# On the Security and Privacy of ACARS

Matt Smith*, Martin Strohmeier*,
Vincent Lenders † and Ivan Martinovic*

*Department of Computer Science,
University of Oxford

† Science and Technology,
armasuisse

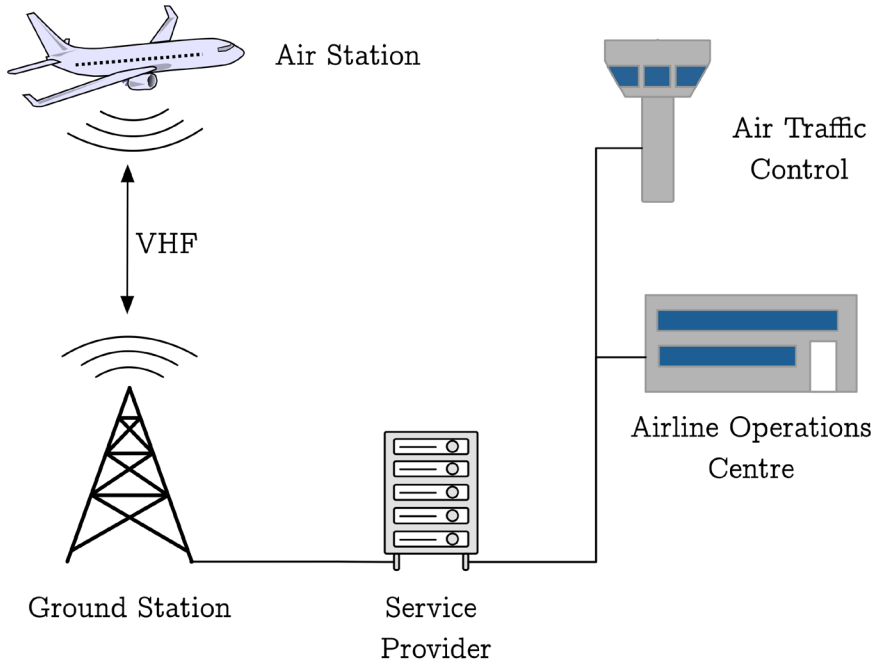
matthew.smith@cs.ox.ac.uk

2016 Integrated Communications Navigation and Surveillance (ICNS) Conference April 19-21, 2016

# Overview

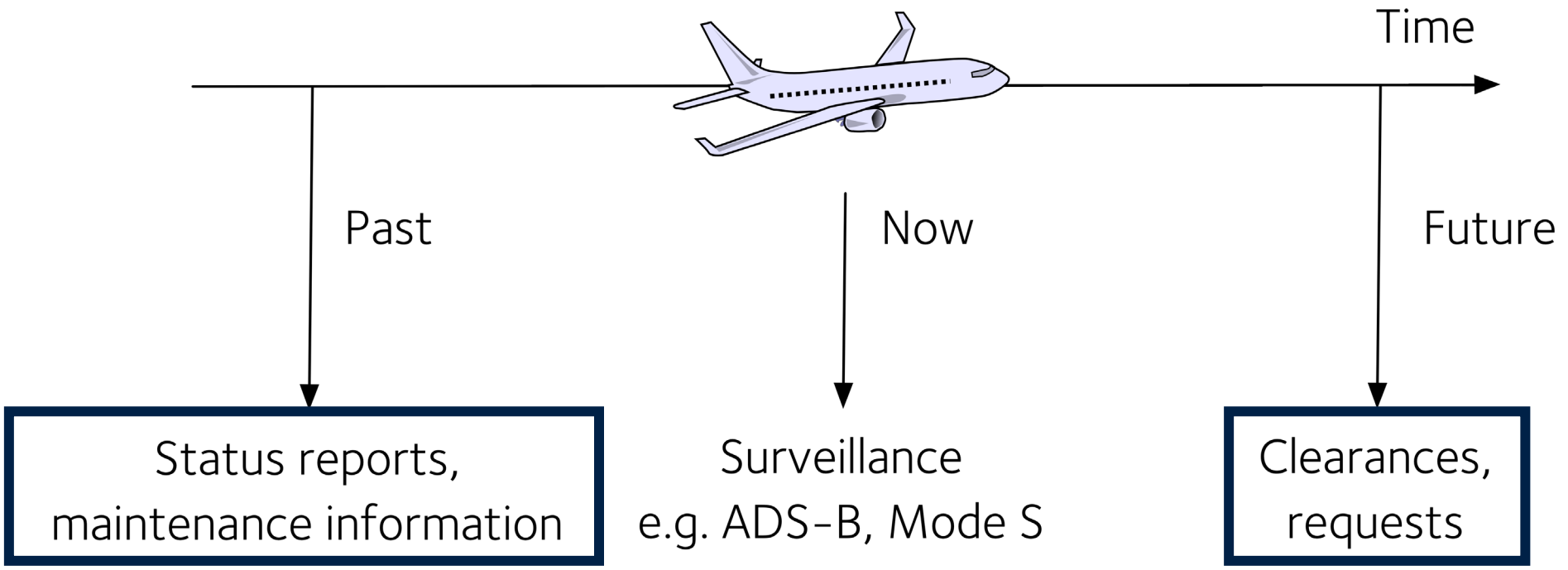
- Why look at ACARS?
- A threat model for ACARS
- Security challenges
- Examples of privacy infringement
- Going forwards

# Introduction to ACARS




- Aircraft Communications Addressing and Reporting System
- Standardised in 1978 by ARINC
- Supports Airline Administrative Control (AAC) and Air Traffic Management (ATM)
- Can provide communications in remote regions and relieve voice in busy areas

# Why look at ACARS?




What has happened up to this point?

What is the aircraft intending to do next?

# Some uses of ACARS

## Flight Plans

Transferred before take-off, such that they can be directly uploaded to the flight management computer

## Free Text

Allowing pilots and crew to directly communicate with ATM or AAC. For example, reporting technical issues so they can be repaired on landing

## Status Reports

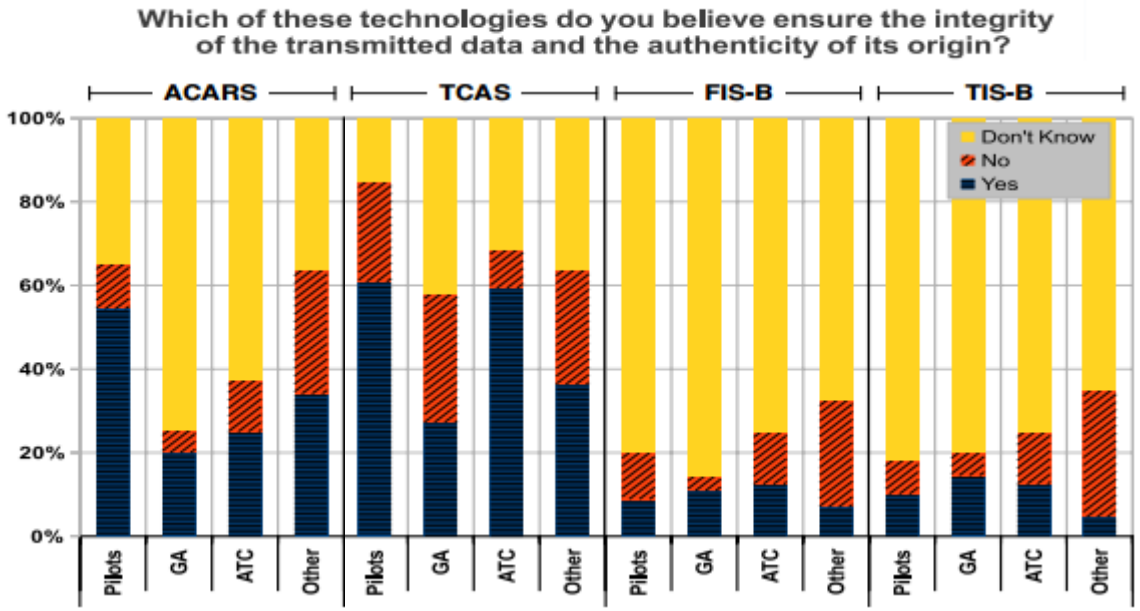
Often containing estimated time of arrival, current position and altitude. Not necessarily tied to ADS-B

## ATC Messages

Enabling traffic to be managed by data connection, ACARS supports ATC clearances requests and responses from aircraft

# Why look at ACARS?

- ACARS provides a key data link between the aircraft and the ground
- Whilst most data is informational, it is considered to have a safety impact
- Those using it have faith in its accuracy and authenticity




From *On Perception and Reality in Wireless Air Traffic Communications Security* (Strohmeier 2016)

# Modelling the threat

- We consider two kinds of attacker – *passive* and *active*
- As in Strohmeier (forthcoming 2016) the threat to avionic systems has changed in recent times
  - Specifically with the rise of cheap software defined radios (SDRs)
- Passive attackers do not interfere with the medium – they simply listen
- Active attackers interfere directly

# Modelling the threat

- We consider two kinds of attacker – *passive* and *active*
- As in Strohmeier (forthcoming 2016) the threat to avionic systems has changed in recent times
  - Specifically with the rise of cheap *software defined radios* (SDRs)

### Passive attacker

- Does not interfere with the medium
- Possible objectives include:
  - Observing out of interest
  - Aggregation
  - Surveillance

### Active attacker

- Directly interferes with the medium
- Possible objectives include:
  - Causing leaks of personal information
  - Attempting to exploit avionic systems
  - Creating confusion for ATC

# Passive attackers

- Often considered weak since they do not do harm directly
- Capabilities consist of listening and collecting data
- Typical setup would include
  - A computer
  - A low-cost SDR
  - A VHF RX antenna


A $10-20 DVB-T USB stick, which can be used as an SDR

*http://swling.com/blog/wp-content/uploads/2013/07/DE_DVB_T_1.jpg*

# Active attackers

- The stronger of the two attackers
- Interferes directly with the system
  - Injection
  - Modification
  - Deletion
- Typically more tightly constrained in order to attack successfully
- A standard setup would include, at a minimum
  - Computer
  - An SDR capable of transmission
  - An amplifiers
  - A TX/RX VHF antenna


A $350 HackRF SDR, capable of TX/RX from 10MHz-6GHz

*https://greatscottgadgets.com/images/h1-preliminary1-445.jpeg*

# Security of standard ACARS

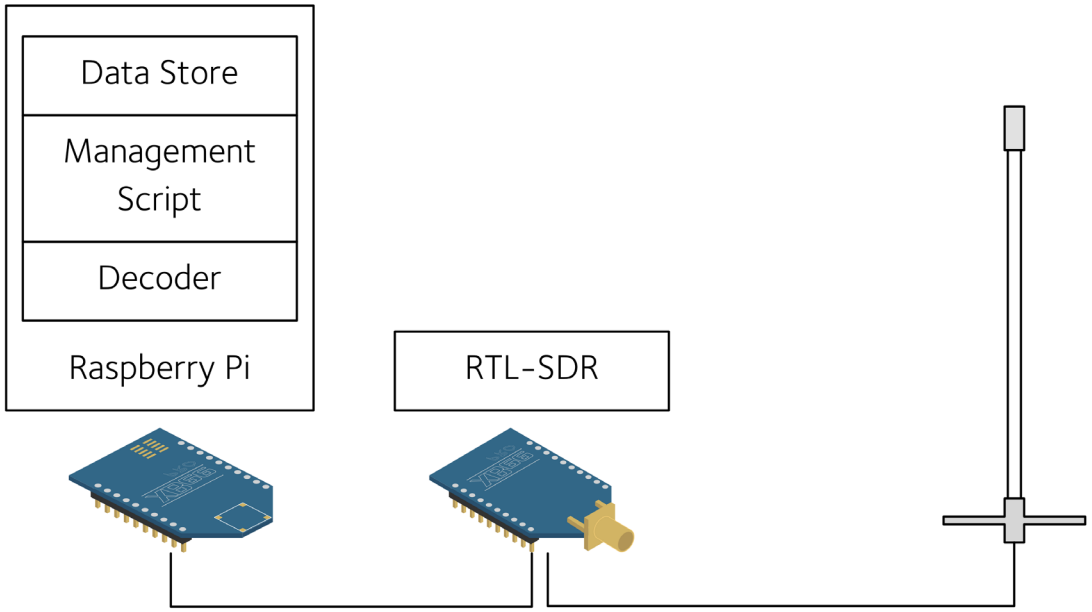
- No security measures as part of the standard
- Common trend in older avionic systems
  - ADS-B – lots of research on its security challenges
  - TCAS – hybrid mode uses ADS-B
- Traditionally difficult and expensive to attack avionic systems, but SDRs changed this
- As such, passive attackers can listen with minimal effort

# Related work

- Much of the existing work considers ACARS 'on paper'
- Roy 2000 - Security strategy for US Air Force to use commercial data link
  - Discusses the applicability of ACARS to USAF needs
  - Highlights the privacy issues of military usage where there is a lack of security
- Roy 2001- Secure aircraft communications addressing and reporting system (ACARS).
  - Proposes *Secure ACARS*, an application layer security system
  - Provides end-to-end security without direct ACARS modification
- Storck 2013 - Benefits of commercial data link security.
  - Identifies the threat from the passive attacker
  - Describes *Protected ACARS*, a more modern application-layer security system

# Experimental Setup

- We wanted to understand ACARS is used in the 'real world'
- Represents our passive attacker
- Uses a RTL-SDR and an open-source ACARS decoder (ACARSDec)
- Standard VHF antenna on top of a four-story building



# Collected Data

- Data collection spanned 63 days, November ‘15 – January ’16
  - ~800,000 messages
  - ~73,000 flights
  - 3962 unique aircraft
- Some aircraft provided positional reports, allowing us to determine our range

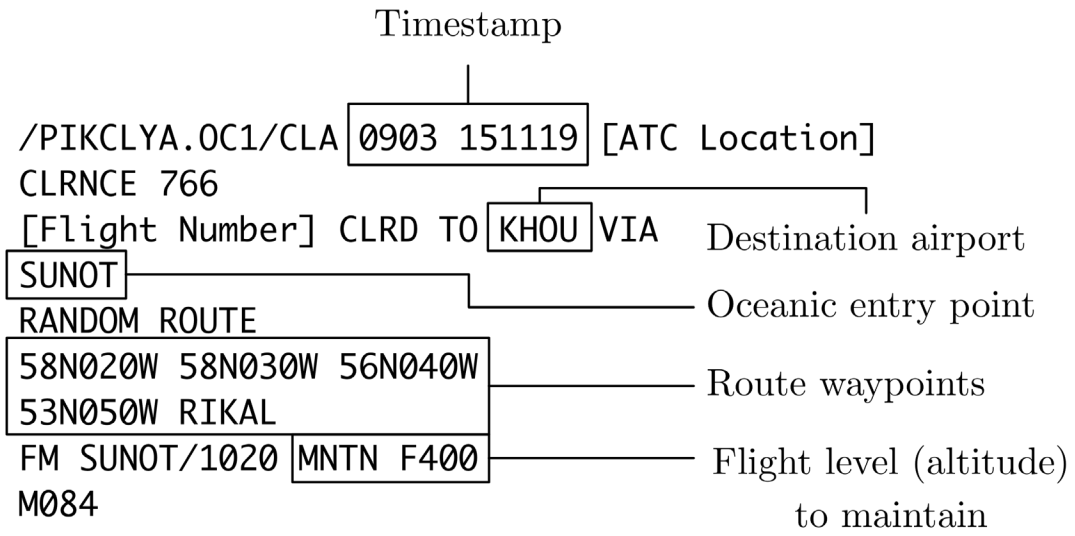
# Encrypted Messages

- Some occurrences of encrypted messages
  - 197 observed from 33 distinct aircraft
- Dominated by one manufacturer of business jets
  - Not all aircraft from this manufacturer sent encrypted messages
  - Not all messages from aircraft sending encrypted messages were encrypted
- Evidence of structure to ciphertext, as if using block mode encryption

# Private civil aviation

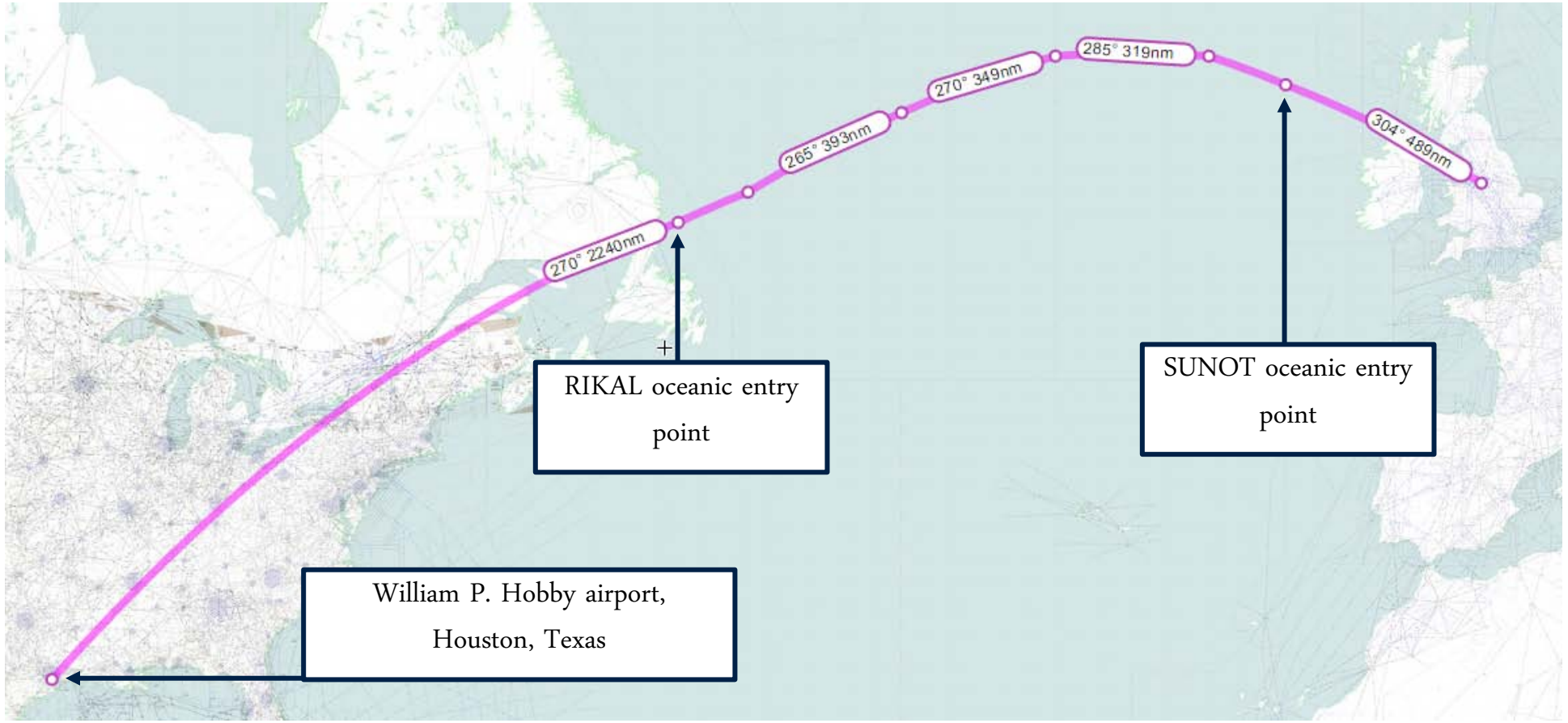
- Many private aircraft do not appear on flight tracking websites
  - Schemes such as the Aircraft Situation Display to Industry (ASDI) allow blocking with a ‘security case’
- Some instances of flight movement being used as ‘insider’ information (Gloven 2012)
  - Tracking when a particular aircraft departs and arrives could reveal business intentions
- ACARS can provide information bypassing ASDI

# Clearance and route information




- We received clearance requests and permissions for oceanic crossings
- Some aircraft had no history of flying at this time, or on this route

# Clearance and route information




https://skyvector.com

# Commercial civil aviation

- Location and intention readily available on flight tracking websites
  - Considered ‘public knowledge’
- ACARS is used heavily for operational and administrative purposes
  - Over time, the uses have outgrown the capability of the system
  - As a result, privacy of those on board is now at risk
- Many examples of privacy breach due to messages in the clear

# Medical issues

Status of unwell passengers reported to the ground to request assistance

*Passenger*

RE PAX SALLY SHE IT
FEELING A LITTLE BETTER
NO FURTHER ASSISTANCE
NEEDED.THANKS

PAX SALLY
HAS COLLAPSED AGAIN
HAVE DECLARED MEDICAL
EMERGENCY

Detailed treatment information passed on to medical staff on the ground

*Departure & arrival airports*

/ EGKK KHOU 21 104017
NO MEDLINK.
PAX TOM 27A HAS LEUKEMIA. GIVEN 2 PUFFS OF INHALER. 325MG ASPIRIN.
ON DRIP FOR REHYDRATION. APPEARS TO HAVE CHEST INFECTION. BP
STAB

# Document issues

Requests for advice on passengers with no travel documents

*'Please advice procedure'*

PLS ADV PROC FOR PAX
WITH POSS NO PASSPORT OR
ID./PAX NAME PAUL.
THANKS

Ground security staff following up on documentation issues for passengers, and advising to monitor them

SECURITY DUTY MNGR
FROM SEC DUTY MANAGER
THIS CONFIRMS PAX ARE SEAMAN. PAX
ROGER HAS
CONNECTING FLT ONTO FR2233 DEP 2230.
MONITOR PAX FOR REST OF FLT.
MANY THANKS FOR YOUR UPDATE.
REGARDS RI

*Flight*

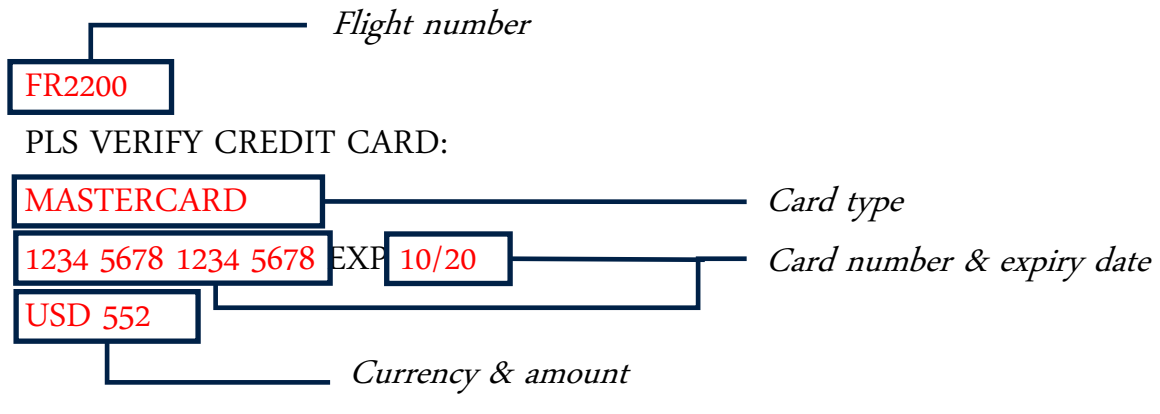
*Flight number, departure time*

# Possessions at risk

Forgotten belongings, including hotel name, room number and specific items

DEAR CCO COULD U PLS
ADVSE CAPT PAUL
TO RECOVER PASSPORT AND PERSONL BELONGING LEFT
THAT CAPT JOHN LEFT IN ROOM 522 HOTEL WESTIN WASHINGTON DULLES AIRPORT

Credit card details, sufficient to make a card-not-present transaction



# What do we do right now?

- Educate crew and pilots about the lack of security on free-text messages
  - It may be the case that the systems they interact with are at a much higher level
- Longer term, move towards ensuring that messages containing sensitive contents are secured in some way
  - Need to begin by classifying what we consider to be sensitive with respect to each type of aviation

# Future Work

- A more geographically distributed investigation to ACARS usage
  - Is our sample representative, or a function of our location?
- Better understanding of how SDRs create security issues for ACARS
  - What can an active attacker do with a reasonable setup?
- Begin to look at how (and whether) we can prevent data being leaked on such a wide scale

# Takeaway points

- ACARS is not designed to transmit sensitive information, despite being widely used to do so
- Whilst systems to help protect the data – such as Secure/Protected ACARS – do exist, they are not used where needed
- It is worth addressing this now, as ACARS will be used in some form for a number of years

2016 Integrated Communications Navigation and Surveillance (ICNS) Conference

April 19-21, 2016

# On the Security and Privacy of ACARS

Matt Smith*, Martin Strohmeier*,
Vincent Lenders † and Ivan Martinovic*

*Department of Computer Science, University of Oxford

† Science and Technology, armasuisse

matthew.smith@cs.ox.ac.uk

# References


A. Roy. Security strategy for US Air Force to use commercial data link. In *19th Digital Avionics Systems Conference (DASC)*. IEEE, 2000.

A. Roy. Secure aircraft communications addressing and reporting system (ACARS). *20th Digital Avionics Systems Conference*, 2:7A2/1–7A2/11 vol.2, 2001.

P. E. Storck. Benefits of commercial data link security. In *Integrated Communications Navigation and Surveillance Conference (ICNS)*. IEEE, 2013.

M. Strohmeier, M. Smith, M. Schäfer, V. Lenders and I. Martinovic. Assessing the Impact of Aviation Security on Cyber Power. *Forthcoming, 8th International Conference on Cyber Conflict (CyCon),* 2016.

D. Gloven and D. Voreacos. Dream Insider Informant Led FBI From Galleon to SAC. 2012. url: http://www.bloomberg.com/news/articles/2012- 12- 03/dream-insider-informant-led-fbi-from-galleonto-sac (visited on 02/12/2016).

M. Strohmeier, M. Schäfer, R. Pinheiro, V. Lenders, and I. Martinovic. On perception and reality in wireless air traffic communications security, 2016. arXiv: 1602.08777. url: arxiv.org/abs/1602.08777.