

INNSS 07 – Budapest

ULE Link Layer Security for DVB Networks

Presenter: Sunil Iyengar
University of Surrey, UK
05/07/07





Outline

- Introduction
- SatIPSec Key Management protocol
- ULE data plane
- SatIPSec for DVB-RCS networks
- Forward Signalling security
- Conclusions

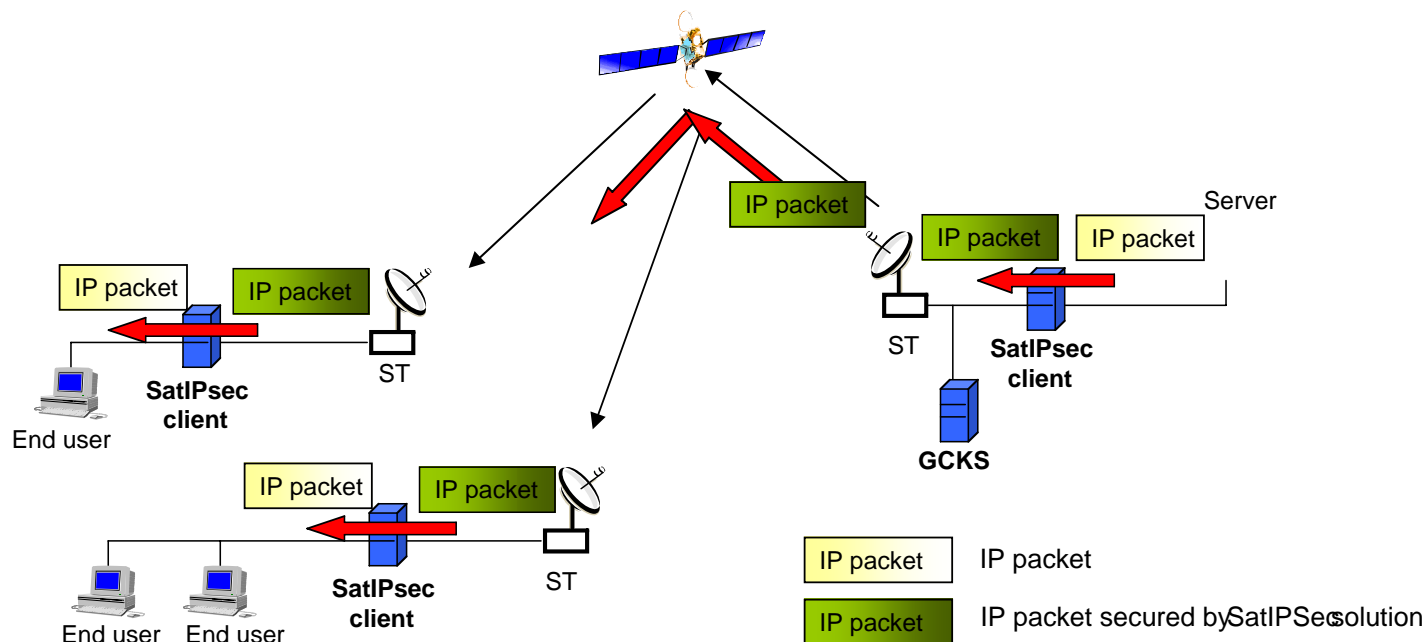


Introduction

- The MPEG-2 Transport Stream (TS) has been widely accepted not only for providing digital TV services, but also as a sub-network technology for building IP networks.
- Unidirectional Lightweight Encapsulation (ULE) mechanism for the transport of IPv4 and IPv6 Datagrams and other network protocol packets directly over the ISO MPEG-2 Transport Stream as TS Private Data.
- ULE must be robust to errors and security threats. Security must also consider both unidirectional as well as bi-directional links.
- The majority of MPEG-2/DVB transmission networks are wireless, and hence are bandwidth-limited, encapsulation protocols must therefore add minimal overhead to ensure good link efficiency while providing adequate security services.

SatIPSec Key Management Protocol

- SatIPSec is a key management protocol at the IP layer which offers a new way of transparently and efficiently securing unicast and multicast satellite transmissions, on forward and return links, in DVB-RCS mesh and star topologies.
 - SatIPSec protocol is derived from IP Security (IPSec) standard protocols.



Application of SatIPSec at Link Level

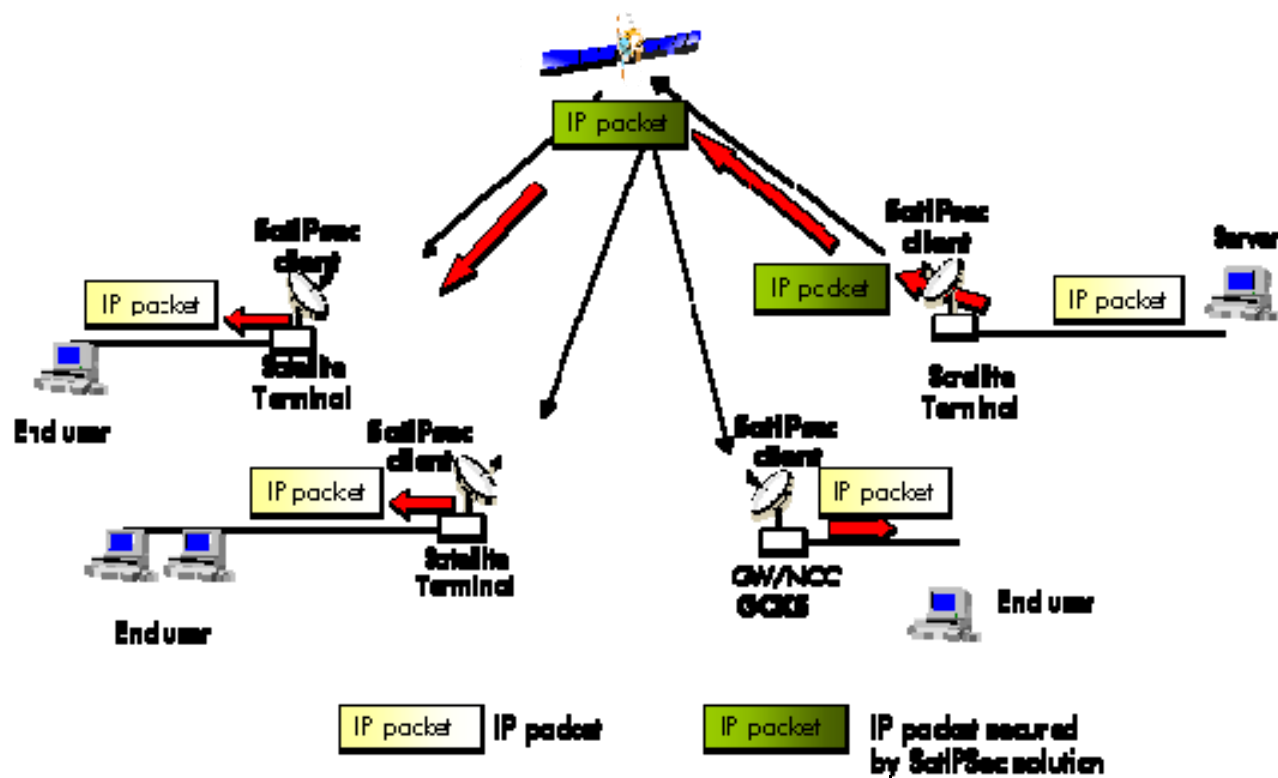


SatIPSec is a generic solution that can be implemented to protect data at IP layer, but also at the link layer.

- A link layer security solution represents several advantages:
- Independence from the type of satellite terminal: A security solution at DVB-RCS level can be used in any types of ST: router or bridge.
- Independence from the type of traffic to protect: A layer 2 solution can secure transparently any types of traffic.
- Compatibility with other Internet Service Providers (ISP) or subscriber security functions: Taking into account the role of the different actors (Access Network Operator, Internet Service Provider), it can be possible to have simultaneously different security schemes.
- Satellite bandwidth optimisation.
- Moreover it provides or can provide additional security services which may be considered major requirements in many DVB-S/RCS satellite networks:
 - Protection of the complete Protocol Data Unit .
 - Protection of Layer 2 Network Point of Attachment (NPA) address.

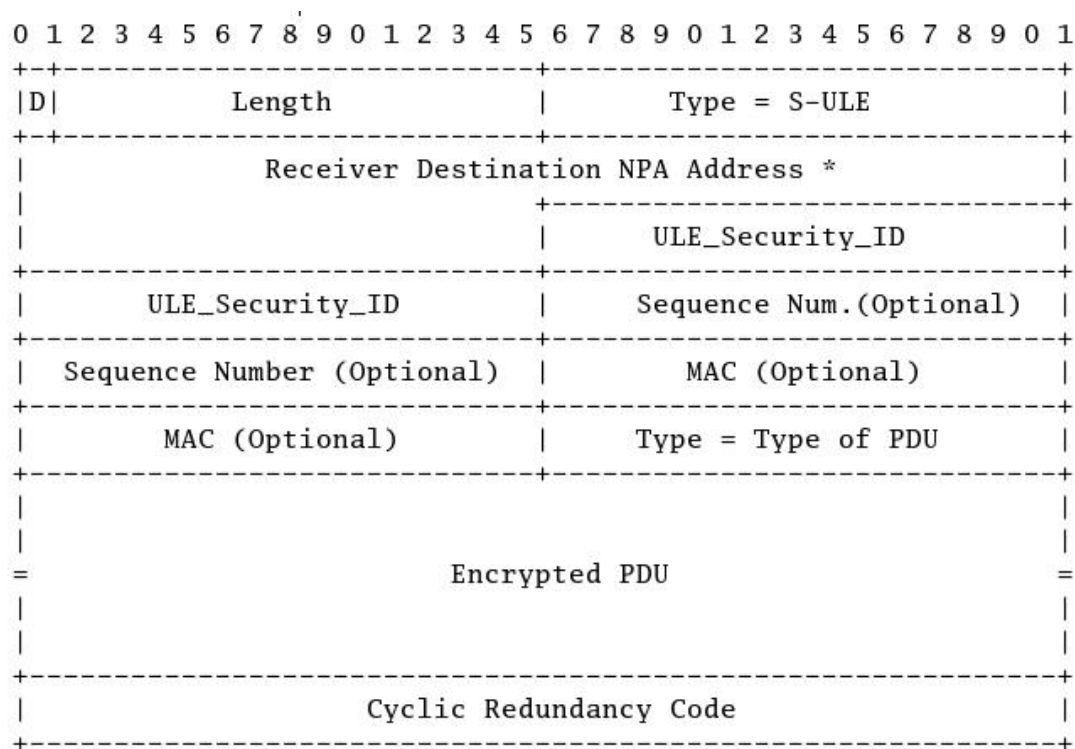
SatIPSec Key Management Protocol

- SatIPSec key management protocol at the Link layer (ULE)

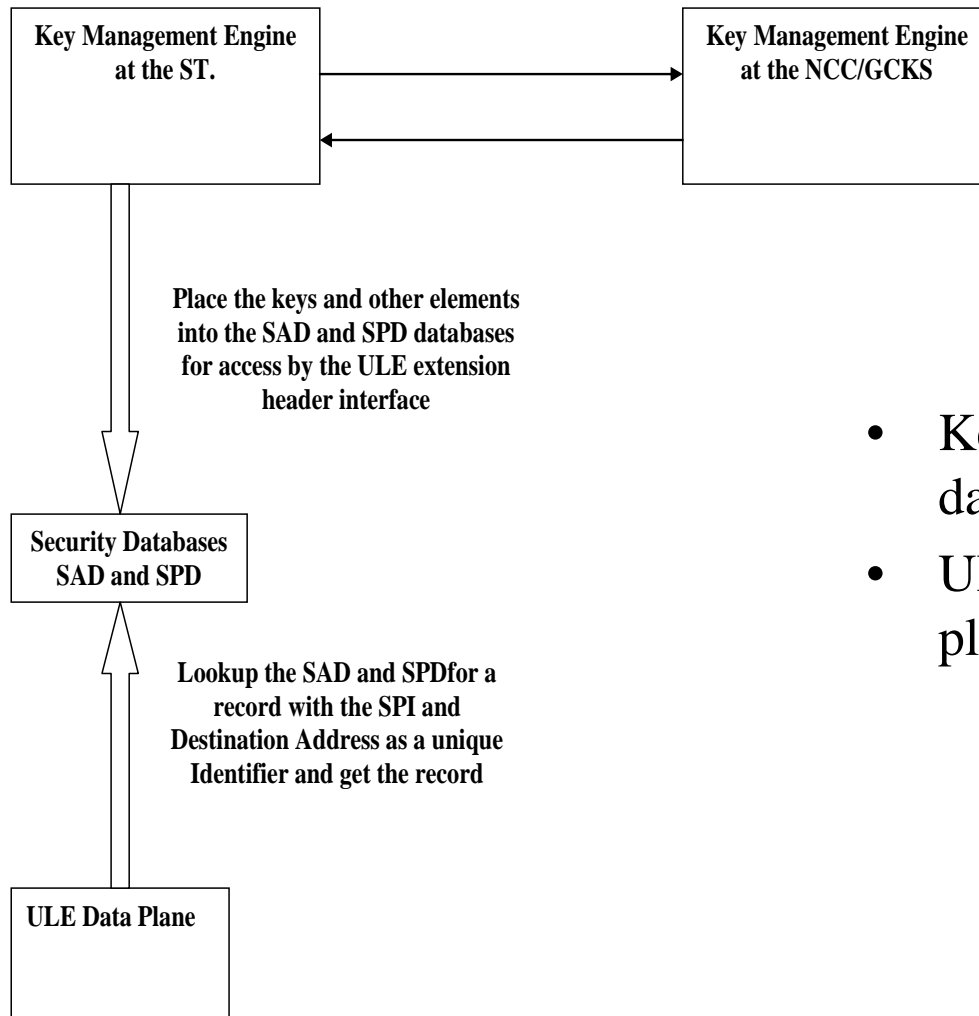


ULE Security Data Plane

- ULE specifies a base encapsulation format and supports an extension format that allows it to carry additional header information to assist in network/Receiver processing.
 - An extension to the encapsulation is therefore being considered to provide confidentiality (encryption) and, optional source authentication.



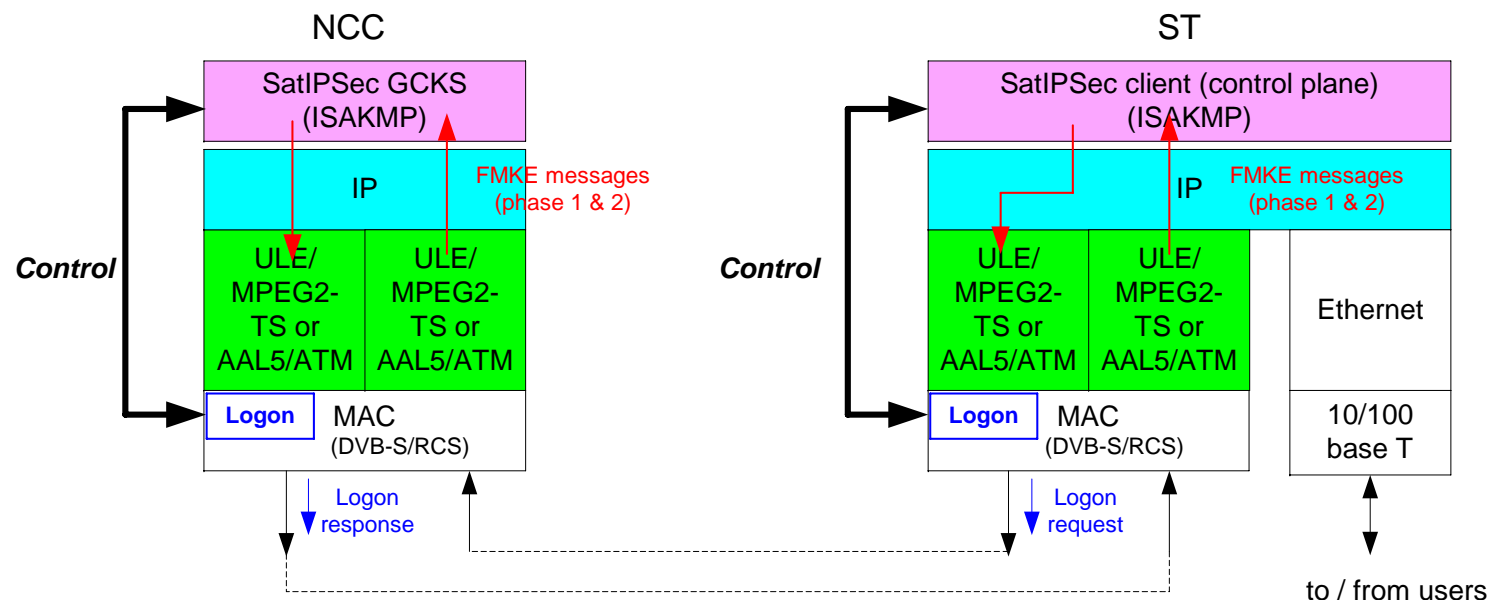
Interface Between SatIPSec and the ULE Data Plane



- Key management \leftrightarrow ULE Security databases
- ULE Security databases \leftrightarrow ULE data plane

SatIPSec for DVB-RCS Networks

- SatIPSec phases are inserted in the DVB-RCS process.
- SatIPSec 2 messages will replace the Security Sign_On, Security Sign_On Response, EKE (and MKE, QKE for DVB-RCS initial version) requests and responses used during DVB-RCS Logon and session for respectively security session establishment and key updates.



Forward Link Signalling Security Requirements



- In a two-way satellite interactive network, consisting of a forward link and return link via satellite, the forward link signalling consists of general System Information (SI) tables, carrying information about the structure of the satellite interactive network, and satellite terminal specific messages sent to individual satellite terminals.
- Requirements:
 - Confidentiality of SI tables, TIM and PCR insertion TS packets.
 - Integrity protection and source authentication (i.e. NCC) of SI tables, TIM and PCR insertion TS packets (optional).
 - Protection against replay attacks of SI tables, TIM and PCR insertion TS packets (optional).

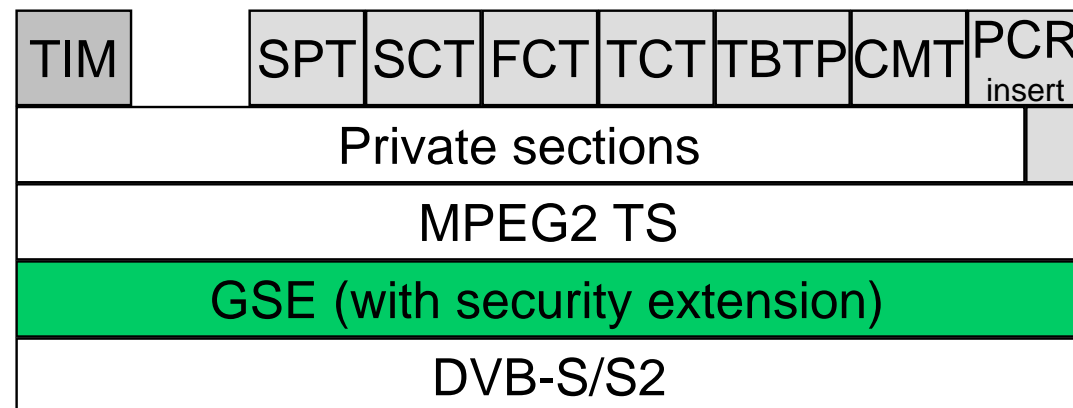
Security Solution for Signalling Traffic Using GSE



- GSE encapsulation allows the transport of MPEG-TS SI tables can be encapsulated using GSE and then sent over the DVB-S/S2 interface.
- The ULE security extension also compatible with GSE encapsulation and can thus be used to protect general SI tables and satellite terminal specific messages, by providing.

RCST specific messages

General SI tables



Forward (transparent control stack) /
Downlink (regenerative control stack)



Conclusions

- Described the SatIPSec key management protocol used at the IP layer and its limitations for layer 2 security.
- SatIPSec can be adapted to be used as a key management protocol for layer 2 (ULE security).
- ULE Security Header format that will be used in the data plane (i.e. the layer where the security services will be applied).
- The interfaces between the Key Management application (SATIPSec) and the data plane (ULE) are further described.
- Finally The risk analysis of the forward link signalling are highlighted and a security solution for control plane security is described.

Acknowledgements



- Gratefully Acknowledge the Support provided by the SATSIX project.



Thanks for your attention !!!!!

Any Questions