A Novel Security Model for Aircraft Crew Authentication & Message Integrity in Aeronautical Data Link Communications

Amjad Ali[1] **and Walid Shawbaki**[2]

Center for Security Studies, University of Maryland University College, Adelphi, Maryland, USA

Summary
Increased demand on air travel worldwide is driving increase in travel capacity, which affects current departure, arrival, and air route structure in the National Airspace System (NAS) in the United States. The ongoing transformation of current air traffic control to net centric architecture to support higher capacity will have higher dependency on information sharing via data link connectivity between aircraft cockpit and ground controllers, which is an expansion to today's voice communication. Aircraft to be a node in the sky on the aeronautical infrastructure network, and similar to any other network; this will be vulnerable to cyber-attacks that could be far serious to safety of flight that affect civil air transportation system as one of the enablers to the nations' economy. An assessment of cyber-attacks risks by domestic and foreign entities against civil air transportation system need to be always in place and updated regularly for such critical infrastructure supporting the air traffic flow and control. Several protections available to provide security to ground segments of the aeronautical network supporting air traffic control, and the same measures provided for systems onboard aircraft; however, connectivity via the aeronautical radios between aircraft in the air and ground segment of the aeronautical network is the center of discussion in this paper. Existing Federal Aviation Administration (FAA) regulations and policies do not specifically address the security for the voice and data link connectivity between aircraft and ground control network, and cyber attackers do not have a limitation on their areas of attacks, and such security need to be part of the safe operation of civil aviation. Within this paper, brief review of current NAS and the plan for transformation to net centric operation presented showing where the aircraft fit in the new aeronautical network. The Confidentiality, Integrity, and Availability (CIA) in addition to Authentication and Non-Repudiation model for secure operation considered the basis for the solution with focus on authentication of the aircrew in command during flight and integrity of message (i.e. Flight Plan & Clearances) being communicated between aircraft and ground. The model for the solution based on implementing separate and parallel data capable radio as the conduit to for authentication and integrity check of Air to Ground(A/G) and Ground to Air (G/A)messages communicated over the main aeronautical data link capable radios.

Key words:
Crew Authentication, aeronautical data link integrity, NextGen, SESAR, Aeronautical Cyber Security.

1. Introduction

Demand for air travel increasing worldwide, FAA annual report about airlines predicting passengers to nearly double in two decades with an average increase of 3.2% per year (FAA, 2012), and world traffic at 6.5% growth as reported the by Internationial Civil Aviation Organization (ICAO, 2012). Such increase in demand places pressure on civil aviation infrastructure including air routes structure, and presenting challenges to handling air traffic flow by ground controllers in addition to causing congestion at airport facilities, runways & taxiways,….etc. In order to cope with such growth, two major projects are under way, namely the Single European Sky ATM Research (SESAR) in Europe and Next Generation (NextGen) air transportation system in the United States. Both projects plan to transform existing airspace to handle higher air traffic capacity through deployment of enabling technologies in Communication, Navigation, Surveillance (CNS) and modernizing the Air Traffic Management (ATM) simply known in the aviation industry as CNS/ATM.

One important factor to the core of both NexGen and SESAR projects is safety, current Air Traffic Control (ATC) procedures depend on keeping wide separation between aircraft in airspace and directing traffic to follow fixed manageable air route structure including separation in time between take-off and landing sequences long enough to support safe operation. However, increased capacity will require reducing separation and time and spacing between aircraft in eth space of operation that will be migrating toward efficient direct routing to save time and fuel. Human limitations in managing increased aircraft flying in large number especially around major airports will be an issue, which requires increase in automation through deployment of CNS/ATM systems based on enabling technologies for net centric operation with high degree of safety. The net centric operation in aviation will have all services such as weather, security, flight plan and active traffic, in addition to entities related to the operation of airlines, controllers…etc. as nodes on the aeronautical network including the aircraft, and real time information updated for use by consumers on the aeronautical network. CNS will enable better situational awareness to both airborne segment (aircraft crew) and ground segment

Manuscript received October 5, 2012
Manuscript revised October 20, 2012

(controllers); however, net centric operation of the civil aviation is also subject to cyber-attacks specially when targeting the critical data link A/G and G/A radio connectivity, which is vital for communicating clearances, flight plans, conflict resolution, and safe self-separation. Even though, the FAA stated as an objective to achieve zero cyber security events disabling or significantly degrading FAA services; however, existing FAA regulations and policy do not specifically address the security for systems networks requirements for aircraft systems (FAA, 2011).

Cyber security aspects of protecting NextGen and SESAR networks need to be treated the same way critical infrastructure are protected similar to those in the network-centric warfare (Tether, 2003). Cyber-attacks on the rise that are not exclusive to individual hackers and crackers, attacks can even be carried out by foreign adversaries as part of the warfare to impact the nation's economy through attack on critical infrastructures associated with air transportation safety and cause disruption of operation.

This paper addresses conceptual model for addressing vulnerability of the aeronautical radio link between aircraft and supporting ground infrastructure network, which is based on crew authentication and message integrity. Section II provides background about current operation and related radio enabling technologies. Section III introduces the conceptual model that addresses both authentication of crew in command of aircraft operation during any phase of flight, and the model for integrity verification of both Air to Ground (A/G) and Ground to Air (G/A) messages being communicated between aircraft cockpit and ground operation. Section IV provides conclusion remarks.

2. Background

Looking at March 2010 FAA Administrator's Fact Book, it is shown that National Air Space operation is characterized by its' heavy traffic where activity for the period handled by Federal Aviation Administration (FAA) Air Route Traffic Control Centers (ARTCC) totaled 40,842,000 flights and 37,289,000 handled by FAA Towers in the period January-December, 2010 (FAA, 2011). Such volume of flights and the plan to triple capacity under NextGen and SESAR by 2025 raises the need for automation of air traffic control. However, we are living in an era where civil aviation is considered as a pillar to the economy of nations, such pillar will be subject to attacks by adversaries, therefore, security becomes of paramount importance to the continuity of civil aviation, which is the theme of this paper.

2.1 Existing Communication with Aircraft

Voice communication between aircraft and controller on ground has been and still the backbone link for issuing clearances, directions, and guidance to aircraft. In United States, FAA uses legacy radio connectivity with aircraft for voice communication to support Air Traffic Control (ATC) operation. These legacy voice switches connects controllers together and different control centres (i.e. ARTCCs) on ground as part of the ground infrastructure of air traffic control. Air traffic ground controllers can also access the Ground to Air (G/A) radio equipment geographically located to support various route structure controller-to-pilot communications. In addition to plain voice communication, some digital communication exists today between ground traffic controllers and flight crews for issuing clearances, instructions, advisories, flight crew requests and reports through the Controller-Pilot Data Communication Link (CPDLC). CPDLC improves air traffic controller productivity, enhances capacity and safety under the net centric environment where aircraft will be a node on the network; however, communication between aircraft and ground controllers as of today are plain and no security measures in place.

2.2 Aeronautical Radio Technologies

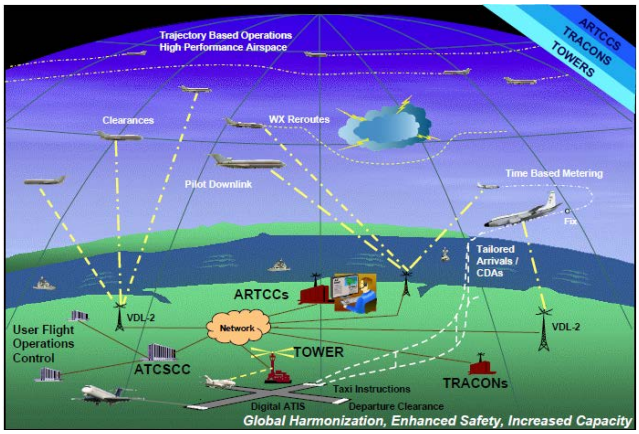
Typical phases of flight consist of operation in terminal area (Departure, Arrival, and Approach) and enroute function, and some Oceanic flights. Current voice communication with civil and commercial aircraft employs Line Of Sight (LOS) aeronautical radios operating in the Very High Frequency (VHF) band 117.975MHz -137.000 MHz for flights over terrestrial regions, and Beyond Line Of Sight (BLOS) means of communication in remote and Oceanic regions using High Frequency (HF) band (2MHz-30MHz) and/or Satellite Communications in the 1.5GHz range.

VHF aeronautical radios evolved through decades of deployment and successive improvements where current radios are compatible with civil aviation requirements and covered by several standards of International Civil Aviation Organization (ICAO), Federal Aviation Administration (FAA), Radio Technical Commission for Aeronautics (RTCA), and others. However; current aeronautical radios characterized by their inefficient spectrum utilization because of the Amplitude Modulation (AM), lack of protection from intentional interference, and lack of security for the communicated messages (voice & data) that provide vulnerability for intruders and unauthorized users to exploit such vulnerability such as "phantom controllers" issuing bogus instructions to pilots (FAA, 1992).

The use of voice communication under NexGen and SESAR will not support information sharing that is required under both programs, and there is a need to migrate to data communication, which requires data capable radios while retaining voice communication capability as a backup. The three spectrums available for data link are the Very High Frequency Data Link (VDL), High Frequency Data Link (HFDL), and DL via Satellite Communications (SATCOM). There is a global harmonization and agreed upon for the data link standards that FAA Advisory Circular (FAA, 2010) and the ICAO data Link (ICAO, 2010). Data link technology has been around for more than two decades of flight operations using an older character oriented protocol for Aircraft Communications Addressing and Reporting System (ACARS®) technology supporting aeronautical services such as graphical weather descriptions, electronic charts, and engine/aircraft health monitoring programs…etc. Additional desired services such as flight information, aeronautical operational control, and Air Traffic Control (ATC) data applications demanded greater bandwidth where VDL technologies moved from character oriented to bit oriented protocol to support greater bandwidth needs by services all operating in the aeronautical mobile VHF frequency band.

Data link connectivity to aircraft cockpit enables information sharing between aircraft cockpit and ground network as depicted in Figure 1 below for the VDL deployment.

Currently VDL Mode 2 is the adopted waveform for CPDLC communications in the form of a Data Link Services as illustrated in Figure 1. For operation in Oceanic and remote region where ground VHF radio infrastructure not available, the data capable Beyond Line of Sight (BLOS) radios that will be used High Frequency (HF) Data Link (HFDL) , and/or onboard aircraft Satellite terminal that is approved for use with Air Traffic Services such as the Inmarsat Aero I and Aero H satellite equipment.



ARTCCS	Air Route Traffic Control Centers	**TOWERS**	Airport control towers
ATCSCC	Air Traffic Control System Command Center	**TRACONS**	Terminal Radar Approach
ATIS	Air Traffic Information Service	**VDL**	VHF Data Link
CDA	Continuous Decent Approach	**WX**	Weather

Figure 1: Typical digital connectivity via VDL 2 (Source; http://www.faa.gov)

2.3 Future Net Centric Aeronautical Operation under NextGen

In an aeronautical data link operation(i.e. NextGen), aircraft receives instructions including air traffic control communication frequency changes, metrological conditions, route clearance, and altitude changes delivered to the cockpit via data communication with voice being reserved for backup. Automation in the process rather than having human in the loop is the goal to enable increasing ground controller's efficiency and ability to manage more traffic, which also reduces pilot workload (JPDO, 2011).

Net centric operation enabling information sharing is the key to success of NextGen and SESAR, and both programs will include a System Wide Information management (SWIM) that will provide infrastructure and services to deliver information access across the NextGen and SESAR where aircraft simply will be a node on the SWIM network as illustrated in Figure 2 below.

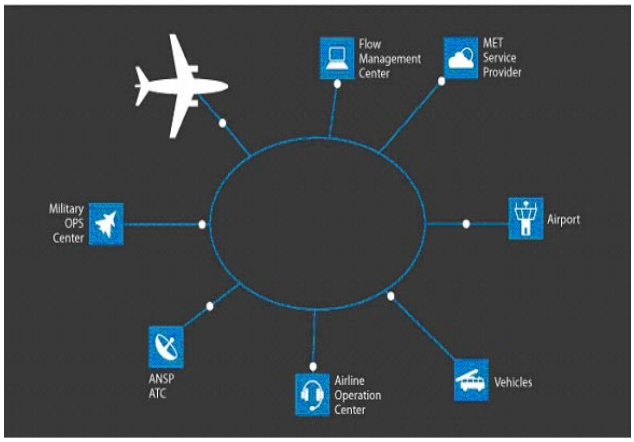


Figure 2: Net-centric SWIM (System Wide Information Management) (Source: http://www.sesarju.eu/programme/workpackages/swim/swim-principles)

Data link capable radios (i.e. VDL) are required to provide connectivity with aircraft enabling better cockpit situational awareness of airspace operation while able to manage aircraft own path as part of the sharing

responsibility in Air Traffic Management (ATM) rather than being controlled by the ground via an Air Traffic Controller (ATC) as currently practiced in airspace control. Current NAS security is covered by security standard that is based on Open Systems Architecture (OSA) and the same information about traffic being relayed between controllers across the US are passed in secure mode. However, communication with the aircraft still being handled via voice or data link data link messages that are in the open and not secure.

2.4 Airlines Industry and Aircraft Equipage

The airline industry exists for profit, and as long as high cost of operation due to labor and fuel exist, it will be difficult to invest in new technologies to support secure communication s operation. Current aeronautical radio technology has evolved through decades of improvements and built on established industry specifications and standards supporting aeronautical communication operation. However, security now days becoming of prime importance, and any changes to be based on needs and in line with the business model of airline industry, current economy, and affordability by airlines. The conceptual model presented in this paper provides an approach for minimal changes to aircraft equipage to meet secure aeronautical communication through providing crew's authentication and message integrity check.

3. Security in Aviation Net Centric Operation

In aviation industry, safety and security are somehow interrelated, safety addressing aircraft airworthiness is being controlled via design processes, procedures, policies, and standards; however, security is the challenging one. When flight operation is dependent on critical information sharing, processing of data distributed in different part of the networks (i.e. cloud computing) need to be protected. Network vulnerabilities become greater in shared environments, which apply to airline industry net centric operation. The challenges arise from the global span of aeronautical networks across several continents and crossing political borders. Threats to civil aviation industry known for decades and defense in depth security to protect access to airplane and elements supporting aircraft mission including the security to cargo holding, access to target areas, passengers, airport, infrastructure, and the critical facilities has been the norm in airline/aircraft security as illustrated in Figure 3 below.

NextGen identified that backbone networks to include a cyber-security approach that safeguards aeronautical related information within acceptable trusting relationships between the information suppliers and consumers (JPDO, 2010). In a SWIM enabled network, it is important to recognize that SWIM is a Service Oriented Architecture (SOA) environment offers "clients" (both air and ground) the ability to discover, retrieve, publish, and register contracts (FAA, 2011). Vulnerability arise from having part of the network such as the aeronautical radio link to airborne nodes (aircraft) unsecure, which introduces vulnerabilities that could affect aircraft mission and safe operation.

Figure 3: Security in depth to facilitate aircraft mission (Source: http://www.jpdo.gov)

3.1 Vulnerabilities of the Aeronautical Radio link

Aeronautical radio links between ground infrastructure and aircraft share the same vulnerabilities with any other wireless networks such as being subject to classical interference and jamming, which could be carried out within the range of radio link transmitted power/ reception distances. However, higher risks for safe operation arise with radios being part of ground infrastructure networks (i.e. air traffic controllers for separation assurance) that are vulnerable for remote access by adversaries. In this situation, there is no need for attackers to be within the radio transmission/reception range. For example, having such links without protection introduce vulnerabilities to different attacks that could include:

- **Jamming**: a type of Denial of Service (DoS) attack that introduces confusion in traffic control operation and coordination between aircraft and controllers.
- **Unauthorized data modification**: a type of malicious attack on messages for clearances, flight plan, messages between aircraft themselves and ground control intercepted, modified, and retransmitted. Malicious intentions can lead to catastrophic consequences in air traffic operation. This is similar to man in the middle attack, which can include message injection such as "Phantom controllers" that uses the

radio links to direct traffic in the air pretending to be the official ground controller (FAA, 1992), and in a net-centric, unauthorized access to Aeronautical Telecommunication Network (ATN) via radio link and able to initiate clearances, guidance, and flight plans and use Man in the middle attacks; high jacking and replay attacks will be possible without the need for the intruder to be within the radio range of the target aircraft.

- **Malicious attacks**: similar to jamming that may result in degraded performance and message distortion where the link is bombarded with several requests that overwhelm aircrew in the cockpit and/or ground controllers to be able to perform their job.
- **Eavesdropping and message analysis**: This can be used for intelligence gathering to expose vulnerabilities in the system for future attacks.

Above are some of the vulnerabilities, since VDL Mode 2 radio has the capability to operate in packetized mode, which means modification to packets carrying critical guidance and clearance information to flying aircraft and retransmit a modified version of the original message would be possible in a net centric operation or create a conflict between actual and modified messages that will cause confusion in the cockpit (or at ground controller position). Therefore, threats to radio links listed above can impact integrity of messages and subject the radio links to unauthorized access, high jacking attack, and replay attack (Prodanovic & Simic, 2007).

3.2 Encryption techniques that can support Aeronautical Radio Security

Several encryption algorithms available protected by deploying advanced symmetric and asymmetric keys with various lengths; and sophisticated encryption techniques that are characterized by their complexities usually demand higher bandwidth tend to cause slow processing. However, aeronautical radio bands already congested where channels spacing were reduced for example in European airspace from 25 KHz to 8.33 KHz to meet increased demand for additional channels, and bandwidth in aeronautical radios is an issue. This means the type of encryption selected needs to consider the limited bandwidth of aeronautical radios and the preferred way of meeting secure operation is to consider using short keys and hash/message digest of the messages for use to provide authentication of crew and message integrity.

4. Approach to Aeronautical Radio Communication Security

Aircraft avionics systems follows safety standards in their design, development, and approval process to ensure new functions/capabilities meet appropriate level of safe operation with highest level of design assurances thus avoiding misleading information to crew in cockpit and ground controllers. For example, design of the aeronautical radios with data capablity need to support a robust information exchanges to enable users performs their roles more efficiently and effectively (JPDO, 2010).

Ideally, protections provided similar to military grade radio communications systems that include Transmission Security (TRANSEC) through frequency hopping techniques and Communication Security (COMSEC) through encryption techniques would secure the data link from cyber-attacks. However, there are some challenges to adopting same military radio technologies for civil operation including scalability of deployment on global and domestic airspace controls uses, logistics of key management across borders. Above all, the economic model of civil aviation industry does not support investment in major avionics and equipment upgrade that will ground aircraft for long time where return on investment is not justified.

The security in a standard network such as those on ground supporting aeronautical operation can be assessed by the basics of Confidentiality, Integrity, and Availability (CIA) through Authentication, Authorization, and Non-repudiation (Valacich & Schneider, 2012). In a typical mitigation of vulnerability assessment risks under the CIA approach, Confidentiality (C) provided through encryption technique, Integrity (I) of the message checked for any alteration or modification through the use of hash (digest) of the message, and Availability (A) requires protection against Denial of Service (DoS) attack.

Data Integrity has been identified by FAA for Ground-based processing applications supporting flight-critical data need to be trustworthy so that the integrity of the data can be assured, and possibility of safety hazards and security threats leading to a loss of data integrity require using vulnerabilities and safety hazard analysis techniques (Lee & Krodel, 2006).

The question remains , what about data integrity of aeronautical messages being communicated between aircraft cockpit and ground elements of the traffic management? And how do we establish a trust relation between flying crew in aircarft and ground controllers handling the flight on it's path form departure to destination? Both are required to insure that no data modifications, impersonation, and actually the messages between both ends are genuine. The answers lies in two areas, one is the mutual authentication between crew in cockpit and ground controllers, and the other in the

integrity for messages communicated between the two parties.

We refer back to CIA model to assess security, and as mentioned previously that complete changes/ re-equipage of commercial airliners' aircraft with new radio technologies to support security may not be the feasible option considering current civil aircraft financial situation.

5. General Concept for Secure Operation

The novel security model presented in this paper based on fully mature radio technologies (standard VDL, HFDL, or SATCOM) that are currently found in typical airliners' aircraft. For example, most aircraft include a Communication Management Unit (CMU) used as a router for data link messages and connect to data link capable radios. The novel crew authentication and data integrity model can be realized via an add on software upgrade to existing CMU and the same data capable radios can be used as used today. A compatible upgrade would be required on eth aircraft controllers systems on ground. However, operation of authentication and message integrity on a different frequency band that those used for main messages would be preferable, which enables security through driving the offenders to invest more in radios to tap to both message and authentication.

The idea of using existing aircraft radios supports the operation of airliners during the modification of onboard Communication Management Unit (CMU) with security software addition thus minimizing the downtime of a revenue generating aircraft. In addition, ground equipment used by air traffic controllers on ground will require an upgrade for compatible operation with the airborne side of the network. Below is a top-level description of operation of the proposed model.

5.1 Air to Ground (A/G) Authentication & Integrity

Assuming aircrew identity obtained at airport of departure while on ground for pre- screened crewmembers with an easily identifiable data to control centers along the path of the flight in the filed flight plan of aircraft. The challenge is to have continuation of trust relationship to counter unauthorized command of the flight (i.e. hijacking), such trust relationship continuity needed to be after gate push back, during taxi, and takeoff all the way to landing and gate arrival at the destination airport. The idea of authentication is to inform ground controllers and destination airport about crew controlling the flight in aircraft cockpit as a mean to satisfy both government and airlines about awareness of crew's identity. This is very beneficial when considering international flights arriving to large entry gateway airport in the United States where the credentials submitted at the departure airport specially for already pre-screened crew will expedite and smooth operation.

Authentication process is built on having Public Key Infrastructure (PKI) where digital signature of crew and controllers can be exchanged. First, the crew authenticated in pre-gate departure as illustrated in Figure 4 by providing their credentials transmitted along with the Flight plans through the ground network to all traffic controllers along the flight plan. The crew receives public keys for all control centers en-route along with destination airport, crew pass their public keys to all control centers en-route, and any communication and trust relationship are maintained through the use of asymmetric keys (private and public key). Those public keys are periodically updated and exchanged for improved security, and will be used to enable mutual authentication to prove the legitimate senders and receiver of messages over the data link radios.

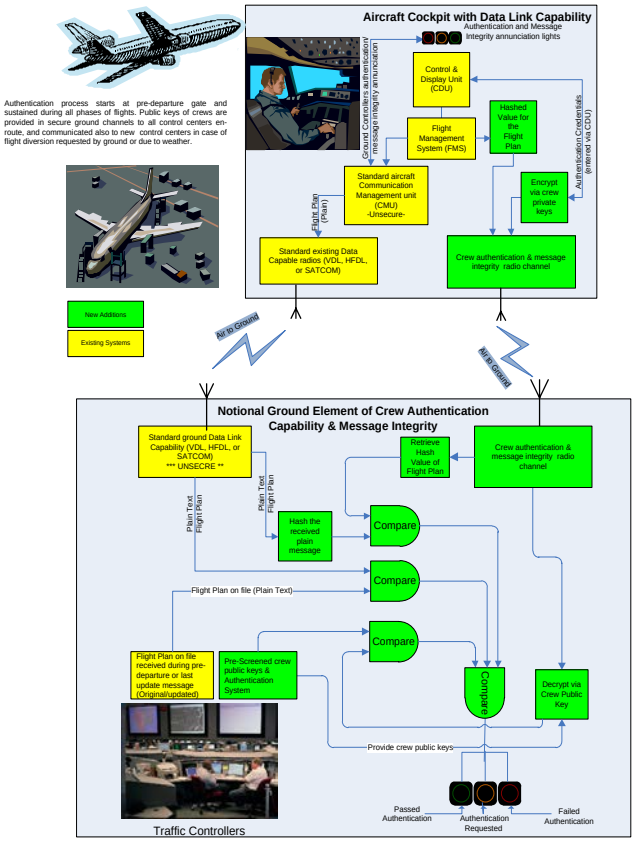


Figure 4: Proposed Novel Model for Secure Air to Ground (A/G) authentication and data integrity in Aeronautical Data Link Communication

As illustrated in Figure 4, it is the preference to have a separate radio channel dedicated for authentication and integrity verification. The separate channel can also be on a separate band such as a modified Mode S transponder. Note that the messages still sent in the open over the existing main aeronautical radios. The messages verified for integrity though comparison to a hashed value of the

message that sent over the authentication and integrity channel shown in Figure 4.

The proposed novel security model for aircraft crew authentication & message integrity in aeronautical data link communications meant to provide the integrity of aeronautical messages communicated from the cockpit to ground controllers. The crew authentication and message integrity continued after departure, and crew can be requested to authenticate while in the air. Any messages communicated with the cockpit, which can include clearances and flight plan upload to cockpit as requested by either the ground control or the crew in the cockpit.

The link with crew credentials and integrity of message provide safe operation and retain the trust level expected in aeronautical communication.

5.2 Ground to Air (G/A) Authentication & Integrity

This is a reversal process where crew will make sure that they are receiving flight clearances and direction in addition to flight plans through a trusted source and not a "Phantom Controller". For example, once an uplink message from ground control is received, the system in cockpit will use appropriate public keys for ground controllers that were received before departure. Decrypting the authentication messages with the public keys of the ground control is the authentication process for Ground to Air (G/A) as illustrated in Figure 5.

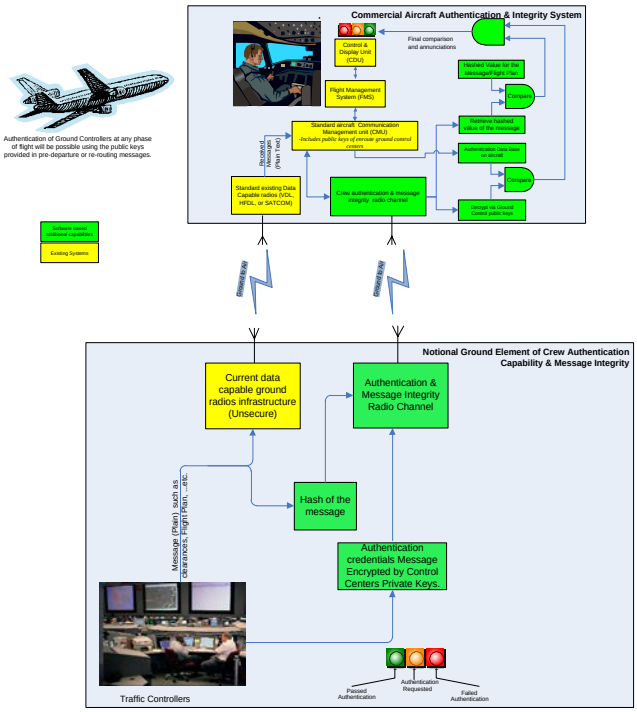


Figure 5: Notional Secure Ground to Air (G/A/) authentication and data integrity

In addition to authentication of the ground controller, the need exist to validate integrity of messages from ground controllers. This achieved via transmitting clearances, guidance, or flight messages sent by the ground controller through the standard aeronautical radio (i.e. VDL), in addition, a hashed value of the message sent via separate authentication and integrity radio channel as shown in Figure 5. The crew system in the aircraft will hash the message received from ground via the standard radio and compare with the hashed value. This is the integrity verification process meant to counter any modification type of attacks on messages from ground to aircraft.

6. Conclusion

Many security technologies currently deployed for use in ground networks to support trust relationship between two parties exchanging information on ground. However, security of airlines that are considered as one of the pillars of the economy is of paramount importance and very dependent on the radio link with the ground. Any plan to increase airspace traffic capacity such as NextGen and SESAR need to consider the security part.

Airline economy is not in best shape, competition, labor, and fuel make operation cost counter profit making goal. Therefore, any plan to improve security needs to consider the economy of the airline industry as a whole, and any investment in new avionics need to consider and be assessed on benefits to operation and revenue.

We need to remember that cyber-attacks are realities that cannot be ignored, and the proposed novel security model for aircraft crew authentication & message integrity in aeronautical data link communications presented in this paper provides protection of the trust between crew and controllers with considerations to the airline industry economy.

References

[1] FAA. (1992). Order 5050.22C: Radio Frequency Interference Investigation and Reporting . Washington D.C.: Federal Aviation Adminstration. Retrieved June 15, 2012, from http://www.faa.gov/documentLibrary/media/Order/6050_22C.pdf

[2] FAA. (2010). AC No 20-140A:Guidelines for Design Approval of Aircraft Data Link Communication Systems Supporting Air Traffic Services (ATS). AIR-130. Washington: Federal Aviation Admistration. Retrieved from www.faa.gov

[3] FAA. (2010). AC No: 20-140A Guidelines for Design Approval of Aircraft Data Link Communication Systems Supporting Air Traffic Services (ATS). AIR-130. Washington D.C.: Federal Aviation Administration. Retrieved June 15, 2012, from http://www.faa.gov/documentLibrary/media/Advisory_Circular/AC%2020-140A.pdf

[4] FAA. (2011). ADMINISTRATOR'S FACT BOOK. Assistant Administrator for Financial Services, Washington,

DC. Retrieved December 10, 2011, from http://www.faa.gov/about/office_org/headquarters_offices/aba/

[5] FAA. (2011). Adminstrator's Fact Book. Assistant Administrator for Financial Services. Washington, DC: FAA. Retrieved December 10, 2011, from http://www.faa.gov/about/office_org/headquarters_offices/aba/

[6] FAA. (2011). NextGen Avionics Roadmap Version 2.0. Joint Planning and Development Office. Washingthon DC: Federal Aviation Adminstration. Retrieved December 8, 2011, from www.JPDO.gov

[7] FAA. (2012). FAA Aerospace Forecast Fiscal Years 2012-2032. Federal Aviation Administartion. Retrieved June 15, 2012, from http://www.faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2012-2032/

[8] FAA. (2012, March 8). Press Release . (H. Price , Producer) Retrieved March 11, 2012, from Federal Aviation Adminstartion: http://www.faa.gov/news/press_releases/news_story.cfm?newsId=13394

[9] Huerta, M. (2011, March 15). Speech – "Cybersecurity and NextGen. Retrieved March 10, 2011, from Federal Aviation Adminstration: http://www.faa.gov/news/speeches/news_story.cfm?newsId=12538&omniRss=speechesAoc

[10] ICAO. (2010). Global Operational Data Link Document (GOLD). Monteral: International Civil Aviation Organization. Retrieved June 15, 2012, from http://www.dca.gov.bm/Flight%20Ops%20News/GOLD%201st%20Edition_14-Jun-10%20(ID%2013727).pdf

[11] ICAO. (2012, January 6). Strong Traffic Growth in 2011 Reflects Improved Global Economic Climate. Retrieved March 10, 2012, from International Civil Aviation Organization (ICAO).: http://www.icao.int/Newsroom/Pages/strong-traffic-growth-in-2011-reflects-improved-global-economic-climate.aspx

[12] JPDO. (2010). Net-centric concept of Operations. Net-Centric Operations Division. Washington D.C: Joint Planning and Development Office. Retrieved from www.jpdo.gov

[13] JPDO. (2010). Net-Centric Operations Concept of Operation Version 1.0. Washington D.C: JPDO.

[14] JPDO. (2011). Targeted NextGen Capabilities for 2025. Joint Planning and Development Office, Washington DC.

[15] Lee, Y., & Krodel, J. (2006). Flight-Critical Data Integrity Assurance for Ground-Based COTS Components. Final Report, Office of Aviation Research and Development-Federal Aviation Administration, U.S. Department of Transportation, Washington DC. Retrieved from actlibrary.tc.faa.gov

[16] Prodanovic, R., & Simic, D. (2007). A Survey ofWireless Security. 15, 10.2498/cit.1000877. doi:10.2498/cit.1000877

[17] Tether, A. (2003, June). Cyber-security must become a feature a network-centric warfare. AVIATION WEEK & SPACE TECHNOLOGY, 158(26), pp. 74-74, 1p.

[18] Valacich, J., & Schneider, C. (2012). Information Systems Today, Managing in the Digital World 5e. Upper Saddle River: Prentice Hall.