An aeronautical data link security architecture overview

Mohamed-Slim Ben Mahmoud, Nicolas Larrieu, Alain Pirovano

AN AERONAUTICAL DATA LINK SECURITY OVERVIEW

Mohamed Slim Ben Mahmoud, Nicolas Larrieu, Alain Pirovano
French Civil Aviation University (ENAC), LEOPART Laboratory, Toulouse, France

Abstract

This paper reviews existing security mechanisms for aeronautical data link communication: current support and availability of such features are described. With an Open Systems Interconnection (OSI) reference model-driven analysis, each solution is classified and analyzed according to the layer where security is deployed and a relevant taxonomy is proposed.

Moreover, advantages, drawbacks, and possible threats of every security mechanisms previously introduced are discussed. According to this security infrastructure overview, a proposal for an efficient security architecture adapted to the aeronautical context is made for future studies. Satellite communication-based system specific problematic is taken into account with a constraint bandwidth and the need of reduced overhead for any additional mechanisms.

Introduction and Problem Statement

Mainly, a data link is a two-way communication between an aircraft and a ground station, such as an air traffic controller or an airline company, used to exchange digital information. Most commonly, for the moment it is used when traditional analog voice communications are no longer possible, typically when crossing oceanic environments. Future Air Traffic Management (ATM) environments no longer rely exclusively on analog voice messages to exchange information. Doubtlessly, transition from analog voice to a predominance of digital data communications will be imminent whether for the coming next generation Air Traffic Services (ATS) or Aeronautical Operational Communications (AOC). Furthermore, with the growing demand for In-Flight Entertainment (IFE) (for instance Aeronautical Passengers Communications - APC) applications such as Internet for the cabin, the use of a permanent data link became a necessity to cope with user's requests.

Since many years, aeronautical data link communications are being provided using different technologies: Very High Frequency Data Link (VDL) under its various modes (VDL mode 2 being the most frequently used one) [1], WiMAX for traffic occurring in the airport area, and Satellite Communications (SATCOM), among others. However, due to the limited throughput afforded by some of these technologies, heterogeneous and demanding traffic can only be conveyed by high data rate technologies such as SATCOM or WiMAX [2].

Besides, in this context we have made the assumption that future aeronautical communication applications will use a single air-ground link in a full IP-based network where all the aeronautical services (safety and non-safety related) will be aggregated. This assumption is based on the fact that digital convergence that we see in such domains as Internet or industrial telecommunications will be deployed in the same way for aeronautical communications in future.

Hence, as usage and dependency on data link communications increase so do security risks. Security requirements for this communication system are more and more complex to fulfill due to many factors such as traffic heterogeneity, aircraft mobility, or scaling issues induced by the number of aircrafts to manage. The implemented security mechanisms must handle some priority mechanisms to deal with the safety related characteristic of the Air Traffic Communications and AOC applications. For example, the current Controller Pilot Data Link Communication (CPDLC) systems are being provided without security.

The Airlines Administrative Communications (AAC) and APC applications have certainly lower priority, but we can easily imagine a scenario where a passenger wants to buy his aircraft e-ticket for his next transfer, and hence, demands for a secured connection so that his confidential data cannot be disclosed. Moreover, unlike terrestrial environment, an aircraft communication cannot tolerate attacks inducing connection breakdown as this would result

978-1-4244-4078-8/09/$25.00

not only in substantial financial losses, but may also lead to loss of precious human lives. Under such circumstances, confidentiality, integrity, authentication, non-repudiation, and availability (see next section) are strongly required to guarantee information insurance either for cockpit or the cabin.

Thus, providing information security in an aeronautical environment is still a significant challenge. Nowadays, multiple aeronautical organizations and industry standard groups are identifying information security needs: the Airline Electronics Engineering Committee (AEEC), the European Organization for the Safety of Air Navigation (EUROCONTROL), the International Civil Aviation Organization (ICAO), and many others attempt to enhance the safety of the flight, the overall objective remains to secure links, data and infrastructure from external attacks.

Unfortunately, having a global overview of these activities is a labored task, doubtless because the majority of these groups work independently from each others. Moreover, few organizations are publishing their digital security related works. As far as we are investigating this topic, there is no paper inventorying completely such activities.

Consequently, this paper aims to give a global outlook of the aeronautical information security field focusing on data link security component. The following section presents the basic concepts of computer communication security. Section III gives an overview of the present literature regarding data link security. Section IV addresses the security requirements and the possible threats and attacks in the already proposed security solutions. In the last section, we give conclusions and possible improvements providing some pointers to future research work.

Basic Concepts of Computer Information Security

Since many years, there has been ongoing research for all aspects related to computer security. Mostly, the basic concepts of security remain relevant to any area where a communication system is involved, such as aeronautical air-ground communication. Many security architecture designs and approaches have been proposed to facilitate the comprehension of these concepts.

For example, the Federal Aviation Administration (FAA) presented a layered pyramid scheme providing the focus for information systems security efforts [3]. It shows that every information system fields can be concerned by security.

Figure 1 illustrates the five security activities and five fundamental security services in an information system. These concepts are explained below. Note that computer information security is such a wide domain we cannot represent all the interfering components and security considerations.

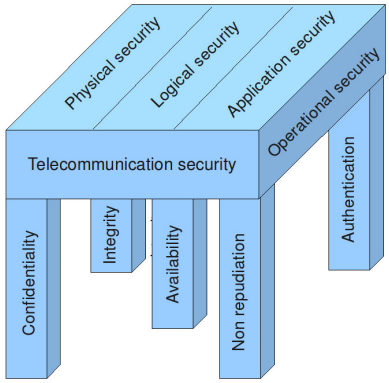

Figure 1. Global Security Architecture for an Information System

The five security activities in an information system are:

- Physical security,
- Operational security,
- Logical security,
- Application security,
- Telecommunication security.

Physical security deals with all the physical aspects in a system and its environment as access control to the equipments or physical redundancy for instance. Operational security is concerned by all the functional aspects of the system (preventive maintenance, backup plane, system's configuration and updates, etc). Logical security looks after the implementation of security mechanisms such as cryptography, password management, deployment of anti-viruses, or authentication procedures.

Application life cycle, implementation methodology, tests, and validation process are among factors affecting application security. Finally,

telecommunication security seeks to offer an end to end security for the final user. A security infrastructure has to be defined for access, communications protocols, operating systems and equipments. Furthermore, a risk analysis step is almost mandatory in every security management infrastructure in order to fix a criticality security level for the manipulated data.

A security policy has to be followed throughout the system life cycle. Obviously, a totally secured system does not and will probably never exist because security is still a risk-based process and risk can only be reduced, never eliminated. Only after a risk assessment process, risk is considered acceptable under a fixed level and thus, will be tolerated.

The five security services holding the global security architecture of a system are:

- *Confidentiality*: information is access-opened only to authorized users;
- *Authentication*: a sender or a receiver dealing with the communication has to be able to prove his identity to the entity he is talking with;
- Integrity: information can be amended only by users who are authorized to do so;
- *Non-repudiation*: Communicating parties cannot deny the happening of a given event (typically the post or the reception of a message);
- *Availability*: services offered by a system must be always accessible by authorized users.

These five ingredients are necessary to ensure the security of the system.

Taxonomy for Aeronautical Data Link Security Architecture

As underlined before, providing information security for data link communication is becoming a huge claim for aviation working groups seeking to satisfy information security needs for present and future applications.

Having a global overview of these activities remains a difficult task. First, the research area is wide and it can take long-time to digest and to comprehend. Then, there are few papers trying to list the yet proposed security architectures in a clear and well explained manner. Nevertheless, [4] tried to take a look at the available security mechanisms for both Internet and Aeronautical Telecommunication Network (ATN) applications [5] and to highlight the lack of a coherent overall aviation security solution.

In this section, we aim to present a taxonomy of what has already been done in aeronautical information security field focusing on data link security component. We divided this task in two sub-tasks for a matter of perspicacity: first, we propose an UML [1] [6] meta-model summing up the fundamental concepts affecting the aeronautical information security. More details are given in the next subsection.

Then, we present a tabular data link security taxonomy for aeronautical communications. This table is an attempt to map the existing security threats with security services and to provide the appropriate security countermeasures met in the literature.

The meta-model and the data link security taxonomy are an attempt to produce a comprehensive framework in order to address the shortcomings of the previous works and propose a unique and adapted data link security solution for aviation (see next section).

Aeronautical Information Security Meta-Model

The meta-model illustrated in Figure 2 embodies all the notions involved in the aeronautical information security. It proposes a formalism of the information security in aviation with the objective to give the reader an overview of the entities and concepts dealing with aeronautical information security in one single shot. Rectangles picture entities. Lines denote relations with cardinalities at the termination points. Arrows evoke specification of a given entity. For instance, “On board” and “Off board” entities are specifications of the “Domain” entity.

[1] The Unified Modeling Language is an open method to specify and construct the components of an object-oriented system.

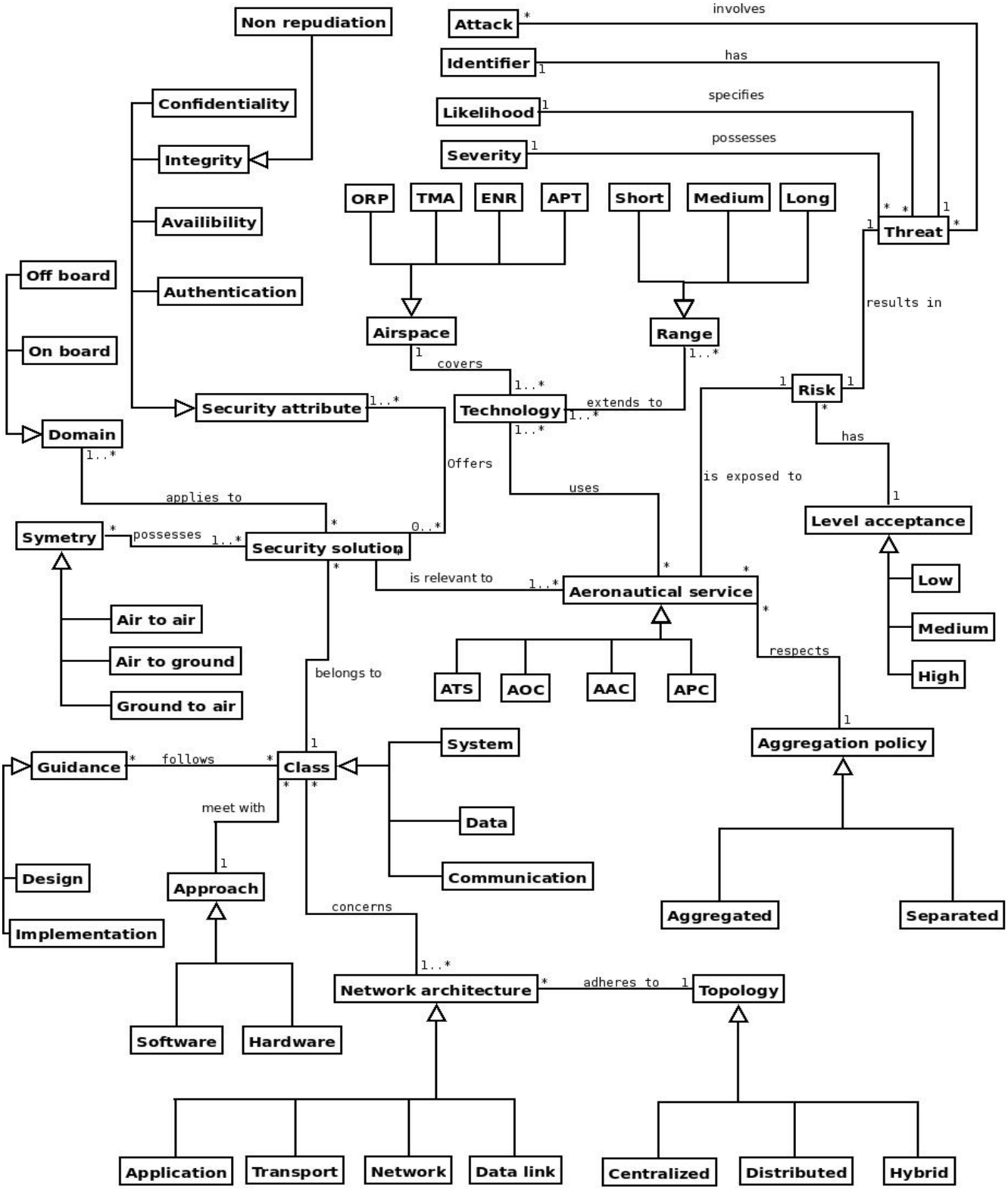

Figure 2. An Aeronautical Information Security Meta-Model

This contribution is the main output we supplied after a state of the art first step. *Security mechanism* is the core of the meta-model. Every security mechanism is applied either *on board* between sub-networks, such as passengers IFE network and crew network for instance, or *off board* between the aircraft networks and aeronautical ground networks. *Security attributes* are the list of services offered by the security mechanism. The proposed solution can secure an a*ir to air* communication between two aircrafts, a half-duplex or full-duplex *air-ground* communication.

Every security mechanism can be used to protect one or many *aeronautical services*. The *aggregation policy* for the aeronautical data streams can consistently influence the security policy to establish. Every security mechanism belongs to a security *class*. *System* class is relevant to software design and implementation policies. Some mechanisms for the Airplane Asset Distribution System (AADS) [7,8] such as Partitioning Communications Systems (PCS) [9,10] and Multiple Independent Levels of Security/Safety (MILS) [11] are examples of security solutions dealing with system engineering.

Communication and *Data* classes regroup security mechanisms involved with data link communications. These two classes are the focus of the paper and will be developed in the next sub-section.

Usually, *design guidance* for network *topology* (*centralized*, *distributed*, or *hybrid*) are given as advices to a specific case. *Implementation* rules are also given for system class security solution. The *technology* used for the communication between the aircraft and ground systems (SATCOM or VDL for instance) which depend on the covered airspace area, e.g. AirPort (APT), Terminal Maneuvering Area (TMA), EN Route (ENR) or Oceanic Remote Polar (ORP), is also an influencing factor on the data security.

Every aeronautical information system is obviously exposed to a specific list of *threats*. A *risk* is assessed and mitigated to an *acceptable level* according to the *likelihood* and the *severity* of every *identified* threat.

A Matrix for a State of the Art of Data Link Security Taxonomy

Although, the existing writings related to the aeronautical data link security are not particularly exhaustive, some security analysis can be found [12-15].

Indeed, [13] identified an initial threat's list for aircraft systems. We extracted from this general list only threats that may target a communication segment focusing on the data link component, namely:

- T.DENIAL: when system resources may become exhausted due to Denial of Service (DoS) attack,
- T.ENTRY: when an individual other than an authorized user may gain access via technical attack for malicious purposes.

Thus, we consider T.DENIAL and T.ENTRY as the two general threat classes. From this point, we detail a list of the specific and potential threats for a data link communication system using the taxonomy suggested by [13] in Table 1 [16].

We give for every threat a type: a passive attack attempts to learn or steal information from the system without affecting its resources, whereas an active attack tries to alter and affect system resources and operations. Also, some attacks linked to the threat are mentioned. Finally, exposed security attributes are listed for every threat.

Here is a description for every identified threat:

- T.DENIAL.FLOODING: an attacker injects a higher number of messages,
- T.DENIAL.INJECTION: an attacker injects unauthorized or faulty messages,
- T.DENIAL.JAMMING: an attacker introduces a source of noise strong enough to significantly reduce the capacity of the channel,
- T.ENTRY.ALTERATION: an attacker delays, modifies, re-directs, re-orders, replays messages,
- T.ENTRY.EAVESDROPPING: an attacker or an unauthorized user can listen without permission to the signaling/data traffic,

- T.ENTRY.MASQUERADING: an attacker can spoof/impersonate an authorized user's identity.

Accidental events are not mentioned since they are already addressed by many safety analyses [13,17,18].

Using the meta-model and the list of threats as an input, we generate a table (Table 2) to propose an aeronautical data link security taxonomy.

Table 1. List of Aeronautical Data Link Security Threats

Threat Class	Threat Identifier	Type of Threat	Examples of Attacks	Affected Security Attributes
T.DENIAL	T.D.F (T.DENIAL.FLOODING)	Active	TCP SYN Flooding, E-mail bombing, ICMP Flooding, MAC Flooding	Availability
	T.D.I (T.DENIAL.INJECTION)	Active	Code injection, SQL injection	Availability
	T.D.J (T.DENIAL.JAMMING)	Active	High frequency modulation	Availability
T.ENTRY	T.E.A (T.ENTRY.ALTERATION)	Active	Stream cipher attack, Malicious software	Integrity
	T.E.E (T.ENTRY.EAVESDROPPING)	Passive	Man In The Middle, Cryptanalysis, Traffic sniffing, Signal analysis	Confidentiality
	T.E.M (T.ENTRY.MASQUERADING)	Active	Social engineering, Forge public key, Forge authentication privilege, Password sniffing, Brute force attack, Dictionary attack, Public key sniffing	Authentication Non-repudiation

Table 2. An Aeronautical Data Link Security Taxonomy

Security Mechanisms	Algorithms/Protocols/ Standards/Devices	Fixed Threats	Project Names
Symmetric encryption	3-DES, AES	T.E.E	ATN [5], SWIM [9], SATSIX [19]
Public key encryption	RSA	T.E.E	ATN, SATSIX, NEWSKY [20]
Hash functions	SHA, HMAC-SHA	T.E.A, T.D.I	ATN, SWIM, SATSIX
Digital signature	ECDSA	T.E.A	ATN, SWIM
Email security	S/MIME, PGP	T.E.A, T.E.E, T.E.M	TSCP [21]
IP security	IPSec, SatIPSec	T.E.A, T.E.E, T.E.M	SWIM, SATSIX
Web security	HTTPS, SET, TLS/SSL	T.E.A, T.E.E, T.E.M	SWIM
Network traffic control	Firewall	T.D.F, T.D.I	NEWKSY, ATN, SWIM
Network traffic monitoring	NIDS, IPS, SPADE-IDS	T.E.A, T.E.E, T.E.M	SigSec™ [22]
Key agreement scheme	IKE, ECDH, MOBIKE	T.E.E, T.E.M	ATN, SWIM, EUROCONTROL [16]
Public key certificate	X.509	T.E.M	Certipath™ [23], TSCP, ATN, SWIM
ACARS security	AMS	T.E.A, T.E.E, T.E.M	ARINC 823 [24,25]
ATN security	Secure CPDLC	T.E.A, T.E.E, T.E.M	ATN
Secure tunneling	VPN, SSH	T.E.A, T.E.E, T.E.M	ATN, NEWSKY
Secure route discovery	SEND, SDHAAD	T.D.F, T.E.M	NEWSKY

It is important to underline that, for a matter of exhaustiveness, the security mechanisms presented here are either recommended for use, simply proposed as a solution, or applied.

System security class is discarded from the taxonomy because it is out of the scope of data link communications security. In front of every security mechanisms, fixed threats and implementation details are provided. We added a last column depicting when available, the working group, the project name, and relevant references that suggested or used the security mechanism. T.DENIAL.JAMMING is out of scope of the study because it has to deal with the physical layer attacks.

All ATN security mechanisms are not quoted in the table because they use the already listed algorithms and protocols. For instance, the ATN Digital Signature Scheme (ADSS) uses the Elliptic Curve Digital Signature Algorithm (ECDSA) [26]. The eighth sub-volume of [5] is dedicated to the ATN security framework where the proprietary public key and cryptographic infrastructures are detailed.

Encryption schemes are used to ensure the confidentiality of a communication. They are divided into symmetric and asymmetric encryption algorithms.

For instance, the symmetric Advanced Encryption Standard (AES) was adopted by ATN and the System-Wide Information Management (SWIM), a network-centric environment developed by the FAA to share data in the National Airspace System (NAS).

Unlike symmetric algorithms which use the same key to encrypt and decrypt messages, asymmetric algorithms as the well known Rivest, Shamir, Adleman (RSA) algorithm (RFC 2313)[2], use two different keys for encrypting and decrypting messages.

Another notable difference between the two encryption method is that asymmetric algorithms are more computational costly that symmetric algorithms.

Generally, the robustness of an encryption system is assessed according to the algorithm's strength, the key's size, the ciphering mode (stream mode and block mode) and the freshness rate of the keys. Many protocols implement these algorithms at different layers of the network architecture.

For instance, AES is used in both network and transport layers when implemented respectively in IPSec (RFC 4309) and in Transport Layer Security (TLS) (RFC 5246).

Hash functions are mathematical procedure allowing generating a fixed-length checksum to identify a data block. They are used usually in digital signature mechanisms. The keyed-Hash Message Authentication Code (HMAC) using the Secure Hash Algorithm (SHA) (RFC 4634) was adopted by both ATN and SWIM for data integrity. Asymmetric ciphers coupled with hash functions are used to produce digital signature schemes such as ECDSA [27] used in ATN. Digital signatures are used for data authentication and data integrity. Hash functions can also be used at different layers of the network architecture such as SHA-1 in IPSec (network layer) and TLS (transport layer).

A global E-mail security architecture was proposed by the Transglobal Secure Collaboration Program (TSCP) [21]. Secure/Multipurpose Internet Mail Extensions (S/MIME) (RFC 3851) and Pretty Good Privacy (PGP) (RFC 3156) are examples of protocols used to protect mails from eavesdropping, alteration, and masquerading threats. These are application level security mechanisms and have to be implemented in the end hosts.

IPSec and Satellite IPSec (SatIPSec) [19] are the two main network layer security mechanisms. SatIPSec is a satellite-adapted variant of IPSec. It was developed to satisfy the security needs in a satellite system. SatIPSec was adapted to the Digital Video Broadcasting Return Channel (DVB-RCS) networks in the Satellite-based communications systems within Ipv6 SATSIX project.

Web security is often provided by Hyper Text Transfer Protocol (HTTP) over TLS using Transport Control Protocol (TCP) (RFC 2817). The Secure Electronic Transaction protocol (SET) (RFC 3538) (application layer) is used specially for electronic payments over Internet and insecure networks.

Firewalls are non cryptographic security mechanisms which control the exchanged traffic between two networks in order to address possible intrusions on the system. They can be used either at network, transport or application layer. Network Intrusion Detection System (NIDS) and Intrusion Prevention System (IPS) are also network protection

[2] All the quoted RFCs are available at http://www.ietf.org/rfc.html

devices used to monitor and fix network attacks [28]. [12] presented a security framework using a Statistical Anomaly Detection Engine based IDS (SPADE-IDS) adapted to aeronautical networks.

Key agreement schemes are used to establish a shared key between two or more communicating parties. Internet Exchange Key (IKE) protocol is used in IPSec to set up a session key (RFC 4306). Elliptic Curve Diffie-Hellman (ECDH) [29] protocol is used in ATN and SWIM as a key establishment protocol. Elliptic curve cryptography is combined with the Diffie-Hellman protocol to fix the man-in-the-middle attack.

EUROCONTROL IP study [30] presented the IKEv2 Mobility and Multihoming (MOBIKE) as a potential solution for security issues introduced by the mobility factor. Key agreement can be used either at network or data link layer.

Public Key certificates like the Telecommunication Standardization Sector (ITU-T) X.509 are used in Public Key Infrastructure (PKI) to bind a public key with the corresponding entity. These certificates use a digital signature given by a Certificate Authority (CA) to avoid authentication and non repudiation issues [31,32].

The Aeronautical Radio Incorporated (ARINC) transport communications provider introduced in 1978 a new data link system called Aircraft Communications Addressing and Reporting System (ACARS) at application layer. This new system allowed the airplane to send data information to the ground stations via the Communications Management unit (CMU). Before the release of a secured version, namely Secure ACARS Message (AMS) protocol, ACARS message were exposed to external attacks [33,34]. An existing website[3] shows how easy for a hacker to listen to an ACARS-based communication with a real-time messages decoder. ARINC presented in the ARINC Project Paper 823 [24,25] a data link security framework and a key management scheme to secure ACARS messages.

ICAO has recommended the use of a PKI in CPDLC application to address masquerading and alteration concerns in ATM environment. [14] detailed a scenario with a secure CPDLC information exchange in ATN at the application layer.

3 http://www.acarsd.org/

Secure tunneling is usually recommended for networks logical separation. Virtual Private Networks (VPN) and Secure Shell (SSH) tunnels are frequently used as means to offer safety: operational data traffic and non-operational data traffic must be either physically or logically separated for a matter of trustworthiness. The authors of [35] presented three network separation scenarios using secure tunneling.

Aircraft's mobility component has undeniably introduced additional security problems related to handover or router discovery for instance. The NEWSKY team proposed some mechanisms to improve security level in a mobile environment such as an aeronautical network: they suggested Secure Neighbor Discovery (SEND) protocol to secure the Neighbor Discovery protocol for IPv6 [35]. They studied also a secure version of the Dynamic Home Agent Address Discovery (DHAAD) for the Mobile IPv6 (MIPv6) protocol [20].

Finally, Table 2 highlights two major issues in aeronautical data link security:

- None of the listed security mechanisms can cover all data link threats and security services listed before,
- These security mechanisms are provided at different network architecture layers.

In the next section, we introduce an original security architecture to manage and fix these issues. Finally, a case scenario is introduced to illustrate the benefits of such a solution.

Toward an Adaptive Security for Aeronautical Communications

According to the security infrastructure overview presented in the previous sections, we can see that there is no unique and totally secured infrastructure for aeronautical data link communications: every security mechanism has its own fields of concern, domains, advantages and drawbacks, implementation layer, etc.

Besides, any “good” security system will be expensive to implement. The strongest security features cannot be applied for each application as the cost will be prohibitive, from an implementation prospect. Using a strong cryptographic key with a weak authentication algorithm may allow an attacker to disturb the data. Using a strong authentication cipher

with a weak encryption algorithm may allow an attacker to decrypt the data. Using both strong authentication and encryption algorithm protects the data but it will decrease the transmission rate and could induce critical resources consumption: it is complicated to provide the best protection, the maximum throughput and the lowest overhead simultaneously on the same link.

Thus, a well-balanced agreement between security and Quality of Service (QoS) has to be found. Besides, Required Communication Performance (RCP), mostly for ATS and AOC services, are precisely defined by an Operational Performance Assessment (OPA) [16] and have to be strictly respected.

The security architecture we are about to expose is adapted to the aeronautical context and also specific to the security-QoS trade-off issue quoted before. Moreover, this infrastructure will be tested and validated within an industrial project titled FAST (Fiber-like Aircraft Satellite Telecommunications).

Indeed, this security infrastructure is part of preliminary tasks for this French Aerospace Valley labeled project started in January 2009 which aims at studying the feasibility and reliability of an airborne satellite *ku*-band infrastructure putting up a high throughput for the aircraft.

Under such circumstances, an additional "security manager" module can be added in order to select the required security features, and consequently, apply the chosen controls related to each different user application needs. The security manager scheme is shown in Figure 3.

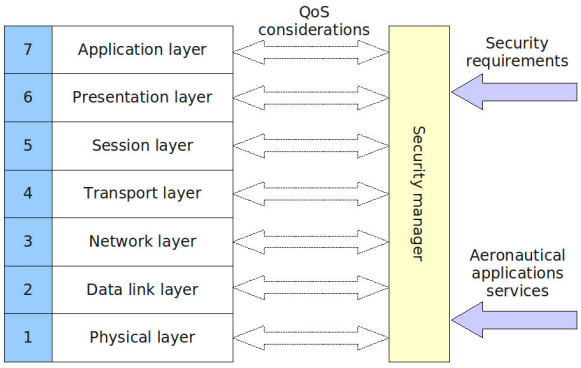

Figure 3. An Adaptive Security Manager for Data Link Communications

Assumptions

With the intention to propose an original security architecture for future data link communications, some assumptions have to be made:

- The network architecture is a classical TCP/IP architecture. As mentioned in the introduction, it is legitimate to foreseen a full IP-based aeronautical network for the upcoming data link communications: benefits are cost saving, high reliability and optimal alignment with the evolution of next-gen communications, passengers' needs, and available high-capacities technologies [36,37]. Furthermore, this may offer a seamless interoperability with existing terrestrial networks.
- For now, the internal architecture of the security manager is out of the scope of this paper. Consequently, the module is seen as a black box.

Only its inputs and outputs of the security manager are explained below:

- *Aeronautical applications services*: different services ranging from ATS, AOC, AAC, and APC shall partially or totally share the aeronautical network architecture, and processed by the security manager module before going through network architecture layers. Obviously, each service here has its own specific applications and imperatives. A preliminary identification study shall be made to establish a formal database of future aeronautical application services used in planes [13].
- *Security Requirements*: for every input service, the level of security needed is expressed on the basis of fundamental security functionalities, typically confidentiality, integrity, authentication, availability, and non repudiation. Again, a previous analysis has to be conducted in order to formally define these requirements. A risk assessment methodology like [16] and [17] would certainly result in a qualitative definition of the security levels (generally ranging from low to high).
- *Real-time QoS considerations*: correspond to the double dashed arrows in Figure 3 linking

the architectural stack to the Security Manager. The module will be able to keep track of information about the security mechanisms already activated, and the network state and resources consumed. A cross-layer approach [38] could be used to report the relevant information every time a change likely to modify the network properties occurs. Cross-layering is a well-known technique in ground networks community, especially because it turns away the strict way-down concept of the OSI modeling, allows delivering a dynamic feedback of the network, and thus, improving the QoS controls. A state table of the active security mechanisms will be dynamically updated with the evolving state and needs of the network.

Security Manager Framework

Mostly, the purpose of the security manager module is to offer a "best effort" security under QoS constraints. Its main role is to match the security requirements of an aeronautical service with one or several relevant security mechanisms according to the level of robustness expressed and the real-time available QoS. If enough network resources are provided, selected security services could match the security requirements. Otherwise, security requirements have to be lowered to avoid a traffic congestion, overload or decrease of network performances such as delay, packet error rate or throughput. A reporting QoS policy has to be established as a precondition of the system.

Inside the module, a support decision algorithm has to be implemented in order to process a mapping between the available security mechanisms and the security needs expressed by users. Also, the security manager will be able to perform a "multilayer security" by selecting several protocols at different layers, depending on the tradeoff between already activated mechanisms, requested levels of security and QoS parameters previously described.

As announced in [16], the upcoming second phase (phase 2) for ATM will see data communications as the primary means of air-ground communication. With such an upheaval, we can imagine a case scenario where APC messages (for instance, a commercial e-transaction on the Internet) have to be exchanged between the cabin and a ground station over a TCP/IP network. This case scenario is shown in Figure 4.

We make the following assumptions for this case scenario:

- The security needs expressed for the transfer are: confidentiality, mutual authentication, and data integrity;
- The security manager is implemented in both air and ground end systems;
- Two security mechanisms are available: IPsec on the network layer and SSL on the transport layer;
- When using IPsec, the Encapsulated Security Payload (ESP) mode is used because it provides confidentiality, authentication and integrity;
- When the security needs for this exchange were expressed, QoS considerations are low enough to allow a best effort security policy.

Generally, a robustness level of the implemented security mechanisms has to be studied and fixed within some comparison criteria, like the key's length for confidentiality mechanisms for instance. [39] presented a technical comparison of security and performance properties for IPSec and SSL. Here is a sum up of this results study, referring only to the security services we are interested in (namely confidentiality, authentication, and integrity):

- IPsec in ESP mode provides the stronger encryption method (112/168-bit 3DES or 128-bit AES) than SSL (a 40- or 128-bit RC4);
- SSL provides an inferior implementation of authentication than IPSec: mutual authentication is mandatory in IPSec and optional in SSL, IPSec supports the use of RSA/DSA digital signature and the use of a random 2048 bit Secret Key while SSL supports only the use of Digital signature, etc;
- Both IPSec and SSL protocols use HMAC-SHA-1 and HMAC-MD5 as hash functions for Message authentication Code (MAC). Nevertheless, SSL provides longer hash digest (20 Byte for HMAC-SHA-1 and 16 Bytes for HMAC-MD5) than IPSec (12 Byte for both HMAC-SHA-1 and HMAC-MD5).

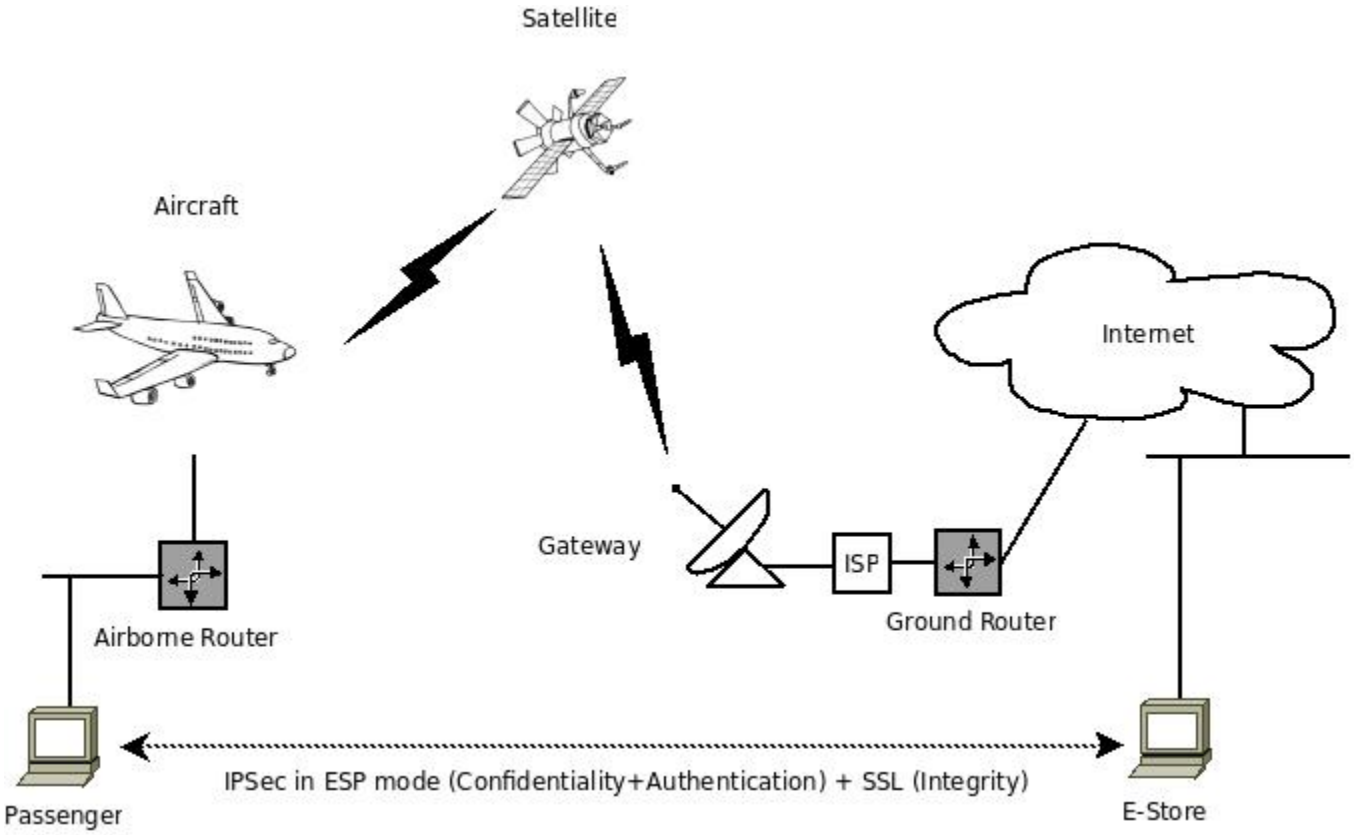

Figure 4. An Illustrative Case Scenario for an Adaptive Multi-Layers Security in Aeronautical Communications

Thus, we establish three order relationships to compare the two protocols:

- IPsec $>_{conf}$ SSL: confidentiality order relation;
- IPsec $>_{auth}$ SSL: authentication order relation;
- IPsec $<_{integ}$ SSL: integrity order relation.

In accordance with the current QoS considerations, the security requirements expressed and the order relationships above, the security manager choose to apply IPSec for confidentiality and authentication and SSL for integrity.

Afterward, if any network trouble is detected or a prior traffic is about to be exchanged (an emergency application as Telemedicine for instance), the security manager module is informed through the cross-layer algorithm in order to lower the consumptions of network resources (mainly, CPU and bandwidth). In the described case, the security manager will switch from an SSL to an IPSec integrity mechanism: as told above, the SSL integrity hash function produces a stronger digest than IPSec at the cost of length (and therefore, bandwidth and CPU consumption). Another benefit to use a full IPSec security is the compression algorithm IPCom (RFC 2393) used. [39] showed that in low bandwidth networks, the use of IPSec compression algorithm improve the throughput speed.

This scenario aims only at illustrating security manager principles and future studies will have to focus on the overhead induced by the combination of various security protocols in aeronautical APC communications as done here for SSL and IPSec.

As a conclusion, the adaptive multi-layer security framework we presented is in complete concordance with the security objectives listed in [13]. The authors stressed on the fact that security controls for aircraft systems should:

- be flexible in order to permit them to be used within a variety of different policies and procedures,
- employ multiple security controls,
- induce minimal computational and network overhead.

Conclusion

With the proposed taxonomy, aeronautical information security can be deeply addressed. Researchers dealing for the first time with the subject will have a sum-up of the existing works to begin with. On the other hand, people already dealing with data link security will find a wide coverage of the area. Of course, this taxonomy is not time-frozen because newer works will be published soon, but its generic design will provide easy periodical updates.

The security manager module we proposed is the first step toward an innovative and adaptive security management for aeronautical communications. Our next challenges are firstly to formalize mathematically the module and its relationships with external entities, then design its internal functions and implement it in a real life context as we plan to do within the industrial project FAST. Finally, the increasing system complexity due to a high number of planes communicating in the same airspace domain at the same time will generate some scaling issues we need to handle carefully.

References

[1] Murawski, Robert W., Steven C. Bretmersb, K. Konangi KJay, 2004, Evaluation of VDL Modes in the En-Route Domain, Cleveland State University.

[2] Niebla, C.P.,N.R. Diaz, S. Scalise, C. Kissling, September 2006, DVB S2-RCS Suitability for the Provision of Air Traffic Management Services, Satellite and Space Communications, 2006 International Workshop on 88-92.

[3] Daniel J.Mehan, November-December 2000, Information Systems Security, The Federal Aviation Administration's Layered Approach.

[4] Wargo, C. A., C. Dhas, March 8--15 2003, Security considerations for the e-enabled aircraft, 4 4 1533—4 1550.

[5] ICAO, 2002, Manual of Technical Provisions for the ATN, Doc 9705, Ed 3.

[6] Object Management Group, March 2000, Unified Modeling Language Specification, Version 1.3, First Ed.

[7] Robinson, Richard V., Mingyan Li, Scott A. Lintelman, Krishna Sampigethaya, Radha Poovendran, David von Oheimb, Jens-Uwe Bußer, Jorge Cuellar, 2008, Electronic Distribution of Airplane Software and the Impact of Information Security on Airplane Safety, 4680 Springer Berlin / Heidelberg 28—39.

[8] Sampigethaya, K., Li Mingyan, R. Poovendran, R. Robinson, L. Bushnell, S. Lintelman, October 2007, Secure wireless collection and distribution of commercial airplane health data, Digital Avionics Systems Conference, 2007. DASC '07. IEEE/AIAA 26th, 4.E.6-1-4.E.6-8.

[9] Stephens, B., October15--19 2006, System-Wide Information Management (SWIM) Demonstration Security Architecture, 1—12.

[10] Uchenick, G. M., 2007, Partitioning Communications System for safe and secure distributed systems, 2.E.5-1—2.E.5-8.

[11] Boettcher, C., R. DeLong, J. Rushby, W. Sifre, 26--30 October 2008, The MILS component integration approach to secure information sharing, 1.C.2-1—1.C.2-14.

[12] Ali, M.S., R. Bhagavathula, R. Pendse, October 2004, Airplane data networks and security issues, Digital Avionics Systems Conference, 2004 DASC 04. The 23rd 2, 8.E.1-81-12 Vol.2.

[13] ARINC, 2005, ARINC Report 811, Commercial aircraft Information Security Concepts of Operation and Process Framework.

[14] McParland, T., V.Patel, W.J. Hughes, October 2001, Securing air-ground communications, Digital Avionics Systems, 2001. DASC. The 20th Conference 2 7A7/1-7A7/9 vol.2.

[15] Stephens, B., Oct. 2004, Security architecture for aeronautical networks, Digital Avionics Systems

Conference, 2004. DASC 04. The 23rd 2, 8.E.2-81-19 Vol.2.

[16] Eurocontrol/FAA, Communications Operating Concept and Requirements for the Future Radio System, Ver. 2.0.

[17] National Aerospace Laboratory (NLR), 2007, Risk assessment of newly proposed concepts to improve in-flight security.

[18] Jacob, J.M., Oct. 2004, High assurance security and safety for digital avionics, Digital Avionics Systems Conference, 2004. DASC 04. The 23rd 2, 8.E.4-8.1-9 Vol.2.

[19] Iyengar, S., H. Cruickshank, P. Pillai, G. Fairhurst, L. Duquerroy, 2007, Security requirements for IP over satellite DVB networks, 1—6.

[20] Bauer, Christian, Max Ehammer, 2008, Securing Dynamic Home Agent Address Discovery with Cryptographically Generated Addresses and RSA Signatures, 555—560.

[21] Transglobal Secure Collaboration Program, August 6 2008, Secure E-Mail: Do-It-Yourself Manual, Ver. 2-3.

[22] Ramakrishnan, V., C. Wargo, S. John, May 2008, GMPLS network security: Gap analysis Integrated Communications, Navigation and Surveillance Conference, 2008. ICNS 2008, 1-7.

[23] CertiPath, June 27 2008, What is CertiPath? The Commercial PKI Bridge For Secure E-Business, Ver. 1.2.

[24] ARINC, 2007, Draft 1 of AEEC Project Paper 823 Data Link Security, Part 1 - ACARS Message Security.

[25] ARINC, 2007, Draft 4 (Strawman) of AEEC Project Paper 823 Data Link Security, Part 2 - Key Management.

[26] Olive, M.L., October 2001, Efficient data link security in a bandwidth-limited mobile environment - an overview of the Aeronautical Telecommunications Network (ATN) security concept, Digital Avionics Systems, 2001. DASC. The 20th Conference 2 9E2/1-9E2/10 vol.2.

[27] American National Standards Institute, September 20, 1998, X9.62-1998 Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA).

[28] Ramakrishnan, V., R.A. Kumar, S. John,May 3 2007, Intrusion Detection Using Protocol-based Non-Conformance to Trusted Behaviors Integrated Communications, Navigation and Surveillance Conference, 2007. ICNS '07, 1-12.

[29] Barker, Elaine, Don Johnson, Miles Smid, March 2007, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, National Institute of Standards and Technology (NIST), NIST Special Publication 800-56A.

[30] Ayaz, Serkan, Christian Bauer , Max Ehammer, Thomas Gräupl, Fabrice Arnal, 2008, Mobility Options in the IP-based Aeronautical Telecommunication Network.

[31] Patel, V., T. McParland, October 2001, Public key infrastructure for air traffic management systems, Digital Avionics Systems, 2001. DASC. The 20th Conference 2 7A5/1-7A5/7 vol.2.

[32] Robinson, Richard V., Mingyan Li, Scott A. Lintelman, K.Sampigethaya, Radha Poovendran, David von Oheimb, Jens-Uwe Bußer, 2007, Impact of Public Key Enabled Applications on the Operation and Maintenance of Commercial Airplanes.

[33] Risley, C., J. McMath, B. Payne, October 2001, Experimental encryption of aircraft communications addressing and reporting system (ACARS) aeronautical operational control (AOC) messages, Digital Avionics Systems, 2001. DASC. The 20th Conference 2 7D4/1-7D4/8 vol.2.

[34] Roy, A., 2001, Secure aircraft communications addressing and reporting system (ACARS), 2 7A2/1--7A2/11 vol.2.

[35] Ehammer, Max, Thomas Graupl, C. -H. Rokitansky, T. Brikey, 2008, Security consideration for IP based aeronautical networks, 2.E.1-1—2.E.1-13.

[36] Dhas C. , T. Mulkerin, C. Wargo, R. Nielsen, and T. Gaughan, 2000, Aeronautical Related Applications Using ATN and TCP/IP Research Report, Computer Networks and Software Inc. Springfield, Virginia, NASA.

[37] Kissling, C., C. Baudoin, 2008, Protocol Stack Options in Heterogeneous Aeronautical Networks, 43—48.

[38] Shakkottai, Sanjay, Theodore S. Rappaport, Peter C. Karlsson, June 23 2003, Cross-layer Design for wireless Networks.

[39] Saito, Takamichi, Abdelnasir Alshamsi, A Technical Comparison of IPSec and SSL, Tokyo University of Technology.

Acknowledgments

We would like to thank Dr. Fabien Garcia from ENAC and Dr. José Radzik from ISAE (Institut supérieur de l'Aéronautique et de l'Espace) for their wise and valuable comments that helped us to improve specific parts of this paper.

Email Addresses

Mohamed Slim Ben Mahmoud: Slim.ben.mahmoud@recherche.enac.fr

Nicolas Larrieu: Nicolas.larrieu@enac.fr

Alain Pirovano: Alain.pirovano@enac.fr