On The Security of Mobile Cockpit Information Systems

Lundberg, Farinholt, Sullivan, Mast, Checkoway, Savage, Snoeren, and Levchenko

Presented by Kyo Kim

Small Aircraft

Pilots use tablets (or similar devices) in the cockpit to view weather and traffic info.

The device is linked to an reciever that have sensors (e.g. GPS, altimeter, and etc) to gather necessary data.

Regulation

The devices are not part of the flight system. Therefore, it does not go through the same electronic security checking.

In aviation community, security == reliability.

But, security != reliability

- Motivated attacker in security
- Nature in reliability

How secure is the system and what are the consequences of compromised system?

MCIS (Mobile Cockpit Information System)

Information Services

- GPS
- ADS-B (Automatic Dependent Surveillance – Broadcast)
- TIS-B (Traffic Information Service – Broadcast)
- FIS-B (Flight Info service-Broadcast)

GPS

No authentication

Vulnerable to replay attack and spoofing

Ground based attack can be easily detected

ADS-B and TIS-B

Automatic Dependent Surveillance-Broadcast

- Self-reports aircraft position to avoid collision
- Satellite can track the position of the aircraft
- FAA mandates all aircrafts to have ADS-B capability by 2020

Traffic Info Service-Broadcast

- Used by FAA ground stations
- Allows aircrafts to know their position by using transponder only

FIS-B

Flight Info Service-BroadCast

- Provides real-time info (.e.g graphical weather data)
- Similar to TIS-B, FAA provides the signal
- Also sends time-sensitive advices to pilots

Aeronautical Info Apps

Similar to EFB (Electronic Flight Bags)

Government Regulations

- EFBs used by air carriers must not show “ownership position”
- The apps display it

Pilots may rely too much on the app

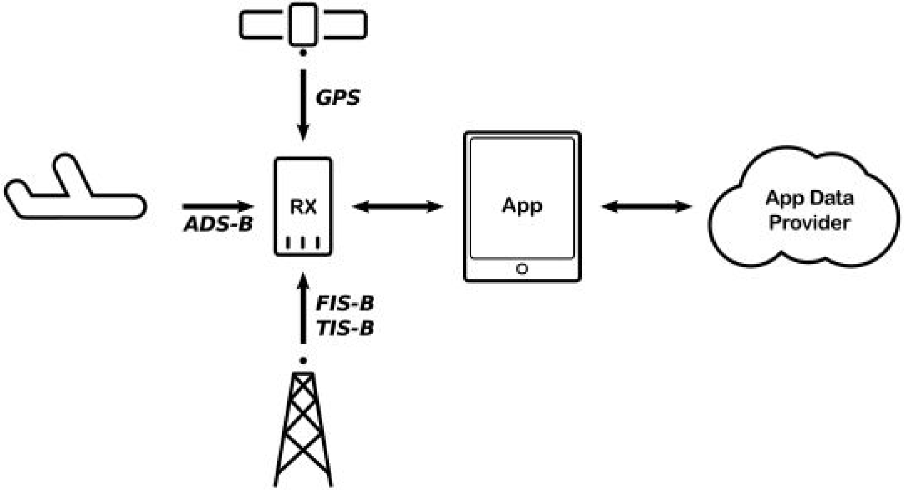
Attack Model

Attack is successful when the target aircraft's flight is disrupted

- Corrupt the MCIS transmission
- Display false information about nearby aircrafts

Attack surface

- Receiver to App channel
- App to Internet Channel
- Receiver
- App and Tablet (device)



Receiver to App

Uses WiFi/Bluetooth channel

EFB data is preloaded before flight

If the channel is not available, pilot can only rely on EFB

Possible to manipulate the data channel

No replay protection

App to Internet

This channel is used to fetch EFB data and firmware attacks

Attacker could manipulate the EFB data and updates.

Devices

Receiver

- If compromised, the attacker could impersonate the receiver
    - Firmware reflashing
        - Preventable if the downloaded contents are signed

App and Tablet

- If compromised, any data presented can be controlled by the attacker

Attacker Model

Brief Proximity

Brief Access

Time-of-use Proximity

Update MITM

Collocated App

Scenarios

Altitude and attitude

- Severity: Catastrophic
- Likelihood: Extremely remote since it can be checked by flight instrument

Position

- Severity: Catastrophic in low-visibility
- Likelihood: Probable in low visibility and remote otherwise

Scenarios

Die Hard / Terrain

- Recalibrate sea level far below normal.
- Severity: catastrophic
- Likelihood: Extremely remote

Weather

- Severity: Catastrophic if Incorrect weather Info is displayed
- Likelihood: Difficult to determine since experience determines it.

Scenarios

Position of other aircraft

- Attacker could suppress info about other aircraft
  - Pilots do not rely on ADS-B/TIS-B for other aircraft ID
- Could add false targets on the display
  - Pilot could rely on auto pilot system
- Could change the reported position of existing plane such that the pilots moves towards the plane to avoid collision.
  - Probable only in certain circumstances

ForeFlight + Appareo Stratus 2

Receiver to APP Integrity

- UDP in WiFi broadcast
  - Unauthenticated and not encrypted
- Managed to Impersonate the receiver
  - False data will overwrite the original data

App to receiver

- Similar problem as above.

EFB was downloaded using SSL and does not accept self signed file.

Garmin Pilot + Garmin GDL 39

Receiver to App Channel

- Channel is encrypted but not authenticated
- With time-of-use proximity, it is possible to impersonate the receiver.

App to Receiver Channel

- Passively listen and spoof the request

Fetches update using HTTP not HTTPS and updates via Bluetooth using Garmin Pilot App

WingX Pro7 + Sagetech Clarity

Receiver to App

- Unencrypted and unauthenticated
- IP address subnet checking

No App to Receiver Channel

EFB data transmitted over HTTP unsigned

Firmware image not encrypted or authenticated. Possible to load custom firmware with brief physical access.

Discussion

Are the described attack scenarios practical for consideration in designing security for MCIS?

What would be the reasonable motivation and payoff for carrying out the described attacks?

Considering that MCIS exists just to provide convenience, is it reasonable to consider security in MCIS?