Security in Aeronautical Communications
José L. S. Freitas

Instituto Superior Técnico – Computer Science Department
Av. Rovisco Pais, 1049-001 Lisboa, Portugal

Abstract. This document present the project for a master’s thesis in the scope of communications security applied to the context of aeronautics. The aviation environment is very prone to enter catastrophic situations when simple security breaches are explored, such as in 9/11. In a very quickly growing worldwide sector the air transport is increasingly more reliable in communications for efficiency. An in-depth study on strengths and weaknesses of the state of the art and the future security in communications strategies will lead to the establishment of a roadmap for security maximization with the application of novel security paradigms and technologies.

Keywords: Security Communications Aviation Aeronautics Anti-Terrorism Distributed Systems Encryption Software Engineering Quantum RFID
1 Introduction

Since the first hijack ever that took place in the world (Macau 1946?) that aviations has been plagued by terrorism or piracy. Though military aviation presents vulnerabilities (Pakistan’s General Zia explosion in his C-130 in 1988), civil aviation reliability has been the most jeopardized with many hijacks during the 60s and 70s, by ethnical terrorist groups’ propaganda, reivindications and blackmail.

In the 80s with the introduction of X-Ray scans boarding with weapons became more difficult, but bombing still caused many lives lost (Air India 747 1985). In the 90s a new type of threat was revealed to the world: the usage of airliners as a “ram” weapon to cause havoc on ground (Air France Airbus A300 hijacked in Algeria intended to crash in Paris which plot was foiled by the French special group GIGN ([C20]).

The maximum expression came with the 9/11 in 2001 attacks were four airliners seized by terrorists brought down the Twin Towers amongst other targets and totally changed the world. Security measures tightened greatly since the moment not only in aviation, but also in the seas, border legislation and civil rights restrictions.

Though no official proof was ever recognized that the accident in 1986, caused the death of Mozambique’s president Samora Machel when his presidential Tupolev 134 crashed on approach to Maputo ([14]), was indeed caused by tampering with radio navigation equipment, it is highly likely that a terrorist attack could be perpetrated by impersonating existing equipment and supplying false information.

Supporting systems such as the baggage ones are also threatened. The Pan Am B.747 destroyed over Lockerbie in Scotland was a victim of bomb planted in a radio, when terrorists used the baggage system vulnerabilities at Frankfurt and Malta airports ([24]).

Very recently, non-professional-terrorist people have been caught in the USA and Australia using simple radios to impersonate Air Traffic Controllers and give false clearances and communications to airliners on arrival. This happened in medium size airports and was more of a youngster prank that a real intent to create any sort of disaster, but can create serious danger to navigation and increase collision risk.

Nicknamed the “Roanoke Phantom”, for early ‘90s an unidentified man pretending to be an air-traffic controller transmitted false radio messages to airplanes above the Roanoke, Virginia, airport. On one occasion he impersonated a pilot and broadcast a distress call. He was an unemployed person using a 500 USD mail ordered radio. Official numbers for such attacks are kept confidential, but the British civil Aviation Authority (CAA) revealed that in the first half of 2000, they had recorded twenty complaints due to false air-traffic-control.

As of today, aviation relies on communications for a huge variety of purposes. Air traffic control, navigation, access to maintenance help, company operations planning, logistics, weather briefing, and revenue from passengers’ services, are all dependent of reliable communications means. Security is a aim in all of them, nonetheless, the degree of achievement and protections greatly varies.

The biggest paradox can happen on an American Airlines Boeing 777-200ER flying from New York’s John F. Kennedy airport to London Heathrow. A passenger in Business class may use it laptop to connect via wifi a LAN to the broadband service that is done with a satellite communications data link. He may be an unsecured wifi link to the hotspot but then connect to his company’s VPN or his bank website using the latest cryptography algorithms and security protocols. Same goes for the secure payment of the wifi access with the credit card.
Meanwhile, in the front of the 150 000 Million USD airplane, the captain may be contacting London Air Traffic Control to receive clearance to land at Heathrow airport, while on a final approach just over Westminster. He will use his microphone that is connected to a very simple VHF radio on an open broadcast frequency. Authentication is done by starting each communications as the own, addressee and message. The next examples “American 132, London Control, on Final approach”, shows an American Airlines flight directing a communication to London Control centre and stating flight status.

Closer, in Portugal, TAP Portugal has one Airbus A319 equipped with the Airbus OnAir system that allows mobile phones to be used in flight. While mobile GSM communications are very difficult to eavesdrop or impersonate, the pilot will be using the VHF open channel for critical communications while the passenger will have access to much higher state of the art secure system for his personal calls.

Not only air people do not know each other by voice, but the fact that there is no pre-emption makes for communications sometimes being cut by others and parts of the messages get lost. In the biggest accident ever in aviation, at Tenerife’s Los Rodeos in 1977, when a KLM Boeing 747 collided with another from Pan Am, one of the major causes of accident was the overlapping of communications in the frequency. In very condensed airspaces and airports hundreds of aircraft of different sizes and countries pass in an hour. The throughputs have been increased in all major airports in the world and the prevision is for growth, despite oil prices and financial crises. Automatic sequencing of aircraft in congested areas like central Europe (inside SESAR, the, Single European Sky ATM Research project) and Northern Atlantic along with reduction of separation minima (RVSM), is the target of Air Traffic organization in Europe and Northern America. This will assume a risk in collisions that will be mitigated with higher technology. Communications will be the major player in these developments as aircraft will be constantly sending out position reports to each other (Automatic Dependent Surveillance-Broadcast—ADS-B) and navigations directives given by ATC controllers will be given via digital data-links such as Controller Pilot Data Link Communications (CPDLC).

Nowadays airplanes cannot be lost of sight by ATC or the others, they must either be visible from the tower when on ground, through radar (primary, secondary or ground), or through transponders or when no surveillance means can cover, pilots must report their position on a regular basis. A transponder is by definition an emitter than responds on request from a given receiver. All aircraft in controlled air space, no matter the size, must have one in operation. Normally the Mode-C transponder (called mode Charlie), responds to interrogations from ground secondary surveillance radars (SSR) by providing a four byte code and the aircraft barometric altitude expressed in hundreds of feet. The four bytes identify the aircraft by correlating it with a database where all flight plans are stored. These byte codes are assigned by ATC service providers and there are specific codes for piracy (5500), communication failures (5600) and emergencies (5700). Airliners that carry more than thirty passengers are required to have a Traffic alert and Collision Avoidance System (TCAS) equipment which, based on transponder exchanges, can provide up to a minute warning on imminent collision This is called a Traffic Advisory (TA), and TCAS can give a avoidance manoeuvre Resolution Advisory (RA) to pilots a few seconds before collision if no avoidance measure was taken after the first warning.

The tampering with the position data given by aircraft can lead to major disasters. One scenario that is worthwhile looking into is the traffic movement at Amsterdam’s Schipol Airport. It is one of Europe’s major hubs and processes over sixty million passengers per year. In a great deal of the year visibility is very low and from the single existing tower, controllers cannot see the whole airport area that comprises six runways and innumerous taxiways and parking stands. Controllers must keep track of dozens of aircraft that look the same as the registration number cannot be seen from more than twenty metres away and most the equipment is KLM painted alike. Ground radar is
used but cannot identify the aircraft and is not reliable with bad weather. So controllers
keep mental image of the aircraft whereabouts while asking for pilot reports of their
positions. It is worthwhile mentioning that a foreign airline pilot will not know the
huge Schipol airport very well and will use a map (paper charts mostly) to move
around. In low visibility operations (LVO) it is frequent that the flight crew sometimes
miss a turn or two. The danger of a collision on ground is still high. A few years ago a
Swedish SAS MD-80 crashed while taking off at Milan Linate, after colliding with a
business jet that had inadvertently entered the same runway, in a bad visibility evening.

New studies have emerged and ADS-B will help to provide instant reliable aircraft
situational awareness. These new systems will be reliable in the sense that the data will
be provided with accuracy and with a very high rate of availability but the security
aspect is far from state of the art. However, as for instance, there is no cipher in these
communications.
2 Objectives of the work to be performed

The objective is to define a roadmap for security measures possible in aeronautical communications to achieve until the end of the next decade. A plan of which technologies and where and how to apply them, and the benefits that arise from their introduction will detail on how to cope with present and emerging threats.

The first sub-objective is to analyze all the communications channels and technologies that are nowadays used in aeronautics. In parallel, initiatives related to future development in the fields will be studied and the roadmaps that are being defined will be scrutinized for weaknesses and strengths. Programmes such as Eurocontrol’s SESAR are the reference in many areas, in this case, in Air Traffic Control.

Independently of all aeronautical ongoing research activities an assessment on present and near-future information security technologies that cover the next decade will be carried out. The aviation business is very conservative in terms of technologies due obvious to safety concerns. The emerging paradigm of quantum security will be the major candidate to apply in.

This study will aim to the civil market, while nonetheless identifying links with the military industry. Technologies developed for these will be assessed, such as NATO Link 11 and 16 encrypted ground-air and air-to-air data links. This already equips the Lockheed-Martin F-16s of the Portuguese Air Force, installed under the running Mid Life Upgrade program, and is a requirement for NATO forces in joint operations. Care will be taken to avoid “reinventing the wheel” as a very great deal of civil aeronautics technology is previously validated in defence systems. The same can be said about many technical achievements in terms of security.

This study shall focus on the technical aspects of security in the aeronautical communications means. Aviations is a very risky market for investment and airlines rarely invest in any equipment unless it is mandatory by air legislation bodies, and even so, only with very strong rationale backing it. All solutions proposed here will have impact on costs, operations and legislation that concerns the aviation. A chapter on “Economical, regulatory and social impact” will discuss how feasible it would be to implement changes.

By aeronautical communications it is not meant only Air-to-Air or Air-to-Ground communications. Other relevant channels such as internal communications inside the airport and baggage control systems will be part of the work. Departure Control Systems (DCS) are becoming increasingly more integrated and complex. They are used to check-in passengers and in some cases communicate passport information for US border security systems, having to deal with newer e-Passport or ID cards. Baggage systems are very outdated and on a verge of major turnaround in terms of tracking. International standardization body IATA has made RFID usage the next target technology for baggage security. These and other communications on ground will be covered as air security is said to start on ground.

Airlines have own air-to-ground communication systems that they use for operational aspects. Airbus has a system called Air Traffic Services Unit (ATSU), an avionics computer built by Airbus for installation in newer models of their aircraft that performs the functions. ATSU serves as an online maintenance port, and engineers can remotely do critical updates and reconfigurations while the aircraft is airborne. This is a serious target for terrorist purposes, despite needing higher complexity technology than they normal hold and grasp for use.

However, the proposed solutions cannot interfere technologically with the aviation equipments and technologies. Safety importance is much beyond security and all systems that are installed on board must comply with a vast set of regulations and
standards. The issue of weight, power consumption and size of any equipment put aboard is also crucial. All security technological solutions studied will have assigned a safety risk assessment.

It is known fact that there will never be a perfect and unbreakable security system. No system can certify the human users, that can make mistakes as simple a putting a password on a post-it stuck to a PC screen. Pirates and terrorists are tireless in learning how systems work and circumventing the protection they offer. In this aspect, the objective is to make it as difficult, complex and costly to explore any vulnerability in the security mechanisms.

3 Related ongoing activities

Many ongoing projects and research clusters/networks/groups address all the aeronautics areas that are proposed for study in the thesis. Most of bigger of the stake holding organisations participate in Research, some of them the leaders of the initiatives.

Due to heavy funding in Europe, via the European Commission and its Framework programmes that support security and aeronautics, there are many results publically available. The participation of the industry, end-users and authorities ensures global vision and validated results.

Commercial minded organisms in the likes of the International Air Transport Association (IATA), the association of airlines and travel agents, have working groups dedicated to improve costs and efficiency of the air transport. Standards are typically the relevant outputs.

The dissertation will consider inputs from the following initiatives:

3.1 Eurocontrol’s SESAR

EUROCONTROL is a European organisation dedicated to the Air Traffic Control improvement in the continent. Their mission is to harmonise and integrate air navigation services in Europe, aiming at the creation of a uniform air traffic management (ATM) system for civil and military users, in order to achieve the safe, secure, orderly, expeditious and economic flow of traffic throughout Europe, while minimising adverse environmental impact.

SESAR is a huge project aimed at carrying out the integration of European airspace, and covers legislation, procedures and technology. One of the security objectives is to determine effective mechanisms and procedures to enhance the response of ATM to security threats and events affecting flights (aircraft and passengers) or the ATM system.

There is a good possibility to standardize the Air to Ground communications as IP networks, and vast developments can be applied in this context.

The USA-led reciprocal programme in North American is the NEXGEN. Compatibly with SESAR will exist to support intercontinental routes, pilot training and qualification, and aircraft onboard equipment standardisation.

3.2 European Commission

The Seventh Framework Programme (FP7) is designed to support a wide range of participants: from universities, through public authorities to small enterprises and researchers in developing countries. It has a variety of areas, which of interest are the Aeronautics and Security and Information and Communication Technologies (ICT).
In Aeronautics past and present, EC has funded projects that are very interesting. In aeronautics we can name: EMMA, SOFIA, ASSTAR, FLYSAFE, for instance.

Security calls have raised some positively innovative results, in some cases directly connected to aviation. Example is the PATIN project. Border security can benefit from GLOBE consortium released materials. In the ICT call a few projects are dedicated to information security, with forums and workshops organised frequently.

The EU-funded project CASAGRAS (‘Coordination and support action for global RFID-related activities and standardisation’) is to be considered. It aims to provide a framework of foundation studies to assist the European Commission and the global community in defining and accommodating international issues and developments concerning radio frequency identification (RFID).

At the job, several proposals have been submitted in the EC FP7 that will prove very helpful as source for information and new developments. They shall come alive during 2009.

3.3 NATO STANAGs
The North Atlantic Treaty Organisation (NATO) is a global defence force comprising many countries in the world, mostly in the EU and North America. Comprehensive studies have been put into creating interoperable response forces, by combining different counties’ armed contingents in single, stronger and effective armies. Harmonisation of communication technologies and integration of procedures and nomenclature have been achieved with prove success.

STANAG is the NATO abbreviation for Standardization Agreement, which set up processes, procedures, terms, and conditions for common military or technical specifications. Secure airborne data links like LINK16 may solve some civil security problems.

3.4 IATA baggage Working Group
IATA is the most important association of commercial aviation. It concerns itself mostly about the economics aspects of air travel, and provides a clearing house for international payments. Notwithstanding, it emphasizes technical developments that improve the efficiency of the industry, through study groups like the Baggage Working Group.

The BWG is open to all IATA member airlines, airports and the participants in the IATA Strategic Partnership Program with an interest in Baggage Management and related issues.

To improve security in baggage handling and processing, the BWG has issued Recommended Practices such as RP 1740C ([6]) that addresses Radio Frequency Identification (RFID) and its technological requirements.

Some systems have reached operational level despite being effective for one airport only. In the USA the McCarran International in Las Vegas and the one at Jacksonville, Florida, stand out as the only two operational RFID baggage systems. In Europe there have been only evaluation trials, at London Heathrow and Amsterdam’s Schipol. In Asia the sole example implemented is Hong Kong’s new airport, Chek Lap Kok.

3.5 ASAS-TN2
ASAS-TN II is shorthand for "Airborne Separation Assistance Systems Thematic Network 2". The main purpose of the ASAS-TN II project is to accelerate the application of ASAS ADS-B operations in European airspace. Traffic surveillance and CPDLC communications are widely studied in this task-force.
Modern airliners fly in 4-D navigation, altitude, latitude, longitude and time. For that purpose they are flown by Flight Management Systems (FMS) and not by hand. FMS is a computer where pilots introduce routes and it makes the aircraft follow it in very precise fashion, aided by GPS and Inertial Navigation System (INS). It is capable of flying orthodomic routes to travel the real minimum distance from A to B, instead of the constant heading navigation that Auto Pilots (AP) do. Separation from other airliners is performed by the pilots via the AP based on orders send by the ATCs. The next paradigm for separation is the Airborne Separation Assistance Systems (ASAS), are FMSs capable of maintenance of time or space distance between aircraft without human intervention. This will enable to reduce separation minima, thus making airspace more efficient and profitable, while upgrading safety.

3.6 International Civil Aviation Organization

ICAO is the international, virtually worldwide actually, organization for civil aviation standardization and procedures harmonization. It is not a regulatory body, but produce many recommendations that almost all civilize countries have adopted. In Portugal, Instituto de Aviação Civil (INAC) is the regulatory that issues the national norms, based on ICAO publications.

Security procedures and technologies are made, _de facto but not de jure_, mandatory by ICAO. The ones relevant to this study are the ones that apply to anti-terrorist procedures, and communications security. Work on CPDLC is performed under ICAO flag.

3.7 Others

Browsing through IEEE, ITU, and other engineering standardisation organisations will prove helpful as well as looking for single non-European countries projects. Universities with historical background in aviation such as Cranfield could have good inputs. The horizons in information collection shall not be limited to the references in the previous sections.

4 Target Framework

In pure technical terms the results of this thesis will yield an information security framework for the aeronautical environments considered. After the careful analysis of threats and benefits, it will produce diagrams and specifications for the updated frameworks, with rationale to support the changes that are proposed.

The technologies involved are already mature or will have achieved a very high degree of maturity until 2020.

4.1 Concept of communications security

The concept COMmunications SECurity (COMSEC) was brought by the US Department of Defence. It has evolved and spread into many areas and is now widely used in communications related literature. The concept can is about the measures and controls taken to deny to unauthorized persons access to information derived from telecommunications and ensure the authenticity of such telecommunications. It includes crypto-security, transmission security, emission security, traffic-flow security, and physical security of all equipment and channels used.

In particular, the understanding of COMSEC in the thesis works is defined as the following set of properties:
• Crypto-security: The component of communications security that results from the provision of cryptosystems and their use to cipher information. This includes ensuring message confidentiality and authenticity.

• Emission security (EMSEC): Measures taken to deny unauthorized persons access to information derived from intercepting emanations from crypto-equipment, automated information systems (computers), and telecommunications systems.

• Physical security: Physical measures necessary to prevent access of unauthorized personnel to classified equipment, material, and documents.

• Traffic-flow security: Measures that conceal the presence and properties of valid messages on a network. It includes the protection resulting from features inherent in some cryptographic equipment, that conceal the presence of valid messages on a communications circuit, normally achieved by causing the circuit to appear busy at all times.

• Transmission security (TRANSEC): The measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis (e.g. frequency hopping and spread spectrum).

4.2 Existing proven technologies

Common IP networks might become standard in aviation, even substituting ground Aeronautical Fixed Telecommunication Networks (AFTN). In the case of aviation it could assume the form of a secure Virtual Private Network (VPN) over a Wide Area Network (WAN).

In wireless IP, security mechanisms, such as WPA or WPA2 are widely used. These can operate in links with WiMAX and Wifi 802.11n.

4.3 Candidate new technologies

Quantum Security is based on Heisenberg Uncertainty Principle, a result from quantum physics. The principle states that the position of a given particle and its momentum of a particle are related such that if you increase your precision of measuring the position, you decrease the precision of measuring the momentum. The postulate obtained for security means that if any sort of spying takes place, the data coded as photons will be corrupted and the receiver can become aware of the security breach. Quantum cryptography was identified in 2002 by the MIT as one of the ten technologies that will change the world. This technology can be used to exchange cryptography keys between two remote communicators connected by an optical fibre cable, and to confirm the secrecy of that exchange. For smaller ranges, an infrared laser beam travelling through the air can be an alternative to the fibre optics cable. It is discussed that laser beams could even be used to communicate between places far apart, through the relay of the laser beam by satellites.

Quantum security has the one of its greatest advantages in key generation and distribution. Key generation strengths come from the bit size of the key and, by how random are underlying the numbers. Random numbers come from computers’ unpredictable internal parameters like the last bit of the clock. Over many keys generated, patterns can be detected and there is history of the fast growing online casinos getting beaten by the random cards being predicted by human players. A solution has been the Quantum computer generated numbers for which products have been industrialized ([23]).

With Quantum Key Distribution (QKD) the advantages of unobservable channels make the problem of distribution keys before communication very safe ([1]). The secure distribution of private keys is the weakest point of shared-key encryption protocols. It is proven that even if an
eavesdropper possesses unlimited computational power and commercial products are already on the information security market.

4.4 Sub frameworks

In the next subsections it will be detailed the scope and predictable improvements on the existing frameworks. For each of them we present the existing technologies, their application in solving existing security problems.

4.4.1 Aircraft Surveillance communications

Problems: The technologies to evolve and their shortcomings are the cooperative ones, meaning all equipment that provides status of given traffic besides the primary radars. TCAS is based on transponders and is a safety net, providing anti-collision functions. Transponders have a serious lack of authentication as the only thing used to identify an airplane is a four byte code. ADS-B is not uniform worldwide and depends on datalinks such as VDL2, VDL4, 1090 ES or UAT, the difference being on band used. The case of TIS-B where ground stations provide information is more delicate since it is easier to impersonate something on ground than an airborne entity.

Solutions: An authentication system with digital certificates must be created for each aircraft and ATC stations. This will ensure is aircraft is which it is intended to be. An asymmetric key system can be used with each having a private and public key. Aircraft airline get ground updates each eighteen days, normally for navigation information updates. This could be used to distribute, via CD, a new par of keys for the aircraft and for all ATC frequencies in the world. QKD can only be done via optical means which invalidates distribution inside air-to-ground channels (via satellite is still too futuristic). Certificates could be provide by aircraft and validated by ATC. It may be complex for aircraft to validate certificates due remoteness of certificate providers.

4.4.2 ATC communications

4.4.2.1 Voice broadcast

Problems: Air to ground voice goes through two types of channels, both analog. Very High Frequency (VHF) is the one normally serving the pilots and controllers. The 118-137 MHZ band is used for aviation purposes with channels separated by 8,33Khz. At this moment no authentication, cipher or any type of privacy is present. The frequencies are open and all transmissions are in broadcast mode. A radio jammed while transmitting deadlock the frequency making it impossible for others to communicate.

The other channel is the High Frequency (HF) and is rarely used over land. It stands out when aircraft are flying outside of VHF range, which is line-of-sight, and its range is limited by the Earth’s curvature. The HF reaches further out due to atmosphere reflection, and can make contact possible with aircraft flying in the middle of the ocean. There is a considerable amount of noise on the HF analog frequencies, so a Selective Calling mechanism (SELCAL) is used when one aircraft is being addressed, and this makes up for the huge congestion in Oceanic voice communications. The same lack of security, and safety, as in VHF is applicable here.

Solutions: The solutions will be similar to the proposed ones for aircraft surveillance. An authentication system with digital certificates created for each aircraft and ATC stations and airline operators. It may be complex to cipher voice and use and HF/VHF to transmit it in real-time with. This will be taken into account and if it is not feasible, authentication can be used without encrypting the data exchanged.
4.4.2.2 Digital Data Links

Problems: The communications between pilot and ATC will benefit from the digital area improvements in data links. The CPDLC’s main goal is to avoid the total congestion of the limitation of the radio bands, as traffic and airports have greatly increased lately. It will work as text messages being exchanged form ATCs to pilots. These will be pre-formatted and very standard though free text will be available.

There are different implementations over the world as no agreement is existent on a standard-The Future Air Navigation System (FANS) 1/A System used by Boeing and Airbus, is primarily used in oceanic routes by wide-bodies long haul aircraft. FANS-1/A is an ACARS based service and, and uses satellite communications provided by the Inmarsat private service.

Europe has an operational ATN/CPDLC network, at Eurocontrol’s Maastricht Upper Airspace Control Centre and has been extended by the LINK2000+ Programme to many other European Flight Information Regions (FIRs). These operate in VDL Mode 2.

CPDLC is transmitted in broadcast, with no cipher and no authentication, despite being on the verge of implementation in a wide scale.

Solutions: Introduce cipher, safe key distribution and authentication on messages and communicators. Care is to be taken to avoid unacceptable bandwidth increase while improving security in such a way that when messages are intercepted, their use for creating problems while be no longer existing.

4.4.3 Radio Navigation

Problems: GPS is the most precise navigation system available with accuracy ranges of a few dozens metres. It is the support for ADS-B and makes the navigation of the aircraft very precise, by data fusion with the inertial (INS) which is gyroscope based, and the radio navigations aids. GPS is unsafe because it is run by a single country. Natural disaster or policies can lead to a degrade mode, as seen during the Gulf War when the open civil signal was downgraded, favouring the military applications including smart weapons Joint Direct Attack Munitions (JDAM). The GPS signal is so weak it can also be jammed easily. Simpler, but safer because of local administration, radio based navigation aids are very helpful for positioning, directions and precision landings. Every country has ADF/NDB for position finding, VOR radial direction support to waypoints, DME for distance to navigation aids, and ILS for precise landings (very important in LVOs, like Lisbon’s Portela when fog or mist is present). These are all analog and operate in HF, VHF and UHF. They are identified, but not authenticated nor ciphered. As mentioned before, Samora Machel may have been a victim of deliberate false navigation aid. GPS based local aids for precision approaches are being tested in the USA and Europe. They are called WAAS and basically are ground based augmentation systems (GBAS) working as differential GPSs. Safety and not security is the concern in the certification of these.

Solutions: These systems need to have authentication on the ground side, as they are mostly emitters and not receivers, in constant broadcast. Private keys must be stored, once and the aircraft will have the public in the navigation databases, along with charts. There is no need to cipher as the information transmitted is always the same and widely known. Adding a digital signature is the most important asset as the airplane becomes assured the messages have been not corrupted intentionally. The digital signature can be very based on a big byte sized key because the frequency of emission, (meaning no now new data) is low in these equipments.

4.4.4 Border security
Problems: Piracy is still the most dangerous threat to air transport and has the potential for the biggest inflicted damage in the communities. Paper passports are actually a secure mechanism for terrorist to travel freely around the world. They are easily counterfeited, by forging on blank stolen ones. Recently the addition of biometrics has made for automatic doors to open on face recognition. The next generation of passports will have 10 finger digital prints, DNA, voice, keystroke, signature and iris bio data encoded in RFID tags embedded inside the document. ICAO is the leader of the worldwide recommendations for implementation of the e-Passport. Already hackers have discovered how to crack the security and how to clone it.

The Schengen area encompasses the most of EU countries plus some others like Norway and, Switzerland will join in this year. Inside the EU ID check resumes to ID card check on check-in at the counter and on boarding. Passports, even the new ones, are not required at all. ID cards are issued by each country with a variety of standards and security levels, and without shared databases.

The new passport will be ineffective inside the Schengen pact nations. Portugal has vastly improved our “Bilhete de Identidade” with the launch of “Cartão do Cidadão”. It has addition of a smart chip JavaCard ([13]) with digital signatures and will serve as a Single-Sign-On token.

Unbelievably, at Frankfurt-am-Main’s (IATA code FRA) Terminal One there are boarding gates consisting of mere turnstiles operated without any ID check’s at all. Frankfurt is the major hub of Lufthansa and the second busiest airport in Europe. It is also possible to enter the baggage collection area directly from the departure floor, without any security, which stands as a motive for baggage check security upgrade.

Solutions: To avoid the non demand on the e-Passport and heterogeneity of ID cards from country to country, changes can be made in boarding passes. These are low-cost pieces of paper printed in paper-roll machines or at home when doing an online check-in. A bar code is machine readable (though rarely used in case of online check-ins). A uniform solution to ID checks could be the insertion of extensive biodata in the boarding passes, and demanding refresh of these while checking in a self-check-in machine or counter DNA and fingerprints could be stored. Many issues have to be addressed, such as the cipher and digital signing of the passports. Retina biodata will be privileged over iris despite needing more bits to code it. Web check-in outputs an A4 format sheet of paper, and printed information would have to be coded with a high resolution to have sufficient data, yet avoid the limitations imposed by low quality home printers. Airline Passenger profiling for allowing home check-in procedures will be studied. The integration of passenger profiling with frequent flyer programmes is one way to avoid duplications of effort.

4.4.5 Cargo and hold baggage security

Problems: Baggage systems are on the verge of a major breakthrough with the introduction of RFID tags, over taking legacy bar-code tags. This is mostly an economic motivated change, because automatic readers identify 80% of bar code tags and RFID can reach as much as 98%. Delta Airlines, now the biggest airline in the world, stated they lose about 100MUSD per year on compensations to passengers due to lost baggage. The Pan Am B.747 that exploded over Scotland was a casualty of a false tag inserted on a bag which concealed the bomb device. About 400 baggage volumes are stolen each day in Lisbon. This happens in many civilized counties and British Airways installed cargo hold cameras in their aircraft to dissuade theft inside planes.

There is nothing more than a bar code with the number Id of the baggage, and the tag with passenger name, origin and destination airports. Even proposed new RFIDs are to do little more than to code the same information in passive radio tags, the leading specification being IATA’s recommended practice RP 1740C ([16]). The specification deals with encoding and data sets, not addressing security at all. Its major result is defining the read/write frequency inside the UHF band, to be operable in conformance to radio frequency law in most of the countries. This is good for data rates at the expense of detection range ([15]). Robbing bag volumes at the collection
areas is easy because there is no match between passenger and volume. Same goes for unattended hand luggage left in the terminal.

**Solutions:** The information in the tag should be ciphered and have a digital signature. Further information such as baggage size, weight, colour and shape should be present to avoid baggage substitution or theft by changing tags. Pass points with timestamps can be stored to reconstruct the trajectory and identify where it could have been tampered with. Encryption algorithms cannot be as slow as to compromise the fast read/write of the conveyor belts baggage terminals’ routing systems. The correlation with boarding passes (§5.4.4), also will provide conciliation and theft reduction.

Note: This study section will not concentrate of market costs and world scale economics, only on technical solutions where common sense will prevail in the feasibility. There is a wide range of tag technology on the market and its use and capabilities are very flexible despite trade-offs.

### 4.4.6 Others

The work will mostly concentrated on the above five frameworks, which will yield a considerable amount of work. This will henceforth enhance the learning of the thesis proposed, and without being repetitive and not taking away attention from the depth of the solutions in the firsts topics.

A few other topics might be explored in a more superficial analysis, while being integrated in the subject of the thesis and having links to the primary frameworks.

#### 4.4.6.1 Aircraft Communications Addressing and Reporting System

ACARS is a digital broadcast link by aircraft, not used by all airlines that anyone can use a low-cost receiver to collect. It can support CPDLC or messages passed from airliners to their Airline Operation Systems (AOC) to inform of delays, hotel bookings etc. Public websites exist where near real time positioning of airliners can be seen. No security exists of any kind.

Similar problems, and the solution approach, apply to Airlines communications ATSU communications.

#### 4.4.6.2 Flight crew incapacitation recovery

The first decent airliners in the later 40s had a five men crew. The URSS did the same until the eighties, to avoid air defection to the West, which happened with one-manned fighter jets. In the late fifties, the crews where reduced to three when aircraft like Boeing B.707s were introduced. In the late 60s jets with only a Captain and First Officer became the norm by the B.737 and DC-9. Widebodies kept three in the cockpit (A.300, B.747, DC-10, Tristar) until the introduction of the B.767 in 1982. Even the huge B-747 became flyable with two in its -400 variant launched in 1988. Now, all new airliners are two pilots independently of the size, even the A380. In the general aviation market Very Light Jets (VLI) are entering the market. Having jet speed performance, low operating cost and price tag, very small (6 passenger cabin normally) and flown by one pilot, they are set to revolutionize the market for air taxis. Concern exists on pilot incapacitation. Work is being done to prevent disasters and one solution is to have an Air Force fighter aircraft redirecting the VLJ onto a safe destination. This would be by uploading a new flight plan and making the unguided jet as on a leash. To ensure proper use of this safety mechanism a short range optical port could be existent of the fuselage and Quantum securitised commands given. An EC FP6 project called SOFIA is addressing this solution’s feasibility.
5  Work evaluation metrics and means

The work done under the scope of the thesis will yield a roadmap for the security improvement in aeronautical communications. Many threats will be analysed and solutions will be studied and proposed to cope with those threats, while taking profit from actual and emerging security technologies and procedures.

The output will of this work is not a software program which implementation can be compared to a specification for benchmarking on achievement of completeness. There will be no performance analysis or checking for operational capability a posteriori. The result is a paper and will not bring attached software of hardware presentable parts, nor any type of websites or any interactive system.

In the case of typical information systems or algorithms there can be such metrics. Internet servers can provide metrics based on their firewalls records in defending a number of different threats. Encryption algorithms’ strengths and time to break can be demonstrated with formal methods ([1]).

Evaluation on the results can be done in two ways, quantitative and qualitative. The first one will consist in the comparison of the amount of threats actual potential detected with the new solutions proposed. A key aspect to the success of any new security solution is the human factor of terrorist withdrawal. The chart in the Annexes depicts a never ending terrorist activity over the decades since air travel became a high scale reality. Changes are made, with metal detectors, X-ray for hand luggage, liquids limitations to 10 x 100ml per passenger deplaning of bags from passengers who miss their boarding and HBS100 (100% screening of Hold Baggage Security) being mandatory on all countries. These methods are used for counteracting previous terrorist threats, which become more and more trained and elusive of any new mechanism.

The other technical assessment method will be through dissemination and expert stakeholder feedback, which will grant a qualitative view on the same results.

The next section will detail the particulars of the each of the means for evaluation.

5.1  Threats raised versus mitigated

New security technologies used where legacy ones are the standard will raise the level of confidence as to creating further distance to the present potential threats. In this document, preliminary solutions are he given in fields of study planned. A break-up of communication systems involved in the aeronautics world will have dedicated attention while there is the goal to maintain the actual level of interoperability.

The level of threat mitigated can be measured on how difficult is to perform an act of terrorism. In the primordial era of aviation all it took was to take a fire weapon on board to take control of the crew, or simply check-in a bag with a bomb and walk away. Procedures and sensors mitigated this. Automatic gun can be boug for as much as 200€. Then, rockets (RPGs), priced in black markets at 10 000 USD, were used in Paris Orly against El Al in the 1970s ([17]) and, a few years ago in Baghdad against a DHL Airbus A300. The Samora Machel attack was much more complex and involved putting up a radio navigation system, with requires a high power and transmitter on considerable complexity. On the other hand, a simple 100€ radio will allow to effectively impersonate a communication in an ATC frequency.

By introducing more advanced security the skill and equipment of terrorist will have to adapt thus demanding higher, and costly, training. This will limit the threat to true professionals which are easier to track by intelligence agencies and clear out aviation from amateurs like the car bombers in Glasgow International Airport. It is important to
emphasise that anti-terrorism security must be concentrated on prevention and not on means to counteract after one such event is initiated.

A minimum profile for a terrorist attack will be presented for each sub-framework. This can, for instance, mean a person that will need to be a Computer Science expert and have in possession a very powerful laptop PC with state-of-the art software to decipher secure messages.

5.2 End-user feedback

From personal activities in relation to aeronautical Research & Development programmes and liaisons obtained in hobbies related to aviation we possess a good deal of contacts that are direct stakeholders in all the frameworks selected for study and improvement. These stakeholders will help us with relevant feedback in the applicability of the work.

From the airborne side, we can explore an agenda with a vast number of airline pilots, national and international, some of them active in R&D projects in diverse countries. On ground, there is acquaintance with several Air Traffic Controllers and engineers who belong to ATC organizations. As the case with pilots, many of them cooperate in development, both for research and for target in-house systems. There are links to be pursued with handling companies (companies that check-in and board passengers and load/unload cargo and baggage) mainly in the Portuguese companies, Groundforce, TRIAM and Portway.

I will explore some contacts I have with national security service operating in airports as well as our national airport operator (ANA).

5.2.1 Interviews

In depth know-how shall be obtained by conducting personal interviews with end-users and stakeholders at different stages of the execution of the thesis development task.

5.2.2 Questionnaires

In the cases where interviews are not possible, a questionnaire will be sent and collected by e-mail.

5.2.3 Dissertation Review

Before the presentation to a IST “Conselho Científico”, a draft of the dissertation will be reviewed by the same stakeholders that participated in the questionnaires and interviews. This maturing step will ensure overall vision and adequacy to world that surrounds the communications.

5.3 Dissemination Plan

It is important to divulge this work in the appropriate circles of aeronautics. I shall contact the Portuguese media aviation publications. The APPLA edited magazine Sirius, where previous cooperation in an article took place the month on January 2009, and the TakeOff journal. Attention will be directed to seeking European conferences where to present a paper based on my thesis dissertation. The thesis document confidentiality level will be Public. There will be no confidential background present and no legal liability danger be possible.
6 Conclusions

It is very evident that aviation security is very unbalanced with respect to investment and technology application in its diverse sub-contexts. For passengers, screening is becoming every day more demanding. New X-Ray screening machines brought controversy in London Gatwick as they portrayed people as naked to the security officers. At London’s Heathrow Airport, novel screening equipment is capable of scanning even through laptops. In USA airports, laptops themselves can be audited by the Department of Homeland Security for terrorist or criminal data stored. Biometrics security is being introduced in a wide scale, recognizing faces, finger prints, iris and retinas. The new passports use face scans to conciliate the documents porter with the owner, and automatic doors are activated by the algorithms after positive IDs (this is operational in Portugal).

Looking at the airplane operations side, the security state of the art presents itself at a much lower standard. The very important voice communications do not have authentications nor any sort of cipher. These are available for everyone to listen and to participate, with very low cost transceivers. Severe cases of security breaches have been reported and no solution is yet at the horizon.

Air transport safety relies considerably on the see-and-avoid philosophy. That means that each aircraft is seeing each other besides the ATC services, especially over water. Transponder equipment helps aircraft monitor the others on a cooperative basis and provide support in case of collision. Security in traffic data exchanges is inexistent nowadays.

Baggage theft and tamper is a major problem in many airports and still a way to introduce terrorist devices on board. The RFID introduction has been and will limits this somehow but security of information stored in the tags is still a problem for the future.

Some of the security problems can have solution by the application of market and field proven technologies. The military are far more advanced and there are many lessons learned to be considered in this study. Unlimited budget and competition between countries are motorways for developments. Revolutionary flying machines like the Lockheed SR-71 “Blackbird” will never exist in the civil context.

Radical improvements in aviation are slow, mostly due to safety concerns. Other factors can be stated out as, EU/USA politics, multinational industry standards that have to converge on consensus, unwillingness of airlines in investing in non-profitable equipment. Poor counties’ airlines fly to the First World and it simply and utopia to make them spend fortunes upgrading their planes without a strong rationale. Strong rationale in aviation, in both safety and security, means a series of high death toll accidents (light private plane that collided with a McDonnell Douglas DC-9 in 1980s over L.A.) and terrorist attacks (911, many TWA hijacks in 1970s).

Terrorists will never be eliminated. The only way to maintain security is to keep changing the rules and difficult their operation by covering the holes that can be exploited.

Many new technologies are emergent and may even further increase the life of the security mechanisms. The major breakthrough and candidate is quantum security.

7 Acknowledgments

It is necessary to thank Professor Pedro Adão for his patience in reviewing and suggesting improvements to this paper. Many thanks also to Professor Paulo Mateus, also from IST, for his briefing on Quantum Security developments, the birth moment of the idea to propose this thesis in the area.
8 References


[10] V. L. Kurochkin1, I. I. Ryabtsev and I. G. Neizvestniy1, Quantum key generation based on coding of polarization states of photons Institute of Semiconductor Physics, Siberian Division, Russian Academy of Sciences, Novosibirsk, 630090, Russia, 17 July 2003


[16] Ost, Laura, System Sets Speed Record For Generation of Quantum Keys for 'Unbreakable' Encryption, USA National Institute of Standards and Technology , May 3, 2004


[23] IDQuantique, Quantis – Quantum Random Number Generator on a USB Device with a bit rate of 4 Mbits/s, December 2006.


[26] RTCA/DO 186A, VHF AM ATC, May 07
[27] RTCA DO-300, Minimum Operational Performance Standards (MOPS) for Traffic Alert and Collision Avoidance System II (TCAS II) Hybrid Surveillance

[28] RTCA Change 1 to DO-260A, Minimum Operational Performance Standards for 1090 MHz Extended Squitter Automatic Dependent Surveillance – Broadcast (ADS-B) and Traffic Information Services – Broadcast (TIS-B)

[29] RTCA DO-231, Design Guidelines and Recommended Standards for the Implementation and Use of AMS®S Voice Services in a Data Link Environment


[31] RTCA DO-230A, Standards for Airport Security Access Control Systems

[32] RTCA DO-225, VHF Air-Ground Communications System Improvements Alternatives Study and Selection of Proposals for Future Action


[34] RTCA DO-211, User Requirements for Future Airport and Terminal Area Communications, Navigation, and Surveillance


[36] The Phantoms Of The Skies, Periscope Newsweek, September 11, 2000


[38] X.509, Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
9 Acronyms and definitions

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expanded</th>
</tr>
</thead>
<tbody>
<tr>
<td>4-D</td>
<td>Four Dimension</td>
</tr>
<tr>
<td>A/C</td>
<td>Aircraft</td>
</tr>
<tr>
<td>ACARS</td>
<td>Aircraft Communications Addressing and Reporting System</td>
</tr>
<tr>
<td>ADF</td>
<td>Automatic Direction Finder</td>
</tr>
<tr>
<td>ADS-B</td>
<td>Automatic Dependent Surveillance-Broadcast</td>
</tr>
<tr>
<td>ADS-C</td>
<td>Automatic Dependent Surveillance-Connection</td>
</tr>
<tr>
<td>AFTN</td>
<td>Aeronautical Fixed Telecommunication Network (AFTN)</td>
</tr>
<tr>
<td>AOC</td>
<td>Airline Operation System</td>
</tr>
<tr>
<td>AP</td>
<td>Auto Pilot</td>
</tr>
<tr>
<td>ATSU</td>
<td>Air Traffic Services Unit</td>
</tr>
<tr>
<td>ARINC</td>
<td>Aeronautical Radio INC.</td>
</tr>
<tr>
<td>ASAS</td>
<td>Airborne Separation Assurance System</td>
</tr>
<tr>
<td>ATC</td>
<td>Air traffic control</td>
</tr>
<tr>
<td>ATN</td>
<td>Aeronautical Telecommunication Network</td>
</tr>
<tr>
<td>CAA</td>
<td>Civil Aviation Authority</td>
</tr>
<tr>
<td>COMSEC</td>
<td>Communications Security</td>
</tr>
<tr>
<td>CMU</td>
<td>Communications Management Unit</td>
</tr>
<tr>
<td>CPDLC</td>
<td>Controller Pilot Data Link Communications</td>
</tr>
<tr>
<td>DCS</td>
<td>Departure control System</td>
</tr>
<tr>
<td>DME</td>
<td>Distance Measuring Equipment</td>
</tr>
<tr>
<td>EASA</td>
<td>European Aviation Safety Agency</td>
</tr>
<tr>
<td>EC</td>
<td>European Commission</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EMSEC</td>
<td>Emission security</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration</td>
</tr>
<tr>
<td>FANS</td>
<td>Future Air Navigation System</td>
</tr>
<tr>
<td>FMS</td>
<td>Flight Management System</td>
</tr>
<tr>
<td>FIR</td>
<td>Flight Information Region</td>
</tr>
<tr>
<td>FP7</td>
<td>Seventh Framework Programme</td>
</tr>
<tr>
<td>GBAS</td>
<td>Ground Based Augmentation Systems</td>
</tr>
<tr>
<td>GIGN</td>
<td>Groupe d’Intervention de la Gendarmerie Nationale</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>GSM</td>
<td>Global System for Mobile communications</td>
</tr>
<tr>
<td>HF</td>
<td>High Frequency</td>
</tr>
<tr>
<td>HBS</td>
<td>Hold Baggage Security</td>
</tr>
<tr>
<td>IATA</td>
<td>International Air Transport Association</td>
</tr>
<tr>
<td>ICAO</td>
<td>International Civil Aviation Organization</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineer</td>
</tr>
<tr>
<td>INS</td>
<td>Inertial Navigation System</td>
</tr>
<tr>
<td>JDAM</td>
<td>Joint Direct Attack Munitions</td>
</tr>
<tr>
<td>ILS</td>
<td>Instrument Landing System</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Union</td>
</tr>
<tr>
<td>LVO</td>
<td>Low Visibility Operations</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>NATS</td>
<td>National Air Traffic Services</td>
</tr>
<tr>
<td>QKD</td>
<td>Quantum Key Distribution</td>
</tr>
<tr>
<td>NDB</td>
<td>Non-Directional Beacon</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-Frequency Identification</td>
</tr>
<tr>
<td>RPG</td>
<td>Rocket Powered Grenade</td>
</tr>
<tr>
<td>RTCA</td>
<td>Radio Technical Commission for Aeronautics</td>
</tr>
<tr>
<td>RVSM</td>
<td>Reduced Vertical Separation Minimum</td>
</tr>
<tr>
<td>RA</td>
<td>Resolution Advisory</td>
</tr>
<tr>
<td>SELCAL</td>
<td>SELective CALLing</td>
</tr>
<tr>
<td>SITA</td>
<td>Société Internationale de Télécommunications Aéronautiques</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>SESAR</td>
<td>Single European Sky ATM Research</td>
</tr>
<tr>
<td>SSR</td>
<td>Secondary Surveillance Radar</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>STANAG</td>
<td>Standardisation Agreements</td>
</tr>
<tr>
<td>TA</td>
<td>Traffic Advisory</td>
</tr>
<tr>
<td>TCAS</td>
<td>Traffic alert and Collision Avoidance System</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TRANSEC</td>
<td>Transmission security</td>
</tr>
<tr>
<td>UAT</td>
<td>Universal Access Transmitter</td>
</tr>
<tr>
<td>VLD</td>
<td>Very high frequency Data Link</td>
</tr>
<tr>
<td>VHF</td>
<td>Very High Frequency</td>
</tr>
<tr>
<td>VLJ</td>
<td>Very Light Jet</td>
</tr>
<tr>
<td>VOR</td>
<td>Very high frequency Omni Range</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
<tr>
<td>WAAS</td>
<td>Wide Area Augmentation System</td>
</tr>
</tbody>
</table>
Fig. 1. Numbers for terrorism in civil aviation