A Secure and Trusted Protocol for Enhancing Safety of On-Ground Airplanes Using UAVs

Raja Naeem Akram[1], Konstantinos Markantonakis[1], Keith Mayes[1]

Pierre-François Bonnefoi[2], Damien Sauveron[2,3], **Serge Chaumette**[3]

1: Information Security Group Smart Card Centre, Royal Holloway, University of London

2: XLIM (UMR CNRS 7252), MATHIS, Université de Limoges

3: LaBRI (UMR CNRS 5800), Université de Bordeaux

Outline

- Introduction
- Our Contributions
- Requirements
  - Security Criteria
  - Trust Establishment
  - Pre-protocol Setup
- Our Secure and Trusted Channel Protocol
- Comparison – Security & Operational Req.
- Formal Mechanical Validation
- Simulation Test-bed
- Conclusions and Future Work

ICNS 2017

Westin Washington Dulles Airport, Herndon, VA

April 18-20, 2017

Introduction

- Aircrafts are expensive
  - *e.g.* Boeing 747-8 Cargo and Airbus A380

    Estimated price: $ 350 million

    (source: https://www.aircraftcompare.com)

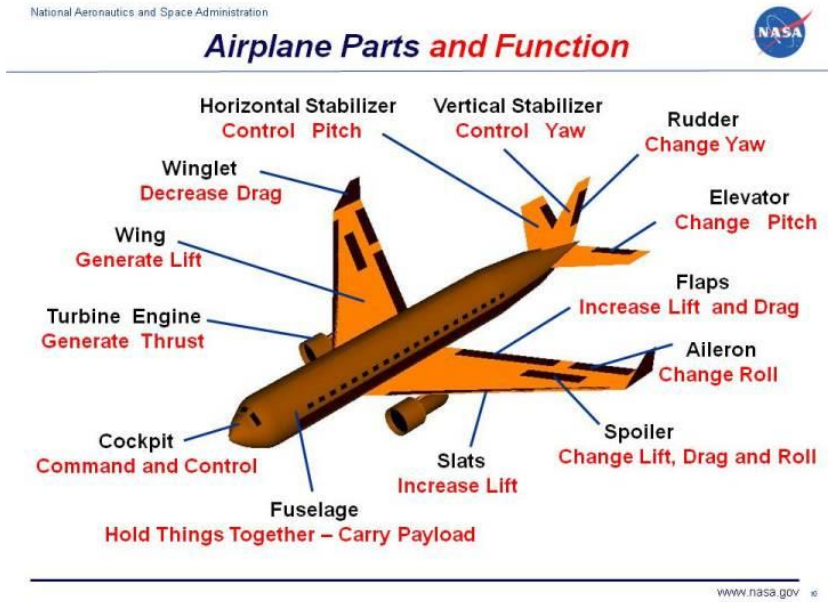
Source: https://www.aircraftcompare.com

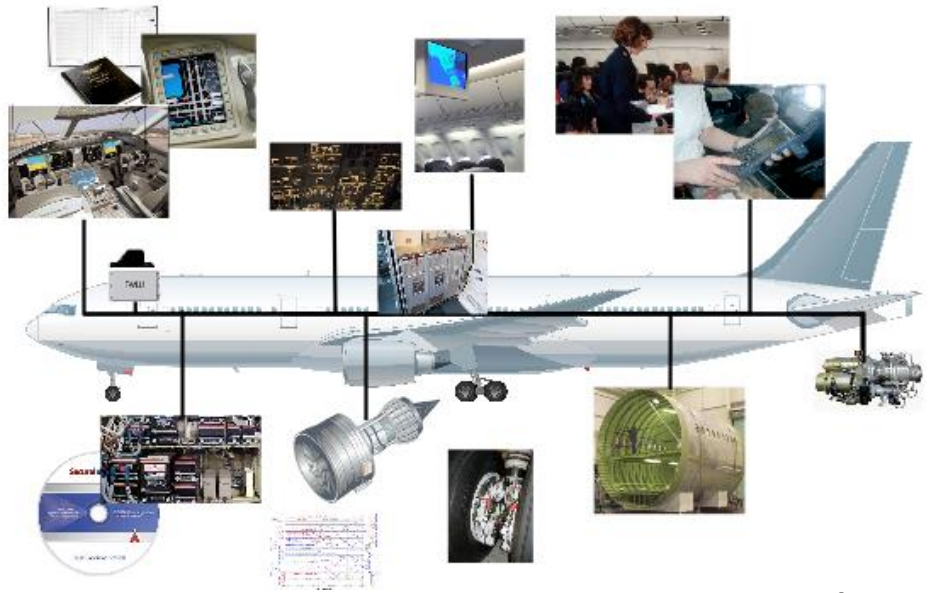
- AOG (Aircraft On Ground) time is not profitable and it thus must be minimized
  - More than several hundred USD per minute
  - However safety checks are done during the stops in airports.
- Rule: **Safety** is the strongest requirement of avionic industries!

Source: https://10mosttoday.com

Introduction (ctd.)

- To minimize AOG time when aircrafts are parked in airport, it is possible to enhance safety and maintenance procedures to:
  - examine fuselage, wings, and other parts of the aircraft
  - collect data recorded by the aircraft during flight(s) by the sensors of the Aircraft Data Networks
  - provide data (parameters, etc.) to the aircraft for the next flight(s)





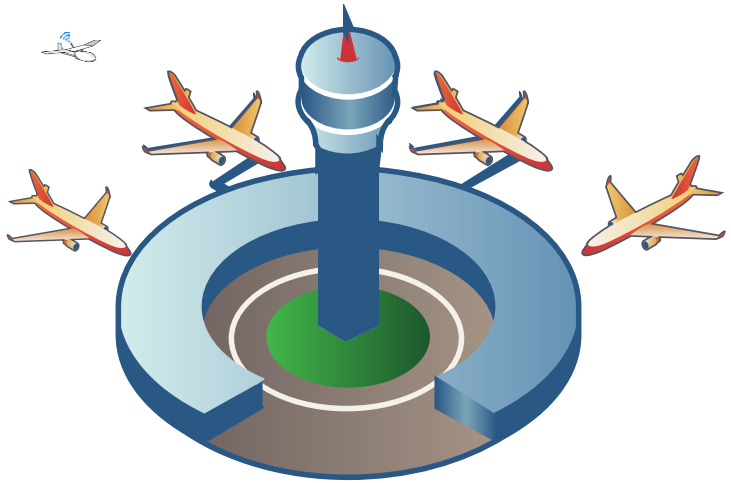
Source: http://www.airinformatics.com/GateLink.html

Introduction (ctd.)

- UAVs will be used in diverse applications from civilian (smart cities, forest fire detection, localization, observation and fighting, quantification of pollutants, etc.) to military (detection of troops, neutralization of adversaries, etc.)

- Our proposal is to use UAVs supervised/controlled by airport authorities to enhance the safety of aircrafts and to minimize the AOG time:

  ➔ Our aim is to be provide the assurance to each party (the UAV and the devices of the ADN) that they exchange only with authorized and trusted devices so as to prevent injection of false data or disclosure of confidential data.



Our Contributions

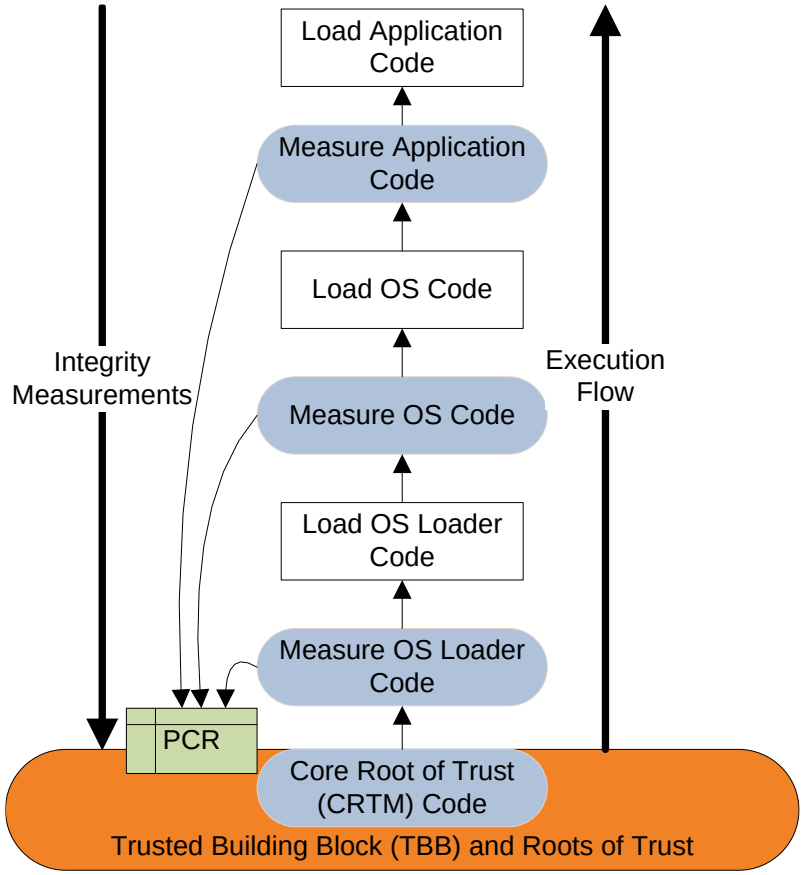
1. A Secure and Trusted Channel Protocol (STCP) for Aircraft Devices (AD) and UAVs that enables to:
   - establish a secure communication between end-points
   - provide assurance that each end-point is secure and trusted
2. The definition of comparison criteria for secure channel protocols
   - related security analysis
   - related performance analysis
3. The validation of the proposed protocol
   - through formal verification with Casper/FDR
   - through Implementation in a simulation testbed

Requirements / Comparison Criteria – Security

1. Mutual Entity Authentication
2. Asymmetric Architecture
3. Mutual Key Agreement
4. Joint Key Control
5. Key Freshness
6. Mutual Key Confirmation
7. Known-Key Security
8. Unknown Key Share Resilience
9. Key Compromise Impersonation (KCI) Resilience
10. Perfect Forward Secrecy
11. Mutual Non-Repudiation
12. Partial Chosen Key (PCK) Attack Resilience
13. Trust Assurance (Trustworthiness)
14. DoS Prevention
15. Privacy

Requirements / Trusting a Device – Trusted Boot (in TPM)

- A Platform Configuration Register (PCR) is a 160 bits (20 bytes) data element
  - stores the result of the integrity measurement (which is a generated hash of a given component)
- $PCR_i = Hash(PCR_i' || X)$
  - X used to cumulate results in PCR_i
- Boot process:
  - Core BIOS => PCR_0
  - Measure of motherboard config + the BIOS => PCR_1
  - ROM Firmware => PCR_2
  - ROM Firmware config => PCR_3
  - OS Loader code, …
- Reporting and Attestation Operations
  - PCRs are signed by the TPM using the Attestation Identification Key (AIK)



Requirements / Pre-Protocol Setup

- Each communicating device (UAV or AD) has a TPM.

- Each communicating device is pre-configured with the signature verification keys (public keys) of the avionic bodies who:
  - have delivered certificates for signature verification keys of its communication partners (*i.e.* public keys of AD and UAV);
  - have delivered certificates for signature verification keys of the TPMs of its communication partners (*i.e.* the public key corresponding to the AIK key used to sign the PCR values stored in the TPM);
  - have signed the trusted and secure PCR values (*i.e.* the values for their trusted and secure state).

- Summary: devices (AD/UAV) and their associated TPM have been certified by the avionic bodies.

Our Secure and Trusted Channel Protocol

Notations

UAV	:	Denotes an unmanned aerial vehicle.
AD	:	Denotes an aircraft device.
$A \rightarrow B$	:	Message sent by an entity A to an entity B.
TPM_X	:	Denotes a TPM of an entity X
X_{ID}	:	Represents the identity of an entity X.
g^{rx}	:	Diffie-Hellman exponential generated by an entity X.
C_X	:	Signature key certificate of an entity X.
N_X	:	Random number generated by an entity X.
$X \| Y$	:	Represents the concatenation of the data items X, Y in the given order.
$[M]_{K_a}^{K_e}$	:	Message M is encrypted by the session encryption key K_e and then MAC is computed using the session MAC key K_a. Both keys K_e and K_a are generated during the protocol run.
$Sign_X(Z)$	:	Signature generated on data Z by the entity X using a signature algorithm [34].
$H(Z)$	:	Is the result of generating a hash of data Z.
$H_k(Z)$	:	Result of generating a keyed hash of data Z using key k.
S_{Cookie}	:	Session cookie generated by one of the communication entities. It indicates the session information and facilitates protection against DoS attacks along with (possibly) providing the protocol session resumption facility.
VR_{A-B}	:	Validation request sent by entity A to entity B. In response entity B provides a security and reliability assurance to entity A.
SAS_{A-B}	:	Security assurance (PCR values) generation by entity A that provides trust validation to the requesting entity B.

Our Secure and Trusted Channel Protocol (ctd.)

1.	$UAV \rightarrow AD$	:	$UAV_{ID} \| AD_{ID} \| N_{UAV} \| g^{r_{UAV}} \| VR_{UAV-AD} \| S_{Cookie}$
2.	$AD \rightarrow UAV$	:	$AD_{ID} \| UAV_{ID} \| N_{AD} \| g^{r_{AD}} \| [Sign_{AD}(AD - Data) \| Sign_{TPM_{AD}}(AD - Validation) \| C_{AD} \| C_{TPM_{AD}}]_{K_a}^{K_e} \| VR_{AD-UAV} \| S_{Cookie}$
		:	$AD - Data = H(AD_{ID} \| UAV_{ID} \| g^{r_{UAV}} \| g^{r_{AD}} \| N_{UAV} \| N_{AD})$
		:	$AD - Validation = SAS_{AD-UAV} \| N_{UAV} \| N_{AD}$
3.	$UAV \rightarrow AD$	:	$[Sign_{UAV}(UAV - Data) \| Sign_{TPM_{UAV}}(UAV - Validation) \| C_{UAV} \| C_{TPM_{UAV}}]_{K_a}^{K_e} \| S_{Cookie}$
		:	$UAV - Data = H(UAV_{ID} \| AD_{ID} \| g^{r_{AD}} \| g^{r_{UAV}} \| N_{AD} \| N_{UAV})$
		:	$UAV - Validation = SAS_{UAV-AD} \| N_{AD} \| N_{UAV}$

$$k_{DH} = (g^{r_{UAV}})^{r_{AD}} \ (mod\ n)$$

$$K_e = H_{k_{DH}}(N_{UAV} \| N_{AD} \| ''1'')$$

$$K_a = H_{k_{DH}}(N_{UAV} \| N_{AD} \| ''2'')$$

Comparison – Security & Operational Req.

Goals	Protocols												
	STS	AD	ASPeCT	JFK	T2LS	SCP81	MM	SM	Asymmetric TKDF	P-STCP	SSH	SSL	Proposed Protocol
G1.	∗	∗	∗	∗	∗	∗	−∗	−∗	∗	∗	(∗)	∗	∗
G2.	∗	∗	∗	∗	∗	∗	∗	−∗	∗	∗	∗	∗	∗
G3.	∗	∗	∗	∗	∗	∗	∗	−∗	−∗	∗	∗	∗	∗
G4.	∗	∗	∗	∗	(∗)	∗			−∗	∗	(∗)	(∗)	∗
G5.	∗	∗	∗	∗	∗	∗	∗	−∗	∗	∗	∗	∗	∗
G6.	∗		∗	∗			∗	−∗	∗	∗	∗	∗	∗
G7.	∗	∗	∗	∗	∗	∗	∗		∗	∗	∗	∗	∗
G8.	∗	∗	∗	∗	∗	∗	∗	−∗	−∗	∗	∗	∗	∗
G9.	∗	∗	∗	∗	∗	∗	∗	∗	∗	∗	∗	∗	∗
G10.	∗		∗	∗	∗	∗			∗	∗	∗	∗	∗
G11.	∗			∗	∗	∗	∗	∗	∗	∗	∗	∗	∗
G12.	(∗)	(∗)	(∗)	(∗)	(∗)	(∗)			∗	∗	∗	∗	∗
G13.			(∗)	(∗)	∗	−∗				∗	(∗)	(∗)	∗
G14.				∗	(∗)					∗	(∗)	(∗)	∗
G15.	(∗)		∗	∗	(∗)				(∗)	∗	(∗)	(∗)	∗

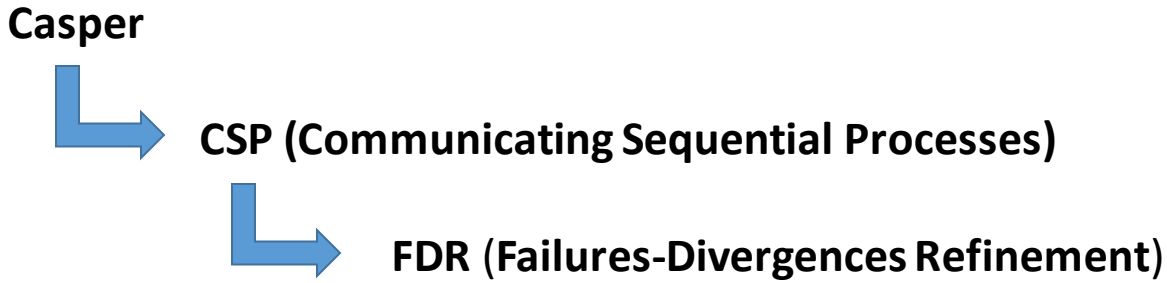
∗ means that the protocol meets the stated goal

(∗) shows that the protocol can be modified to satisfy the requirement

−∗ means that the protocol (implicitly) meets the requirement, not because of the protocol messages but because of the prior relationship between the communicating entities.

Mechanical Formal Analysis

- Using Casper/FDR



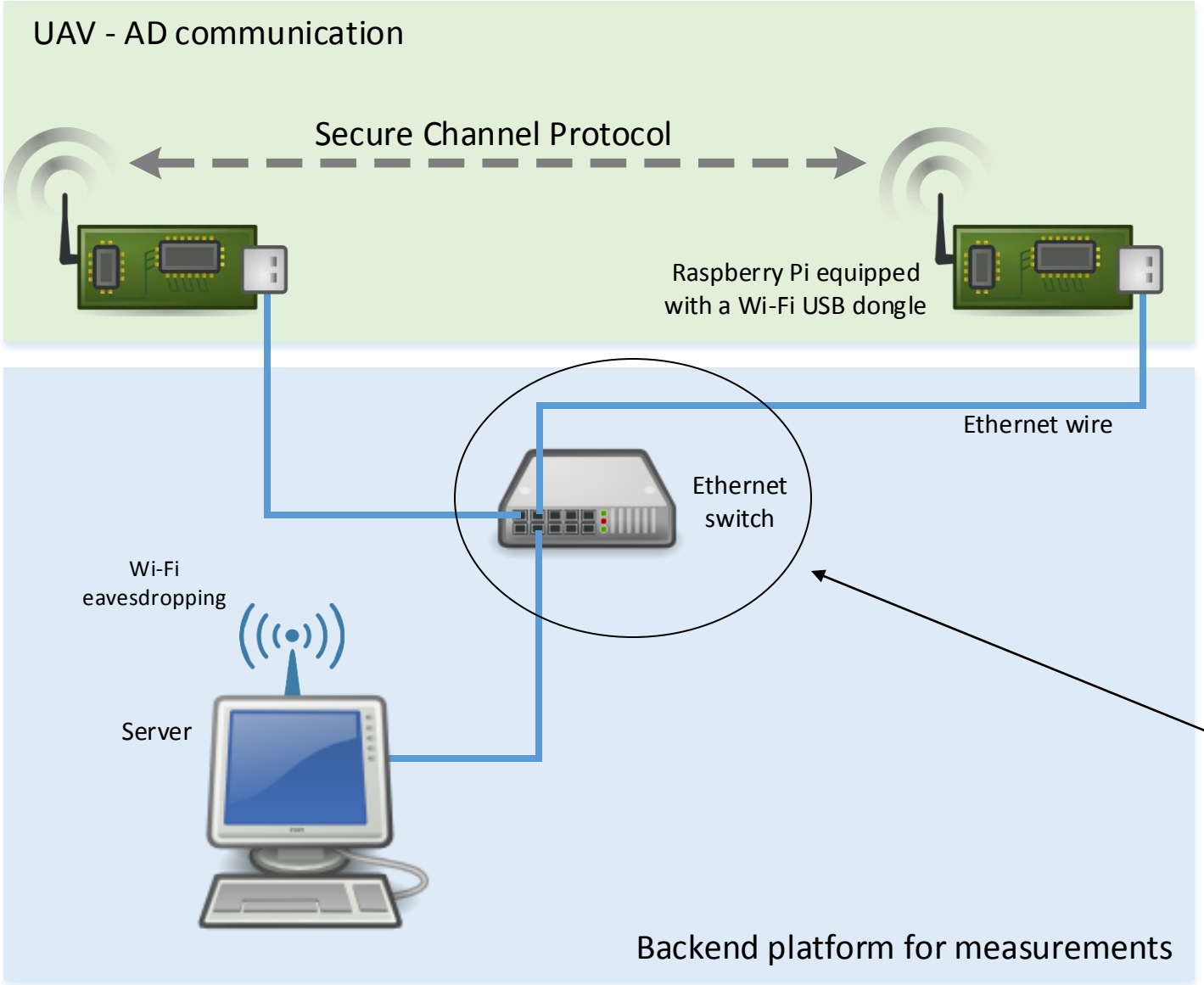
we evaluated the protocol

→**The analysis tool did not find any viable attack with given threat model**

i.e. an intruder:

- can masquerade any entity in the network,
- can read the messages transmitted in the network
- cannot influence the internal process of a TPM in the network.

Simulation Test-bed for UAV – AD communication



Conclusions and Future Work

- As shown UAVs (supervised by relevant authorities) can help to enhance the safety of aircraft and can help to minimize the AOG time

- We will extend the proposal to use UAVs as RFID readers to inventory and track items tagged with RFIDs, both on board of aircrafts along with those used in the area of the airports (*e.g.* luggage and tools for maintenance)

Acknowledgements to

- the **SFD** (**S**ecurity of **F**leets of **D**rones) project
  - funded by Region Limousin;

- the **TRUSTED** (**TRUS**ted **TE**stbed for **D**rones) project
  - funded by the CNRS INS2I institute through the call 2016 PEPS (*"Projet Exploratoire Premier Soutien"*) SISC (*"Securité Informatique et des Systèmes Cyber-physiques"*);

- the **SUITED** (**S**uited sec**U**r**I**ty **TE**stbed for **D**rones), **SUITED2** and **UNITED** (**U**nited **N**etwork**I**ng **TE**stbed for **D**rones), **UNITED2**
  - projects funded by the MIRES (Mathematiques et leurs Interactions, Images et information numérique, Réseaux et Sécurité) CNRS research federation;

- the **SUITED-BX** and **UNITED-BX** projects
  - funded by LaBRI and its MUSe team.

Thank You!
Any Question or Suggestion