An introduction to IPSEC

Rémy Giraud

Expert Team on Enhanced Use of Data Communication Systems

Montreal, Canada, 27-31 May 2002

IPSec Introduction

IPSec (Internet protocol security) has been developed with IPv6. However it is designed to work and to be compatible with IPv4. IPSec is a securiy architecture rather than a protocol. IPSec is defined in RFC2401.

RFC2401:

"IPSec is designed to provide interoperable high quality, crytpographically-based security for IPv4 and IPv6. The set of security services offered includes access control, connectionless integrity, data origin authentication, protection against replays, confidentiality, and limited traffic flow confidentiality. These services are provided at the IP layer offering protection for the IP and upper layer protocols. "

IPSec Introduction

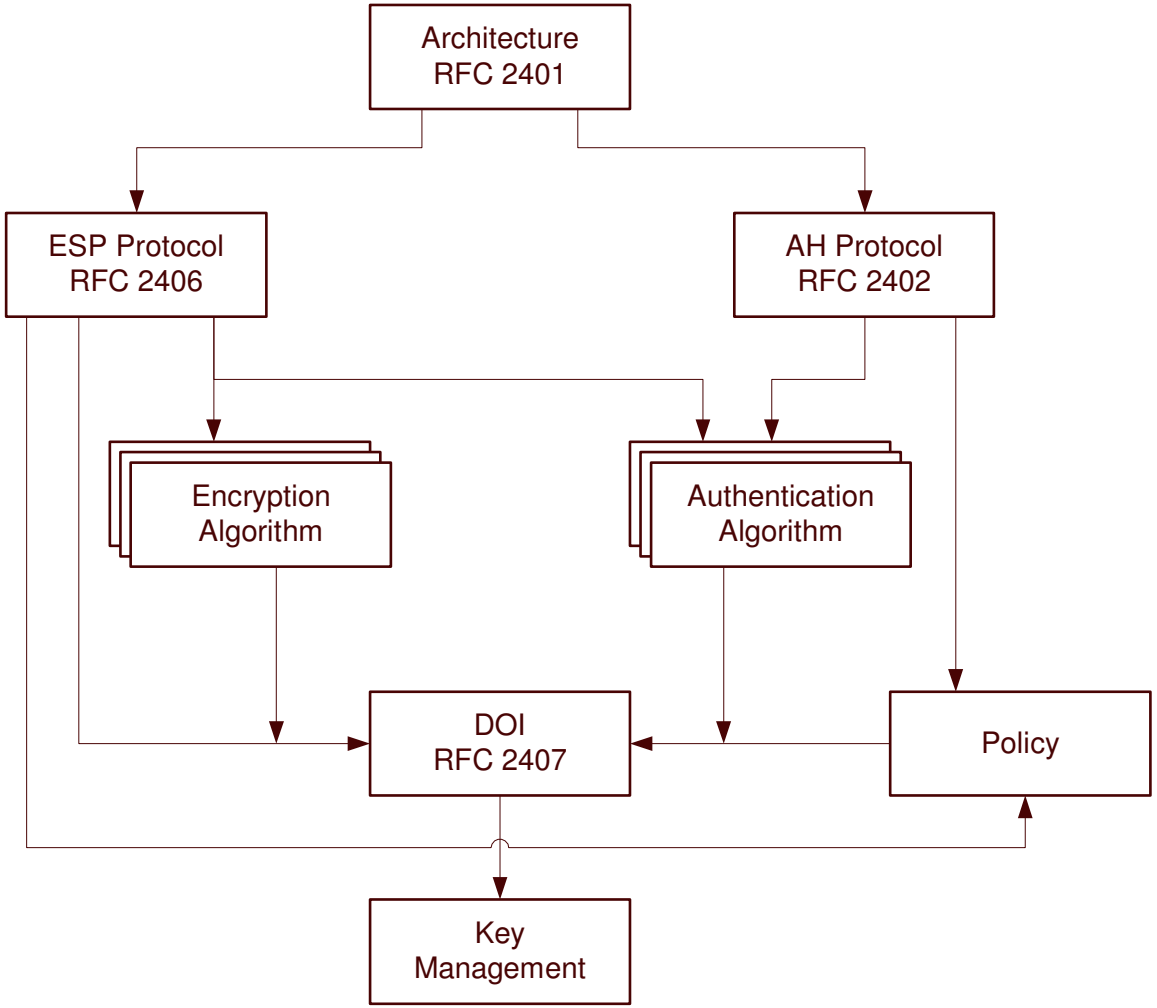
Application areas for IPSec

- IPSec provides the capability to secure communications across a LAN, across private and public WAN's, and across the Internet. Examples of the use are (Fig 13.1.)
  - Secure branch office connectivity over the Internet
    - Virtual Private Network (VPN) to reduce costs and need for private networks
  - Secure remote access over the Interent
    - flexibility, travelling employees
  - Establishing extranet and intranet connectivity with partners
  - Enchancing electronic commerce security
- The principal feature of IPSec enabling these application is that it encrypts and authenticate *all traffic* at the IP level. Thus all distributed applications can be secured, also many security ignorant ones.

IPSec Architecture

- The IPSec specification is quite complex. The overall architecture of the specification can be seen as a suite of interacting protocols.
- IPSec Documents (most important)
  - RFC 2412: Overview of the architecure
  - RFC 2402: Packet authetntication extension to IPv4 and IPv6
  - RFC 2406: Packet encryption extension to IPv4 and IPv6
  - RFC 2408: Key management
- Documents located at http://www.ietf.org/html.charters/ipsec-charter.html
- Support for the features is mandatory for IPv6 and optional for IPv4.
- In both cases the security features are implemented as extension headers that follow the main IP header.
  - the extension header for authentication is known as AH and that for encryption as ESP (Encapsulating security payload).

IPSec document overview



IPSec Architecture

The other IPSec documents are divided into seven groups (figure):

- *Architecture* covering the general concepts, security requirements, definitions and mechanisms defining IPSec technology.
  - defines the capabilities hosts and routers should provide
  - for example, it is required that the hosts provide confidentiality using ESP. However this document does not specify the header format.
  - describes the interaction between IPSec and rest of TCP/IP
- *Encapsulation security payload* ESP and *Authentication header* (AH)
  - define the protocol, the payload header format and the services they provide.
  - define the packet processing rules
  - *do not* specify the cryptographic transforms that are used to provide these capabilities. This allows the transforms to be changed if they become cryptographically insecue without any change in the base protocol.

IPSec Architecture

- *Encryption algorithm and Authentication algorithm*
  - a set of documents that describe how various encryption algorihtms are used in ESP or how various authentication algorihtms are used in AH and authentication part of EPS.
  - define the algorithm, the key sizes, the derivation of keys, transformation process, any algorithm-specific information.
  - the definitions have to be very specific in order to obtain interoperability.
- *Key management* describing the key management schemes.
  - keys are generated with Internet Key Exhange (IKE) in IPSec protocols
  - The payload format of IKE is very generic. It can be used to negotiate keys in any protocol. IKE is also used for negotiating keys for other protocols outside IPSec.
  - The genericity is achieved by separating the parameters IKE negotiates from the protocol itself.

IPSec Architecture

- *Domain of Interpretation* (DOI) contains values needed for the other documents to relate to each other, i.e. identifiers for approved encryption and authentication algorithms, operational parameters like key lifetime.
  - the parameters negotiated by IKE are defined in DOI
- *Policy* is an important component
  - determines if two entities will be able to communicate with each other, and if so, which transforms to use.
  - *Policy representation* deals with definition, storage and retrieval of policy.
  - *Policy implementation* addresses the application of policy for actual communication involving e.g. the application of negotiated keys in the communication.

IPSec Services

- IPSec provides security services by enabling a system to
  - select required security protocols
  - determine the algorithms to use for the services
  - put in place the cryptographic keys needed to provide the requested services
- Two protocols are used to provide security:
  - an authentication protocol designated by the header, Authentication Header (AH)
  - a combined encryption/authentication protocol designated by the format of the packet for that protocol, Encapsulating Security Payload (ESP)

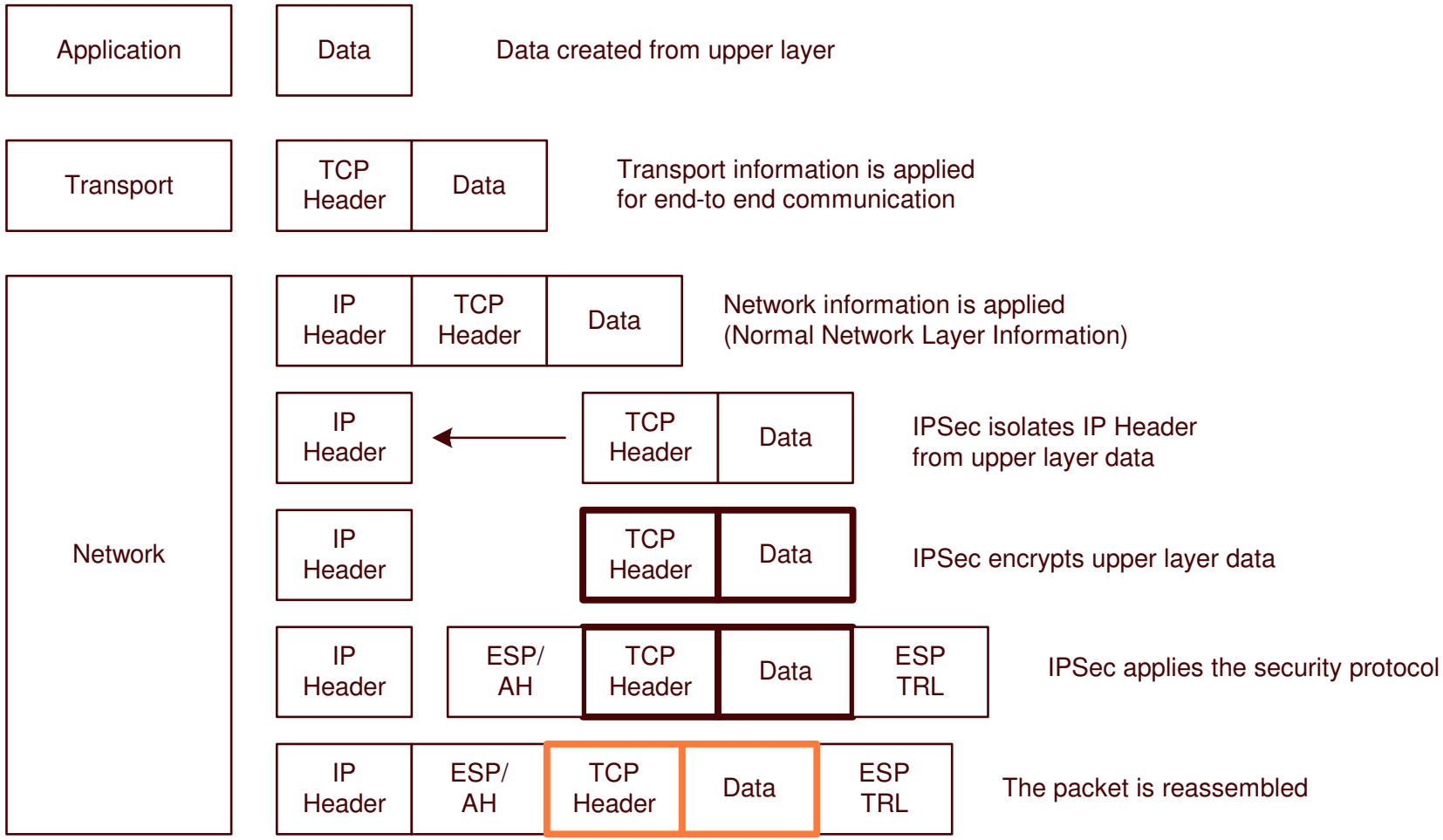
IpSec Services

	AH	ESP (Encryption Only)	ESP (Encryption and authentication)
Access Control	➳	➳	➳
Connectionless Integrity	➳		➳
Data origin authentication	➳		➳
Rejection of replayed packets	➳	➳	➳
Confidentiality		➳	➳
Limited traffic flow confidentiality		➳	➳

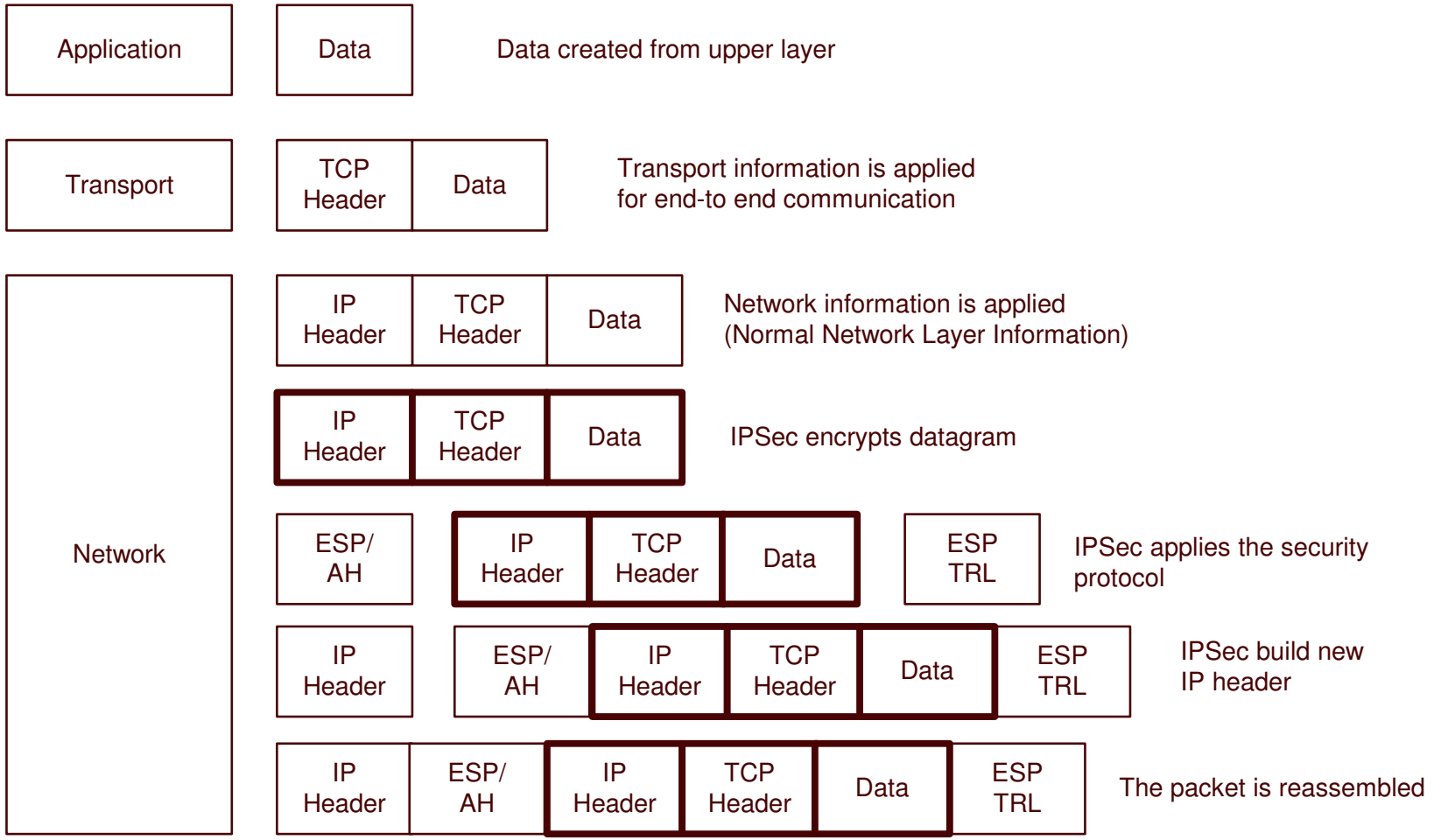
IPSec Modes

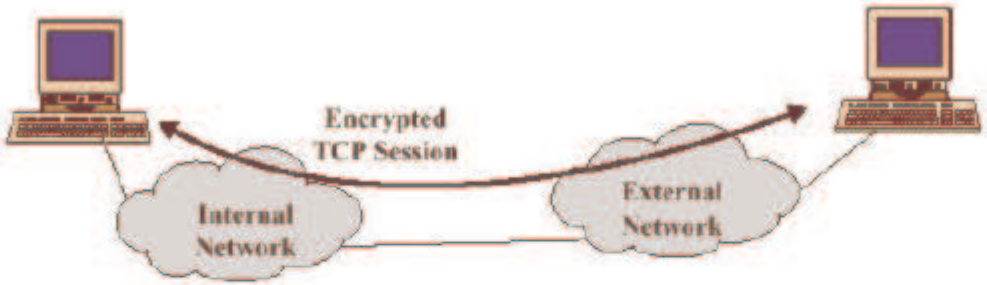
- IPSec protocols can be used in two modes, *transport mode* and *tunnel mode*.
- Both protocols, ESP and AH support both modes. This gives four different combinations shown in table 13.2.
  - In practice AH in tunnel mode is not used because it protects the same data that AH in transport mode protects.
- The AH or ESP headers do not change in different modes. The difference is a semantic one – what is it the headers are protecting, IP packet or IP payload?

IPSec operations within transport mode

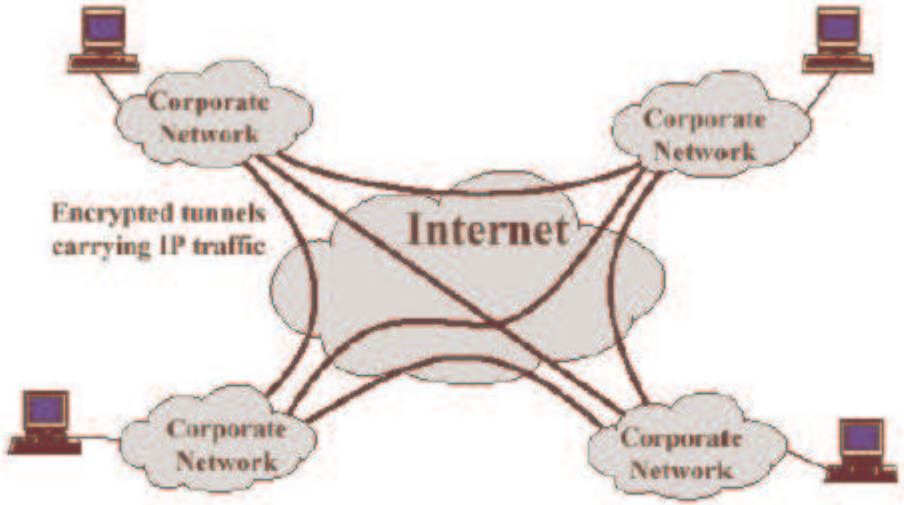


IPSec operations within tunnel mode





(a) Transport-level security



(b) A virtual private network via Tunnel Mode

IBM

AH

- AH provides data integrity and authentication of IP packets.
  - data integrity ensures that endetected modification to a packets content in transit is not possible
  - authentication feature enables an end system or networt device to authenticate the user or application and filter traffic accordingly.
  - prevents the addres spoofing attacks that are rather common in the Internet.
  - protects against the reply attack
- Authentication is done by use of a MAC, so a common secret key is required.
- The fields in the AH are
  - *next header* to identify the type of the header following AH
  - *payload length*
  - *SPI* for identifying an SA
  - *sequence number* is a monotonically increasing counter used for anti-replay protection
  - *authentication data* contains the Integrity Check Value ICV (MAC) for this packet.

ESP

- ESP provides confidentiality services including message and limited traffic flow confidentiality. As an option ESP provides the same authentication services as AH.
- The fields in the ESP are
  - *next header* to identify the type of the header following AH
  - *payload length*
  - *SPI* for identifying an SA
  - *sequence number* is a monotonically increasing counter used for anti-replay protection
  - *payload data* is a transport-level segment (transport mode) or IP packet (tunnel mode) that is portected by encryption.
  - *authentication data* contains the Integrity Check Value ICV (MAC) calculated over the ESP packet minus the Authentication Data Field.
- Fig. 13.7 shows the coverage of authentication and confidentiality services.

ESP

Encryption and authentication algorithms

- The mandatory to implement algorithm is DES in CBC mode.
- A number of other algorihtms have been assigned identifiers in the DOI document, and can therefore easily be used for encryption. These include
  - Three-key triple DES
  - RC5
  - IDEA
  - Three-key triple IDEA
  - CAST
  - Blowfish
- The choises for MAC are the same as in AH.

Internet Key Exchange (IKE)/ISAKMP

- ISAKMP defines the language for negotiation.
  - A protocol framework that defines payload formats, the mechanics of implementing a key exchange protocol, and the negotiation of a security association.
  - ISAKMP does not dictate a specific key exchange algorithm, rather it consists of a set of messge types that enable the use of a variety of key exchange algorithms.
- Oakley and SKEME define the steps two peers must take to establish a shared, authenticated key. The ISAKMP language is used to express these (and other) exhanges.
  - Oakley is a key exchange protocol that defines how to derive authenticated keying material. It is based on the Diffie-Hellman algorithm but providing added security. Oakley is generic in that it does not dictate specific formats.
  - SKEME is a key exchange protocol that defines how to derive authenticated keying material, with rapid key refreshment.

In this brief introduction to IPSec, we have seen that :

- Two modes exists : Tunnel and Transport
- Two protocols partially redundant are defined : ESP and AH
- Security Association are created and maintained by three different protocols
- Authentication can be achieve through two possible algorithms
- Encryption rely on DES (which is insecure) and 6 others protocols. A new one AES will probable overcome all others

We have neither covered nor introduced other aspects which may also be relevant in IPSec :

- Diffie-Helmann protocol to create keys
- Certificates
- PKI –Public Key Infrastructure
- …

VPN, in some aspect, is quite a vague concept, IPSec, one of the VPN solution is not much clear !

So, despite the rather ugly face of the protocol, the various options, the risk of incompatibility, IPSec is now widely implemented and available on a lot of platform, including, routers, dedicated boxes, firewalls, hosts…