sources. In the selection phase, a pilot must decide whether to accept information from the MCIS or from the refuting sources, a determination that will rely heavily on trust.

Trust in automated systems, both information and control, is an active area of study in the Human Factors community. Experiments have shown that trust increases with reliability [10, 12, 30, 64]. Thus, the more reliable a system is in normal operation, the greater the potential for damage when the system is compromised.

Trust in automated systems has also been found to be *inversely* proportional to operator self-confidence. The less confident an operator is in her own skills (especially when refuting information is indirect), the more likely she is to trust the automated system [10, 32, 45].

Automation bias is the term given to increased reliance on automated systems, which can lead to reduced crew vigilance [4, 33, 36, 44]. Automation bias, however, is not universal; in some studies, operators were found to place greater trust in conventional systems [37].

Finally, even when one system is not considered more reliable than another, a pilot may continue to rely on a faulty instrument despite evidence that it is unreliable. (This was the case in at least two major aviation accidents—Korean Air Cargo flight 8509 on December 22, 1999, and Copa Airlines flight 201 on June 6, 1992.)

Experience. More experienced operators generally fare better in many decision-making tasks, and we expect our setting to be no different. Experience also attenuates the effect of factors such as workload and operator confidence.

Environment. Environmental factors, notably, weather, will affect a pilot's ability to rely on visual references, eliminating a major source of refuting information.

5.2 Scenarios

With these factors in mind, we consider seven scenarios in which an attacker tampers with some combination of variables presented by an MCIS (Table 1). For each scenario, we assign a likelihood. We rely on our own judgement, necessarily imperfect, to make this determination. Aviation safety experts may disagree on the likelihood of each outcome.

5.2.1 Altitude and attitude

In this scenario, an attacker manipulates reported altitude and attitude (pitch and roll) information displayed by the MCIS. Both are critical flight parameters. Incorrect perception of altitude, attitude, or speed is termed *spatial disorientation*; unless remedied immediately, spatial disorientation rapidly leads to catastrophic outcomes.

Severity. The severity of this outcome is catastrophic.

Likelihood. Both altitude and attitude can be directly determined from primary flight instruments, which provide a continuous indication of both. Therefore, we consider a failure to detect a hazardous condition and select the correct instrument to be remote to extremely remote.

5.2.2 Position (cruise)

In this scenario, an attacker tampers with the reported position of the aircraft in the cruise stage of flight. This scenario encompasses a family of scenarios varying in how long it takes the pilot to detect deviation from expected position.

Severity. In poor visibility, a pilot may not realize at all that she has deviated from the intended course, resulting in controlled flight into terrain or mid-air collision, both catastrophic outcomes. Scenarios in which a pilot becomes aware of her incorrect position past the point at which an airfield landing can be made range in severity from minor to catastrophic, while recognizing deviation from the intended course early, allowing for a normal landing, has minimal to minor severity.

Likelihood. The likelihood of detection and selection of correct information source depends on a number of factors. The most significant is whether the pilot is navigating primarily by visual reference to terrain (VFR – Visual Flight Rules) or by relying on navigation instruments (IFR – Instrument Flight Rules).

A pilot monitoring conventional navigation instruments and communicating with air traffic control is both more likely to detect a problem and correctly choose conventional instruments. We consider the likelihood of the late recognition scenario to be remote to extremely remote in IFR flight. Unfortunately, only 28% of private pilots in the United States are licensed to operate under IFR.[2] Moreover, less experienced pilots are more likely to trust automation, so that, even when a pilot detects a problem, she may continue to rely on the MCIS-provided GPS data.

For VFR flights in poor visibility and hazardous terrain, we judge the likelihood of the pilot relying on incorrect position with catastrophic outcome to be remote to probable.

5.2.3 Position (approach)

In this scenario, an attacker tampers with the reported position of the aircraft on approach. While similar to position tampering in cruise considered above, approach to landing presents its own unique challenges. Among them: increased workload and narrow error margins because of proximity to terrain and other aircraft. On the other hand, on final approach, a pilot may rely on visual references (runway and visual approach slope indicator lights) or the Instrument Landing System (ILS) than on the MCIS.

Severity. Position error on approach can result in controlled flight into terrain or a mid-air collision, both catastrophic outcomes.

Likelihood. In a scenario with poor visibility, no ILS, and hazardous terrain, we judge the likelihood of catastrophic outcome to be remote to probable.

5.2.4 Die Hard 2

In the classic action film *Die Hard 2*, the villain causes an aircraft to crash on final approach when he issues the order to "recalibrate sea level . . . minus two hundred feet." In an MCIS version of this attack, an attacker tampers with the altimeter setting shown to the pilot in a METAR, a textual weather report that includes this variable. The altimeter setting is used to calibrate a barometric aircraft altimeter.

[2] Based on 2012 data reported by the FAA: http://www.faa.gov/data_research/aviation_data_statistics/civil_airmen_statistics/2012/

Severity. An incorrect altimeter setting will result in an incorrect altitude displayed on the conventional altimeter, which can lead to a catastrophic outcome.

Likelihood. The primary source of the altimeter setting is a prerecorded terminal information (ATIS) message or an automated weather (ASOS/AWOS) report and airport tower air traffic controllers will often repeat the altimeter setting when clearing an aircraft to land. Thus, we believe the likelihood of this scenario to be extremely remote.

5.2.5 Weather

Weather information, both textual and graphical, affects a pilot's navigation-related decisions. A pilot not equipped to fly in poor weather can be led into such conditions by erroneous weather information. According to the FAA, "twenty five percent of all weather-related accidents are fatal and a failure to recognize deteriorating weather continues to be a frequent case or contributing factor of accidents" [21]. In poor weather conditions, a pilot is likely to turn to the MCIS to determine whether to continue flight and how to navigate around bad weather. The graphical weather display (e.g., Figure 2, right) presents highly salient weather information which is not available from any other conventional source in the cockpit.[3] In this scenario, the attacker is also aided by the psychology of pilots flying in poor weather. General aviation pilots have a well-established pattern of flying into deteriorating weather conditions [4, 5, 40, 63], an effect that is positively correlated with flight duration (more likely at end of long flight) and negatively correlated with experience.

Severity. Clearly, incorrect weather information can lead to catastrophic outcomes.

Likelihood. Pilots are likely to rely on weather information presented by an MCIS. However, the likelihood of this reliance leading to a catastrophic outcome is difficult to estimate, because it depends on the weather conditions and pilot experience.

5.2.6 Position of other aircraft

There are three types of attack on aircraft position information obtained from ADS-B/TIS-B. In the first attack type, an attacker can suppress information about other aircraft. However, pilots do not rely on ADS-B/TIS-B for aircraft identification, both as a matter of training, and because this feature is explicitly advertised as incomplete.

The second type of attack involves adding false targets to the display. Because of the possibility of a collision, a pilot is likely to accept MCIS information. While we judge the likelihood of this happening to be frequent, the severity is minimal to minor. We consider the scenario in which a false target causes a deviation resulting in an accident to be extremely remote. Moreover, trust of an automated system deteriorates rapidly when it shows itself to be unreliable. After a few false targets, we expect pilots to place little weight on MCIS-reported aircraft.

The third type of attack involves changing the reported position of an existing target. An adversarially-chosen change in target position could result in a pilot deviating *toward* the target to avoid collision.

Severity. The outcome severity of a mid-air collision is catastrophic.

Likelihood. The likelihood of a mid-air collision caused by suppression of ADS-B/TIS-B data is, therefore, extremely remote to extremely improbable. However, under the right circumstances—reduced visibility and proximity to another aircraft—the likelihood of a catastrophic outcome in the last scenario is probable. While an attacker may not have the ability to arrange such circumstances, he can wait for them to occur naturally.

5.2.7 Terrain and procedures

In this scenario, an attacker modifies critical information on an aeronautical chart or approach plate. Obstacle elevations, navigation aid frequencies, procedure altitudes can all result in a catastrophic outcome. The *Die Hard 2* attack can also be carried out by modifying the altitudes on an instrument approach plate. Such an attack is particularly dangerous because directly refuting information is only available from another chart or plate. Pilots are unlikely to check for this discrepancy. The remaining source of refuting information is visual observation and air traffic control, the second of which is not always available.

Severity. The outcome of this scenario—controlled flight into terrain—is catastrophic.

Likelihood. In poor visibility, we judge the likelihood of an catastrophic outcome to be probable to remote, largely dependent on a pilot's familiarity with the terrain.

5.3 Summary

The manipulation of weather, own-ship position, position of other aircraft, and EFB information introduces significant risk. The likelihood of most attacks having an undesirable outcome increases greatly in poor weather, which limits a pilot's access to visual refuting information. A pilot relying on an MCIS in reduced visibility faces significant risk if the MCIS is compromised by a malicious adversary.

6. ANALYSIS OF EXISTING SYSTEMS

In this section we evaluate three existing MCISes, consisting of an iOS app and a receiver: ForeFlight with the Appareo Stratus 2, Garmin Pilot with the Garmin GDL 39, and WingX Pro7 with the Sagetech Clarity.

6.1 ForeFlight with the Appareo Stratus 2

ForeFlight is the most popular iOS aviation app. The FAA has recently approved the use of ForeFlight as a class 2 EFB (Section 2.3) on all Frontier Airlines flights [23]. ForeFlight only works with two models of UAT receivers, the first-generation Stratus and the Stratus 2, both made by Appareo.[4] The app requires a $74.99 per year subscription, which includes FAA aeronautical charts and a number of real-time weather products retrieved while the device has an Internet connection. Our evaluation is based on version 5.6 of the ForeFlight app.

The Appareo Stratus 2 (Figure 2, left) is the second generation of the Stratus device. Both the first generation Stratus and the Stratus 2 only work with the ForeFlight app. The Stratus 2 costs $899 and incorporates a GPS receiver, 1090ES receiver, UAT receiver, and an AHRS module. The Stratus 2 communicates with the iPad via WiFi in infrastructure mode by acting as an access point. The user configures the iPad to connect to this access point in order for the ForeFlight app to receive data from the unit. Our Stratus 2 was running firmware version 1.3.0.389.

[3] Satellite radio subscription services that provide graphical weather information are available, many using mobile apps for display, however, we assume a pilot will only rely on the MCIS weather display.

[4] ForeFlight also interacts with XM weather services and several other GPS-only devices.

6.1.1 Receiver to App Channel Integrity

The Stratus 2 receiver sends information to the app via UDP broadcast on its WiFi network. All data is broadcast unencrypted and unauthenticated using a proprietary, but easy to reverse-engineer, protocol. The ForeFlight app ensures that it is communicating with the Stratus 2 unit by checking the SSID and IP address subnet assigned by the AP. We were able to impersonate the receiver and inject arbitrary information, which the app accepted and displayed.

We could also concurrently connect a malicious device to the Stratus 2 and broadcast data to the same broadcast address used by the Stratus 2 itself; the Stratus 2 (acting as an access point) relayed our forged data to the iPad. This behavior can be exploited by a malicious app to inject spoofed packets into the receiver to app channel. With this attack, the iPad receives both legitimate and forged data. However, because the user interface is updated at fixed intervals, an attacker sending forged messages immediately after the Status 2 itself will cause the app to immediately overwrite the correct data.

We were thus able to inject arbitrary data into the receiver to app channel, including invalid and inconsistent data, which the app displayed. Such an attack can be carried out with a concealed device on board the aircraft during flight, or using a transmitter of sufficient power outside the aircraft. Once an AP association has been established, it is possible to inject packets surreptitiously without the need to receive packets transmitted by the Stratus 2 AP.

Vulnerability. An attacker with time-of-use proximity or collocated app capability can manipulate all receiver-originated data.

6.1.2 App to Receiver Channel Integrity

The reverse channel, from app to receiver, is also neither encrypted nor authenticated. The app (and, therefore, the attacker) can adjust 802.11 transmitter power level and indicator LED brightness.

Vulnerability (minor). An attacker with time-of-use proximity or collocated app capability can modify some receiver settings.

6.1.3 EFB Data Integrity

The ForeFlight app downloads subscription data using an SSL connection. The app did not accept self-signed certificates. We were unable to tamper with this data.

6.1.4 Receiver Integrity

Receiver firmware can be updated using the ForeFlight app when connected to the Stratus 2. The firmware is packaged with the app and updated with the app. Although it is possible to extract the firmware from the app bundle as well as to capture it during an update, the firmware image itself is encrypted or scrambled, which we failed to break with a modest reverse-engineering effort.

Vulnerability. An attacker with brief proximity or collocated app capability can downgrade receiver firmware.

6.2 Garmin Pilot with the Garmin GDL 39

The Garmin Pilot app provides features similar to ForeFlight. It interoperates with the Garmin GDL 39 receiver and Garmin GLO GPS-only receiver. Garmin Pilot requires a $75 subscription. We evaluated Garmin Pilot version 6.0.1.

The GDL 39 receiver costs $599 and incorporates a GPS receiver, 1090ES receiver, UAT receiver. (A more expensive model, the GDL 39 3D, also includes an AHRS module.) Unlike the Stratus 2 or the Clarity, the GDL 39 communicates with the iPad using Bluetooth. The Bluetooth link uses RFCOMM, which provides RS-232 emulation over a Bluetooth link. Our unit had firmware version 2.80.

6.2.1 Receiver to App Channel Integrity

When the Garmin Pilot app connects to the receiver, the two devices engage in a handshake. The receiver sends a nonce and a key to the app; the app then encrypts the nonce 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. We suspect that this unusual algorithm is meant to mutually authenticate the app and receiver. The code to carry out this process in included in the app and the receiver firmware image; it was extracted by a hobbyist and posted on the Web.[5] We did not attempt receiver to application attacks; however, we believe it is possible to impersonate the receiver (requires time-of-use proximity).

6.2.2 App to Receiver Channel Integrity

We were able both to passively listen on this channel using a script written by the aforementioned hobbyist and to spoof requests from the app to the receiver. We were also able to determine the address of the GDL 39 wirelessly via sniffing and then connect to the device without pairing.

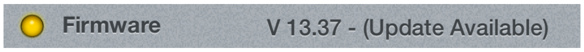
6.2.3 EFB Data Integrity

The Garmin Pilot app updates its documents and charts over HTTP. We were able to modify the aeronautical charts retrieved by the app and presented to the pilot. Other communication (i.e., weather and flight plan filing) was carried out over HTTPS. The app did not accept self-signed certificates.

Vulnerability. An attacker update man-in-the-middle capability can tamper with EFB data use by the app.

6.2.4 Receiver Integrity

The GDL 39 firmware can be updated via Bluetooth using the Garmin Pilot app or a GDL 39 utility app. Because the receiver communicates with the iPad using the Bluetooth link, the iPad can remain connected to the Internet while communicating with the GDL 39. The firmware update relies on this: both the Garmin Pilot app and the GDL 39 Utility app check for new firmware when connected to the device and an Internet connection is available. All update-related communication is unencrypted and unauthenticated; we were able to redirect both apps to download our own firmware image:



● Firmware V 13.37 - (Update Available)

Vulnerability. An attacker with brief proximity, collocated app, or update man-in-the-middle capability can install arbitrary receiver firmware.

6.3 WingX Pro7 with the Sagetech Clarity

WingX Pro7 is an independent app that interoperates with eleven different UAT receivers. WingX Pro7 requires a $99.99 per year subscription. It provides FAA aeronautical charts and a number of real-time weather data products retrieved while the device has an Internet connection. We evaluated WingX Pro7 version 7.1.2.5 with the Sagetech Clarity UAT receiver.

The Sagetech Clarity CL01 UAT receiver costs $1,150 and incorporates a GPS receiver, 1090ES receiver, and UAT receiver. (The CL02 model includes an AHRS module and costs $250 more.) The Clarity unit communicates with the iPad via WiFi in ad-hoc mode. The Clarity uses a message format very similar to the Garmin GDL 90 Data Interface Specification. In addition to this format, it includes messages with information about the current firmware, the serial number, and device status.

[5] http://www.chartbundle.com/tech/gdl39/

6.3.1 Receiver to App Channel Integrity

The Clarity receiver transmits all data unencrypted and unauthenticated. The WingX Pro7 app checks that the IP address subnet is correct, but performs no other device authentication. As with the Stratus 2 and ForeFlight app, it is possible to impersonate the Clarity device to the WingX Pro7 app and to inject packets into the channel. We were successful in doing both.

Vulnerability. An attacker with time-of-use proximity or collocated app capability can manipulate all non-EFB data.

6.3.2 App to Receiver Channel Integrity

The Clarity is unique among the three devices we examined in that it does not receive any data from the app. A user cannot adjust any internal settings or trigger a firmware update using the app. Firmware updates require connecting the Clarity unit to a PC via USB.

6.3.3 EFB Data Integrity

All app data is retrieved unencrypted over HTTP, except for monetary transactions, which are done through the Apple App Store. We were able to modify the aeronautical charts and other information retrieved by the device.

Vulnerability. An attacker update man-in-the-middle capability can modify EFB data use by the app.

6.3.4 Receiver Integrity

To update the firmware on the Clarity, the unit must be connected to a Windows PC via USB. The firmware can then be updated using the Sagetech Clarity Firmware Update application. The firmware image is bundled with the application itself; updating the firmware requires downloading a new version of the Update application. The update itself relies on the standard USB DFU protocol. While the DFU protocol standardized how data is transferred over USB, it does not specify a format for the update image, treating it as a sequence of bytes only. In the case of the Clarity, the firmware image is not encrypted or authenticated. We were able to update the Clarity firmware with a modified firmware image.

Modifying with device firmware requires either physical access to the unit or the ability to modify the Update application, either on the user's PC or while it is being downloaded. The Firmware Update application is downloaded from Sagetech over HTTP; HTTPS is not supported.

Vulnerability. An attacker with brief access or update man-in-the-middle capability can install arbitrary receiver firmware.

6.4 Malicious Firmware Attack

To demonstrate attacks on receiver integrity on the Sagetech Clarity and the Garmin GDL 39, we developed a modified firmware image for each. The modified firmware perturbs GPS coordinates within 20 miles of an "attractor," so that a pilot attempting to fly in a straight line through the area is led to deviate toward the center. We were able to install the malicious firmware on both the GDL 39 (via brief proximity) and the Clarity (via brief access or update man-in-the-middle tampering).

6.5 Malicious Collocated App Attack

We also developed a malicious iOS app that carries out two attacks. In the first attack, the malicious app impersonates Stratus broadcasts to the ForeFlight app, causing it to display incorrect data. In the second attack, our app downgrades the Stratus 2 firmware. The first attacks requires the app to run in the background while the ForeFlight app is running, while the second attack does not require the app remain running after the downgrade.

We also developed an Android[6] app attacking the GDL 39. Our app updates the GDL 39 firmware without user knowledge (see Section 6.4). This attack requires the app to be launched when the GDL 39 receiver is powered and paired with the Android device.

Gaining the collocated app capability necessary to carry out the above attack can be achieved by tricking the user into installing an app on her device. There are several ways of doing so: by developing a new app users might be lured into trying (and, for the first two attacks, keeping) or by cloning a popular app (e.g., Flappy Bird) [34]. An attacker can also buy an existing app and its user base from the app developer, and then release an update with the attack functionality.

7. RECOMMENDATIONS

The attacks described in Section 6 can be prevented by following well-established secure design recommendations described in prior work on similar systems [6, 49].

7.1 Receiver to App Channel

Data sent from the receiver to the app should be signed by the device. Device private keys should be stored in non-volatile memory only accessible by the signed code. (Most modern SoCs provide secure non-volatile memory storage, as well as AES hardware.) Furthermore, each receiver should have its own private key, so that even if a private key is extracted from one device, it cannot be used in another.

Pairing. The receiver and app should be paired, and the app should only accept data from the receiver to which it has been paired. Pairing should always require explicit user interaction.

Replay protection. The data authentication scheme should also protect against replay, for example, by using a nonce randomly generated by the app and a message sequence number. The receiver should also generate periodic, time-stamped heartbeat messages. The app should ensure that the message time stamps are within the expected period, allowing for a small amount of clock drift.[7] This prevents an attacker from significantly delaying information from the receiver.

Preventing selective denial. In Section 4.1 we pointed out the possibility that an attacker could attempt to selectively block certain messages. With both WiFi and Bluetooth protocol stacks, it is possible to arrange reliable, in-order message delivery to the application layer. Therefore, an application should not silently drop messages that fail to authenticate and should not ignore gaps in the message sequence numbers, as this indicates adversarial message tampering, rather than natural transmission errors.

7.2 App to Receiver Channel

Any receiver configuration changes sent by the app to the receiver should be signed by the paired app (see Pairing above). The same session nonce and sequence number mechanism should be used as for the receiver to app channel. Pairing should should require user input, for example, pressing the power button rapidly three times.

7.3 Firmware Updates

[6] While we developed the app for the Android platform, there is no technical reason why a similar app could not be developed for iOS.

[7] Many tablet PCs have a built-in GPS receiver, which can eliminate the need to compensate for clock drift.

Firmware updates should be signed by the developer. The signature should be checked by a secure bootloader. Ideally, program flash should be large enough to hold two firmware images, so that, should an update fail, the bootloader could load the previously working image.

It is advisable for the bootloader to be able to handle revocation of the public developer key used to authenticate firmware images.

7.4 EFB Updates

EFB updates should be signed by the app data provider. Most aeronautical data has a pair of "effective from ... to" dates. These should be used to prevent an attacker from downgrading aeronautical data. Ideally, the entire FAA to MCIS supply chain should be secured. However, to our knowledge, the FAA does not digitally sign the aeronautical data it provides. At the very least, the aeronautical data provider should download the data from the FAA site using HTTPS to prevent man-in-the-middle tampering.

7.5 Aeronautical Information Services

The security issues of today's aeronautical information services have been discussed in prior work (see Section 2.1). We hope that these problems will be remedied in the future. When this happens, MCISes should be updated to authenticate the information received via these services.

7.6 Security-Aware Software Development

The vulnerabilities described in Section 6 resulted from a failure to consider security threats in the design of the MCIS. We did not look for traditional programming errors, such as buffer overflows, because we did not need to: design flaws alone were sufficient to successfully attack these systems. MCIS developers should also ensure that their software development practices do not undermine the security of their systems.

8. CONCLUSION

We motivated this work with the question: Do mobile cockpit information systems provide the security guarantees expected of similar avionics systems? Our examination of three of the most popular systems showed that the answer is No. Existing systems allowed an attacker to compromise system integrity in multiple ways, allowing attacker-controlled information to be presented to the pilot. To understand the potential impact of such attacks, we explored several scenarios in which an attacker-controlled MCIS could severely compromise flight safety.

Fortunately, the vulnerabilities we identified in existing systems are easily fixed by adhering to existing computer security best practices. We presented a set of recommendations that eliminate existing vulnerabilities.

9. ACKNOWLEDGMENTS

We are grateful to Brian Kantor and Cindy Moore, who provided technical assistance and computing support for this work, and to Jennifer Folkestad for assistance with administrative matters. We are grateful to Jessica Gross for modeling the Stratus 2 (Figure 2 left) and Sporty's Pilot Shop for the permission to use their screenshots of ForeFlight and Garmin Pilot apps (Figure 2 center and right). This work was supported by the National Science Foundation grant NSF-0963702 and by generous research, operational and/or in-kind support from the UCSD Center for Networked Systems (CNS).

References

[1] Davide Balzarotti, Greg Banks, Marco Cova, Viktoria Felmetsger, Richard Kemmerer, William Robertson, Fredrik Valeur, and Giovanni Vigna. An Experience in Testing the Security of Real-World Electronic Voting Systems. *Software Engineering, IEEE Transactions on*, 36(4):453–473, July 2010.

[2] Michael Becher, Felix C Freiling, Johannes Hoffmann, Thorsten Holz, Sebastian Uellenbeck, and Christopher Wolf. Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In *2011 IEEE Symposium on Security and Privacy (S&P)*, pages 96–111, 2011.

[3] Ali Broumandan, Ali Jafarnia-Jahromi, Vahid Dehghanian, John Nielsen, and Gérard Lachapelle. GNSS Spoofing Detection in Handheld Receivers Based on Signal Spatial Correlation. In *Proceedings of IEEE/ION PLANS 2012*, pages 479–487, April 2012.

[4] Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile. Study on GPS Events. http://www.bea-fr.org/etudes/etudegpsa/etudegpsa.pdf, August 2005.

[5] Barbara K. Burian, Judith Orasanu, and Jim Hitt. Weather-realted decision errors:differences across flight types. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2000.

[6] Stephen Checkoway, Damon McCoy, Danny Anderson, Brian Kantor, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *Proceedings of the USENIX Security Symposium*, San Francisco, CA, August 2011.

[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 *Blackhat USA 2012*, July 2012.

[8] Ang Cui, Michael Costello, and Salvatore J Stolfo. When firmware modifications attack: A case study of embedded exploitation. In *Network and Distributed System Security Symposium (NDSS)*, 2013.

[9] Saeed Daneshmand, Ali Jafarnia-Jahromi, Ali Broumandon, and Gérard Lachapelle. A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array. In *Proceedings of the ION GNSS Meeting*, 2012.

[10] Peter de Vries, Cees Midden, and Don Bouwhuis. The effects of errors on system trust, self-confidence, and the allocation of control in route planning. *International Journal of Human–Computer Studies*, 58(6):719–735, 2003.

[11] Fabio Dovis, Xin Chen, Antonio Cavaleri, Khurram Ali, and Marco Pini. Detection of Spoofing Threats by Means of Signal Parameters Estimation. In *Proceedings of the ION GNSS Meeting*, pages 416–421, September 2011.

[12] Mary T. Dzindolet, Scott A. Peterson, Regina A. Pomranky, Linda G Pierce, and Hall P. Beck. The role of trust in automation reliance. *International Journal of Human–Computer Studies*, 58(6):697–718, 2003.

[13] Mica R. Endsley and Debra G. Jones. *Designing for Situation Awareness*. CRC Press, 2012.

[14] Arye R. Ephrath and Renwick E. Curry. Detection by pilots of system failures during instrument landings. *IEEE Transactions on Systems, Man, and Cybernetics*, 7(12):841–848, December 1997.

[15] FAA PARC/CAST Flight Deck Automation Working Group. Operational use of flight path management systems, September 2013.

[16] Federal Aviation Administration. *System Safety Handbook*. December 2000.

[17] Federal Aviation Administration. Use of Class 1 or Class 2 Electronic Flight Bag (EFB), Advisory Circular no. 91-78, July 2007.

[18] Federal Aviation Administration. The Apple iPad and Other Suitable Tablet Computing Devices as Electronic Flight Bags (EFB), InFO 11011, May 2011.

[19] Federal Aviation Administration. Guidelines for the Certification, Airworthiness, and Operational Approval of Electronic Flight Bag Computing Devices, Advisory Circular no. 120-76B, June 2012.

[20] Federal Aviation Administration. Order 8040.4A: Safety Risk Management Policy. http://www.faa.gov/documentLibrary/media/Order/8040.4A%20.pdf, April 2012.

[21] Federal Aviation Administration. Fact Sheet – General Aviation Safety. January 2014. Online: http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=13672.

[22] Adrienne Porter Felt, Matthew Finifter, Erika Chin, Steve Hanna, and David Wagner. A survey of mobile malware in the wild. In *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 3–14, 2011.

[23] ForeFlight. ForeFlight and Frontier Airlines Announce Approval for ForeFlight Mobile in the Cockpit. October 2013. Online: http://blog.foreflight.com/2013/10/09/foreflight-and-frontier-airlines-announce-approval-for-foreflight-mobile-in-the-cockpit/.

[24] WesLee Frisby, Benjamin Moench, Benjamin Recht, and Thomas Ristenpart. Security Analysis of Smartphone Point-of-sale Systems. In *Proceedings of the 6th USENIX Conference on Offensive Technologies (WOOT)*, 2012.

[25] gps.gov. Gps.gov. Online: http://gps.gov.

[26] Steven Hanna, Rolf Rolles, Andrés Molina-Markham, Pongsin Poosankam, Kevin Fu, and Dawn Song. Take Two Software Updates and See Me in the Morning: The Case for Software Security Evaluations of Medical Devices. In *Proceedings of the 2nd USENIX conference on Health Security and Privacy*, 2011.

[27] David Hoey and Paul Benshoof. Civil GPS Systems and Potential Vulnerabilities. In *Proceedings of the ION GNSS Meeting*, pages 1291–1295, September 2005.

[28] Todd E Humphreys, Brent M Ledvina, Mark L Psiaki, Brady W O'Hanlon, and Paul M Kintner Jr. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In *Proceedings of the ION GNSS Meeting*, 2008.

[29] Todd E Humphreys, Jahshan Bhatti, and Brent Ledvina. The GPS Assimilator: a Method for Upgrading Existing GPS User Equipment to Improve Accuracy, Robustness, and Resistance to Spoofing. In *Proceedings of the ION GNSS Meeting*, 2010.

[30] Barry H. Kantowitz, Richard Hanowski, and Susan Kantowitz. Driver Acceptance of Unreliable Traffic Information in Familiar and Unfamiliar Settings. *Human Factors*, 39(2): 164–176, 1997.

[31] Brent M. Ledvina, William J. Bencze, Bryan Galusha, and Issac Miller. An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers . In *Proceedings of the 2010 International Technical Meeting of The Institute of Navigation*, pages 698–712, January 2010.

[32] John D. Lee and Neville Moray. Trust, self-confidence, and operators' adaptation to automation. *International Journal of Human–Computer Studies*, 40(1):153–184, 1994.

[33] John D. Lee and Katrina A. See. Trust in Automation: Designing for Appropriate Reliance. *Human Factors*, 46(50), 2004.

[34] McAfee Labs. McAfee Labs Threats Report. http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q1-2014.pdf, June 2014.

[35] Charlie Miller. Battery Firmware Hacking: Inside the innards of a Smart Battery. July 2011.

[36] Kathleen L. Mosier, Linda J. Skitka, Susan Heers, and Mark Burdick. Automation Bias: Decision Making and Performance in High-Tech Cockpits. *International Journal of Aviation Psychology*, 8(1):47–63, 1998.

[37] Kathleen L. Mosier, Jeffrey Keyes, and Roberta Bernhard. Dealing with Conflicting Information—Will Crews Rely on Automation? In *Proceedings of the Fifth Australian Aviation Psychology Symposium*, 2000.

[38] B. Motella, M. Pini, M. Fantino, P. Mulassano, M. Nicola, J. Fortuny-Guasch, M. Wildemeersch, and D. Symeonidis. Performance Assessment of Low Cost GPS Teceivers under Vivilian Spoofing Attacks. In *5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, pages 1–8, December 2010.

[39] National Institute of Standards and Technology. Guide for conducting risk assessments: Information security. NIST Special Publication 800-30 Revision 1, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[40] National Transportation Safety Board. Risk factors associated with weather-related general aviation accidents. NTSB/SS-05/01, 2005.

[41] Tyler Nighswander, Brent Ledvina, Jonathan Diamond, Robert Brumley, and David Brumley. GPS Software Attacks. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 450–461, October 2012.

[42] Jon Oberheide and Farnam Jahanian. When mobile is harder than fixed (and vice versa): Demystifying security challenges in mobile environments. In *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, pages 43–48, 2010.

[43] Brady W. O'Hanlon, Mark L. Psiaki, Todd E. Humphreys, and Jahshan A. Bhatti. Real-Time Spoofing Detection Using Correlation Between two Civil GPS Receiver. In *Proceedings of the ION GNSS Meeting*, 2011.

[44] Raja Parasuraman and Dietrich H. Manzey. Complacency and bias in human use of automation: An attentional integration. *Human Factors*, 52(381):381–410, 2010.

[45] Lawrence J. Prinzel, III. The Relationship of Self-Efficacy and Complacency in Pilot Automation Interaction. Technical Report TM-2002-211925, NASA, September 2002.

[46] Mark L. Psiaki. Developing Defenses Against Jamming & Spoofing of Civilian GNSS Receivers. In *Proceedings of the ION GNSS Meeting*, pages 3407–3417, September 2011.

[47] Mark L Psiaki, Brady W O'Hanlon, Jahshan A Bhatti, Daniel P Shepard, and Todd E Humphreys. Civilian GPS Spoofing Detection Based on Dual-Receiver Correlation of Military Signals. In *Proceedings of the ION GNSS Meeting*, 2011.

[48] K. Deergha Rao, M.N.S. Swamy, and E.I. Plotkin. Anti-Spoofing Filter for Accurate GPS Navigation. In *Proceedings of the ION GPS Meeting*, pages 1536–1541, September 2000.

[49] Michael Rushanan, Denis Foo Kune, Colleen M. Swanson, and Aviel D. Rubin. SoK: Security and privacy in implantable medical devices and body area networks. In *Proceedings of IEEE Symposium on Security and Privacy*, May 2014.

[50] Matthias Schäfer, Vincent Lenders, and Ivan Martinovic. Experimental Analysis of Attacks on NextÊGeneration Air Traffic Communication. In *Proceedings of the International Conference on Applied Cryptography and Network Security (ACNS)*, pages 253–271, June 2013.

[51] Daniel P. Shepard and Todd E. Humphreys. Characterization of Receiver Response to a Spoofing Attacks. In *Proceedings of the ION GNSS Meeting*, pages 2608–2618, September 2011.

[52] Daniel P Shepard, Jahshan A Bhatti, Todd E Humphreys, and Aaron A Fansler. Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. In *Proceedings of the ION GNSS Meeting*, 2012.

[53] D. H. Stamatis. *Introduction to Risk and Failures: Tools and Methodologies*. CRC Press, 2014.

[54] Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. Security of ADS-B: State of the Art and Beyond", July 2013.

[55] Peter F. Swaszek, Richard J. Hartnett, Matthew V. Kempe, and Gregory W. Johnson. Analysis of a Simple, Multi-Receiver GPS Spoof Detector. In *Proceedings of the 2013 International Technical Meeting of The Institute of Navigation*, pages 884–892, January 2013.

[56] Hugo Teso. Aircraft Hacking (Hack-in-the-Box 2013 presentation). Online: `https://www.nruns.com/fileadmin/downloads/n.runs_Vortrag_Aircraft_Hacking_by_Hugo_Teso.pdf`.

[57] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the Requirements for Successful GPS Spoofing Attacks. In *Proceedings of the 18th ACM Conference on Computer and Communications Security*, CCS '11, pages 75–86, October 2011.

[58] Timothy Vidas and Nicolas Christin. Sweetening Android lemon markets: Measuring and combating malware in application marketplaces. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy*, pages 197–208, 2013.

[59] Hengqing Wen, Peter Yih-Ru Huang, John Dyer, Andy Archinal, and John Fagan. Countermeasures for GPS Signal Spoofing. In *Proceedings of the ION GNSS Meeting*, pages 1285–1290, September 2005.

[60] Kyle Wesson, Mark Rothlisberger, and Todd Humphreys. Practical Cryptographic Civil GPS Signal Authentication. *Navigation*, 59(3):177–193, 2012.

[61] Kyle D. Wesson, Daniel P. Shepard, Jahshan A. Bhatti, and Todd E. Humphreys. An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing. In *Proceedings of the ION GNSS Meeting*, 2011.

[62] Christopher D. Wickens and Colin Kessel. The Effects of Participatory Mode and Task Workload on the Detection of Dynamic System Failures. *Systems, Man and Cybernetics, IEEE Transactions on*, 9(1):24–34, January 1979.

[63] Douglas A. Wiegmann, Juliana Goh, and David O'Hare. The role of situation assessment and flight experience in pilots' decision to continue visual flight rules flight into adverse weather. *Human Factors*, 44(2):189–197, 2002.

[64] Michelle Yeh and Christopher D. Wickens. Display Signaling in Augmented Reality: Effects of Cue Reliability and Image Realism on Attention Allocation and Trust Calibration. *Human Factors*, 43(355):355–365, 2001.

[65] Wu Zhou, Yajin Zhou, Michael Grace, Xuxian Jiang, and Shihong Zou. Fast, Scalable Detection of "Piggybacked" Mobile Applications. In *Proceedings of the Third ACM Conference on Data and Application Security and Privacy*, pages 185–196, 2013.

[66] Yajin Zhou and Xuxian Jiang. Dissecting Android malware: Characterization and evolution. In *Security and Privacy (SP), 2012 IEEE Symposium on*, pages 95–109, May 2012.