

Security Issues in the BRAHMS System

M. Annoni, G. Boiero, N. Salis

Telecom Italia Lab S.p.A

Via G. R. Romoli, 274 - 10148 Torino - Italy

Tel: +39 011 228 7228, email: {marco.annoni, gianluca.boiero, nicoletta.salis}@tilab.com

ABSTRACT

The paper presents the requirements and the solution developed by the IST-BRAHMS Project for the introduction of an IPSec scenario in a generic Broadband Satellite Multimedia system. The guideline of the proposed Multi-Layer IPSec methodology is discussed with specific reference to the characteristics of the generic satellite network architecture addressed by the project. The issue related to the functional integration of the security management mechanism in the BRAHMS Network Layer architecture are finally addressed.

I. BRAHMS Project Overview

A number of broadband satellite systems have been proposed in recent years offering alternative solutions. The highest possible level of commonality is desirable especially for user terminals, even when different satellite transmission systems are used, in order to reduce the cost of the user equipment and expand the satellite services market. The goal is to offer a convergence path from current satellite systems to a more generic next-generation system with common terminal architectures supported by new standards.

The need for standardisation in broadband satellite systems has been recognised by industry and has resulted in the setting up of a working group on Broadband Satellite Multimedia (BSM) in ETSI SES, to which the BRAHMS project has contributed [6] [7] [8]. The BRAHMS (BRoadband Access for High speed Multimedia via Satellite) project [10] contributed in defining a universal communication infrastructure for a broadband access via satellite (see Fig. 1) open to different satellite system implementations and with the objective to harmonise most of the common satellite access network functions. This flexibility (e.g. for frequency, access type, orbit) is obtained by separating physically-related functions from common service and access ones: the higher layer Radio-Technology Independent (RTI) access network functions “hide” the lower layer Radio-Technology Dependent (RTD) functions from the user and the core network.

The common RTI layers in the user (BSAT) and hub (BHS) stations in access networks support a full range of multimedia services (e.g. broadband and Internet) and connections to alternative customer premises and core networks.

In this way, the transport and delivery of IP-based applications and services seamlessly complement the available terrestrial broadband services and propose, in some niche markets, added-value services as compared to terrestrial ones.

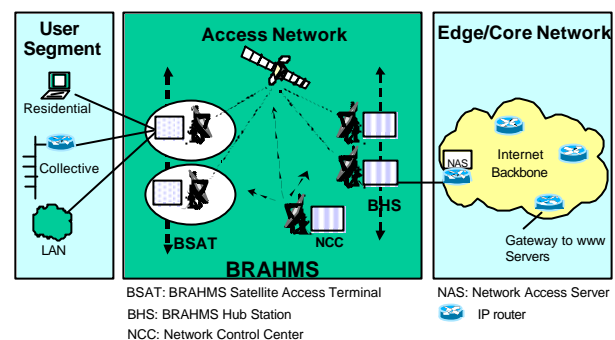


Fig. 1: BRAHMS Overall Architecture

The BRAHMS project has developed a general model for an IP-oriented satellite architecture in which a range of existing and future satellite technologies can be accommodated and exploited by IP-based applications. Such a satellite system concept, relying directly on IP technology, brings advantages even in terms of simplification of components, mechanisms or interfaces. The proposed model addresses not only satellite transport, but also issues related to IP networking, such as: IP QoS (Quality of Service) provision, IPv4 and IPv6 mobility support, multicast support, security, IP performances enhancement over the satellite link (header compression, TCP spoofing). These features are offered independently of the used satellite technology.

II. Security Requirements in BSM. The BRAHMS approach

Internet diffusion and increasing use of broadband communications foster the introduction of new services for many different business and private purposes where security is certainly a mandatory requirement. Security involves all the architectural levels and therefore must be considered as one of the key elements in the design, development and deployment of any future satellite system. With reference to the BRAHMS Reference Architecture [1], the security issues has been addressed by relating to the concept of separation between Radio Technology Dependent (RTD) and Radio Technology Independent (RTI) functions. Only the RTI part of the

security mechanism has been defined as the project did not address any specific RTD solution (i.e. satellite system). RTI security issues refers to the upper ISO/OSI layers and so they are logically equivalent to the ones addressed for the Internet environment. They can be categorised in:

- Application layer security, proposed for special purpose applications (e.g. financial applications, stock trading, ... etc.);
- IP layer security (IPSec).

The BRAHMS reference architecture is IP-based. As a matter of fact, TCP/IP is today the most widely used protocol suite due to the existence of a large number of quality applications written for this environment. However, current IP suite has still many known vulnerabilities including authentication threats (e.g. spoofing), confidentiality threats (e.g. sniffing), session overtaking (or hijacking) and integrity threats (an attacker intentionally tweaks some bits in packets); these threats limit and complicate the use of large IP networks for sensitive communications.

III. IPSec Principles

The IETF (Internet Engineering Task Force) has developed a protocol called IPSec [2] for providing high quality, cryptography based security for IPv4 able to guarantee secure communications over the public Internet. IPSec can provide and flexibly support combinations of:

- connectionless data integrity,
- origin authentication,
- data confidentiality,
- access control,

for communications between any two hosts.

These services are provided at the IP layer, offering protection for IP and/or upper layer protocols.

IPSec is an open security protocol: it does not restrict the user to a specific encryption or authentication algorithm, but, instead, it provides a general framework that allows each pair of communicating endpoints to choose algorithms and parameters (e.g. key size).

By addressing the security issues at the IP layer and rendering the security services in a transparent manner, IPSec attempts to relieve software developers from the need of implementing any security mechanisms at different layers or for different Internet applications. However, the security offered by use of these protocols ultimately depends on the quality of their implementation. Moreover, the security of a computer system or network is a function of many factors and IPSec is only one of the elements of a complete system security architecture.

The IPSec fundamental concept is described in Fig. 2, showing the different networks involved in a datagram transaction. They are:

- the protected and trusted local network at the source (Network A, for example a company's private LAN);
- the untrustworthy public Internet segment;

- the protected and trusted local network at the destination (Network B).

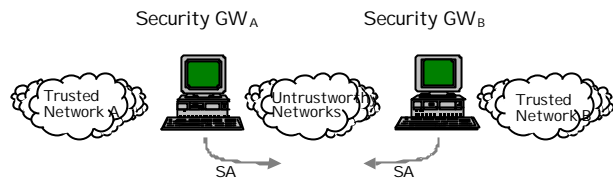


Fig. 2 - Network elements involved in IPSec

IPSec envisages security gateways (A and B) at each boundary between trusted and untrustworthy networks. When Network A needs to establish a secure link with Network B, a Security Association is initially established. A Security Association (SA) is a simplex “connection” that affords security services to the traffic carried by it. In the example shown in Fig. 2, before starting the actual data transaction, the Security Gateway A establishes a Security Association with the Security Gateway B and viceversa. The SA constitutes a security relationship about *negotiation* of security services and shared secrets. Before any IP datagram is sent through the untrustworthy Internet, the Security Gateway A encrypts and/or signs it, using an IPSec protocol. When it reaches the Security Gateway B, the datagram is decrypted and/or checked for authentication. Then it is forwarded to the final destination in the Network B.

Instead of changing the basic datagram header or creating an IP option, IPSec uses separate fields to carry authentication and/or encryption information in standard IP datagram, as shown in Fig. 3. So, by keeping a standard IP header, the IPSec packet can be routed with standard IP equipment, providing backward compatibility with IP routers.

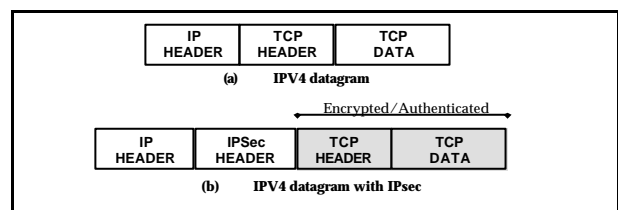


Fig. 3: IPSec datagram structure

IV. Application of IPSec to the BRAHMS Scenario

BRAHMS did not target any specific satellite system, but rather concentrated on the definition of a generic “system independent” RTD/RTI interface. For this reason, even if additional security requirements may likely be applied to the satellite radio access segment (RTD layers) they are not discussed in this paper as they were out of the scope of the project. In general, it is advisable to apply security technologies to the upper ISO/OSI layers, so a certain level of information protection is always assured, independently of the specific RTD technology and the eventually related security mechanisms.

Moreover, it is important to discuss the impact of IPsec on the performance of TCP and other common Internet protocols, over a satellite link.

The particular problem posed by the adoption of IPsec in satellite-based communications is that encryption hides all details of higher layer protocols so making impossible for any intermediate routing and switching node processing of the related information. The recent development of IPsec in IETF is incompatible with a new set of networking paradigms that place more and more controls inside the network in intermediate nodes rather than in end nodes. In particular, any service that requires knowledge of the TCP port number anywhere other than in the end host cannot function if IP packets are encrypted; such services include most firewalls, many DiffServ implementations¹, MPLS (Multi Protocol Label Switching), RSVP and RED (Random Early Discard)².

Other functions that are affected by IPsec include TCP spoofing, header compression, Network Address Translation, TCP traffic shaping, layer 5 switching, transparent web caching, etc. This could certainly be an issue for any future broadband systems and, in particular, for the BRAHMS functional architecture. As a matter of fact, most of the solutions being developed to enhance the connectionless best effort service offered by the IP over a satellite link have been integrated as strict requirements:

- Adoption of efficient resources management strategies able to optimise the throughput, especially at the TCP layer.
- Introduction of Quality of Service management for multimedia applications.

IPsec encrypts every IP datagram, including the TCP headers that contain information needed for satellite gateways to perform TCP PEP (Proxy Enhancing Performances) or other intelligent routing functions.

Some basic rules for TCP optimisation techniques used in satellite communications and the implications they might have on the IPsec security protocols have been pointed out by [3]. In particular, if the optimisation techniques involve the intermediate routers and require read or write access to the TCP encapsulated data, the IPsec services cannot be used without some kind of interfering with security or adaptation; otherwise (not involving of the intermediate routers, no access to TCP data encapsulated), they can be used with all IPsec services.

Some work on the subject has been carried out recently by Hughes Network System. This IPsec extension has been called Multi Layer-IPsec (ML-IPsec): it defines a complex security relationship that involves not only the sender and the receiver of a security service, but also selected intermediate nodes along the traffic stream; the main idea is to divide the IP datagram into several parts

and apply different protection schemes to each part [4] (see Fig. 4).

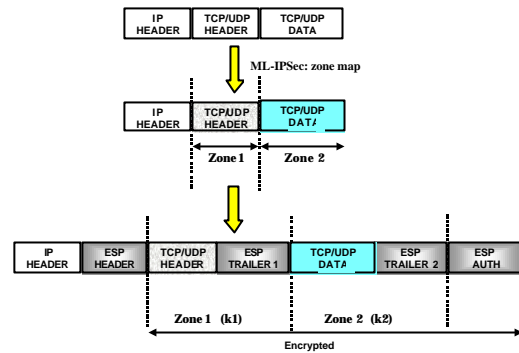


Fig. 4 – ML-IPsec datagram structure

V. Multi Layer IPsec in the BRAHMS network

As the security issue in the BRAHMS network has to inter-work with the other performance enhancing functional aspects just mentioned, the main problem is their compatibility with ML-IPsec. Since now the security service is provided on a “zone-by-zone” basis (see Fig. 4), individual security relationship can be used to cover each zone of the IP datagram, and then build a new type of SA, called Composite SA (CSA). With reference to Fig. 5, when a user in the Network A wants to establish a secure link with a node in the Network B, the Security Gateway A (in the BSAT) establishes the needed Security Associations with the Security Gateway B and with all authorized intermediate gateways (e.g. the one in the BHS), before starting the actual data transaction. The SA_i constitute different levels of security relationships related to the negotiation of security services. Before any IP datagram is sent through the untrustworthy Internet, the Security Gateway in the BSAT encrypts and/or signs it, using an ML-IPsec protocol. When the datagram reaches the Security Gateway B, it is decrypted and/or checked for authentication. Then it is forwarded to the final destination in the Network B. When the ML-IPsec protected datagram flows through an authorized intermediate node (e.g. BHS), if needed, a certain part of the datagram (e.g. the TCP header) may be decrypted and/or modified and re-encrypted, but the other part will not be compromised. In this scheme, the BHS performs, among others, the function of ML-IPsec PEP-Gateway having the key needed to decrypt the TCP header part and to perform RSVP, TCP spoofing, header compression, etc.

It can be noticed that the BHS can operate both as an End Host Security Gateway (e.g., if the end user is in the Trusted Network C in Fig. 5) and as an Intermediate Security Gateway. On the contrary, the BSAT always operates as an End Host Security Gateway because it is always connected to the edge of a Trusted Network.

The status of the IP datagram while travelling in the network is shown in Fig. 5. The different encryption and

¹those requiring more information than that one provided by the DS field

²with penalty box

security levels applied at any specific node of the network can be easily identified.

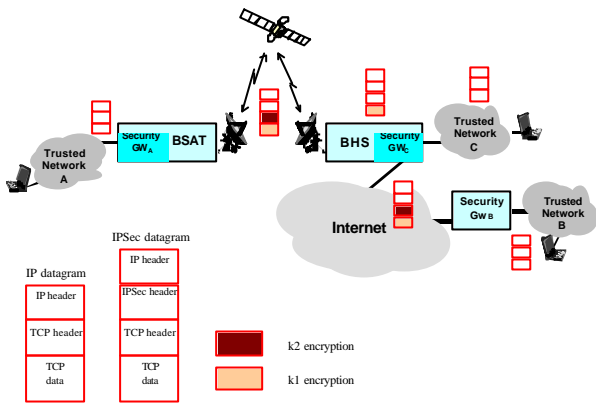


Fig. 5 Status of the IP Datagrams in the BRAHMS Network in presence of ML-IPSec

Fig. 6 shows the different nodes of the BRAHMS reference architecture and the message sequence chart characterizing the encryption/decryption phases in an ML-IPSec mode. The following steps can be identified:

- The User (Network A) asks to create a secure connection with a node in the Network B (e.g. an IP server). Before transmitting the IP-datagram, the security requirements are established (CSA) and the network gateways are informed.
- The BSAT performs QoS management (i.e. RSVP), TCP spoofing. Then, it authenticates and encrypts the IP datagram by using two different keys. If needed, it performs header compression on the IP Header (it might be noticed that, because of the previous encryption of the whole TCP segment, the TCP header is no longer available for header compression). Finally it transmits the datagram to the BHS through the satellite.
- Because of the encryption, IP security level is assured on the satellite link.
- The BHS performs header decompression and operates a partial decryption on the received datagram. Before forwarding the datagram, if needed, it operates QoS management and then, in order to ensure security during the transit over the Internet, re-encrypts the TCP part.

The Security GW is an end-host that is able to properly decrypt all the IP datagram. When data are transmitted from the IP server (Network B) to the end user (Network A) the BSAT and the BHS maintain their functions of End Host Security Gateway (BSAT) and of Intermediate PEP Security Gateway (BHS), but their specific processing is modified to reflect the change of direction of the data flow (e.g. TCP spoofing in this case is carried out by the BHS).

It can be noticed that the partial “k2 re-encryption” occurring on the satellite link is optional and does not modify the overall ML-IPSec scheme. In addition, the process described in Fig. 6 could be simplified if some operations (i.e. header compression/decompression,

spoofing, etc.), depending on the specific system requirements, are not implemented.

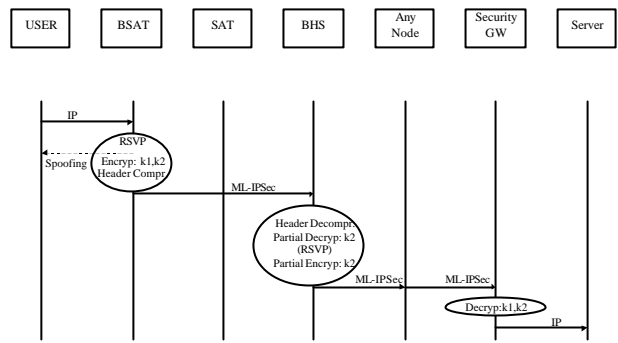


Fig. 6 – MSC of the encryption/decryption phases in the BRAHMS ML-IPSec mode

VI. BSAT functional architecture: Security Management in the BRAHMS Network Layer

The BRAHMS layer model (shown in a simplified way in Fig. 7) points out the separation between radio technology independent and dependent (RTI/RTD) functions. The high-level (RTI) functions identified by BRAHMS [5] can be divided into:

- IP “standard” functions, such as Routing, IGMP, QoS management, Address Resolution, IP mobility support;
- BNL performance-enhancing functions for IP and higher layers, namely adaptations or additional functions introduced for satellite links. In particular, these functions include: TCP PEPs (and, eventually, other possible PEPs), Security management and Transport efficiency enhancement (e.g. header compression).

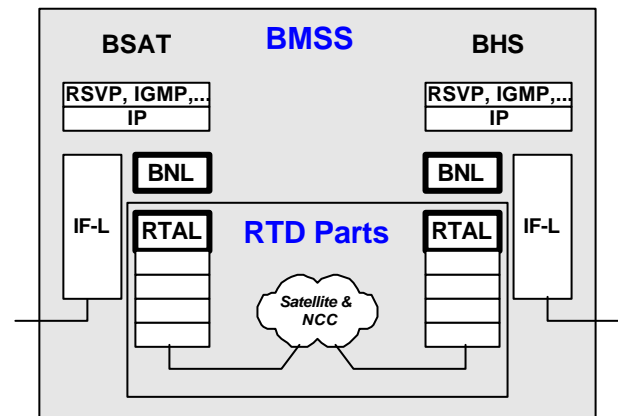


Fig. 7 - BRAHMS Layer Model

The RTD part includes all radio specific functions, including if necessary an adaptation layer (RTAL) below the BNL [BSM3].

The design of the BNL follows three main principles:

- Satisfying important requirements of security for communication via satellite;

- Allowing processing of upper protocols control information by intermediate nodes for performance enhancing purposes;
- Allowing a network operator to configure a satellite architecture appropriately and find the best compromise between performance enhancement needs and bearable computational cost.

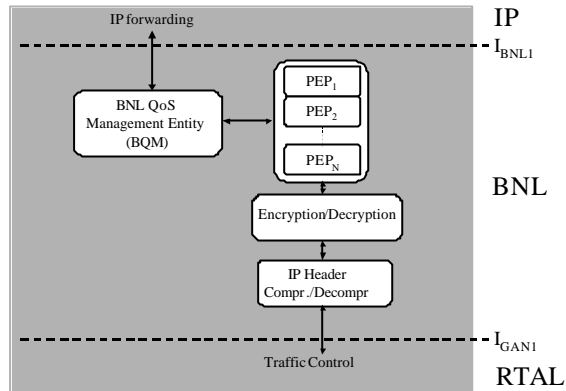


Fig. 8 - BNL entities in BSATs

The first two goals are met by adopting ML-IPSec [MLSE], which allows to encrypt/decrypt IP headers and upper layer headers separately through multiple keys, together with a number of PEPs and an IntServ and/or Two-Bit DiffServ IP QoS policy. The third goal is achieved by leaving the number, type and organisation of PEPs undetermined, together with the choice to support IntServ or DiffServ or both classes of service.

In Fig. 8 the interactions among the protocol entities in the BNL and with the IP layer and the RTAL are represented. We can distinguish a downstream data flow (from the IP layer to the RTAL one) and an upstream data flow (from the RTAL to the IP layer). The following processing is designed to allow a BSAT to be a security gateway for the CPN it is attached to.

As regards to the downstream flow, a datagram is passed from the IP layer to the BQM entity for its classification. Data traffic (TCP or UDP) is classified into one of the five IntServ or Two-Bit DiffServ classes of services. Classified datagrams are passed along to the PEP entities, which process them, adding control information in the BNL headers, created in this phase. An example of applicable PEP is TCP spoofing whose goal is to improve throughput of TCP connections over the satellite link.

The IP payload of each datagram is then encrypted using ML-IPSec. Its task is to encrypt the IP payload, using separate keys for the TCP/UDP header and the TCP/UDP payload once control information in datagrams headers has been processed by PEPs or QoS provision.

Before their passing to the RTAL layer, datagrams have their IP header compressed by the appropriate entity: it is important to note that IP header compression has to be performed only after ML-IPSec encryption, which

cannot work on a datagram with a compressed IP header. In this way [5], the IP header de/compression works properly, because compression is performed after any protocol processing is implemented in the packet and decompression is done before any protocol processing is activated. This procedure is compatible with RFC 2507 [9] and with ML-IPSec decryption, working zone by zone on every packet.

In the upstream flow the reverse operation occurs. BNL PDUs from the RTAL have their IP header decompressed. The IP payload is then decrypted. Datagrams are processed by PEP modules to be finally passed to the IP layer. In the BHSs, the above operation slightly differs from that in the BSATs.

VII. Conclusions and open issues

The solution developed by the IST-BRAHMS Project for the introduction of an IPSec scenario in a generic Broadband Satellite Multimedia system by means of a Multi-Layer IPSec methodology has proven feasible and is being discussed in the frame of ETSI SES BSM. However, the acceptance of the proposed approach in the IETF frame would need a large support to establish an actual consensus. Areas for further work remain and are related to key distribution issues and migration towards IPv6.

REFERENCES

- [1] IST-BRAHMS - Deliverable 4 - *BMSS Target Architecture*
- [2] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998
- [3] Guvara Noubir et al, "Security Issues in Internet Protocols over Satellite Links", IEEE VTC'99
- [4] Yongguang Zhang, "Multi-layer Internet Security for satellite & wireless networks", HRL Technical Report 99-611
- [5] IST-BRAHMS - Deliverable 6 - *BMSS Functional and Subsystem Specification*
- [6] "BMSS Security aspects", May 2001
- [7] "BRAHMS Network Layer (BNL)", May 2001
- [8] "BMSS architecture, BRAHMS Network Layer (BNL) and Radio Technology Adaptation Layer (RTAL)", September 2001
- [9] M. Degermark, et al, "IP Header Compression", RFC 2507, IETF
- [10] <http://brahms.tilab.com>

Acknowledgments

This work is based on activities performed in the frame of the IST-BRAHMS Project, partially funded by the EC. The authors would like to thank all the BRAHMS Team for their valuable contribution and support during the two years of the project.