

# SECURITY CONSIDERATIONS FOR IP BASED AERONAUTICAL NETWORKS

*M. Ehammer, T. Gräupl, C.-H. Rokitansky, University of Salzburg, 5020 Salzburg, Austria  
T. Brikey, Deutsche Flugsicherung GmbH, 63225 Langen, Germany*

## Abstract

The internet protocol version 6 (IPv6) is the intended network protocol for the future ATN. In order to fully benefit from IP security capabilities it is important to understand the various mechanisms and the environment in which they will operate. This paper discusses the security conditions of aeronautical communication and analyzes the relevant issues in a generic way. More concrete considerations are given in the second part of the paper where threats (in terms of communication security) to the vision of NEWSKY are briefly discussed and IPv6 security service mechanisms are introduced.

## Introduction

Due to predicted air traffic growth in the near future, initiatives like NEWSKY [1,2] aim to pave the way to All-IP networks for aeronautical communication. Not only because of the intended paradigm shift from ATC voice to ATC data communication but also due to expected cost reductions. Introducing IP to the ATN is often identified with the introduction of “Commercial Off the Shelf Products” (COTS). From a security point of view this means that protocols are introduced into the network whose security strengths and vulnerabilities are well known in advance due to their widespread use and mature state of implementation.

In order to guarantee the security and safety of ATC and AOC communications, a security infrastructure enabling transparent authentication, confidentiality, and integrity has to be introduced. This security infrastructure shall be usable on an as-needed basis and be accessible by all applications and objects operating within the NEWSKY environment. One key question thereby is at which layer such services should be provided. At the time of this writing, ICAO WG-I members are finalizing their considerations about IPS in aeronautics, including security issues. The intention of ICAO

WG-I is rather to provide a framework supporting the introduction of the Internet Protocol Suite than a detailed specification. Therefore, only base protocols which may be used in future COTS products are considered. Please note that the current version of the “Manual for the ATN using IPS Standards and Protocols (Doc 9896)” [3] specifies IPS security only as an option.

Nevertheless, providing security services such as authentication, confidentiality, or integrity requires one or more mechanisms for the safe and trustworthy exchange of the credentials of the involved communicating partners. For such methods real-time communication security is required. The communicating parties have to be capable of interactively negotiating and authenticating each other and must be able to establish a session key. This session key may then be used to derive other keys for data encryption and integrity algorithms. In order to authenticate communicating peers in a trustworthy manner, elements of an aeronautical Public Key Infrastructures (PKI) may be used. Certification Authorities (CA) should then guarantee the correctness of a certificate (credential) of a communicating peer. However, political and operational constraints have to be respected to provide for a worldwide support of certificates. Especially during the transition from legacy networks to the new IP-based infrastructure operational constraints arise. The scenario of failed authentication has to be considered in depth. Denial of ATM services due to failed authentication is not an option, implying that a fallback solution has to be provided. Note that a fallback to VHF voice communication may not always be possible in regions of high density air traffic. However, it is an absolute necessity that each communication party can be authenticated in a trustworthy manner (and in real-time); otherwise the safety of air traffic services can be easily compromised through malicious acts.

This paper introduces the NEWSKY security concept considerations against threats to the aeronautical communication environment. Only threats within the scope of the project (research and development) are regarded. Therefore, only technical threats are discussed. That is unauthorized access and denial of service. Other, non technical (e.g. social) threats are not discussed here. Several technical approaches are presented. Additionally, implications to the envisaged mobility and Quality of Service (QoS) mechanisms are elaborated.

The paper is organized as follows. First a problem statement including assumptions and analysis of the aeronautical communication system is given. Afterwards a brief sketch of the NEWSKY threat analysis is provided. The main topic of this paper is discussed in “the Internet Protocol Suite (IPS) and aeronautics” section.

## **Problem Statement and Assumptions**

An anticipated feature of the future communication infrastructure is that it will provide communication to different service domains. Some of these domains (most notably ATS) are considered operational, while others are considered non-operational. It is highly important that operational messages are delivered authenticated and unmodified to the intended destination. The future ATN network infrastructure may comprise a number of private networks interconnected over leased lines, where some of these lines may be part of the public network infrastructure. In addition, it is recognized that the ATN cannot remain isolated and will have to be inter-connected with other (military and civil) non-ATN networks. Thus a trusted communication environment has to be set up over a potentially untrustworthy communication infrastructure. This is accomplished when entity authentication and message integrity services are provided to the aeronautical stakeholders regardless of the underlying network infrastructure.

Within this paper we use the term Aeronautical Telecommunications Network (ATN) in its most generic sense and independent from any particular implementation. If a particular implementation is addressed it is indicated with a suffix (e.g. ATN/OSI or ATN/IPS).

The following sub-chapters indicate factors of the aeronautical communication environment which are relevant to establish a security context for NEWSKY.

### ***Data Traffic***

We distinguish between two fundamental types of data traffic: operational data traffic and non-operational data traffic. We make the simplifying assumption that any traffic that qualifies to be transmitted directly over the ATN is to be considered operational. This does not include traffic that is only forwarded (i.e. logically separated e.g. in VPN tunnels) over the ATN.

We assume that operational traffic must be forwarded over trustworthy networks and that non-operational traffic must not be forwarded over trustworthy networks. Further we assume that it is acceptable to forward non-operational traffic over a trustworthy network if it is logically separated (i.e. logically segregated at the network layer or below e.g. by the use of tunnels).

### ***Aircraft Infrastructure***

Communication is separated into service domains (ATC/AOC, AAC, APC), each using a separate router for its own purpose. However, there are strong tendencies towards the integration of these routers into a single airborne device. Independently of the number of airborne routers, it is assumed that each service domain resides in its own segregated sub-network.

It is assumed that operational domains and non-operational domains are logically separated in the router (even if it is a single device).

### ***Network Infrastructure***

The topological and physical layout of the future aeronautical ground network infrastructure is still unknown. Yet, some reasonable assumptions can be made. It is anticipated that there will be a set of aeronautical communication providers offering communication services dedicated for operational services. The most probable link technologies comprise custom satellite and terrestrial systems. It is recognized that a communication provider wishing to support operational communication will

have to adhere to special regulations. We assume that such networks are reasonably trustworthy and therefore directly integrated into the ATN.

A number of communication providers will want to offer communication services dedicated for non-operational service (e.g. passenger entertainment). This is most likely to materialize in the form of general purpose satellite links. We consider these networks as potentially untrustworthy and as parts of the public Internet.

We assume that it is possible that a communication service provider may choose to offer both types of services. However, this does not change the (un)trustworthy status of the network (i.e. a network is either part of the ATN or not) nor the need for logical separation of both traffic domains.

In the case of an access provider offering operational and non-operational communication services it is assumed that access to both network domains is handled separately. Whether an access provider is offering mobility services as well depends on the provider itself. Access to mobility services is therefore authorized independently from network access.

Based on these considerations we define the ATN as a trustworthy network. All non-ATN networks are considered untrustworthy.

### ***Network Interconnection***

It is assumed that the various sub-networks of the ATN are interconnected over a dedicated ATN backbone infrastructure which may comprise leased lines.

It is recognized that the ATN will have to be interconnected with other networks. Any service provider offering operational and non-operational services will have to be connected to the ATN and the public Internet. In addition it is anticipated that the ATN will need to have interconnections to other non-public networks (e.g. military networks).

### ***Authentication Infrastructure***

It is assumed that the infrastructure needed for the identification and authentication of aeronautical stakeholders (e.g. Public Key Infrastructure (PKI))

is part of the ATN and maintained by one or several organizations that can be considered trustworthy.

## **Analysis**

This chapter of the paper analyzes the network security according to the assumptions made above.

### ***Purpose of Network Separation***

Within our analysis we have identified the need to separate the ATN logically and operationally from other networks. The rationale for this is that such separation enables the aeronautical community to enforce the deployment of security measures that are usually not deployable in commercial networks. These measures include technical means and operational procedures (e.g. clear legislative accountability). However, it is recognized that security measures are subject to cost-benefit analysis, too. Therefore it is unrealistic to expect the deployment of all known (or even of all recommended) security measures. Thus it should be noted: The ATN can not be considered completely secure. There is no such thing as a completely secure network.

The implemented security measures shall be suitable to make large scale attacks from inside the ATN an extremely unlikely event (e.g. distributed denial of service attack (DDOS) from a huge number of compromised ATN hosts). In addition the security measures shall allow controlling attacks from outside the network (e.g. DDOS or hacking from other networks). However, small scale attacks from inside the ATN (e.g. malicious actions of single persons) itself have always to be expected and should be considered inevitable.

### ***Purpose of Authentication and Integrity***

The last section provided a rationale that the most probable sources of security problems are small scale attacks from inside the ATN itself. Typical threats comprise the impersonation of authorities (e.g. controllers) or altering or spoofing of messages.

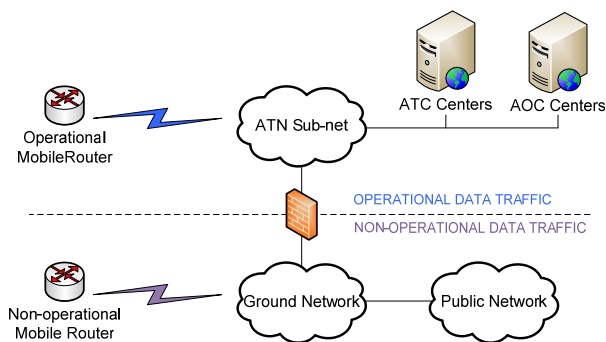
All operational communication should therefore be authenticated and protected against modification. Confidentiality of operational traffic is considered optional.

An additional benefit of this measure is the enhanced capability of legal recording of operational traffic by Aeronautical Navigation Service Providers (ANSPs). Authentication and integrity provide powerful means for traceability and non-repudiation (for a detailed description of non-repudiation consult [4]).

### Modes of Network Separation

A provider may offer operational communication services, non-operational communication services or both services. From the perspective of the aircraft this results in three possible network attachment scenarios. Due to regulatory constraints, one of these scenarios is of theoretical nature (scenario 3).

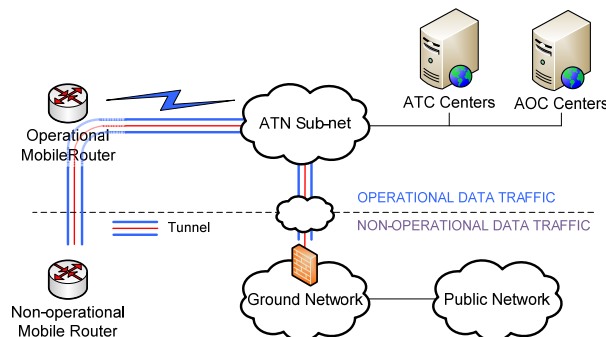
In the first case operational and non-operational communication are already physically segregated at the link layer. This includes the case where an access provider offers only services dedicated for operational traffic. See Figure 1.



**Figure 1. Scenario 1 - Network Separation Based on Physically Separated Links**

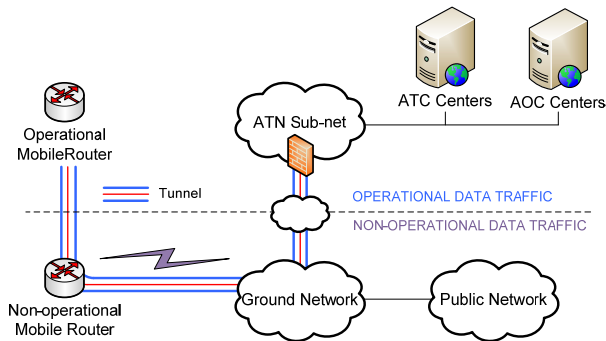
The second and third case deal with communication service providers offering IP datagram forwarding for operational and for non-operational communication. In the second case we consider an access provider offering only operational communication services. The provider network is therefore part of the ATN and considered trustworthy. Non-operational data traffic has to be separated at the network layer. This is achieved by tunneling non-operational traffic through the ATN from the mobile router to an entry point of the public Internet. See Figure 2.

*Note: It is irrelevant in this scenario whether operational and non-operational data are actually transmitted over the same physical link (which may not be possible due to radio regulations). The key point of this scenario is that both types of traffic are injected into the same access network and, therefore, have to be logically separated.*



**Figure 2. Scenario 2 – Network Separation Based on Tunneling of Non - Operational Data via Operational Link Technologies**

In the third scenario operational and non-operational communications share the same link, too. However, in this case the communication service provider is considered as non-trustworthy and directly connected to the public Internet. In order to segregate operational data from non-operational a tunnel between the mobile router and an access gateway is established. Non-operational traffic can be directly delivered to the Internet. Note again, that regardless whether the different communication services are offered via the same link, or segregated at the link layer, the access network will have to carry both types of traffic. Therefore, logical separation is required (This scenario is currently not possible due to regulatory constraints). See Figure 3.



**Figure 3. Scenario 3 – Network Separation Based on Tunneling of Operational Data via Non-Operational Link Technologies**

## NEWSKY Threats

As mentioned in the introduction, the NEWSKY project focuses solely on the threats within the scope of the project. In particular the threat analysis concentrates on Access, Entry, and Denial of Service. Access means an authorized user may gain unauthorized access via technical or non-technical attack for malicious or non-malicious purposes; Entry means an individual other than an authorized user may gain access via technical or non-technical attack for malicious purposes; and Denial of Service means system resources may become exhausted due to system error, non-malicious user actions, or denial of service (DoS) attacks. These threats have a direct impact on the NEWSKY communication protocols and have to be mitigated through the implementation of security features.

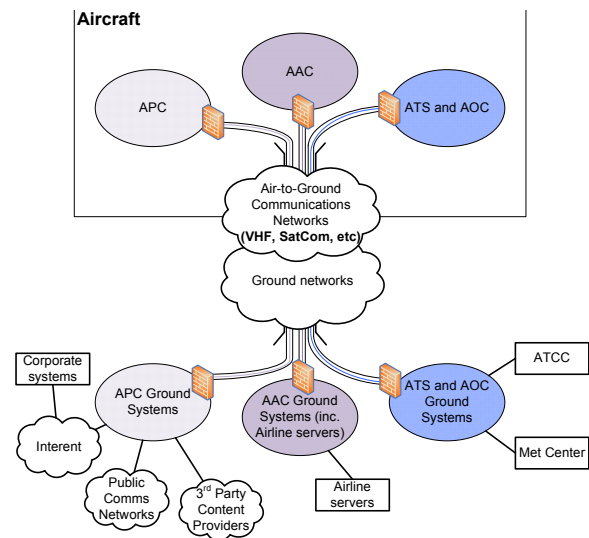
In order to assess the threats properly the impact (severity) on different business goals (safety, flight regularity, and protection of business interests) in the different communication domains (ATC, AOC, AAC, and APC) has been studied. Within the context of this paper ATC and AOC fall under the category operational data traffic – AAC and APC are considered non-operational data traffic. Furthermore, the severity of the threats has been compared to the likelihood of a specific threat. Within this context likelihood is defined as a combination of motivation and capability. Finally threats have been categorized into “acceptable risks”, “moderate risks”, and “unacceptable risks”. This means that “moderate risks” may need and

“unacceptable risks” need mitigation through security service mechanisms.

The next step of the security concept definition of NEWSKY contained the definition of security objectives. Among others these objectives indicated methods which should mitigate the earlier identified “unacceptable risks” and “moderate risks”.

Based on these objectives a high-level logical security architecture has been derived (shown in Figure 4). It shows the various domains (APC, AAC, and ATS/AOC) each within their own (secure) tunnel. Each of these tunnels is itself within the communication path between aircraft and ground facilities. The security aspects of each tunnel are described briefly:

- APC Tunnel: Provides assured separation between the APC traffic and the other NEWSKY traffic, this could be provided by encryption. Such separation would also provide some level of privacy to APC traffic.
- AAC Tunnel: Provides confidential, integrity and authenticity protection of traffic, if necessary.
- ATS and AOC Tunnel: Provides integrity and authenticity of traffic. If confidentiality is needed for AOC services the tunnel shall provide confidentiality as well.



**Figure 4. High Level Logical Security Architecture**

On top of the security infrastructure a thorough analysis on the security requirements has been carried out. For a detailed analysis on the NEWSKY threat analysis and security requirements definition please refer to section 6 of NEWSKY deliverable D15 [5].

## **IP Based Aeronautical Networks**

Based on the NEWSKY security infrastructure different options and mechanisms may be used to fulfill the security objectives and requirements, respectively. While consolidating the security infrastructure and the different security service options the impact on different NEWSKY workpackages had to be considered as well (i.e. Quality of Service (QoS), Mobility, and Hand-over mechanisms).

Note that the aeronautical communication network is currently based on ISO/OSI protocols and the intent for a possible NEWSKY implementation is to migrate towards IPv6. As a result of this all following considerations are based on the fact that IPv6 is used as the standard network protocol.

The often touted benefit of IPv6 is the promise of ubiquitous and scalable security at IP level. On top of that it is believed that the usage of IPv6 alone enables end-to-end security. In order to realize these goals it is relevant that IP security capabilities are fully understood, implemented, and consistent across all systems.

First we discuss some general issues which are necessary to regard when thinking about the introduction of IPv6 in the aeronautical communication world. Afterwards we briefly summarize IPv6 node requirements, an overview of mandatory network layer and security protocols in order to run IPv6 baseline capabilities. Then we talk about identified security service mechanisms necessary for the vision of NEWSKY.

### **Main Issues**

Analyzing security objectives and requirements, led to five main issues which are of interest when considering security services:

- Open Standard
- Failure Resistance

- Adaptability
- Separability
- Cryptography

### **Open Standard**

Today many protocols are available within the IETF [6] which are specially focusing on security issues. One of them is describing the IPsec architecture and says *“The security of a computer system or network is a function of many factors, including, personnel, physical, procedural, compromising emanations, and computer security practice. Thus, IPsec is only one part of an overall system security architecture”* [7].

In other words the variety of services required (not only for security) cannot be served by a single communication protocol. For NEWSKY it is very important to introduce only a small set of protocols, as each additional line of code which has to be implemented increases not only cost but also complexity, hence reducing the probability of fail-safe operation. Therefore, the guideline for NEWSKY is to implement only mandatory protocols and not optional ones. Moreover, these protocols should be open standards in order to reduce manufacturer dependency and increase benefits from user communities and wide-spread use of protocols.

### **Failure Resistance**

The implemented security methodology shall be capable to operate properly, even if certain security mechanisms fail. The reasoning is that the access to operational flight safety systems shall never be restricted, even if the security mechanisms fail. It should be considered, though, that this should not happen at the cost of flight safety.

### **Adaptability**

Adaptability within this context means that policies might change over time and the implemented security mechanisms need to be capable of that change. In other words some mechanism to configure a security framework must be available for any implemented protocol.

### **Separability**

Within the analysis of this paper it has been identified that it is stringently necessary to separate the ATN logically and operationally from other networks. The implemented security measure shall make any large scale attack from inside the ATN

extremely unlikely. In addition the security measures shall allow controlling attacks from outside the network.

Note, currently the aeronautical communication environment does not allow the transaction of combined traffic over the same certified link. Hence, regulations demand separation of data traffic.

### **Cryptography**

Authentication is the assurance to one entity that another entity is who he, she, or it claims to be [4]. In theory we have two possibilities of authentication, namely entity identification and data origin identification.

By entity identification the process of identifying a certain entity (person) who wants to access a system is meant. This process is in total isolation of any action the entity wants to perform later on. A strong mechanism is needed in order to ensure a secure system. However, NEWSKY as a R&D project does not focus on that issue.

The relevant part for NEWSKY is the data origin identification, which identifies a specific entity as the source of a given piece of data. This is especially important for ATS communication in order to prevent impersonation of authorized personnel.

Integrity is the assurance to an entity that data has not been altered (intentionally or unintentionally) between “there” and “here” or between “then” and “now” [4]. Data integrity is the assurance of nonalteration. This is definitely a must have for ATS communications as undetected altered data could cause catastrophic consequences. Data integrity could be achieved by Cyclic Redundancy Codes (CRC) or parity bits, but these methods are mainly designed to detect accidental bit errors. Such methods do not protect against deliberate data manipulation.

To protect data against such deliberate manipulation, cryptographic techniques are required. This means proper algorithms and key material need to be provided in order to support data integrity protection. The necessary key material may be established through automated mechanisms.

Confidentiality is the assurance to an entity that no one can read a particular piece of data except the receiver(s) explicitly intended [4]. Confidentiality is the assurance of data privacy and is needed only partially for NEWSKY. Nevertheless, proper algorithms which are safe – considering current standards – and bandwidth-saving have to be applied for those applications which need confidentiality.

### ***IPv6 Node Requirements***

IPv6 requires complementary protocols for proper operation. Furthermore, there are some protocols which are “nice to have” but are not stringently necessary. RFC 4294 [8] summarizes IPv6 node requirements.

Any IPv6 node has to support one or more IPv6 link-layer specifications. At the time of this writing the intended communication technologies are not fully specified yet, hence these IPv6 layer specifications have to follow afterwards. It is worthwhile to note that all communication links intended for aeronautical communications will be Non-Broadcast Multiple Access (NBMA) links. This means that special care has to be taken in order to support IPv6 base technologies.

The main protocols to be supported regarding the network layer are IPv6 9, the Internet Control Message protocol [10], the Stateless Auto-configuration protocol [11], the IPv6 addressing architecture [12], the Default Address Selection for IPv6 [13], and the Neighbor Discovery protocol [14] or some special protocol which emulates this behavior. From the security point of view an IPv6 node needs to implement the Security Architecture of IP [7], the Encapsulating Security Payload protocol [15], the Authentication Header protocol [16], and manual configuration of keying material must be supported.

Some of these protocols may or may not cause security problems. Consider that any network enhancement needs additional protocols, which may cause security concerns. At the time of this writing it is our view that the IP interface configuration causes most concerns in terms of security.

## **Security Service Mechanisms**

*“Whoever thinks his problem can be solved using cryptography doesn’t understand his problem and doesn’t understand cryptography.”*

***Needham and Butler Lampson***

Based on the previously mentioned security objectives, architecture, requirements, main issues, and IPv6 node requirements we have identified several security service mechanisms which need consideration in order to provide a secure network. We consider service mechanisms as a security service as long as it can be associated with one of the following terms: Availability, Integrity, Authenticity, or Confidentiality. The following discussion includes protocol options, implications towards other protocol deployments within NEWSKY (QoS, Mobility, and Hand-over), and failure situations.

### **Router Discovery**

This mechanism should provide router discovery on the currently attached link. The procedure itself is provider dependent hence NEWSKY has no direct influence on that topic. Nevertheless, a homogeneous methodology is to be preferred.

RFC 4861 [14] Neighbor Discovery for IPv6 protocol is more or less a reengineering of the IPv4 functions of Address Resolution, Router Discovery, and ICMP Redirection. It also includes a neighbor unreachable detection. If this protocol cannot be supported due to link constraints (e.g. NBMA), a separate document has to be specified how the used link supports Neighbor Discovery functionality.

In any case Routers in an IPv6 network must support sending Router Advertisements and processing Router Solicitation messages. On the other hand Hosts must support the Router Discovery procedure.

If Neighbor Discovery is not secured it is vulnerable to various attacks. Potential threats are documented in RFC 3756 [17]. The Secure Neighbor Discovery (SEND) protocol documented in RFC 3971 [18] specifies mechanisms to secure the Neighbor Discovery protocol. NIST SP500-267 [19] states that this protocol might be useful in some environment, but generally discourages the usage of such a protocol.

In principle we can assume a trust relationship between operator and clients; hence a router should not misbehave. In case the Router Discovery mechanism does not work properly, communication could be limited or blocked. Therefore, in terms of availability, the Router Discovery mechanism should be redundant.

Regardless how the implementation of the protocol looks like, it should not limit QoS and Mobility mechanisms. Advanced Hand-over protocols might be influenced by the Router Discovery procedure, though.

### **IP Interface Configuration**

This mechanism should provide a possibility to configure the IP interface. The procedure is partially provider dependent hence NEWSKY has no direct influence on that topic. Nevertheless, a homogeneous method is to be preferred.

IPv6 provides complete address auto configuration. During this process hosts acquire global and local IPv6 addresses. Currently two different modes may be used: Stateless Address Auto-configuration RFC 4862 [11], and its stateful equivalent, Dynamic Host Configuration Protocol for IPv6 (DHCPv6) RFC 3315 [20]. In any case, routers and hosts are required to support the procedures of Stateless Address Auto-configuration in order to create link local addresses and for detecting duplicate addresses on interfaces.

The stateless approach is limited to address configuration. Usually hosts require more than just address configuration. Therefore, a subset of DHCP has been defined [21] to augment the stateless approach by providing such information. Additionally, if required, the stateless approach may use privacy extensions [22].

Similar to the Router Discovery procedure we can assume a trust relationship between provider and clients; hence the IP configuration procedure should not misbehave. Special care has to be taken if the Duplicate Address Detection mechanism is not implemented according to RFC4861. If this mechanism fails, availability might be limited.

IP Interface Configuration should not have any influence on QoS and Mobility mechanisms. Advanced Hand-over mechanisms might need special protocols in order to operate properly, though.

## Network Access Authentication

Through this mechanism a network operator authenticates its clients – network access should be gained for authorized entities only.

The network access authentication may be very link dependent, where each link may implement its own methodology (probably based on the Extensible Authentication Protocol – EAP [23]). EAP is typically not mutual; therefore, it fits for the purposes of network access authentication as the access router itself usually does not have to authenticate itself to users. Again, this topic is provider dependent hence NEWSKY has not much influence on that. However, network authentication shall be provided in order to limit DoS attacks.

The Network Access Authentication process is also dependent on the used credentials (see next sub-chapter). In case the credentials can not be authenticated general access should be denied. In order to provide communication capabilities relevant for the safety of flight the local Aeronautical Navigation Service Provider (ANSP) has to provide some indication (e.g. temporal certificate) toward the communication service provider that it needs communication with the involved party.

The Network Access Authentication procedure has influence on QoS, Mobility, and Hand-over procedures. If a network access authentication procedure cannot be carried out in advance to network change, latency will be very high. In case of network authentication failure only limited access should be granted.

## Entity Authentication

This mechanism shall provide authentication of an entity with which communication should take place.

Two major possibilities are available to provide credentials. One way is certificates (e.g. X.509) [24] and the other way is pre-shared secrets. It has to be considered that these credentials are used to generate a common session key from which all cryptographic keys are derived. Note that lawful interception and legal recording are necessary requirements. Pre-shared keys might complicate these procedures.

In order to authenticate a certificate so called certification authorities (CA) are used. The

authentication of a pre-shared key can be done during the negotiation phase of IPsec using the Internet Key Exchange (IKEv2) protocol [25]. It has to be noted, though, that this method is considered a weak authentication mechanism.

This procedure has similar effects like the Network Authentication mechanism; if it fails communication cannot take place. Entity Authentication has a different context, though, as it might be used for integrity and data source authentication as well.

The Entity Authentication procedure has no influence on QoS (it has only an indirect influence if packets are dropped due to failed authentication). Mobility and Hand-over mechanisms might be influenced.

## Session Key Establishment

This mechanism shall provide a mean to establish a common session key, which is later used to derive further keys for secure communication. This mechanism can only be used in direct combination with the used end-to-end security procedure.

A common session key can be established using the Internet Key Exchange (IKEv2) protocol [25], either with a public key certificate (e.g. X.509) or with a pre-shared secret. Another possibility to establish a common session key is the Transport Layer Security (TLS) protocol [26] – current version TLS 1.2. This protocol also allows pre-shared keys or public keys taken from certificates. Session keys might be established at application layer level as well, but up to now no publicly available and widespread standards exist. Due to known constraints of application layer security public standards may probably never appear for that kind of option.

In case a Session Key cannot be established no secure communication can take place. Message Source Authentication and Integrity cannot be guaranteed. Therefore, the ANSP has to provide some mechanism to offer data communication for the safety of flight.

This procedure has a direct influence on QoS, Mobility, and Hand-over procedures. Dependent on the layer at which the session key is established questions regarding the number, latency, and possibility to re-key a Session Key arise.

## **Data Traffic Separation**

This mechanism shall provide a mean to separate data traffic.

Data traffic can be separated using different data link technologies (and physical layer technologies, respectively). Current regulations provide a separation of ATS data traffic from all other data traffic on the physical layer. This means that ATS data traffic uses separate interfaces with separate network addresses. Other data traffic domains which may be sent over the same data link layer technology may be separated at network layer level where each data traffic domain builds its own sub-network. Separation may be enforced through IP tunnels, which may or may not be encrypted. It is important to note, that routing table entries for the various communication domains must be separated from each other. In such a way separation is enforced and easier to configure.

Although other mechanisms might be feasible it is believed that data traffic separation should be based on network layer only – this includes separation at data link layer if it's applicable as well.

If data traffic separation fails an error must have occurred earlier during network configuration procedures.

The traffic separation procedure has influence on QoS, Mobility, and Hand-over procedures, dependent on the kind of tunneling used.

## **Secure End-to-End Communication**

This mechanism shall provide a mean to communicate securely.

End-to-end security can provide integrity, authenticity, confidentiality, or a combination of the aforementioned services. The question is what kind of services we need to apply to each communication domain. For ATS communication the mobile node (aircraft) and the corresponding node (ATC controller or AOC centre) need to know that they are receiving information from the proper peer. If this cannot be guaranteed false information could be distributed within the ATN and cause unwanted situations in air traffic. Therefore, mutual authentication is desirable. Note, that ATC communication must not be encrypted due to current regulations.

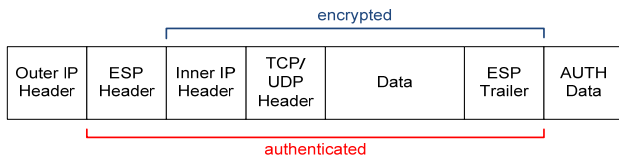
Most times integrity and authenticity are covered by the same mechanism; hence in terms of end-to-end security it can be distinguished between integrity protected and confidentiality protected data traffic. A combination of both modes is possible as well.

The decision on the end-to-end security mechanism has strong impact on QoS, Mobility, and Hand-over procedures. Therefore, we discuss this topic in depth. Standards for real-time security protocols, which could be based on public-key cryptography are Internet Security Protocol (IPsec) and Transport Layer Security (TLS). Standards for real-time security protocols at application layer level do not exist.

Using IPsec as a security protocol has the drawback that IP addresses do not identify the user directly. Despite the fact that IPsec is capable of authenticating a specific IP address it is still not the user who is authenticated. For this reason an additional instance is needed: i.e. a certification authority (CA). This could be established in a PKI environment.

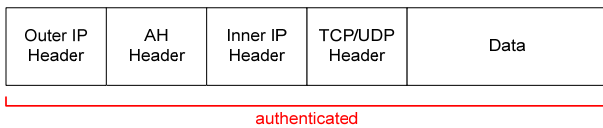
IPsec (especially IKEv2) offers a large variety of options how to protect data traffic (encryption algorithms, integrity algorithms, pseudo random functions, and Diffie-Hellman groups). Considering certification processes this might cause troubles for software developers to get certified. Additionally, many options may cause longer negotiation phases (considering the protocol itself).

Network layer protection using ESP introduces the problem that the inner IP header and especially the inner TCP/UDP header cannot be investigated by intermediate nodes; regardless which mode of protection is used (current situation). This causes a problem especially if Firewalls or L4-Gateways (e.g. Proxy Enhancing Protocol) need to inspect the traversing packet. QoS protocols which need to look at the TCP header do not work in such a configuration either. Figure 5 depicts an IP datagram which uses ESP encapsulation in tunnel mode for confidentiality and integrity. The figure shows the part which is encrypted and unreadable for intermediate nodes. Also, the part which is authenticated is shown.



**Figure 5. Using IPsec with ESP in Tunnel Mode**

Figure 6 depicts an IP datagram which uses the Authentication Header (AH). Therefore, the complete datagram is authenticated. Considering an IPsec configuration where confidentiality is not required the Authentication Header (AH) could be used as an alternative. The IP Authentication Header (AH) is used to provide connectionless integrity and data origin authentication for IP datagrams and protection against replays (ESP does this as well). Inspection of the data packet by intermediate nodes becomes not easier, though.



**Figure 6. Using IPsec with AH in Tunnel Mode**

Usually Ip Stacks Are Implemented In A Way That Everything Below Layer 4 (Including Tcp) Is Implemented In The Operating System, And Anything Above Is Implemented As A User Process. In The Case Of Transport Layer Security (Tls) No Changes To The Operating System Are Required, As Tls Operates Above Layer 4. Therefore, The Applications Have To Interface The Api Of Tls And Not That Of Tcp. This Means That Transport Layer Security Can Only Be Implemented On An End-System (Or A Tls Supporting L4-Gateway).

Up To Now Tls Is Specified For Tcp Only Which Means That Udp Messages Could Not Be Protected Through Tls. Additionally, Tls Provides Encryption Only For Point To Point Connections. It Is Hardly Believable That Tls Would Work For Multicast Messages.

Considering The Newsky Architecture Tls Seems Not Reasonable Due To The End To End Component Of Tls. Newsky Would Most Probably Provide Airborne Routers And Ground Based Routers, Which Means That Every Application Itself (Which Is Bounded To A Separate Ip Address) Would Need To Establish A Shared

Secret With Its Peer. This Would Sum Up To A Considerable Overhead. Additionally, If Data Traffic Is Encrypted Local Network Administrations Might Drop Packets (I.E. Encrypted Traffic Is Not Allowed To Enter Demilitarized Zones). Moreover If Applied The Security Of A Network Would Be The Responsibility Of The End User, Which Is Not Acceptable.

Application Layer Security Has To Be Implemented In End-Hosts. Providing Security At Application Layer Level Has Some Advantages Such As:

- Easy Access To User Credentials (Such As Private Keys)
- Complete Access To User Data (Better Support For Non-Repudiation)

The Implication Of Application Layer Security Is That The Applications Themselves Have To Incorporate Security Mechanisms Independently. Each Application Would Have To Define Its Own Security Mechanism, Which Opens Opportunities For Attacks As Mistakes In The Individual Solutions Are More Likely

Application layer security shall be mainly seen as “Secure Sign On” procedures, where the access to a system, which provides (strong) security features, should be secured by good methods of user authentication. This authentication process should be no implication to the regular operation of the system.

### Network Protection Devices

A mechanism to protect portions of or the complete network.

Currently there is a complete lack of public specifications for the capabilities and required behavior of network protection devices. Should viable specifications of Firewall and/or Intrusion Detection Systems (IDS) become available over time, such should be considered. NIST [19] has compiled Network Protection Device Requirements, which might be useful for IPv6 deployment in ATN as well.

Network protection devices such as firewalls, intrusion detection systems (IDS), intrusion prevention systems, and the like are nowadays a

necessary part of any network connection. This won't change with the introduction of IPv6.

Network Protection Devices have a very strong impact on the QoS, Mobility, and Hand-over procedures. Therefore, it is of utmost importance that Network Protection Devices are coordinated with NEWSKY protocols.

## Conclusion

Within this paper we have tried to explain the situation for aeronautical communication in the future. We have introduced the topic with a generic problem statement and an according analysis. The NEWSKY threat analysis as such was too comprehensive in order to present details within this paper. Therefore, we briefly discussed ideas of this assessment. In the next step we focused on the main topics which are of interest when introducing IPv6.

As a concluding remark we think it is important to state that the introduction of IP in the aeronautical communication world does not only bring benefits. With each additional protocol necessary for any communication enhancement, the potential of a security leak elevates. Additionally, overhead and communication latency increases. The basic mechanisms and protocols have been shown. For the basic security framework we strongly recommend the usage of IPsec and a selected set of its companion protocols. Any dead code should be avoided. The complexity of the security framework should be low. The establishment of an IP based security framework should be an iterative process where basic functionality is provided first - enhancements may be added later.

In a next step we want to assess security solutions suitable for aeronautical communications in more detail in order to provide best possible guidance for the aeronautical communications stakeholders.

## References

[1] Schnell, Michael, S. Scalise, 2006, "NEWSKY – A concept for networking the SKY for civil aeronautical communications", DASC06.

[2] <http://www.newskey-fp6.eu>

[3] ICAO, Aeronautical Telecommunication Network (ATN), Manual for the ATN using IPS Standards and Protocols (Doc 9896).

[4] Adams Carlisle, S. Lloyd, 2002, "Understanding PKI", Addison Wesley, 2nd Edition.

[5] NEWSKY, 2008, "D15 - Security Concept".

[6] <http://www.ietf.org>

[7] RFC 4301, Kent, S., K. Seo, 2005, "Security Architecture for the Internet Protocol".

[8] RFC 4294, Loughney, J., 2006, "IPv6 Node Requirements".

[9] RFC 2460, Deering, S., R. Hinden, 1998, "Internet Protocol, Version 6 (IPv6) Specification".

[10] RFC 2463, Conta, A., S. Deering, 1998, "Internet Control Message Protocol (ICMPv6) for IPv6 Specification".

[11] RFC 4862, Thomson, S., et al., 2007, "IPv6 Stateless Address Auto-configuration".

[12] RFC 3513, Hinden, R., S. Deering, 2003, "Internet Protocol Version 6 (IPv6) Addressing Architecture".

[13] RFC 3484, Draves, R., 2003, "Default Address Selection for Internet Protocol version 6 (IPv6)".

[14] RFC 4861, Narten, T., et al., 2007, "Neighbor Discovery for IPv6".

[15] RFC 4303, Kent, S., 2005, "IP Encapsulating Security Payload (ESP)".

[16] RFC 4302, Kent, S., 2005, "IP Authentication Header (AH)".

[17] RFC 3756, Nikander, P., et al., 2004, "IPv6 Neighbor Discovery (ND) Trust Models and Threats".

[18] RFC3971, Arkko, J., et al., 2005, "SEcure Neighbor Discovery (SEND)".

[19] NIST Special Publication 500-267 (Draft), 2008, "A Profile for IPv6 in the U.S. Government".

[20] RFC 3315, Droms, R., et al., 2003, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[21] RFC 3736, Droms, R., 2004, "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6".

[22] RFC 4941, Narten, T., et al., 2007, "Neighbor Discovery for IPv6".

[23] RFC 3748, Aboba, B., et al., 2004, "Extensible Authentication Protocol (EAP)".

[24] RFC 5280, Cooper, D., et al., 2008, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[25] RFC 4306, Kaufman, C., 2005, "Internet Key Exchange (IKEv2) Protocol".

[26] RFC 5246, Dierks, T., E. Rescorla, 2008, "The Transport Layer Security (TLS) Protocol Version 1.2".

### **Email Addresses**

M. Ehammer: [mehammer@cosy.sbg.ac.at](mailto:mehammer@cosy.sbg.ac.at)

T. Gräupl: [tgraeupl@cosy.sbg.ac.at](mailto:tgraeupl@cosy.sbg.ac.at)

C.-H. Rokitansky: [roki@cosy.sbg.ac.at](mailto:roki@cosy.sbg.ac.at)

T. Brikey: [Thorsten.Brikey@dfs.de](mailto:Thorsten.Brikey@dfs.de)

*27th Digital Avionics Systems Conference  
October 26-30, 2008*