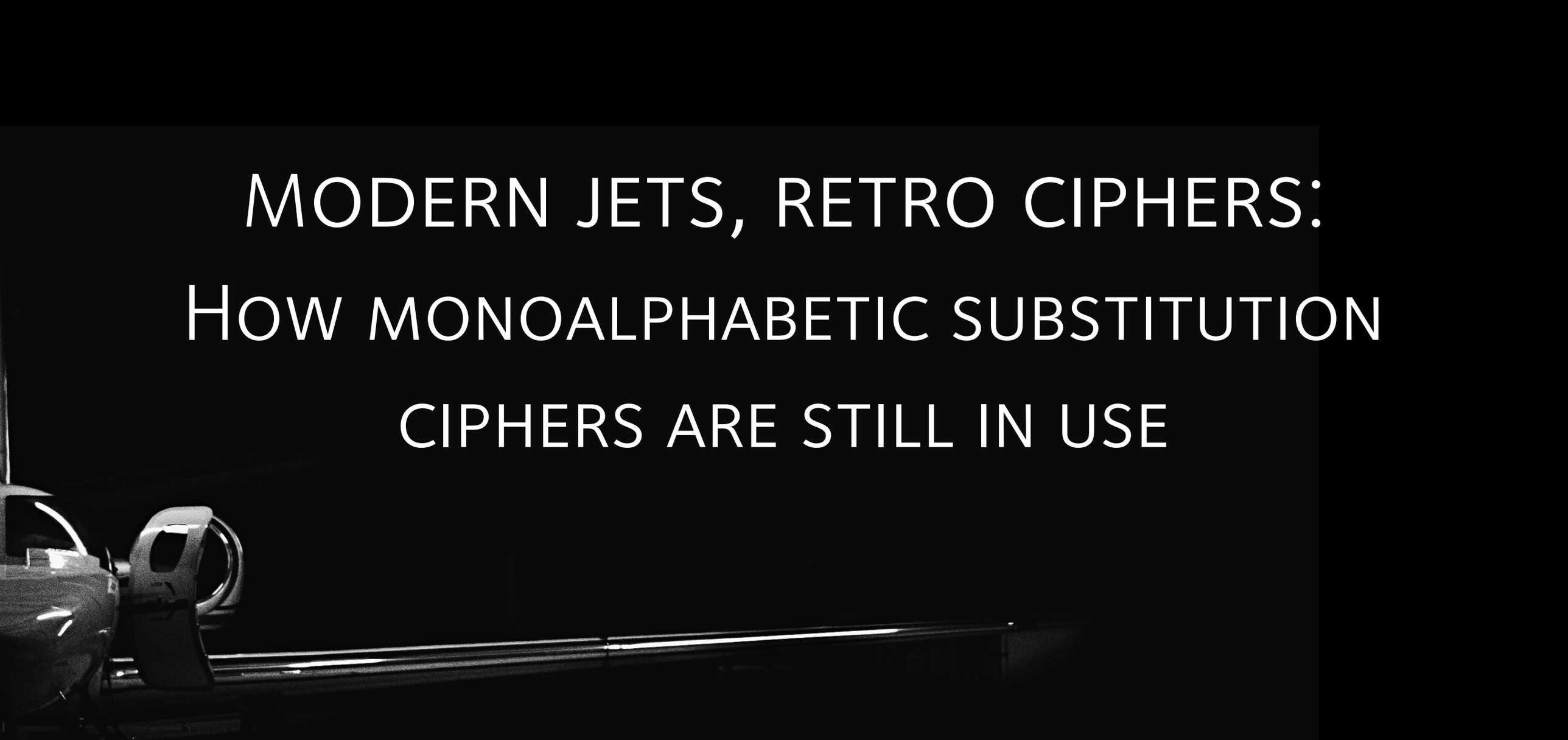
Modern jets, retro ciphers:
How monoalphabetic substitution ciphers are still in use



Matthew Smith*, Daniel Moser$, Martin Strohmeier*,
Vincent Lenders¥, Ivan Martinovic*

*University of Oxford
first.last@cs.ox.ac.uk

$ETH Zurich
first.last@inf.ethz.ch

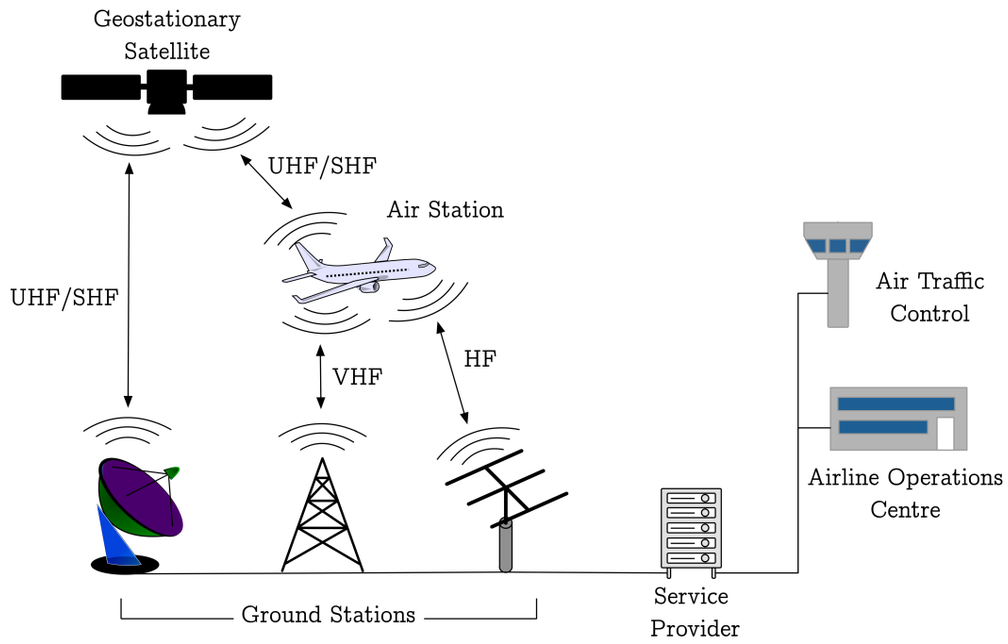
¥armasuisse
first.last@armasuisse.ch

Real World Crypto 2018, January 10-12, Zurich

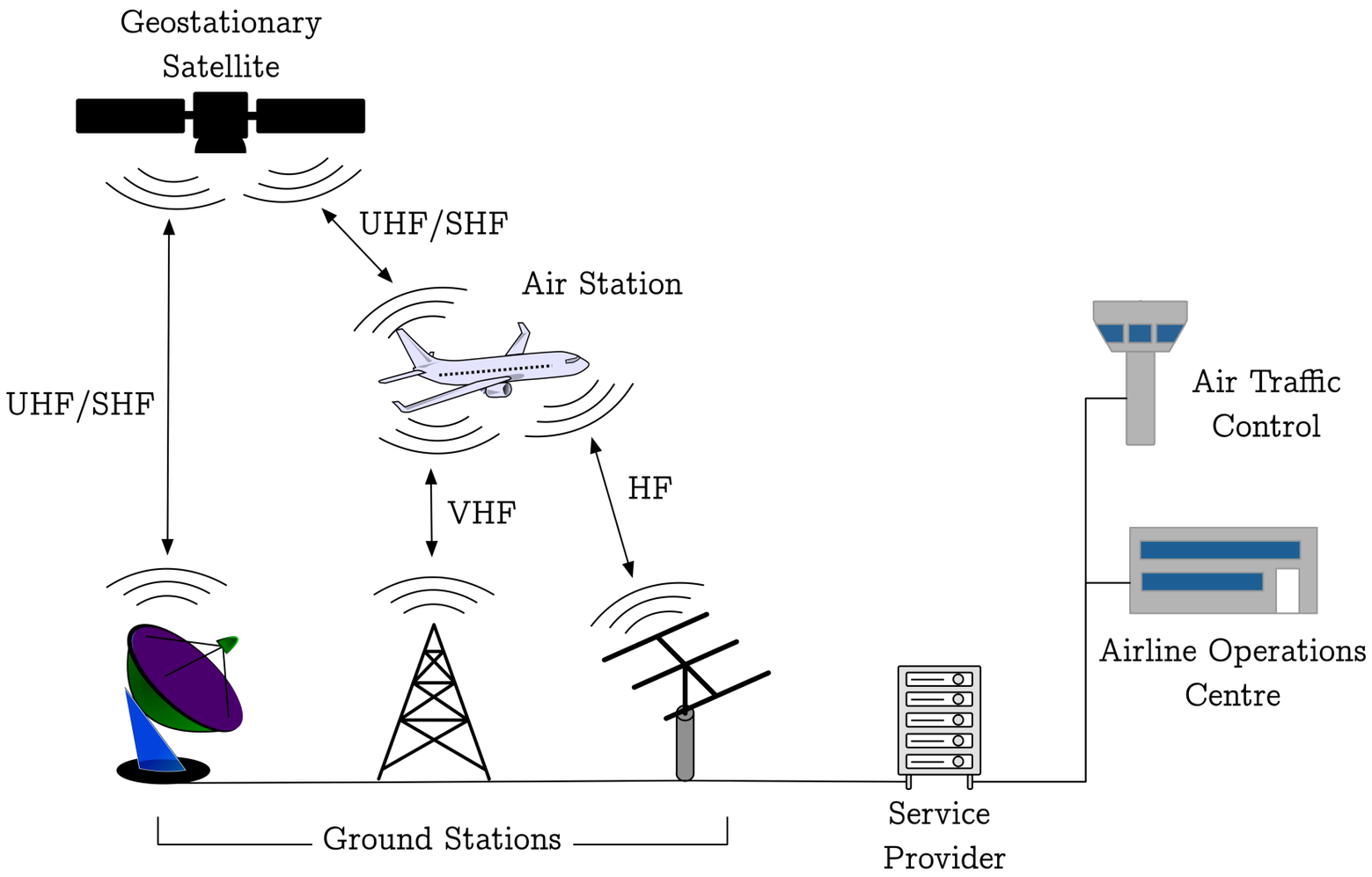
UNIVERSITY OF OXFORD

What is ACARS?

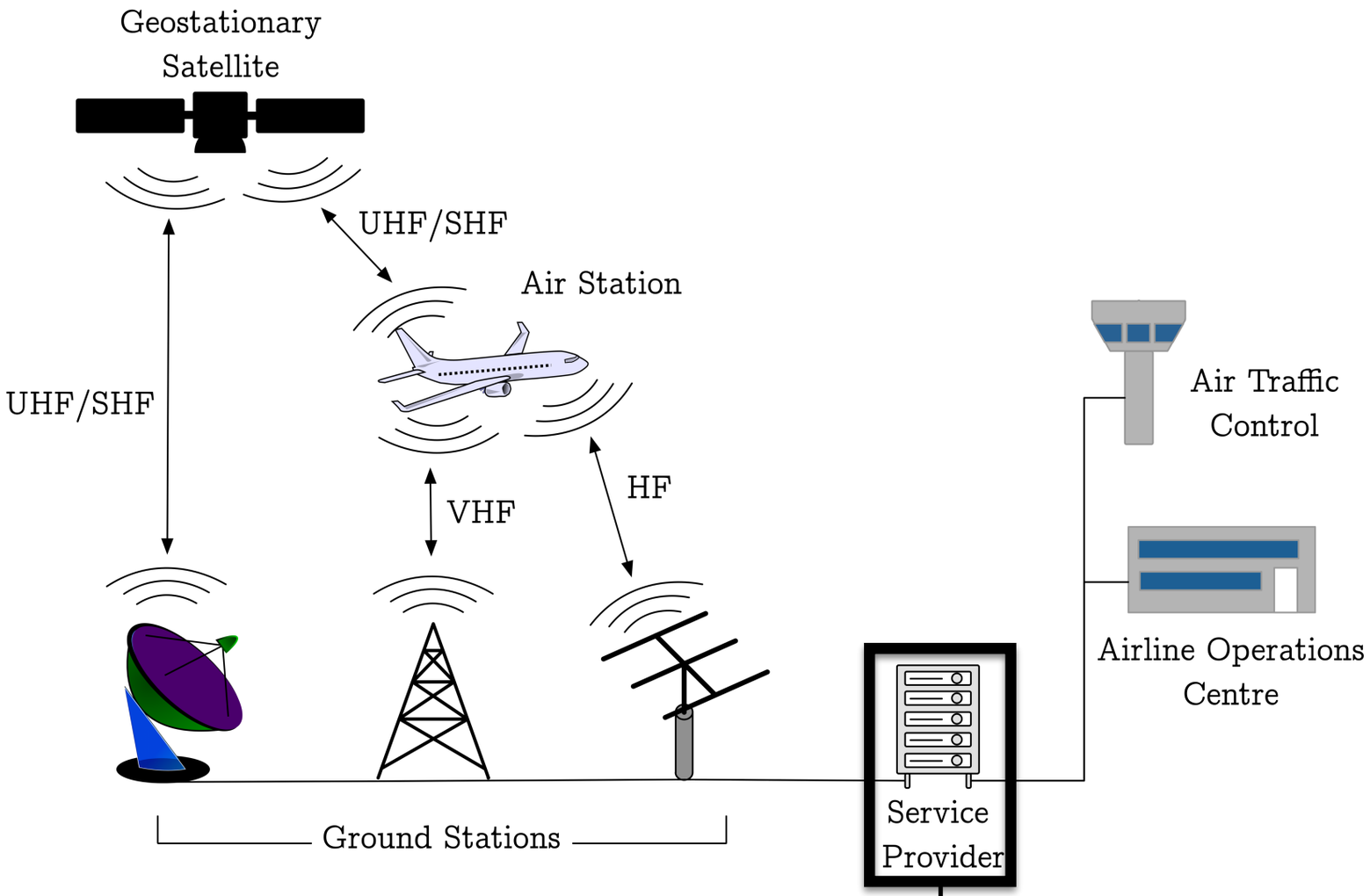
- Aircraft Communications Addressing and Reporting System (ACARS) is a widely-used avionic data link on both commercial and non-commercial aircraft
- Around since late 1970's, it is now used for vastly different purposes to its original intention
- Since then, it has become multi-medium and multi-purpose
- Easily collectible with $10 hardware



What is ACARS?

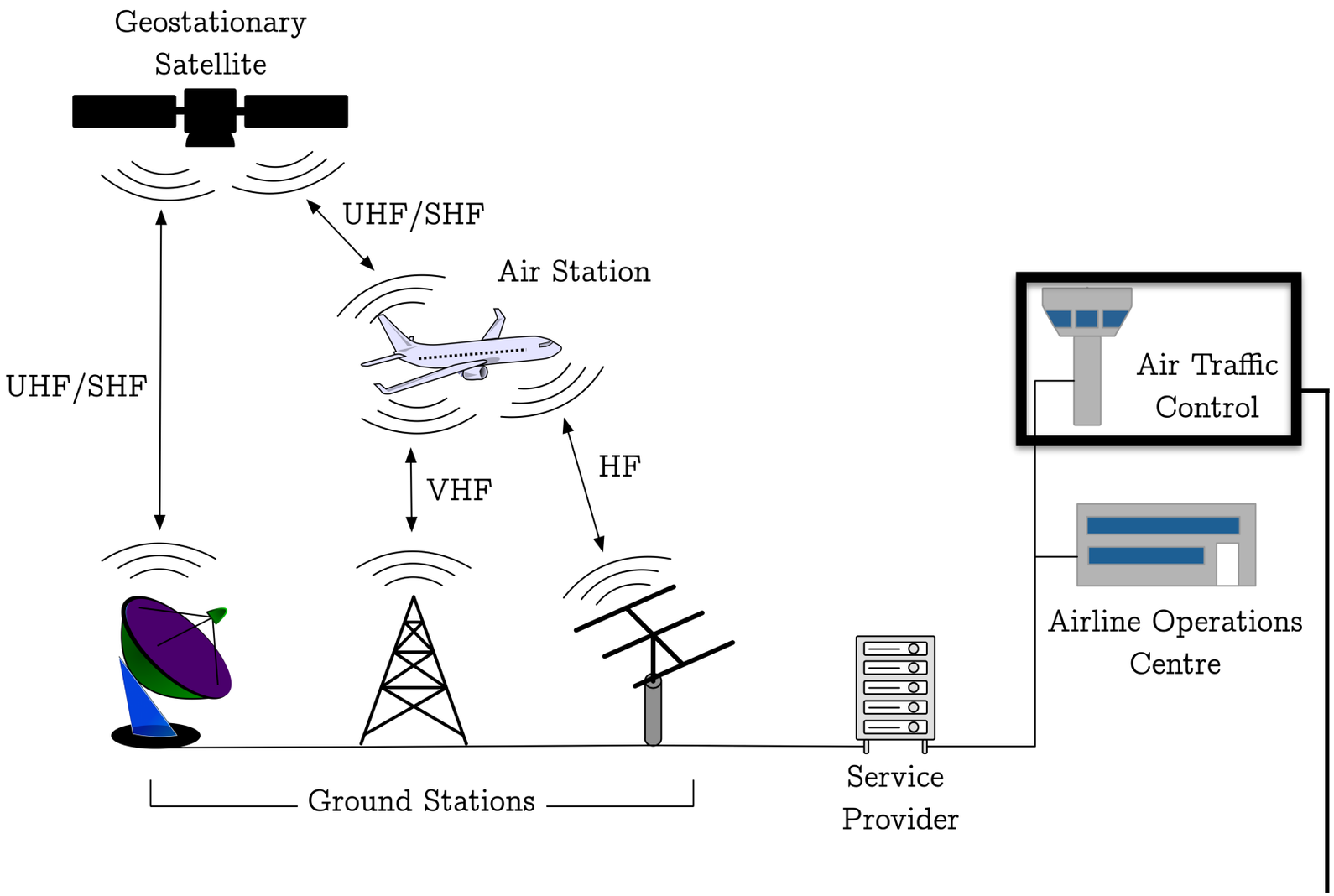


What is ACARS?



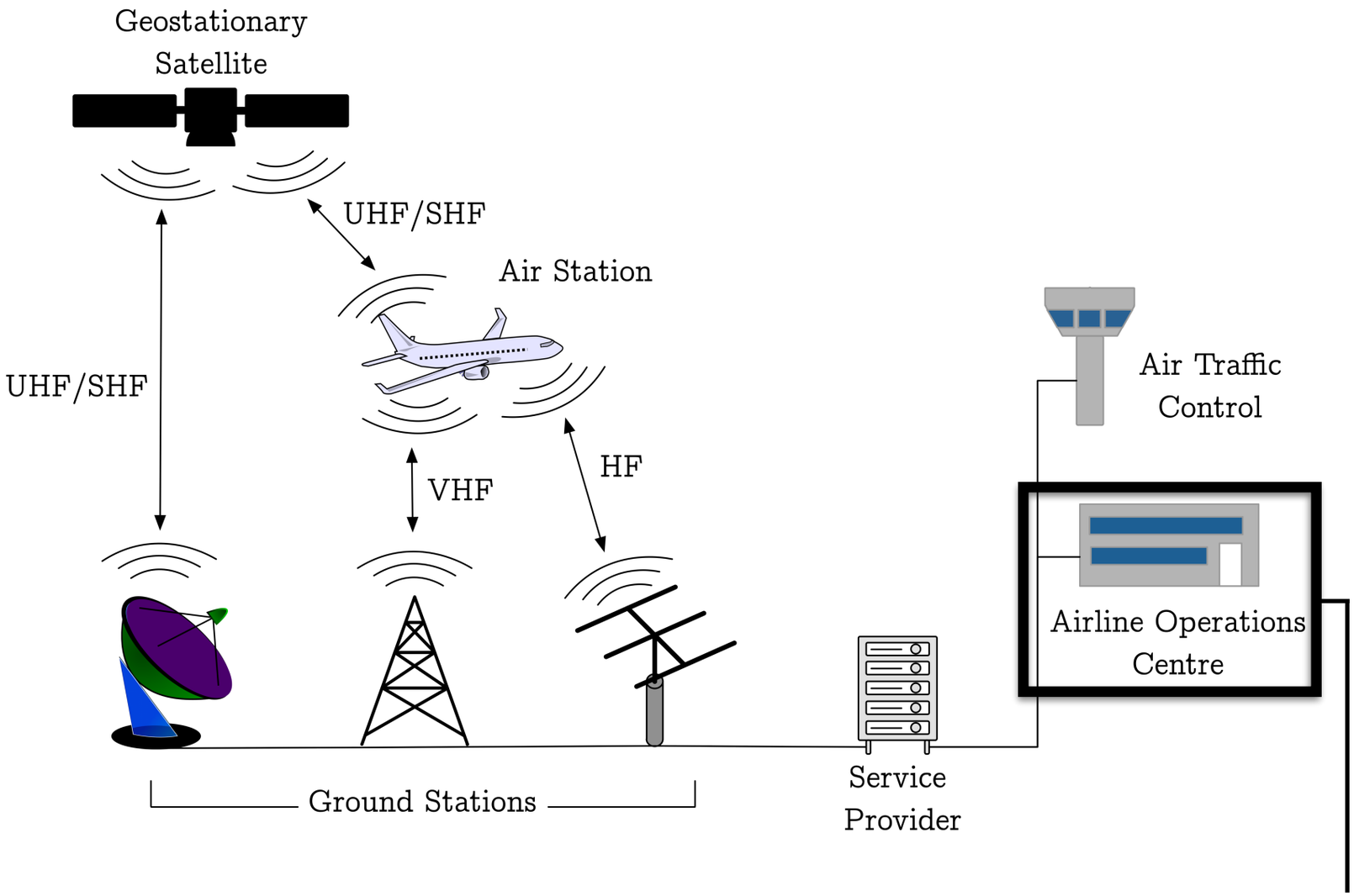
Service provider handles messages – like cell networks

What is ACARS?



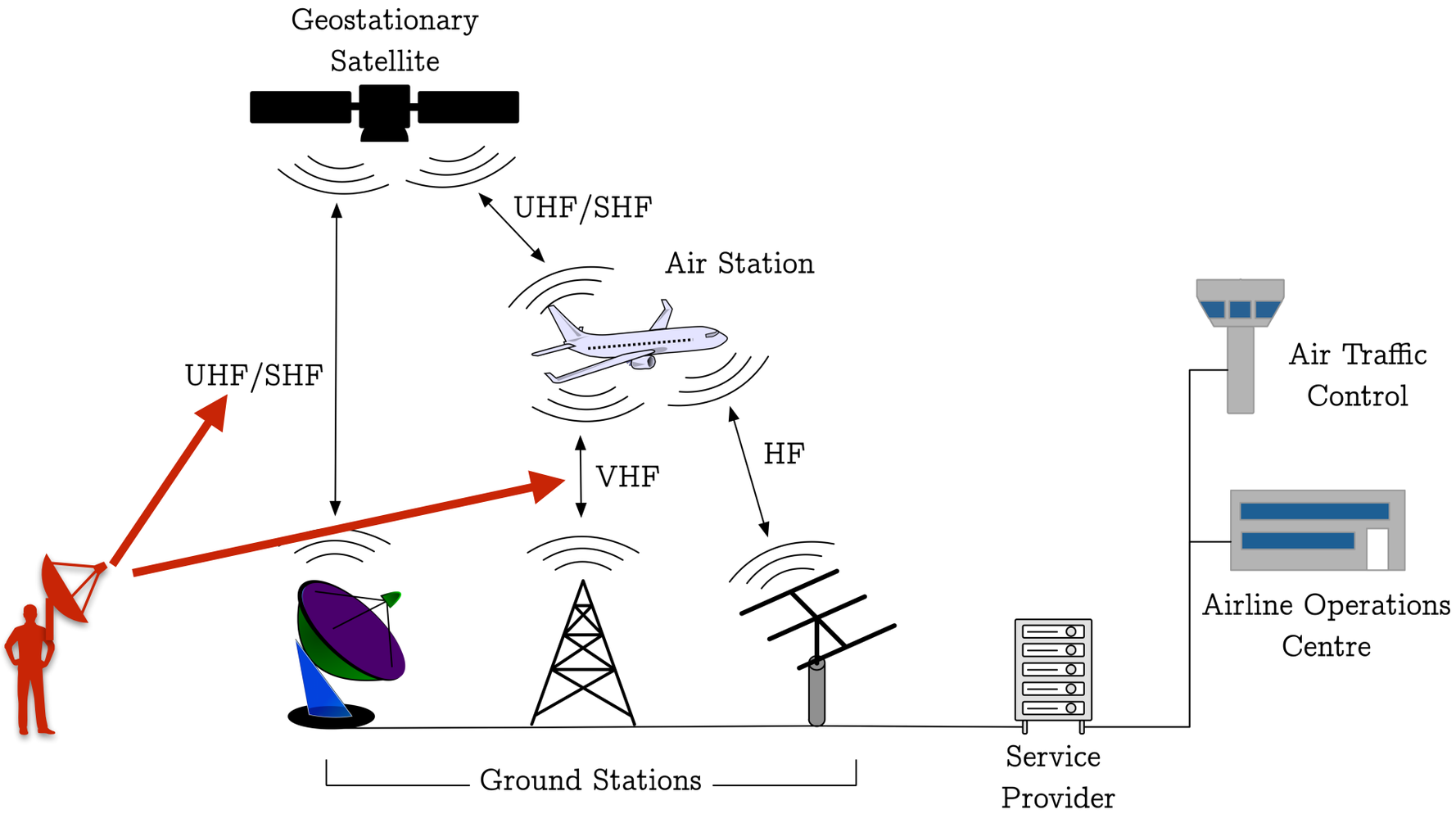
ATC use ACARS to control aircraft without requiring voice

What is ACARS?



AOC communications allow administration in-flight, e.g. passenger updates, gate information

What is ACARS?



Software defined radios collected from one location over 9 months - ~1 million messages

Security in ACARS

- A number of ACARS applications clearly require some authentication or confidentiality – but ACARS has no security as standard
  - ‘Post-hoc’ solutions exist (e.g. Secure ACARS)
- However, it costs extra on top of existing ACARS – this deters users – no use thus far

Security in ACARS

- A number of ACARS applications clearly require some authentication or confidentiality – but ACARS has no security as standard
  - ‘Post-hoc’ solutions exist (e.g. Secure ACARS)
- However, it costs extra on top of existing ACARS – this deters users – no use thus far

Many users require privacy but don’t want to pay

Analysing messages

- We collected over a million VHF and SATCOM ACARS messages, and noticed that some business aircraft were sending scrambled messages

```
07*?X.0)Emk.;M].;4;Dm)m..) Y(*)]s($).M4U).U;;).MmD)..D+0
07*?X.0)EmUmkm]..D00M)4k.)]rr6) Y-\).k.<);4<k);000).;;+U
07*?X.0)EmUmUU]..D0Mk)m;.)]E{-) 6-r).k.;);;;;);4;;)..U+.
```

Analysing messages

- We collected over a million VHF and SATCOM ACARS messages, and noticed that some business aircraft were sending scrambled messages

Key identifier

```
07*?X.0)Emk.;M].;4;Dm)m..) Y(*)]s($).M4U).U;;).MmD)..D+0
07*?X.0)EmUmkm]..D00M)4k.)]rr6) Y-\).k.<);4<k);000).;;+U
07*?X.0)EmUmUU]..D0Mk)m;.)]E{-) 6-r).k.;);;;;);4;;)..U+.

08,suL}Zq`cLLK=LLa`aLZ`YLZP\,0ZPf0,ZLaLYZLKeeZLc}KZLLc[`
08,suL}Zq`tee}=LLaL}KZ}vvZ=yy~ZPuAfZLaYYZYevLZY}eLZLLc[t
08,suL}Zq`KYev=LLK}aKZ}tLZbZbZLaYYZYevvZY`YvZbbbbb

09|\L46c+Ns6,,G4418,hcN84cGeodc-r!Lc4Bh1c8B4hc8BBBc44Z5Z
09|\L46c+N,BZ,G44BBZNc614c-r|Gc-W|Pc4BhZc48hNc48BZcbbbbb
09|\L46c+Ns8NhG44s6,,c6B4c-W|Pc-r.-c4B68c888Bc88NZc44B5,
```

Cipher & usage properties

- 9 static keys were used by all aircraft using the cipher
- Using frequency analysis (and some deduction), we could recover ~76% of the substitutions for the 9 keys using 2690 messages
- All aircraft used the Honeywell Primus avionics suite

Bombardier Learjet 45

Gulfstream G650

Aircraft type

Manuf.	A			B			C	D	E
Model	A-1	A-2	A-3	B-1	B-2	B-3	C-1	D-1	E-1
Avg. Manuf. Year	2008	2008	2014	2014	2010	2012	2010	2002	2011
No./Model	118	56	12	11	3	2	1	1	1
No./Manuf.	186			16			1	1	1

Aircraft type

Manuf.	A			B			C	D	E
Model	A-1	A-2	A-3	B-1	B-2	B-3	C-1	D-1	E-1
Avg. Manuf. Year	2008	2008	2014	2014	2010	2012	2010	2002	2011
No./Model	118	56	12	11	3	2	1	1	1
No./Manuf.	186			16			1	1	1

Aircraft type

Manuf.	A			B			C	D	E
Model	A-1	A-2	A-3	B-1	B-2	B-3	C-1	D-1	E-1
Avg. Manuf. Year	2008	2008	2014	2014	2010	2012	2010	2002	2011
No./Model	118	56	12	11	3	2	1	1	1
No./Manuf.	186			16			1	1	1

Aircraft type

Manuf.	A			B			C	D	E
Model	A-1	A-2	A-3	B-1	B-2	B-3	C-1	D-1	E-1
Avg. Manuf. Year	2008	2008	2014	2014	2010	2012	2010	2002	2011
No./Model	118	56	12	11	3	2	1	1	1
No./Manuf.	186			16			1	1	1

Hidden aircraft

- A significant proportion of aircraft using this cipher also used a block, so do not appear on flight trackers.

Hidden aircraft

- A[illegible]ed a

Hidden aircraft

Hidden aircraft

- A significant proportion of aircraft using this cipher also used a block, so do not appear on flight trackers.
- This implies that they are privacy sensitive – and so are being undermined by the weak cipher

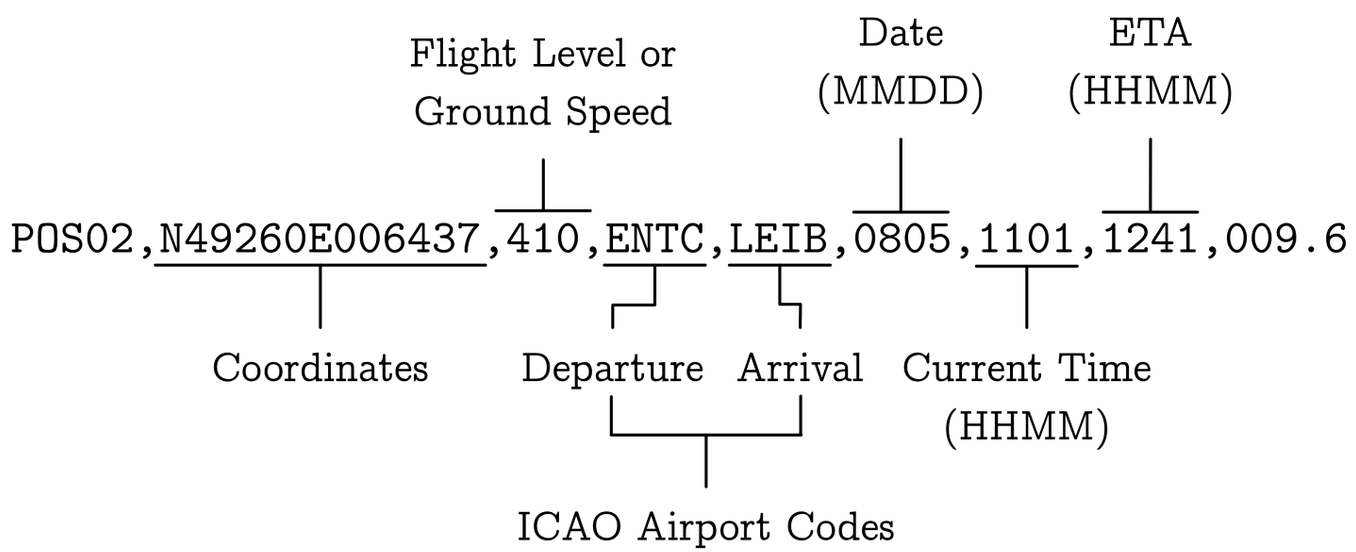
Hidden aircraft

- A significant proportion of aircraft using this cipher also used a block, so do not appear on flight trackers.
- This implies that they are privacy sensitive – and so are being undermined by the weak cipher

Data Set	Not Blocked	Blocked	Total
VHF	5 (10%)	44 (90%)	49
SATCOM	10 (6%)	146 (94%)	156

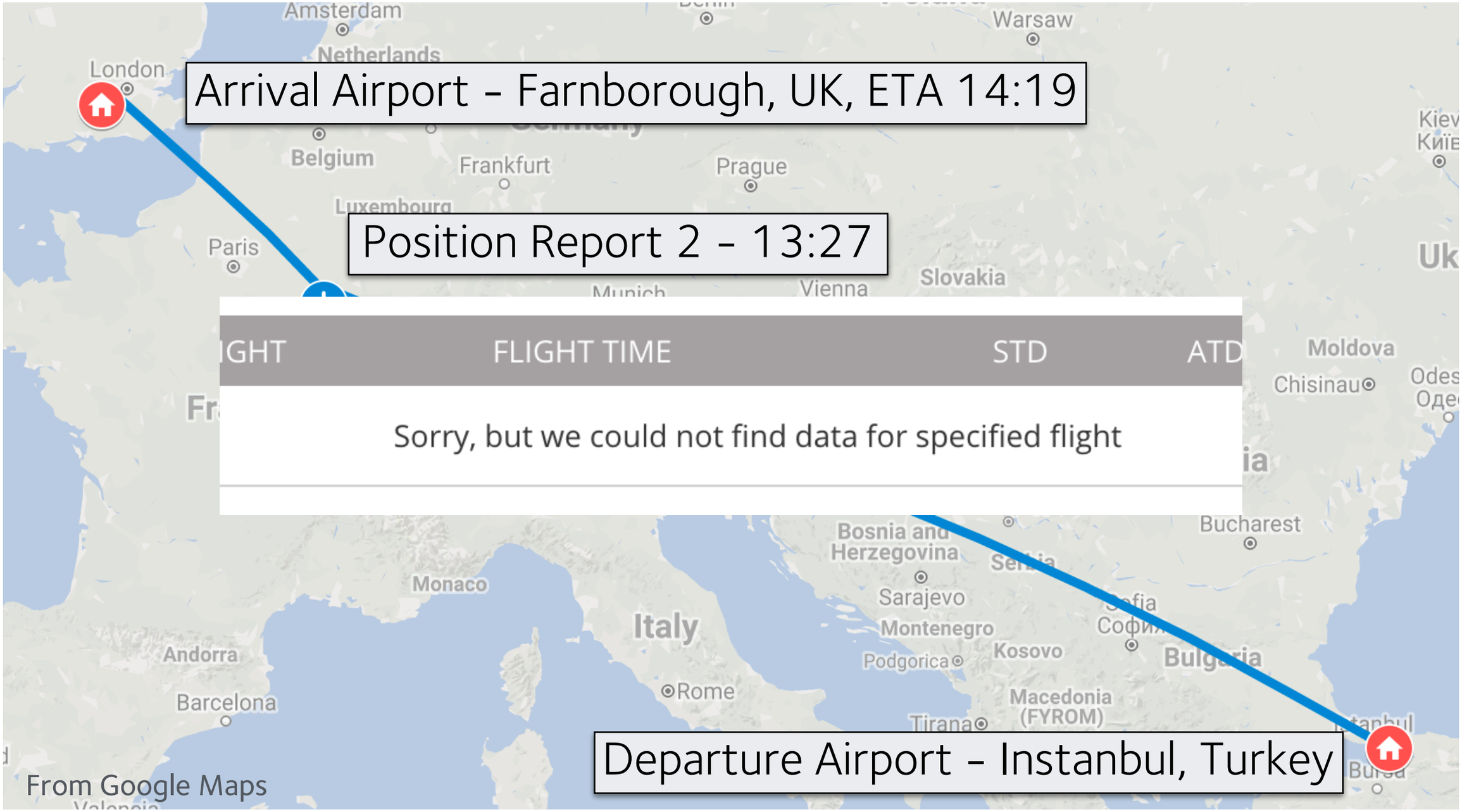
Message content

- 29% of messages were status reports, revealing position, departure and arrival airports



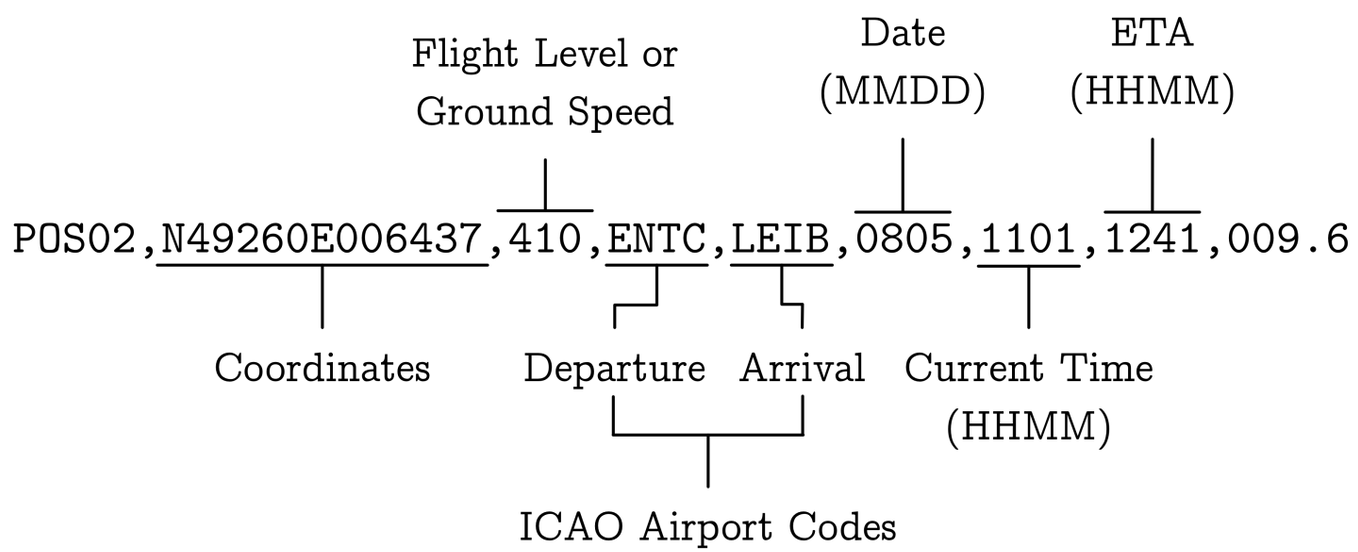
Message content

Message content



Message content

- 29% of messages were status reports, revealing position, departure and arrival airports
  - Blocked aircraft sent 90% of all status reports



Responsible disclosure

- Reported to Honeywell prior to publication and met with a resounding ‘it’s not a problem’
- Cipher isn’t encryption but obfuscation thus not a security risk

> “Obfuscation becomes encryption when a high level of confidentiality is assured. The confidentiality assurance of the substitution cipher is low.”

Full paper: Economy Class Crypto: Exploring Weak Cipher Usage in Avionic Communications via ACARS – FC2017

Questions

Matthew Smith*, Daniel Moser$, Martin Strohmeier*,
Vincent Lenders¥, Ivan Martinovic*

*University of Oxford
first.last@cs.ox.ac.uk

$ETH Zurich
first.last@inf.ethz.ch

¥armasuisse
first.last@armasuisse.ch

Real World Crypto 2018, January 10-12, Zurich

UNIVERSITY OF OXFORD