Security Architecture Design for Satellite Aeronautical Data Link Communications

Mohamed Slim BEN MAHMOUD*, Nicolas LARRIEU†, and Alain PIROVANO‡
French Civil Aviation University (ENAC), Toulouse, 31400, France

This paper presents some security design principles for future satellite aeronautical data link communications. The architecture we introduce is dynamic and flexible with regards to several factors such as traffic density or service priorities thanks to an adaptive security management according to available system and network resources.

I. Introduction

Future aeronautical environment is expected to go through some radical and progressive changes in the near future. The aviation industry is evolving rapidly and means of communication is one of the affected aspects.

The problematic addressed in this paper aims at designing a security architecture for the whole set of digital aeronautical communications. This security architecture, focused on aeronautical data link communications, would have to consider the different parts of aeronautical communications related to aircraft segment, satellite air-ground segment and ground segment. Consequently, this security architecture would be able to interconnect in a secure way the “aircraft” world and the “outside” world (Internet for instance). Thus, the architecture we introduce is dynamic and flexible with regards to several factors such as traffic density or service priorities thanks to an available network resources based adaptive security management.

The secure infrastructure we foresee to present will be tested and validated within an industrial project entitled FAST (Fibre-like Aircraft Satellite Telecommunications), co-funded by the Aerospace Valley pole and the French government (Direction Générale de la Compétitivité, de l’Industrie et des Services - DGCIS, Fonds Unique Interministériel - FUI). The security architecture proposed in this paper is part of research tasks for this project started in January 2009. The aim is to study the feasibility and reliability of a high-capacity airborne satellite infrastructure. The project federates research efforts from industrial partners (Axess Europe, EADS Astrium, Vodea and Medes) and academic/institutional partners (CNRS/LAAS, ISAE, ENAC and Telecom Bretagne).

Section II introduces the issue aiming at securing future aeronautical datalink communications. In section III we detail our system architecture and QoS management principles. Section IV introduces our adaptive security management proposal. Finally, section V concludes this paper and presents a few prospective works about this research area.

II. Context and problem statement

A. Aeronautical communication evolutions

In civil aviation, a data link is a two-way communication between an aircraft and a ground station, such as an air traffic tower control or an airline company, used to exchange digital information. Most commonly, it is used to cope with increasing demands on air traffic control, decrease the workload of air traffic controllers,
and avoid frequency saturations of traditional analog voice communications. For instance, the Controller to Pilot Data Link Communications (CPDLC) system is such a digital communication mean between controllers and pilots. With the growing demand for In-Flight Entertainment (IFE) applications, such as the Internet for Aeronautical Passengers Communications (APC), airline companies have to satisfy passenger’s requests and Air Traffic Management (ATM) environments can no longer relay exclusively on analog voice messages. Thus, the use of digital data communications becomes a necessity for future ATM systems.

According to civil aviation actors, transition from analog voice for pilot controller communications to a predominance of digital data communications is imminent for the coming next generation services. As a matter of fact, the European Organisation for the Safety of Air Navigation (EUROCONTROL) and the Federal Aviation Administration (FAA) have both produced a technical document titled “Communications Operating Concept and Requirements for the Future Radio System” (COCR1) where new data-based Air Traffic Services (ATS) and Aeronautical Operational Control Services (AOC) are identified. These new data services are dedicated to be deployed progressively from the year 2020. Moreover, the possibility to offer new on-board safety-related services such as medical supervision and video surveillance systems gives us a challenging scenario in which satellite communication systems play a key role (e.g. FAST project is an example of such a system). Medical supervision system is an embedded terminal which supports detailed remote medical assessment using cabin crew as operators, whereas video surveillance system is a monitoring terminal connected to a set of cameras dispatched through the aircraft to observe and trigger alerts when specific events are detected during the flight.

With such an important number of aeronautical services, the air-ground traffic is becoming heterogeneous, heavy and really complex to handle. On the other hand, thanks to new link capacities (e.g. SATCOM), it seems appropriate to mix these different services on a single link, mainly for cost-saving reasons. Previously, Radzik and Pirovano2 have shown the feasibility of a system providing both passenger application traffic access (including Internet and GSM) and an high-reliability channel for aeronautical applications using the same satellite link.

Also, in order to facilitate the interoperability between the Aeronautical Telecommunications Network (ATN) and the other IP-networks involved in the exchange, the International Civil Aviation Organisation (ICAO) has established an ATN/IPS3 (Internet Protocol Suite) infrastructure to modernize global ATM system and make it flexible, modular and manageable through the use of existent and already deployed Commercial-Off-The-Shelf (COTS) products. Therefore, aeronautical data-based communications should be reliable, cost-effective, and adapted to the next generation aeronautical context.

B. Aeronautical data link security considerations: the new challenges

However, such evolutions have certainly some consequences that must be considered. First, many issues rise up when it comes to converge “safety-related” traffic with other on-board services: ATN traffic requires high priority and full availability, also new pre-operational services (medical supervision and video surveillance systems for instance) may have restricting Quality of Service (QoS) requirements to be satisfied. Then, as usage and dependency on data link communications increase so do security risks. Security requirements for the communication system are more and more complex to fulfil due to additional factors such as traffic heterogeneity, aircraft mobility or scaling issues.

Thus, security has become a major concern for the coming aeronautical communications. Recently, aeronautical actors, such as experts and researchers, have highlighted growing needs for security technologies, able to avoid malicious uses for embedded hardware or software proposed to airline companies, or directly to their passengers. With the next coming Internet on-board service, this security need is going to become a high priority for airplane manufacturers and airline companies. At this time, there is no global security solution intended to manage this type of communications (i.e. APC) and to exchange them among the other types of regular air-ground traffics (i.e. ATS and AOC).

APC services have certainly the lowest priority, but we can easily imagine a scenario where a passenger wants to buy one e-ticket for some entertainment activities, and hence, demands for a secure connection so that his secret bank code cannot be disclosed. Moreover, unlike terrestrial environment, an aircraft satellite
communication cannot tolerate faults and connection breakdowns as this would result not only in substantial financial losses (either for the passenger or the company), but may also lead to loss of precious human lives. Under such circumstances, confidentiality, authentication, non-repudiation, integrity, and availability are strongly required to secure all the different on-board services.

Thus, in this paper, we propose an efficient security architecture for aeronautical data link communications. Satellite communication-based system specific issues are taken into account mainly through its unique link with a constraint bandwidth and the need of reduced overhead for additional security mechanisms. The aim of this paper is to propose a secure interconnection between the “aircraft world” and the “outside world” using a QoS-aware adaptive security policy.

The challenge of this work is to inspect existent aeronautical standards, to integrate them as starting points, and to make the necessary modifications to finally get a secure architecture with total respect to amendments and recommendations. Indeed, a global security solution focusing on aircraft, satellite air-ground and ground segments will be efficient only if it considers from the beginning the security requirements of each crossed environment and the whole standards already deployed for them. Hence, our proposal is original given that we propose to associate different security levels to each communication sub-network (ATS, AOC or APC) and to take them into account to adapt user applications’ security policy.

C. Related works

As underlined before, providing information security for data link communications is becoming a significant claim for aviation working groups. A few works tried to address these issues and satisfy information security needs for connected aircrafts. For instance, a secure framework of the Aircraft Communications Addressing and Reporting System (ACARS) called AMS\(^4\) (ACARS Message Security) was proposed (but not implemented) by ARINC (Aeronautical Radio, Incorporated) to protect data link messages exchanged between aircraft and ground systems. Indeed, ACARS messages were previously exposed to passive attacks: for instance, on www.acarsd.org website, anyone can download a free decoder and then listen to ACARS-based communications. Even if the security framework was well-designed (key management, life-cycle management of cryptographic keys, etc), AMS becomes out-of-date as long as ACARS will be superseded by ATN/IPS for ATS and AOC services over the next 20 years.

Olive\(^5\) recommended the use of some techniques to optimize the ATN security solution such as elliptic curve cryptography or compressed certificates, but some important constraints for the future air-ground communications (e.g. interoperability and service priorities) were not considered. Besides, DVB-RCS\(^6\) (Digital Video Broadcasting - Return Channel via Satellite), which is actually the standard used for the return satellite link in FAST project, has a “link layer” security framework, which makes it vulnerable to “network layer” attacks (e.g. IP spoofing). Moreover, the used authentication protocol is not protected against Network Control Center (NCC) rogue attacks.\(^7\) Finally, passive attacks, such as eavesdropping, are also possible.

Previously, we made an exhaustive state of the art study\(^8\) to summerize aeronautical data link security activities and works. A relevant taxonomy was used to classify existing security mechanisms, identified threats, and emphasises the lack of a coherent overall and unique security solution for the mobile bandwidth-limited aeronautical communication environment.

III. Communication system architecture and QoS management

In this section, we provide an overview of the global system architecture and the QoS policies deployed for FAST project which aims at designing an high-capacity airborne satellite infrastructure.

A. Communication system architecture

Figure 1 represents the system architecture we designed. The infrastructure is decomposed into two parts: the right part is the ground system. This is a relatively classic system formed by a satellite gateway (GW) connected to two routers: an ATN router for aeronautical services, and an Internet router for passengers services. The most challenging aspect was to design the embedded network, which is the left part of the
system architecture. In fact, two routers are connected to a satellite terminal: one ATN/IPS router for ATS, and a “Next Generation” router (NG) for the remaining on-board services. As noted before, Digital Video Broadcasting (DVB) standards were withheld for the design of the satellite terminal: DVB-S2 and DVB-RCS are used respectively for forward and return link based on the European Telecommunications Standards Institute (ETSI) Broadband Satellite Multimedia (BSM) architecture for IP-based satellite links.

The NG router is connected to an AOC “standard” sub-network, based on the airline data services listed in the COCR document (e.g. passenger personal information for present time or weather forecast in the next future), the video surveillance system, and several wireless access points (WAP), dispatched across the aircraft. WAPs offer a full coverage for the Internet on-board service and the medical supervision terminal, which requires, by the way, an absolute mobility to treat a sick passenger no matter where he is inside the aircraft. APC sub-network and the medical supervision terminal being connected to the same WAP, a logical separation is made for security purposes and resource management facilities: Multi-SSID (Service Set IDentifier) logically divides the WAP into several virtual access points all within the same hardware device.

B. QoS and network resources management

A two-level QoS policy is defined for the system to manage priorities and resource allocation as presented in figure 2.

The first QoS level is deployed on the NG router using a DiffServ (Differentiated Services) architecture. DiffServ is a scalable and efficient set of network mechanisms to classify and manage traffic QoS on IP-networks. Inasmuch as several traffic classes are aggregated at the NG router, an IP classifier is used in order to associate each sub-network to a different and prioritized queue. Unlike the NG router, there is no need to differentiate or prioritize the traffic on the ATN router: ATS is the only type of traffic considered by this specific router.

The second QoS level is deployed on the satellite terminal: two ports are used to connect NG and ATN routers providing a physical separation between the ATS traffic and the other type of traffic. This separation is actually mandatory in accordance with the ICAO Standards and Recommended Practices (SARPs). Then, a mapping is set up in order to manage traffic priorities using the Priority IDentifiers (PIDs), assigned to each class of service, and the Queueing IDentifiers (QIDs) at the satellite terminal using a classifier based

Figure 1. Satellite-based aeronautical system architecture
on packet source differentiation.

The final step of QoS management is the MPEG (Moving Picture Experts Group 2) segmentation and encapsulation at the Satellite Link Control (SLC) layer whereas capacity and bandwidth assignments are made at the Satellite Medium Access (SMAC) layer using the DAMA\textsuperscript{10} protocol (Demand Assigned Multiple Access). Therefore, a segregation between Satellite Dependent (SD) and Satellite Independent (SI) layers is provided according to the BSM reference model for IP-based satellite networks.

IV. An adaptive security management architecture proposal

In this section, an enhanced security management is presented where an adaptive security architecture is provided using a dedicated Security Manager (SecMan) module, which will be introduced.

A. Securing the communication system architecture

The on-board security architecture is presented in figure 3. Two SecMan Proxies (SMP)'s are deployed and connected to the NG and ATN routers. Every SMP is isolated in a Demilitarized Zone (DMZ) using filtering features thanks to stateful firewalls deployed on each router. Those firewalls are renowned to be efficient and powerful against complex attacks (e.g. Denial of Service - DoS): Stateful Packet Inspection (SPI) is performed in order to keep track of TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) flows. Indeed, stateless firewall features are not sufficient because of their basic filtering rules (generally looking to the values of IP header fields) which cannot avoid advanced intrusion attempts (e.g. Reverse TCP attacks\textsuperscript{12}). Application layer firewalls could be a good alternative, but the CPU load and the heaviess of the filtering process should slow down air-ground exchanges and would induce a delay which cannot be tolerated when an adaptive security policy is used to enhance system and network performances.
B. Security management system operational modes

SecMan is designed to work in two operational modes in order to guarantee flexibility and priority management:

1. **Intra-class mode**: used when only one type of traffic is passing through SMP. In this mode, the priority is not considered and the security policy is established under network and system resource QoS constraints. In the modified system architecture (see figure 3), the SMP located in the DMZ2 works in intra-class mode.

2. **Inter-class mode**: used when different traffic classes are passing through SMP. In this case, service priorities and QoS constraints are considered by SecMan to establish the right security policies. In the modified system architecture, the SMP located in the DMZ1 works in inter-class mode.

Besides these operational modes, SecMan can be compliant with any kind of connection requests through four security modes:

1. **Unsecure mode**: packets are routed and transmitted normally without security enhancement (e.g. video streaming for passengers) using a ByPass policy. This mode is useful for flows which do not require security or when available resource level is too low and security mechanism deployment is not possible according to current system (SMP) or network (routers and satellite link) configurations.

2. **Transparent secure mode**: data flows are secure in a transparent way using for instance IPsec13 (IP Security) mechanism. In this configuration, everything remains transparent for users given that security mechanisms are deployed at the network level or below (thanks to specific security mechanisms deployed with DVD-RCS for instance).

3. **Secure transport proxy mode**: SMP makes an end-to-end transport level secure connexion using for instance TLS14 (Transport Layer Security) mechanism. In this mode, SMP works as a proxy securing every application thanks to a secure socket connection (e.g. https, imaps or ftps data flows will be initiated).

4. **Secure application proxy mode**: SMP makes an end-to-end application level secure connexion using dedicated secure protocol such as SRTP15 (Secure Real-Time Protocol) providing secure video streaming...
for passengers. The advantage of this last mode is to provide a specific security mechanism according to application features contrary to the “Secure transport proxy mode” where every “application level” data flow are secure thanks to the same “transport level” security mechanism.

C. SecMan framework

The goal of this module is to select (among the four different security modes previously introduced in section 3) and activate the right security mechanism according to three factors: the user application security policy, the set of deployed security mechanisms in the communication system and the level of available resources (based on system and network indicators introduced in the next paragraphs). Figure 4 depicts the general SecMan framework.

Given the fact that SecMan is intended to establish security policies for an aeronautical IP-based network, the module is designed to work above the Future Radio System (FRS) boundary on the control plan. Data services, security requirements and real-time network state represent module inputs: security requirements are defined using a risk assessment method and ranked from low to high. Network metric values are sent using Simple Network Management Protocol (SNMP) agents located on each router. Information such as ifSpeed for the available bandwidth or tcpCurrentEstab for active tcp connexions are retrieved from the Management Information Bases (MiBs) and sent to a Network Management Systems (NMS). The use of the third version of the SNMP protocol is recommended: SNMP requests and responses are secure and thus, intruders cannot disclose network information exchanges.

Based on received inputs, a Multi-Criteria Decision Making Algorithm (MCDMA) is used to make the best choice and activate one or many security mechanisms at the SMP TCP/IP stack. MCDMA’s are well-suited for complex systems in the social, economic and management domains, its goal is to provide support for decision making when numerous and conflicting criteria are evaluated. Most of these methods use series of mathematical computations to finally take the best option from a set of alternatives.

Analytic Hierarchy Process (AHP) is a well-known MCDMA approach specially for its simple and hierarchical way to model a complex system. First, a tree is established with a goal as a root and sets of criteria, sub-criteria, and alternatives. Then, weights are assigned to every element on each level of the hierarchy. Pair wise comparison is then processed between the elements of the same level to obtain local weights. Compound weights are calculated combining local weights of one level with those from the preceding level. Finally, alternatives are classified according to the algorithm outputs.

In SecMan, AHP is used to select adapted security features, delivering basic security services (i.e. confidentiality, integrity, and authentication) according to several criteria such as cryptographic key length, block

---

*Figure 4. SecMan design principles*
size of the encryption cipher, end to end authentication delay, and so on. The alternatives are the security mechanisms and cryptographic algorithms supported by SMP and the ground entity involved in the exchange. These alternatives are beforehand negotiated using a secure protocol defined to establish a common Supported Security Protocols Database (SSPD). The reason why we need such a mechanism is that a ground entity may provide some ciphers which are not supported by on-board SMP’s, and then the establishment of a secure connexion would be impossible. Moreover, SecMan needs a set where to pick up the security mechanisms to activate. This is why a negotiation protocol is necessary for the global SecMan framework. However, this negotiation protocol is out-of-scope of this paper and we intend to investigate it in future works.

We would like to focus rather on the selection process for security mechanisms deployment. For each supported air-ground security mechanism, the AHP decision making algorithm will provided security and network/system scores. They will be used to establish the dedicated application security policy according to the best trade-off between security mechanism robustness level and network/system resources consumption. It is important to note that the final security policy has to match to the security level required initially by the concerned application.

D. Performance study for SecMan

We designed a testbed platform to implement and validate the communication architecture introduced in section III and the different SecMan mechanisms detailed in section IV. The main goal of this environment is to emphasize advantages of adaptive selection for security mechanisms assignment. We experiment only intra-class operational mode for SecMan by focusing on a specific traffic class of FAST project: Air Traffic Services (ATS).

Our testbed platform uses Marionnet environment which aims at emulating our different systems (ATS client, ATS server, SecMan, ATN/IPS router and satellite connection). Marionnet environment implements Linux User Mode to run the different virtual machines, more information on this development method can be found in Marionnet’s authors paper.19

In our experiments, we consider different ATS application flows, each one is generated with IPERF application (http://www.iwerf.fr) with a reference throughput equal to 100 kB/s. These expirements do not attempt to represent in an accurate way ATS traffic that is why every flow has the same throughput. Our main goal is to validate improvements for resource allocation based on our adaptive security mechanism management. To do so, we increase the number of ATS flows exchanged between ATS client and server through the ATN/IPS router and SecMan module. For each new flow, SecMan selects the best security mechanism to deploy in order to satisfy initial ATS application security needs and also system and network resources available when the connection needs to be established.

Figure 5 represents for each new ATS flow, the robustness level provided by SecMan according to ATS application security needs and the different security mechanisms it can select based on its SSPD and its different security modes (refer to section II for details). In this experiment, to satisty application security needs and based on network and system resource level, SecMan’s decision is to select between 4 different security policies. Note that SSPD has many more available security mechanisms but in this scenario SecMan do not need to use all of them to optimize resource and security level. Moreover, there are two references in this chart, first one is the maximum robustness which one flow can get through SecMan according to the most secure mechanism available in the SSPD. The second one is the minimum robustness which SecMan can provide according to the less secure mechanism it can pick up in the SSPD. We can see in figure 5 that SecMan adapts for each new ATS flow the robustness level it provides thanks to its adaptive algorithm. The robustness is always better than the minimum robustness level considering initial application security needs but not equal to the maximum level of robustness given that this last value is not the optimal one for network and system resource allocation (as we are going to see in the following figures).

Indeed, figure 6 illustrates improvements for network and system resource allocations. We compare on the same chart network (with network security mechanism overhead evolution on the left part of the figure) and system (with consumed CPU percentage on the right part) resource allocations provided by the adaptive SecMan management and two static security policies based on the minimum and the maximum level of
Figure 5. Robustness level for the different ATS flows managed by SecMan

robustness that SSPD can provide.

Figure 6. Network and system resource allocation improvements with SecMan management
We can easily notice that SecMan uses less resources (both at network and system side) than a static security policy. Then, SecMan allows serving more ATS flow than a traditional static security policy assignment. Even if we consider the less robust policy, resource consumption is still more important than with SecMan adaptive policy. This last result is important because it shows that robustness level and consumed resources do not vary on the same way and then, it is not possible to select, a priori, a static policy to optimize resource allocation. In our experiments, global improvement with adaptive security management is on average respectively 15% for network resources and 7% for system resources, so more ATS application flows can be serve on the aircraft with the same available network capacity and CPU than with traditional and static security mechanism assignment.

1. Expected benefits

According to our experiments, we illustrated that our adaptive security management has some benefits which deserve to be underlined:

- **An optimized QoS and resource management**: adapting the security level of the applied policy allows us to reduce the security overhead, and thus, avoid any resource wastage;

- **Priority-aware security**: when the inter-class mode is used, the priorities are considered before the security policy establishment in order to provide more resources for a high priority traffic class for instance;

- **Selective and multi-layer security**: SecMan is able to define an individual policy, using a single security mechanism, or a hybrid policy, using many security mechanisms, depending on the security level expressed by the user application;

- **Enhanced interoperability**: SecMan module works above the FRS boundary which makes it technology-independent, reusable and compatible with any access network.

V. Conclusion and future works

In this paper, an adaptive security architecture for future aircraft digital communications is introduced. Issues such as inter-class priorities, QoS and network/system resource management are considered in the secure system architecture. The advantages of the global infrastructure are highlighted and the interconnection principles between the network components are detailed.

However, some security issues remain and need to be addressed soon. First, with the increasing aircraft number in the worldwide airspace, some scaling problems may arise: signalling and data messages induced by the exchanges of keys and certificates belonging to the embedded entities (passengers for instance) have to be performed at lower cost. Thus, a performance-aware Public Key Infrastructure (PKI) has to be defined with particular emphasis on the verification and revocation procedures using for instance dedicated mechanisms such as the Online Certificate Status Protocol (OCSP\textsuperscript{20}). This PKI should have also provide security properties to the negotiation protocol for the SSPD establishment.

Currently, a communication platform testbed for FAST project is being built using a SATCOM emulator, the SecMan component and different traffic generators implemented expressly for the sake of the project (e.g. COCR-based traffic generator for ATS and AOC services). The aim is to perform the security architecture through some pre-defined scenarios in order to assess the security robustness improvement and the real induced network overhead.

Nonetheless, in order to propose the security architecture to civil aviation professionals and make it usable in an airborne environment, some considerations have to be verified. In fact, software considerations in airborne systems and equipment certification are extremely important and have to follow guidances as quoted in the Radio Technical Commission for Aeronautics (RTCA) and EURONTROL DO-178B\textsuperscript{21} document. For this purpose, a Multiple Independent Layer Security and safety (MILS\textsuperscript{22}) architecture will be considered. MILS is a high-assurance approach to design secure and safe critical embedded systems, which make it particularly adapted to aircraft systems (for instance as an implementation of the previous introduced security architecture and SecMan component).
References

6 ETSI, “Digital Video Broadcasting (DVB); Interaction channel for satellite distribution systems, EN 301 790, V1.4.1,” September 2005.