A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems

Matt Smith‡, Martin Strohmeier‡†, Jonathan Harman, Vincent Lenders† and Ivan Martinovic‡

‡Department of Computer Science, University of Oxford, United Kingdom
Email: first.last@cs.ox.ac.uk
Twitter: @avsecxford

†Cyber-Defence Campus, armasuisse Science + Technology, Switzerland
Email: first.last@armasuisse.ch
Twitter: @cydcampus

Network and Distributed Systems Symposium (NDSS) 2020

23–26th February 2020
Security Research in Aviation
Security Research in Aviation

Wireless Attacks on Aircraft Instrument Landing Systems

Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir

Khoury College of Computer Sciences
Northeastern University, Boston, MA, USA

USENIX 2019
Security Research in Aviation

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems

Wireless Attacks on Aircraft Instrument Landing Systems

Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir
Khoury College of Computer Sciences
Northeastern University

Experimental Analysis of Attacks on Next Generation Air Traffic Communication

Matthias Schäfer¹, Vincent Lenders², and Ivan Martinovic³

USENIX 2019

ACNS 2013
Security Research in Aviation

Wireless Attacks on Aircraft Instrument Landing Systems
Harshad Sathaye, Domien Schepers, Aanjhan Ranganathan, and Guevara Noubir
Khoury College of Computer Sciences
Northeastern University

Experimental Analysis of Attacks on Next Generation Air Traffic Communication

Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices
Andrei Costin, Aurélien Francillon
Network and Security Department
EURECOM
Sophia-Antipolis, France
Email: andrei.costin@eurecom.fr, aurelien.francillon@eurecom.fr

USENIX 2019
ACNS 2013
Blackhat 2012
Security Research in Aviation

Wireless Attacks on Aircraft Instrument Landing Systems
Harshad Sathaye, Domien Schepers, Aanjan Ranganathan, and Guevara Noubir
Khoury College of Computer Sciences
Northeastern University

Experimental Analysis of Attacks on Next Generation Air Traffic Communication

Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices
Andrei Costin, Aurélien Francillon
Network and Security Department

Paul M. Berges

USENIX 2019

ACNS 2013

Blackhat 2012

Masters Thesis, 2019
**Security Research in Aviation**

**On the Requirements for Successful GPS Spoofing Attacks**

Nils Ole Tippenhauer  
Dept. of Computer Science  
ETH Zurich, Switzerland  
tnilti@inf.ethz.ch

Christina Pöpper  
Dept. of Computer Science  
ETH Zurich, Switzerland  
poepperc@inf.ethz.ch

Kasper B. Rasmussen  
Computer Science Dept.  
UCI, Irvine, CA  
kbrasmus@ics.uci.edu

Srdjan Ćapkun  
Dept. of Computer Science  
ETH Zurich, Switzerland  
capkuns@inf.ethz.ch

**Experimental Analysis of Attacks on Next Generation Air Traffic Communication**

Harshad Sathaye  
Northeastern University

**Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices**

Andrei Costin, Aurélien Francillon  
Network and Security Department


Paul M. Berges

CCS 2011

ACNS 2013

Blackhat 2012

Masters Thesis, 2019
Security Research in Aviation

On the Requirements for Successful GPS Spoofing Attacks

Nils Ole Tippenhauer
Dept. of Computer Science
ETH Zurich, Switzerland
tinis@inf.ethz.ch

Christina Pöpper
Dept. of Computer Science
ETH Zurich, Switzerland
poepper@inf.ethz.ch

Kasper B. Rasmussen
Computer Science Dept.
UCI, Irvine, CA
kbrasmus@ics.uci.edu

Srdjan Ćapkun
Dept. of Computer Science
ETH Zurich, Switzerland
capkuns@inf.ethz.ch

Experimental Analysis of Attacks on Next Gen ADS-B

Ghost in the Air(Traffic): On insecurity of ADS

Andrei Costin, Aurélien Francillon
Network and Security Department


Paul M. Berge

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems

CCS 2011

DEF CON 20

Blackhat 2012

Masters Thesis, 2019
Security Research in Aviation

On the Requirements for Successful GPS Spoofing Attacks
Nils Ole Tippenhauer
Dept. of Computer Science
ETH Zurich, Switzerland
tinis@inf.ethz.ch

Maureen Pöpper
Dept. of Computer Science
ETH Zurich, Switzerland
poeppe2@inf.ethz.ch

Kasper B. Rasmussen
Computer Science Dept.
UCI, Irvine, CA
kbrasmus@ics.uci.edu

Srdjan Čapkun
Dept. of Computer Science
ETH Zurich, Switzerland
capkuns@inf.ethz.ch

Experimental Analysis of Attacks on Next Gen ADS-B

Ghost in the Air(Traffic): On insecurity of ADS-B and ADS-B devices

Security Research in Aviation

The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication

Martin Strohmeier*, Matthew Smith*, Vincent Lenders†, Ivan Martinovic*

*University of Oxford, UK  †Armassuisse, Switzerland

DEF CON 20

EuroS&P 2018

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems
Security Research in Aviation

On the Requirements for Successful GPS Spoofing Attacks

Nils Ole Tippenhauer
Dept. of Computer Science
ETH Zurich, Switzerland
tnills@inf.ethz.ch

Christina Pöpper
Dept. of Computer Science
ETH Zurich, Switzerland
poepperc@inf.ethz.ch

Kasper B. Rasmussen
Computer Science Dept.
UCI, Irvine, CA
kbrasmus@ics.uci.edu

Srdjan Ćapkun
Dept. of Computer Science
ETH Zurich, Switzerland
capkuns@inf.ethz.ch

Experimental Analysis of Attacks on Next G

Ghost in the Air(Traffic): On insecurity of ADS-B

(TCAS) Through Software

How well do pilots handle these attacks?

The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication

Martin Strohmeier*, Matthew Smith*, Vincent Lenders†, Ivan Martinovic*

*University of Oxford, UK †Armament, Switzerland

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems

CCS 2011

DEF CON 20

EuroS&P 2018
LAST LINE OF DEFENCE

Pilots are regularly assessed on their fault-handling abilities, usually in a flight simulator.
Pilots are regularly assessed on their fault-handling abilities, usually in a flight simulator.

They also form a ‘last line of defence’ against faults, through well-defined procedure.

Baltic Aviation Academy, Wikipedia [5]
Last Line of Defence

Pilots are regularly assessed on their fault-handling abilities, usually in a flight simulator.

They also form a ‘last line of defence’ against faults, through well-defined procedure.

How well does fault-handling skill translate to attack mitigation?

Baltic Aviation Academy, Wikipedia [5]
LAST LINE OF DEFENCE

Pilots are regularly assessed on their fault-handling abilities, usually in a flight simulator.

They also form a ‘last line of defence’ against faults, through well-defined procedure.

How well does fault-handling skill translate to attack mitigation?

Can we use flight simulation to understand the impact of attacks?

Baltic Aviation Academy, Wikipedia [5]
**Method**

- We invited 30 currently type-rated A320 pilots to fly scenarios in our simulator
Method

- We invited 30 currently type-rated A320 pilots to fly scenarios in our simulator
- Carried out attacks on collision avoidance, ground proximity and landing systems
METHOD

- We invited 30 currently type-rated A320 pilots to fly scenarios in our simulator
- Carried out attacks on collision avoidance, ground proximity and landing systems
- Uses XPlane 11 with a high-quality aircraft model
- Experimenter provided flying support (enabling modes/pressing buttons on command)

Photo of simulator set up
METHOD

• We invited 30 currently type-rated A320 pilots to fly scenarios in our simulator
• Carried out attacks on collision avoidance, ground proximity and landing systems
• Uses XPlane 11 with a high-quality aircraft model
• Experimenter provided flying support (enabling modes/pressing buttons on command)

PROTOCOL
1. Familiarisation flight
2. For each attack:
   a) Simulator flight including attack
   b) Debrief interview about flight
3. Overall debrief interview
Method

- We invited 30 currently type-rated A320 pilots to fly scenarios in our simulator
- Carried out attacks on collision avoidance, ground proximity and landing systems
- Uses XPlane 11 with a high-quality aircraft model
- Experimenter provided flying support (enabling modes/pressing buttons on command)

Protocol
1. Familiarisation flight
2. For each attack:
   a) Simulator flight including attack
   b) Debrief interview about flight
3. Overall debrief interview

Experience demographics

Photo of simulator set up
### Attacker Model

<table>
<thead>
<tr>
<th>Capabilities</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Motivation</td>
<td>Cause delay, financial loss, reputational harm or a reduction in safety</td>
</tr>
</tbody>
</table>
### Attacker Model

**Capabilities**

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Cause delay, financial loss, reputational harm or a reduction in safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>Means</td>
<td>• Trigger go-arounds</td>
</tr>
<tr>
<td></td>
<td>• Force unexpected maneuvers</td>
</tr>
<tr>
<td></td>
<td>• Push crew to switch systems off</td>
</tr>
<tr>
<td>Understanding of avionics standards</td>
<td></td>
</tr>
<tr>
<td>Mobility to create radio software</td>
<td></td>
</tr>
<tr>
<td>Deploy in a single or multiple locations</td>
<td></td>
</tr>
</tbody>
</table>
# Attacker Model

## Capabilities

<table>
<thead>
<tr>
<th>Motivation</th>
<th>Cause delay, financial loss, reputational harm or a reduction in safety</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Means</strong></td>
<td>• Trigger go-arounds</td>
</tr>
<tr>
<td></td>
<td>• Force unexpected maneuvers</td>
</tr>
<tr>
<td></td>
<td>• Push crew to switch systems off</td>
</tr>
<tr>
<td><strong>Ability</strong></td>
<td>• Understanding of avionics standards/systems</td>
</tr>
<tr>
<td></td>
<td>• Ability to create radio software for attacks</td>
</tr>
<tr>
<td></td>
<td>• Deploy in a single or multiple locations</td>
</tr>
</tbody>
</table>
**ATTACKER MODEL**

**Capabilities**

**Motivation**  Cause delay, financial loss, reputational harm or a reduction in safety

**Means**
- Trigger go-arounds
- Force unexpected maneuvers
- Push crew to switch systems off

**Ability**
- Understanding of avionics standards/systems
- Ability to create radio software for attacks
- Deploy in a single or multiple locations

**Equipment**

- Scientific-grade Software Defined Radio (SDR) e.g. Ettus USRP
- High-gain amplifier
- Directional antenna
Traffic Collision Avoidance System

TCAS aims to prevent mid-air collisions by automatically de-conflicting potential close-encounters.
TRAFFIC COLLISION AVOIDANCE SYSTEM

TCAS aims to prevent mid-air collisions by automatically de-conflicting potential close-encounters.

Intruder

Mode S Interrogation

Mode S Response

Ownship

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems
TCAS aims to prevent mid-air collisions by automatically de-conflicting potential close-encounters.
TCAS aims to prevent mid-air collisions by automatically de-conflicting potential close-encounters.
Traffic Collision Avoidance System

TCAS aims to prevent mid-air collisions by automatically de-conflicting potential close-encounters.

Aircraft transmit data requested by air traffic control data to the ground via Mode S.

Other aircraft listen for these transmissions and use them to monitor nearby aircraft.
As each aircraft continues to move, they will predict the flight path of the others.
Traffic Collision Avoidance System

As each aircraft continues to move, they will predict the flight path of the others. If the flight paths suggest the aircraft are too close, but not yet a risk, a Traffic Advisory (TA) will be issued.
Traffic Collision Avoidance System

As each aircraft continues to move, they will predict the flight path of the others.

If the flight paths suggest the aircraft are too close, but not yet a risk, a Traffic Advisory (TA) will be issued.

This will be announced in the cockpit automatically.
If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA).
Traffic Collision Avoidance System

If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA).

The aircraft will communicate to coordinate their planned RA movements.
Traffic Collision Avoidance System

If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA).

The aircraft will communicate to coordinate their planned RA movements.

The RAs will be announced in-cockpit as compulsory instructions.

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems
Traffic Collision Avoidance System

If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA)

The aircraft will communicate to coordinate their planned RA movements

The RAs will be announced in-cockpit as compulsory instructions

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems

8
**Traffic Collision Avoidance System**

If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA).

The aircraft will communicate to coordinate their planned RA movements.

The RAs will be announced in cockpit as compulsory instructions.
**Traffic Collision Avoidance System**

If the aircraft remain on a course to a close encounter, the aircraft will issue a Resolution Advisory (RA).

The aircraft will communicate to coordinate their planned RA movements.

The RAs will be announced in- cockpit as compulsory instructions.

TCAS procedure broadly expects aircraft to be cooperative.
TCAS – ATTACK

- Mode S has been shown to be insecure in previous work by Costin, Schäfer [3]
TCAS – Attack

- Mode S has been shown to be insecure in previous work by Costin, Schäfer [3]
- **Attacker** listens for Mode S interrogations issued by the aircraft and responds
  - Target aircraft believes an aircraft is flying towards it
  - Eventually this will cause a TA then RA, requiring avoiding action
TCAS – Attack

- Mode S has been shown to be insecure in previous work by Costin, Schäfer [3]
- **Attacker** listens for Mode S interrogations issued by the aircraft and responds
  - **Target aircraft** believes an aircraft is flying towards it
  - Eventually this will cause a TA then RA, requiring avoiding action
- Simulator scenario saw the participant exposed to this multiple times in a flight

[Diagram showing TCAS attack with ground-based attacker injecting false Mode S response leading to a resolution advisory.]
TCAS – Attack

- Mode S has been shown to be insecure in previous work by Costin, Schäfer [3]
- **Attacker** listens for Mode S interrogations issued by the aircraft and responds
  - Target aircraft believes an aircraft is flying towards it
  - Eventually this will cause a TA then RA, requiring avoiding action
- Simulator scenario saw the participant exposed to this multiple times in a flight

**Aim:** Force aircraft to repeatedly fly unwarranted Resolution Advisories
TCAS – Results

- Pilots found the repeated RAs so distracting that 26 (87%) pilots reduced the sensitivity of TCAS, with 11 switching to ‘Standby’

- TA-Only after 4.5 RAs, Standby after a further 2.8 RAs
TCAS – Results

- Pilots found the repeated RAs so distracting that 26 (87%) pilots reduced the sensitivity of TCAS, with 11 switching to 'Standby'.
- TA-Only after 4.5 RAs, Standby after a further 2.8 RAs.
- Causes loss of full TCAS use for the rest of the flight & increased air traffic control burden.

TCAS shwh Results

- Pilots found the repeated RAs so distracting that 26 (87%) pilots reduced the sensitivity of TCAS, with 11 switching to 'Standby'.
- TA-Only after 4.5 RAs, Standby after a further 2.8 RAs.
- Causes loss of full TCAS use for the rest of the flight & increased air traffic control burden.

---

<table>
<thead>
<tr>
<th>Final Selected TCAS Mode</th>
<th>TA/RA</th>
<th>TA-Only</th>
<th>Standby</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue on route</td>
<td>4</td>
<td>10</td>
<td>8</td>
<td>22</td>
</tr>
<tr>
<td>Avoidance Maneuver</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Divert to Origin</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>4</td>
<td>15</td>
<td>11</td>
<td>30</td>
</tr>
</tbody>
</table>

Effectively switching TCAS off
TCAS – Results

- Pilots found the repeated RAs so distracting that 26 (87%) pilots reduced the sensitivity of TCAS, with 11 switching to ‘Standby’

- TA-Only after 4.5 RAs, Standby after a further 2.8 RAs

- Causes loss of full TCAS use for the rest of the flight & increased air traffic control burden

- Excess fuel burn in following RAs – but no choice

### Final Selected TCAS Mode

<table>
<thead>
<tr>
<th></th>
<th>TA/RA</th>
<th>TA-Only</th>
<th>Standby</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue on route</td>
<td>4</td>
<td>10</td>
<td>8</td>
<td>22</td>
</tr>
<tr>
<td>Avoidance Maneuver</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Divert to Origin</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>4</td>
<td>15</td>
<td>11</td>
<td>30</td>
</tr>
</tbody>
</table>

Effectively switching TCAS off
TCAS – RESULTS

- Pilots found the repeated RAs so distracting that 26 (87%) pilots reduced the sensitivity of TCAS, with 11 switching to 'Standby'

- TA-Only after 4.5 RAs, Standby after a further 2.8 RAs

- Causes loss of full TCAS use for the rest of the flight & increased air traffic control burden

- Excess fuel burn in following RAs – but no choice

- Most pilots continued on route but some felt the need to make extra maneuvers or divert

**Final Selected TCAS Mode**

<table>
<thead>
<tr>
<th></th>
<th>TA/RA</th>
<th>TA-Only</th>
<th>Standby</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue on route</td>
<td>4</td>
<td>10</td>
<td>8</td>
<td>22</td>
</tr>
<tr>
<td>Avoidance Maneuver</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Divert to Origin</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>4</td>
<td>15</td>
<td>11</td>
<td>30</td>
</tr>
</tbody>
</table>

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems
TCAS – Results

- Pilots found the repeated RAs so distracting that 26 (87%) pilots reduced the sensitivity of TCAS, with 11 switching to ‘Standby’
- TA-Only after 4.5 RAs, Standby after a further 2.8 RAs
- Causes loss of full TCAS use for the rest of the flight & increased air traffic control burden
- Excess fuel burn in following RAs – but no choice
- Most pilots continued on route but some felt the need to make extra maneuvers or divert
- Attacker can push pilots to fly unnecessary RAs and reduce TCAS sensitivity

<table>
<thead>
<tr>
<th>Final Selected TCAS Mode</th>
<th>TA/RA</th>
<th>TA-Only</th>
<th>Standby</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continue on route</td>
<td>4</td>
<td>10</td>
<td>8</td>
<td>22</td>
</tr>
<tr>
<td>Avoidance Maneuver</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>Divert to Origin</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Total</td>
<td>4</td>
<td>15</td>
<td>11</td>
<td>30</td>
</tr>
</tbody>
</table>
TCAS – ANALYSIS

• Participants noted that individual RAs were rare in normal flight – suggests something is wrong
TCAS – ANALYSIS

- Participants noted that individual RAs were rare in normal flight – suggests something is wrong

One pilot had less than 10 in 17 years of flying
TCAS – Analysis

- Participants noted that individual RAs were rare in normal flight – suggests something is wrong

One pilot had less than 10 in 17 years of flying

- Weather would have made attack identification much harder – cannot visually check
TCAS – ANALYSIS

- Participants noted that individual RAs were rare in normal flight – suggests something is wrong

One pilot had less than 10 in 17 years of flying

- Weather would have made attack identification much harder – cannot visually check

- Sudden, repeated RAs might have knock on effects for other aircraft

28 (93%) participants felt that this attack lowered the safety of the aircraft
TCAS – Analysis

- Participants noted that individual RAs were rare in normal flight – suggests something is wrong
  - One pilot had less than 10 in 17 years of flying

- Weather would have made attack identification much harder – cannot visually check

- Sudden, repeated RAs might have knock on effects for other aircraft

- 28 (93%) participants felt that this attack lowered the safety of the aircraft

- Pilots forced to reduce sensitivity of key safety system due to distraction
  - A participant highlighted a ‘crying wolf’ effect, which might impact future responses to TCAS
Aircraft follow a glidepath to the touchdown zone on the runway.
In aeronautics, the Instrument Landing System (ILS) facilitates landings by providing critical guidance. Aircraft follow a glidepath to the touchdown zone on the runway using the ILS. The glideslope, a part of the ILS, provides guidance along the ideal glidepath using overlapping lobes. This system helps pilots maintain a safe descent rate and alignment as they approach the runway, ensuring a smooth and controlled landing.
GLIDESLOPE – ATTACK
GLIDESLOPE – ATTACK

Attacker transmits a false glideslope corresponding to further along the runway

Runway
**GLIDESLOPE – ATTACK**

Attacker transmits a false glideslope corresponding to further along the runway.

Touchdown zone too deep into runway.

Glidepath: The correct glideslope.

False Glidepath: The misleading glideslope transmitted by the attacker.

Runway: The path the aircraft is expected to follow during landing.

~350 ft: The vertical distance difference between glidepath and false glidepath.

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems
**GLIDESLOPE – ATTACK**

Attacker transmits a false glideslope corresponding to further along the runway

If the aircraft intercepts from above, or the attacker overpowers the real GS, the aircraft will follow the false GS

Touchdown zone too deep into runway

Runway

False Glidepath

Glidepath

~350 ft
**Glideslope – Attack**

Attacker transmits a false glideslope corresponding to further along the runway.

Touchdown zone too deep into runway.

False Glidepath

Glidepath

~350 ft

If the aircraft intercepts from above, or the attacker overpowers the real GS, the aircraft will follow the false GS.

Similar concept to Sathaye et. al., USENIX ’19 [2]
GLIDESLOPE – ATTACK

Attacker transmits a false glideslope corresponding to further along the runway.

Touchdown zone too deep into runway.

If the aircraft intercepts from above, or the attacker overpowers the real GS, the aircraft will follow the false GS.

Aim: Have the aircraft overshoot the runway and abort the approach or land deep.

Similar concept to Sathaye et. al., USENIX ’19 [2].
• Participants **consistently identified a problem** with ILS
• 26 (87%) participants **aborted** their first approach
• Subsequent approach methods **avoided the glideslope**, instead using different approaches
ILS/GS – Results

- Participants consistently identified a problem with ILS
- 26 (87%) participants aborted their first approach
- Subsequent approach methods avoided the glideslope, instead using different approaches methods
- Mean distance from touchdown at the point of go-around was 1.1 miles, at a height of 930 ft
ILS/GS – Results

- Participants consistently identified a problem with ILS
- 26 (87%) participants aborted their first approach
- Subsequent approach methods avoided the glideslope, instead using different approaches methods
- Mean distance from touchdown at the point of go-around was 1.1 miles, at a height of 930 ft
- In the cases of landing on first approach, pilots had to make a steep correction – not always possible
ILS/GS – Results

- Participants consistently identified a problem with ILS
  - 26 (87%) participants aborted their first approach
- Subsequent approach methods avoided the glideslope, instead using different approaches methods
- Mean distance from touchdown at the point of go-around was 1.1 miles, at a height of 930 ft
- In the cases of landing on first approach, pilots had to make a steep correction – not always possible
- Attacker can push pilots to miss an approach and abandon the glideslope
ILS/GS – Analysis

- All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach
ILS/GS – Analysis

- All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach
- Runway lighting key in identifying the issue
ILS/GS – Analysis

- All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach
- Runway lighting key in identifying the issue

Participants noted that poor weather would have made this much harder to spot
ILS/GS – Analysis

- All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach
- Runway lighting key in identifying the issue
- Much harder to manage in low-fuel situations

Participants noted that poor weather would have made this much harder to spot
ILS/GS – Analysis

- All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach
- Runway lighting key in identifying the issue
- Much harder to manage in low-fuel situations
- Concern about a ‘short’ glideslope landing before the runway

Participants noted that poor weather would have made this much harder to spot
ILS/GS – Analysis

• All participants identified an issue and lost confidence in the glideslope – unlikely to work beyond one approach

• Runway lighting key in identifying the issue

• Much harder to manage in low-fuel situations

• Concern about a ‘short’ glideslope landing before the runway

• Wide range of second approach methods suggests uncertainty – though experience with GS oddities helps

Participants noted that poor weather would have made this much harder to spot
## General Findings

<table>
<thead>
<tr>
<th>Observation</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>If attacks cause spurious alarms, the system will be turned off</td>
<td></td>
</tr>
</tbody>
</table>
**General Findings**

**Observation**
If attacks cause spurious alarms, the system will be turned off

**Effect**
Attackers ‘force’ pilots away from systems by attacking them
GENERAL FINDINGS

Observation

- If attacks cause spurious alarms, the system will be turned off
- Attacks have real potential for disruption, though specific disruption is hard to predict

Effect

- Attackers ‘force’ pilots away from systems by attacking them
General Findings

Observation

- If attacks cause spurious alarms, the system will be turned off
- Attacks have real potential for disruption, though specific disruption is hard to predict

Effect

- Attackers ‘force’ pilots away from systems by attacking them
- Can have a wider, more unpredictable system impact
General Findings

Observation

- If attacks cause spurious alarms, the system will be turned off
- Attacks have real potential for disruption, though specific disruption is hard to predict
- Participants generally fast to identify unusual behaviour

Effect

- Attackers ‘force’ pilots away from systems by attacking them
- Can have a wider, more unpredictable system impact
**General Findings**

**Observation**

- If attacks cause spurious alarms, the system will be turned off.
- Attacks have real potential for disruption, though specific disruption is hard to predict.
- Participants generally fast to identify unusual behaviour.

**Effect**

- Attackers ‘force’ pilots away from systems by attacking them.
- Can have a wider, more unpredictable system impact.
- Indicates that existing procedure provides a sound base.

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems
**General Findings**

**Observation**

- If attacks cause spurious alarms, the system will be turned off
- Attacks have real potential for disruption, though specific disruption is hard to predict
- Participants generally fast to identify unusual behaviour
- Attack success partly depends on wider system effects

**Effect**

- Attackers ‘force’ pilots away from systems by attacking them
- Can have a wider, more unpredictable system impact
- Indicates that existing procedure provides a sound base

---

A View from the Cockpit: Exploring Pilot Reactions to Attacks on Avionic Systems
**General Findings**

**Observation**
- If attacks cause spurious alarms, the system will be turned off
- Attacks have real potential for disruption, though specific disruption is hard to predict
- Participants generally fast to identify unusual behaviour
- Attack success partly depends on wider system effects

**Effect**
- Attackers ‘force’ pilots away from systems by attacking them
- Can have a wider, more unpredictable system impact
- Indicates that existing procedure provides a sound base
- Traffic, weather, ATC load, pilot tiredness
LESSONS LEARNED
LESSONS LEARNED

1. Diagnosis is key

Due to grey areas in procedure existing around the attacks, a lot of time was spent diagnosing the closest possible failure
LESSONS LEARNED

1. **Diagnosis is key**
   Due to grey areas in procedure existing around the attacks, a lot of time was spent diagnosing the closest possible failure.

2. **Value of simulation**
   Allows unexpected situations to emerge, scenarios to unfold fully and highlights factors which might not have been considered in analysis.
Lessons Learned

1. Diagnosis is key
   Due to grey areas in procedure existing around the attacks, a lot of time was spent diagnosing the closest possible failure

2. Value of simulation
   Allows unexpected situations to emerge, scenarios to unfold fully and highlights factors which might not have been considered in analysis

3. Real usage matters
   Understanding how and why humans in the loop of safety critical systems act like they do is important in security analysis
**Summary**

- Attacks cause disruption, even when pilots can mitigate part of the effect of the attack.
- Responses take a variety of forms, leading to attacks causing unpredictability.
- In many cases, attacks push pilots to disable safety-related systems.
- Existing procedure provides an ideal starting point for new steps to handle attacks.
A VIEW FROM THE COCKPIT: EXPLORING PILOT REACTIONS TO ATTACKS ON AVIONIC SYSTEMS

Matt Smith†, Martin Strohmeier‡, Jonathan Harman, Vincent Lenders§ and Ivan Martinovic†

†Department of Computer Science, University of Oxford, United Kingdom
Email: first.last@cs.ox.ac.uk
Twitter: @avsecoxford

‡Cyber-Defence Campus, Armasuisse Science + Technology, Switzerland
Email: first.last@armasuisse.ch
Twitter: @cydcampus
References


• Slide 1 – Photo by NeONBRAND on Unsplash – https://unsplash.com/photos/c56y966z0Xc

• Slide 19 – Photo by Eric Bruton on Unsplash