

A security architecture for Broadband Satellite Multimedia (BSM) networks

H. Cruickshank¹, R. Mort², R. Goodings³

Abstract— Satellites are expected to provide an essential role in bridging the “digital divide”; satellite networks are likely to be the only way to provide broadband services to regions that cannot be economically reached by terrestrial networks, in particular the more remote regions of Europe and the rest of the world.

This paper presents the ETSI BSM security architecture which accommodates link and network layer security (Internet) security systems. This architecture also includes interworking with RADIUS/DIAMETER authentication entities and Satellite Protocol Enhancement Proxies.

Index Terms— Security, ETSI, IPsec, IP multimedia, DVB-RCS.

I. INTRODUCTION

A major goal is that broadband services be independent of urban or rural location, and offer users the ability to migrate between different satellite networks, and between satellite and terrestrial networks. The development of broadband satellite systems providing services based on the Internet Protocol (IP) needs to be stimulated by means of common standards. These standards will allow building blocks and services for such satellite systems to become more readily available. The Broadband Satellite Multimedia (BSM) working group ensures that this work can be carried out in a timescale that will allow development of universal access consistent with the eEurope 2005 programme, with the objectives to provide access to broadband and associated e-services to everyone, everywhere via a combination of private and public internet access points with a focus on the less favoured and remote regions.

The ETSI BSM work is focussed on the efficient transport of IP data streams and on how to interoperate resulting satellite networks with terrestrial IP networks. The BSM standards are being designed to use existing standards such as DVB-RCS while remaining open to emerging standards and other available technologies (the ultimate choice is left to the market). This is a necessary step to build universally available e-services in the broadest sense.

The paper focuses on the current work in defining the security architecture for BSM satellite networks.

This paper is organized as follows: Section I provides an overview of current ETSI view of Broadband Satellite Multimedia architecture. Section II provides an overview of various security technologies that might be used to secure BSM networks. Section III presents the proposed BSM security architecture in details with two specific use cases for using IPsec and link layer security technologies. Finally section IV concludes this work with a summary of the main ideas in this paper.

There is a large amount of related work to this paper. The related work can be divided into three areas:

1. The IETF work in IPsec and the MSEC groups [1].
2. DVB-RCS standard [2] and the SATLABS work.
3. The European Space Agency work [3].

This work is different from all the above because it considers all satellite network that can provide IP multimedia service by using a common interface between the satellite specific and non-specific layers. This is called SI-SAP in BSM terminology, which will be explained in the next paragraph.

The general BSM architecture, [4], [5] and [6] is presented in Figure 1 with the general BSM protocol stack for IP services in the Satellite Terminals (ST) and the Gateways (GW). An important feature is the Satellite Independent Service Access Point interface or SI-SAP interface. This interface provides the BSM with a layer of abstraction for the lower layer functions and makes use of a BSM specific identifier, the BSM_ID, to address BSM points of attachment. It allows the BSM protocols developed in the satellite independent layer to perform over any BSM family. Moreover, the SI-SAP also enables the use of standard Internet protocols for example address resolution or multicast group management, directly over the BSM or with minimal adaptation to BSM physical characteristics. Finally the SI-SAP even makes it possible to envisage switching from one satellite system to another and to even a non-satellite technology while preserving the BSM operator's investment in layer 3 software development.

Figure 1 shows that there are only a small number of generic functions that need to cross the SI-SAP and those are related to connection/session management, resource management or security. The BSM protocols are based on the OSI layered protocol stack. For the IP services most of the work has concentrated on the network layers with links to the

¹ Centre for Communication Systems Research, University of Surrey, Guildford, UK

² SysTek, Havant, UK

³ ETSI, BSM WG, Sophia Antipolis, France

underlying data link and MAC layers. The reason for this is simple: the developed protocols for IP over BSM should primarily be located in the satellite independent part of the BSM stack to be applicable to a range of different satellite dependent lower layers such as for example DVB-RCS [2].

The security message flows pass through the SI-U-SAP (User), SI-C-SAP (Control) or SI-M-SAP (Management) depending on the nature of these messages.

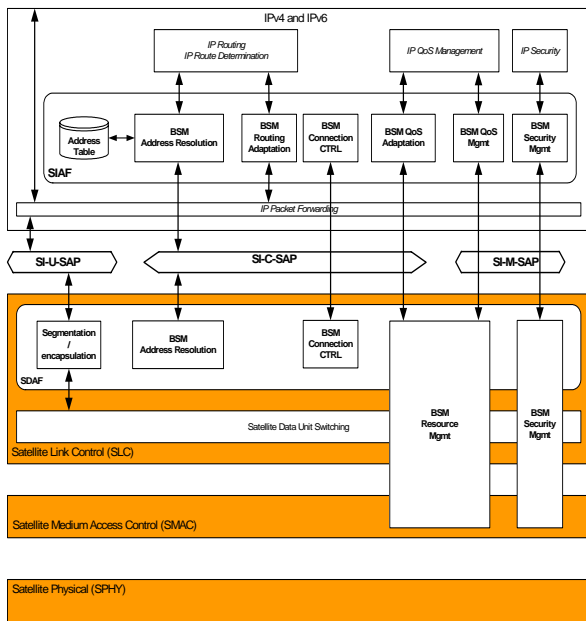


Figure 1: BSM Protocol Stack for unicast services (security)

II. CHOOSING A SECURITY TECHNOLOGY

The BSM security report [7] and technical specifications [8] presents a detailed overview of various security technologies. A summary of these technologies is presented in Figure 2. Security may be provided at any level of the BSM protocol stack such as link, network, transport or application layers using various technologies. The security operations may be visible to end users and applications if they are implemented at the application level, or they can be transparent if implemented in the lower layers.

The characteristics of these security technologies can be summarized as follows:

- Link layer: DVB-S conditional access is only suitable for broadcast applications. DVB-RCS and ATM Security can provide BSM ST-to-Gateway and ST-to-ST security services. They are good candidates for their own networks.
- Network layer: IPsec makes no assumptions about the link layer technology, i.e. it can be used in every network that includes satellite links. In addition, today it is mostly used in security firewalls (security gateways) to build Virtual Private Networks (VPNs) and provide users remote access to their company networks. Therefore IPsec is a very flexible security

technology and hence it can be used both on hosts and BSM ST/Gateways.

- Transport layer: Moving up the protocol stack, SSL/TLS is based on TCP and provides an effective end-to-end security and user authentication. Similar to IPsec, SSL/TLS can be used in every network with or without satellite links. The major restriction is that SSL/STL does not support multicast and UDP operations.
- Application layer: This type of technology again provides an effective end-to-end security and user authentication. However, such security system has to tailor made for each application.

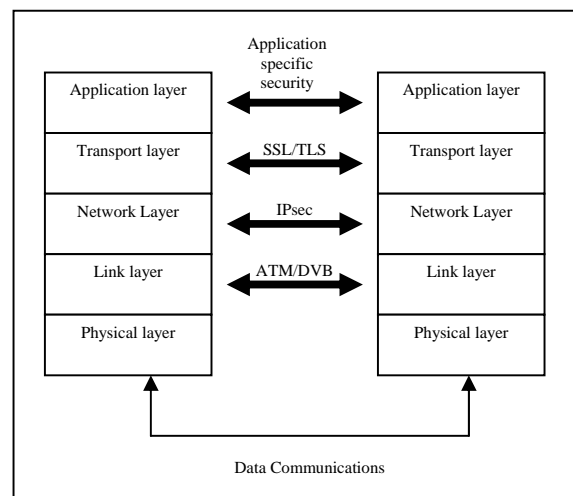


Figure 2: Existing security technologies

There are some scenarios might even require deploying two security technologies in combination. E.g. secure ATM/DVB-RCS may provide basic security service for all communications and additionally SSL may be used for applications that require special security services like strong encryption and authentication.

In general, there is a need to establish a trust relationship between users of the end-to-end security system through a security management system. The security operations may be visible to end users and applications if they are implemented at the application level, or it can be transparent if implemented in the lower layers.

In contrast, satellite network security focuses on access control and data encryption/integrity mechanisms within the BSM satellite network boundaries. Link layer security is the best solution here. The satellite network can star and mesh configurations with regenerative or bent pipe satellites. DVB and ATM security procedures can be used to secure satellite links. IPsec can be used to provide satellite network security by implementing IPsec tunnels.

III. BSM SECURITY FUNCTIONAL ARCHITECTURE

This section presents the detailed security system in various architectural cases. These security cases are focused on the

positioning of security functions above or below the SI-SAP in the STs (terminal) and GWs (Gateway). For example the security key management and data encryption entities can both be above or below the SI-SAP, or one above and one below.

In addition, the concept of BSM Security association Identity (SID) is presented. For example, if there is a secure connection between an ST and a GW, then SID is the reference number that is used to convey security information between BSM Local and Network security managers such as encryption keys, digital signature methods and security policy exchanges.

If there is only one single BSM Network security manager, then SID will be unique for the whole BSM network. If there are several Network security managers (for example one for each ISP), then SID must be used in conjunction with BSM-ID of the source and destination entities, in order to identify a security association between two BSM entities.

In addition, interactions with authentication entities such as RADIUS and DIAMETER are addressed in these cases. Remote Authentication Dial In User Service (RADIUS, RFC2865, [1]) was initially deployed to provide dial-up PPP and terminal server access. This protocol is widely implemented and used. Experience has shown that it can suffer degraded performance and lost data when used in large scale systems. As a result, DIAMETER (RFC 3588, [1]) is considered as an alternative to RADIUS.

IPsec can be used with both RADIUS and DIAMETER. For example in RFC3162 [1], RADIUS support for IPsec is not required. However, IPsec support is mandatory in DIAMETER, and TLS support is optional. In BSM networks, communications between RADIUS/DIAMETER client and server are transparent to BSM security. However if RADIUS is used then either IPsec or link layer security must be used to carry such authentication/authorisation messages.

For the purpose of this document, the RADIUS/DIAMETER concepts are abstracted. Therefore, three authentication entities are defined below and the authentication process is illustrated in Figure 3:

- **Supplicant:** The client or machine requesting access to the network.
- **Authenticator:** The second component of the architecture is the access device or gateway, which is typically a switch or an access-point or a hub. The device in an authentication system that physically allows or blocks access to the network.
- **Authentication server:** This is typically a RADIUS/DIAMETER server or others against which the users will authenticate and from which they can even receive their authorization rules.

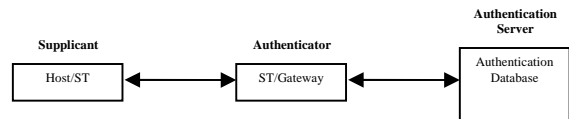


Figure 3: Host/machine authentication process

A. Case 1: IPsec and security entities in BSM

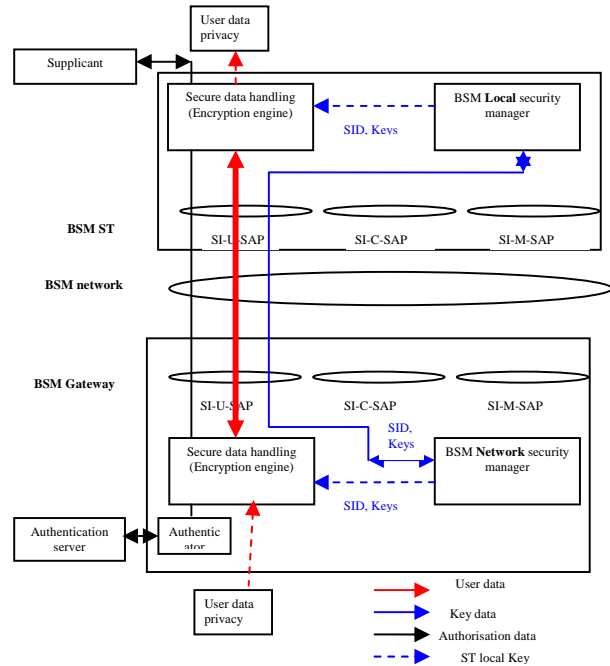


Figure 4: Case 1 IPsec and BSM security entities

As shown in Figure 4, this case illustrates the use of IPsec over BSM network in a security gateway-to-gateway configuration such as VPN over satellites scenario. IPsec protocol operates above the SI-SAP. Security is provided between a security gateways (that can be co-located with BSM ST or Gateway). The security gateway consists of two functional entities:

1. **Secure data handling entity (privacy/integrity engine):** IPsec must operate in tunnel mode.
2. **key management entity:** In a star topology, there will a **Network** security manager for the whole BSM network (co-located with BSM gateway/hub). In addition there is a **Local** security manager in each ST.

Figure 4, shows all security entities are above SI-SAP. The diagram also shows that the SI-U-SAP (the user interface) ONLY is used to communicate all secure information (user data and key management messages).

The client authentication process (supplicant, authenticator and Authentication server entities) is shown here as well, where IPsec is used to carry authentication information (such as user name and password) between Supplicant and authentication server.

Both the authentication server and the BSM network manager communicate with the BSM Network Control Centre (NCC) regarding security and authorisation. These

interactions are not shown here in order to simplify the diagram. Security association must be established between the BSM **Network** security manager and **Local** security managers in each ST. In the case of IPsec, the IETF Internet Key Exchange (IKE) protocol (RFC 4109, [1]) must be used to establish all security associations. This will ensure the mutual authentication between all security entities, establishing the keys used subsequently to secure the user data. Using IKE will also ensure compatibility between BSM and the general Internet (terrestrial) security systems.

The Security association identity SID must be used in all security management message exchanges.

However IPsec for multicast (star topology) is a challenge because IPsec tunnels must be set from the BSM gateways per ST. This is effectively a unicast configuration and the benefits of IP multicast are lost. There is some work in progress in the IETF msec group on IPsec extensions for multicast (msec-ipsec-ext) describes extensions to (RFC4301, [1]).

B. Case 2: Mixed link layer security entities in BSM (security manager above SI-SAP and security engine below SI-SAP)

As shown in Figure 5, this case illustrates the use of link layer security (below SI-SAP) with the key management as an application (above the SI-SAP). Typical examples of such system are DVB-RCS with MPE or Unidirectional Lightweight Encapsulation (ULE) (RFC4326, [1]) IP encapsulation.

Like case 1, the security is provided between security gateways (can be co-located with BSM ST or Gateway). The security gateway consists of two functional entities:

1. Secure data handling entity (privacy/integrity engine): e.g. is DVB-RCS security which performs data encryption below SI-SAP
2. Key management entity: There is a **Network** security manager for the whole BSM network (e.g. co-located with BSM gateway/hub). In addition there is a **local** security manager in each ST.

The client authentication process (supplicant, authenticator and Authentication server entities) is shown here as well, where secure link layer is used to carry authentication information (such as user name and password) between supplicant and authentication server.

Figure 5 shows security entities above and below the SI-SAP. The diagram also shows that the SI-U-SAP (the user interface) is used to communicate secure user information, while the key management secure information is passed through the SI-C-SAP interface. The client authentication messages use the SI-U-SAP interface.

Again, both authentication server and the BSM Network manager communicate with the BSM NCC regarding security and authorisation. These interactions are not shown here in order to simplify the diagram. Also security association must be established between the BSM **Network** security manager and **Local** security manager in each ST.

In the case of link layer security, the specific satellite

systems security must be used. For example, for DVB-RCS satellite systems, the logon and key exchanges procedures of DVB-RCS recommendations 06] must be used to establish all security associations. For BSM systems operating with ULE, then the ULE specific key management procedures must be used. This will ensure the mutual authentication between all security entities, establishing the keys used subsequently to secure the user data. Using link layer security will also authenticate BSM terminals (STs and gateways), which is not possible with using IPsec (case 1).

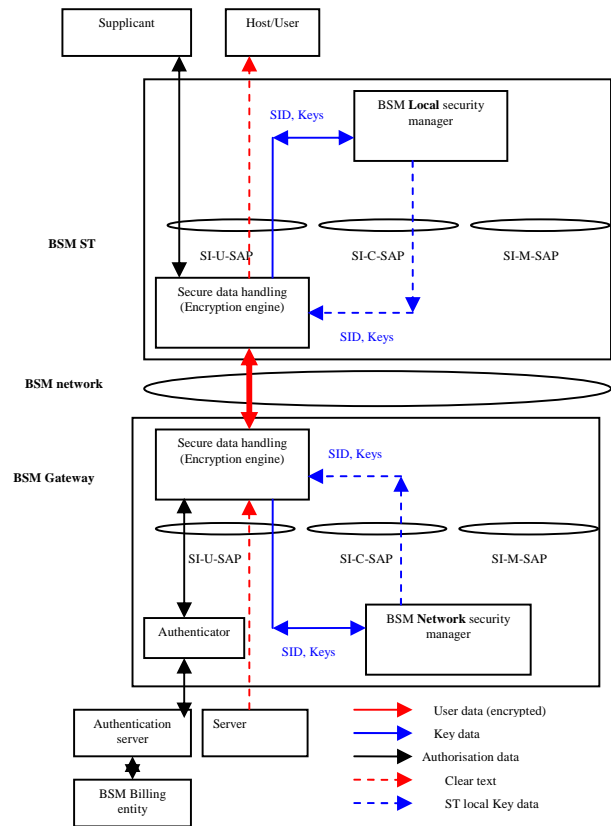


Figure 5: Case 2 Mixed link layer BSM security entities

The Security association identity SID must be used in all security management message exchanges.

C. Interactions with Performance Enhancing Proxies (PEPs)

The Transmission Control Protocol (RFC0793, [1]) (TCP) is used as the transport layer protocol by many Internet and intranet applications. However, in satellite environment, TCP and other higher layer protocol performance is limited by the link characteristics. Performance Enhancing Proxy (PEP) can perform mitigation techniques (RFC 3135, [1]).

A PEP is used to improve the performance of the Internet protocols on network paths where native performance suffers due to characteristics of a link (such as satellite links). A large spectrum of PEP devices exists (RFC3449, [1]), ranging from simple devices (e.g., ACK filtering) to more sophisticated devices (e.g., stateful devices that split a TCP connection into two separate parts).

However there are some security implications for using PEP in satellite environment. The most detrimental negative implication of breaking the end-to-end semantics of a connection is that it disables end-to-end use of IPsec. In general, a user or network administrator must choose between using PEPs and using IPsec. If IPsec is employed end-to-end, PEPs that are implemented on intermediate satellite nodes in the network cannot examine the transport or application headers of IP packets, because encryption of IP packets via IPsec's ESP header (in either transport or tunnel mode) renders the TCP header and payload unintelligible to the PEPs. Without being able to examine the transport or application headers, a PEP may not function optimally or at all.

However there are some steps which can be taken to allow the use of IPsec and PEPs to coexist. If an end user can select the use of IPsec for some traffic and not for other traffic, PEP processing can be applied to the traffic sent without IPsec. Another alternative is to implement IPsec between the two PEPs of a distributed PEP implementation. This at least protects the traffic between the two PEPs. (The issue of trusting the PEPs does not change).

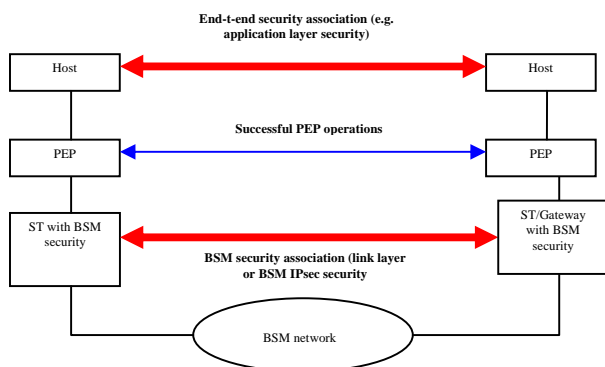


Figure 6: Suitable Security associations for interworking with PEPs

In BSM networks and as shown in Figure 6, PEPs can be used successfully in the following configurations:

- With Link layer security which operates on the satellite link only (such as DVB-RCS security).
- With IPsec provided that IPsec is used between the BSM ST/Gateway, where IPsec encryption is performed on incoming traffic after the PEP operations and decryption is performed on outgoing traffic before the PEP operations.

Thus the requirement is that security must be implemented in such way that allows PEP entity access to the transport protocol headers (such as TCP). Therefore link and application layer security are transparent to PEPs. If IPsec is used, then PEP operations must be performed outside the IPsec processing as shown in Figure 6. Reference [3] provides further information about PEPs and security issues over satellites.

IV. CONCLUSION

Satellites are expected to provide an essential role in bridging the “digital divide”; satellite networks are likely to be the only way to provide broadband services to regions that cannot be economically reached by terrestrial networks. The ETSI BSM work is focussed on the efficient transport of IP data streams and on how to interoperate resulting satellite networks with terrestrial IP networks. The BSM standards are being designed to use existing standards such as DVB-RCS while remaining open to emerging standards and other available technologies.

The paper focused on the current work in ETSI BSM group in defining the security architecture for BSM satellite networks. Two detailed architecture cases were presented. Case1 for the use of IPsec over BSM satellite networks, and case 2 for using link layer security such as DVB-RCS. In addition, the architecture presents interworking with other entities such as RADIUS/DIAMETER and satellite PEPs.

ACKNOWLEDGEMENT

This work was sponsored by the European Telecommunications Standards Institute (ETSI) [9] and support by the European Commission [10]. The authors gratefully acknowledge the support of the EU Information Society Technologies SATLIFE Project [11].

REFERENCES

- [1] IETF document: www.ietf.org
- [2] ETSI. Digital Video Broadcasting (DVB); DVB specification for data broadcasting. ETSI EN 301 790 V1.4.1 (2005-04). Interaction channel for satellite distribution systems”, 2005-04.
- [3] IABG final report. ESA project “IP security over satellites”. Contract No. 15555/01/NL/US. 2002
- [4] ETSI TS 102 292, “Satellite Equipment and Systems (SES); Broadband Satellite Multimedia; IP Interworking over Satellite; BSM Functional Architecture”.
- [5] ETSI TR 101 984: “Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; Services and Architectures”.
- [6] ETSI TR 101 985: “Satellite Earth Stations and Systems (SES); Broadband Satellite Multimedia; IP over Satellite”.
- [7] ETSI TR 102 287, “Satellite Equipment and Systems (SES); Broadband Satellite Multimedia; IP Interworking over Satellite; security aspects.”
- [8] ETSI TS 102 465, “Satellite Equipment and Systems (SES); Broadband Satellite Multimedia; IP Interworking over Satellite; BSM Security Functional Architecture”.
- [9] ETSI home page: http://portal.etsi.org/Portal_Common/home.asp
- [10] European Commission home page: <http://www.cordis.lu/>
- [11] SATLIFE web: www.satlife.org