A Cryptographic Evaluation of IPsec.

Neils Ferguson and Bruce Schneier

presented by

Rajdeep R Larha

About the Authors

- Niels Ferguson:- Presently, an independent cryptography consultant, working at Amsterdam, The Netherlands.

  Cracked the HDCP system developed by INTEL.

  Censorship in action: Silenced by the DMCA.
- Bruce Schneier:- Founder and CTO of Counterpane Internet Security Inc.

  Author of six books for Cryptography and Security.

Cryptographic Algorithms (Basics)

A Crypto Algorithm is a procedure that takes the plain text data and transforms it into ciphertext in a reversible way.

A Cryptographic Key is a special type of data that directs the crypto device to encrypt the message in a distinctive way.

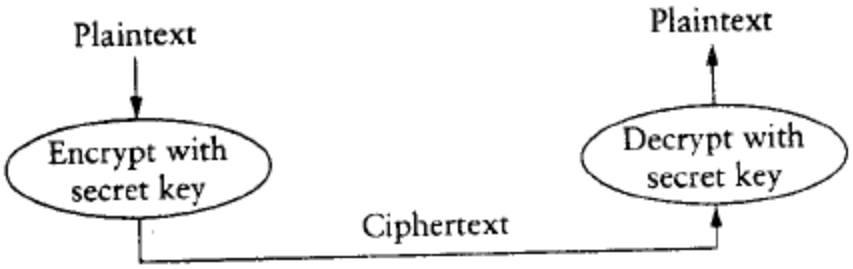
Basics continued..

Three Types of Cryptographic Algorithms:-

- **Secret Key Algorithm:-** Both participants share a single key.
- **Public Key Algorithm:-** Each participant have a private key which is not shared and a public key which is published to all.
- **Hashing Algorithms (Message Digest):-** A large message is mapped into a fixed-length number.

Basics continued..

Secret Key Encryption (Symmetric)



Same key is used to encrypt and decrypt the message.

e.g. Data Encryption Standard (DES).

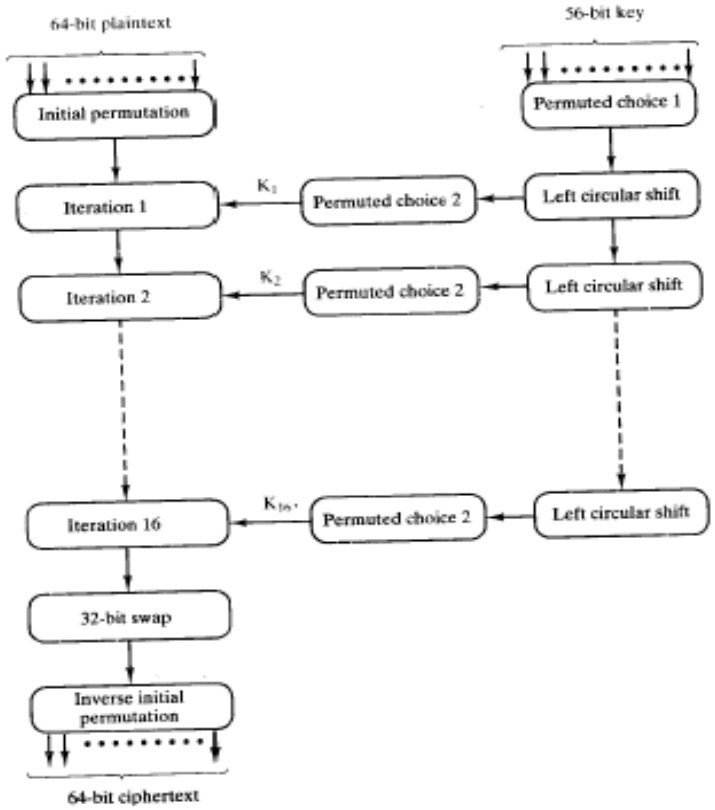
DES

- Encrypts a 64 bit plaintext with 64 bit Key.
- The 64 bits in the message block are permuted.
- Sixteen rounds of identical operation are applied to the resulting data and the key.
- The inverse of original permutation is applied to the result.
- The following rules are applied during each round i

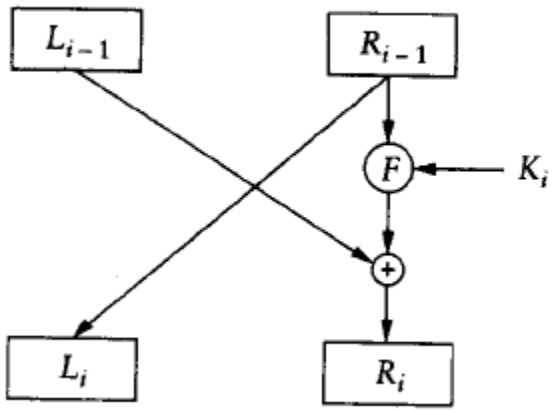
$L_i = R_{i-1}$

$R_i = L_{i-1}$ XOR F(Ri-1,Ki)

DES

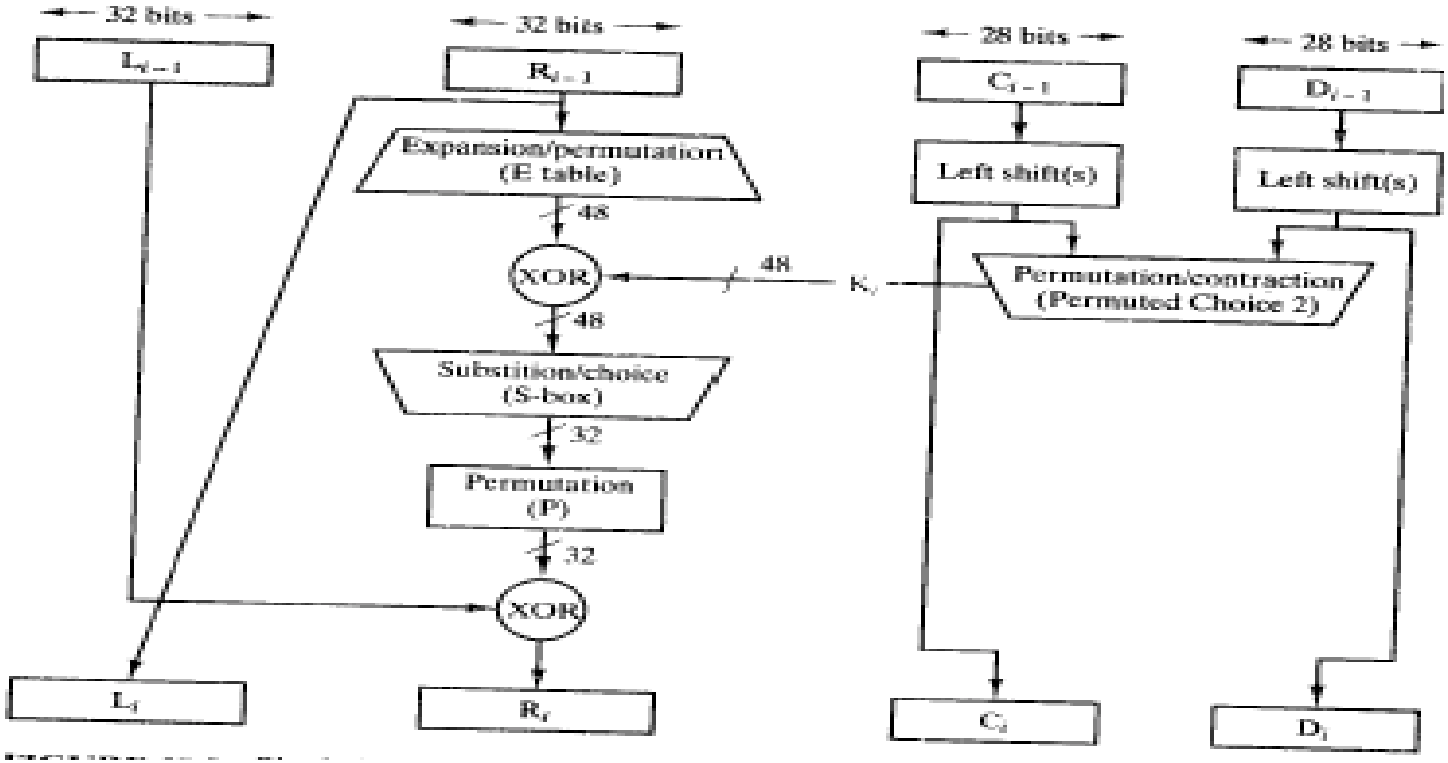

64-bit plaintext
56-bit key
Initial permutation
Permuted choice 1
Iteration 1
K_1
Permuted choice 2
Left circular shift
Iteration 2
K_2
Permuted choice 2
Left circular shift
Iteration 16
K_{16}
Permuted choice 2
Left circular shift
32-bit swap
Inverse initial permutation
64-bit ciphertext

DES



Manipulation done at each round in DES.

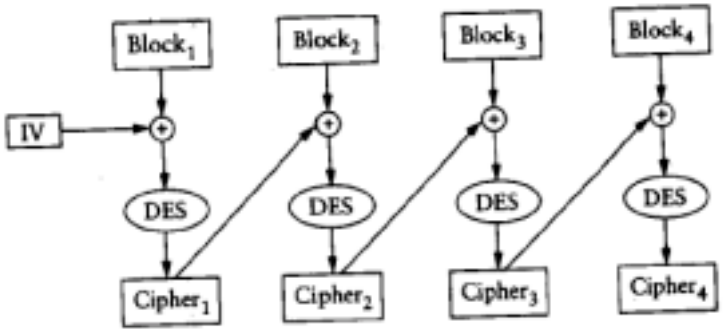
DES



Detailed Single iteration in DES.

DES

To encrypt message over 64 bit size, Cipher Block Chaining is used.



IV is the Initialization Vector used for the nonexistent ciphertext for block 0.

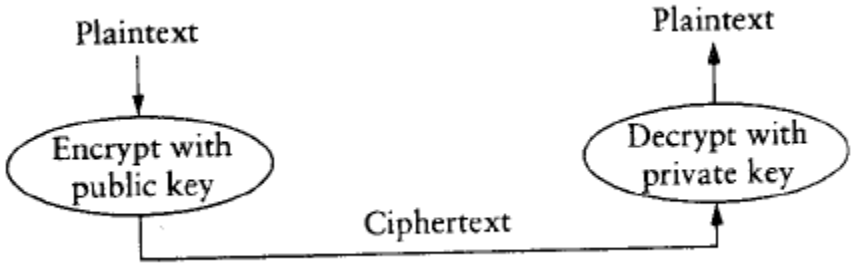
DES

- To break DES it requires to search exhaustively for 2^{56} keys, which is not difficult as with the speed of processors available now and the task of searching a key space is highly parallel.

- No satisfactory reason for using initial permutation and final permutation (Confusion and Diffusion).
- Triple DES:- is more effective as it uses 2 keys and on each side three instances of DES is used. The effective key length is 112 bits.

RSA (Ravist ,Shamir, and Aldeman)

Public Key Encryption (Asymmetric)

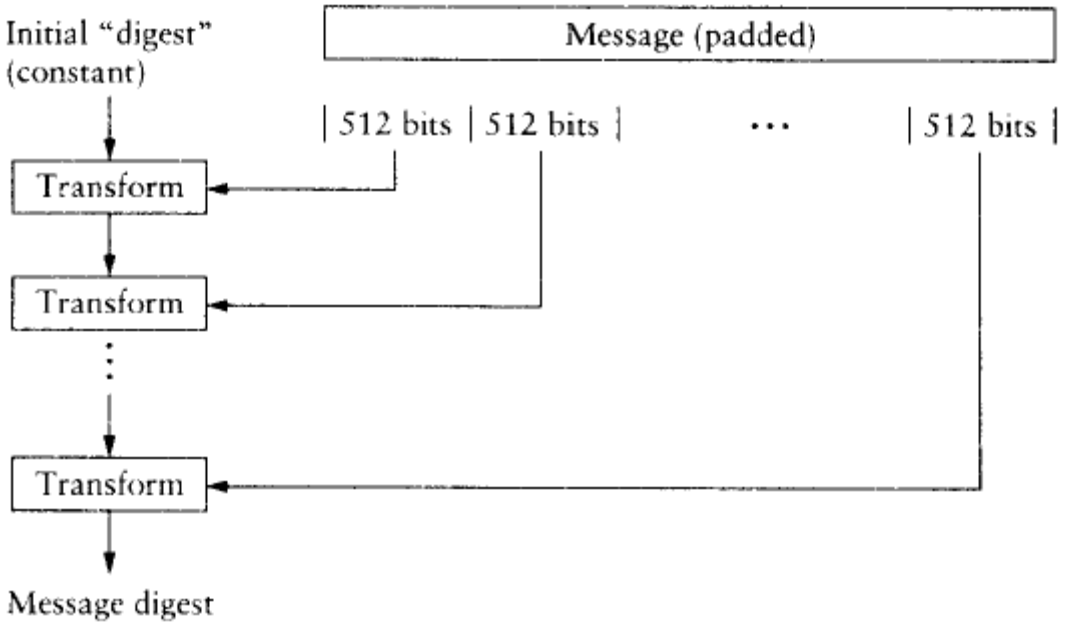


- Uses two keys (Pubic and Private).
- Grounded in Number Theory, requires enormous computation power. The key length is 512 bits.

Message Digest version 5 (MD5)

- It computes the cryptographic checksum over the message.
- It is not computationally feasible to find two messages that hash to the same cryptographic checksum. i.e. $H(m1) \neq H(m2)$
- The message is padded so that its length is congruent to 448 mod 512 as the last 64 bit are used in the message to represent the length in bits of the original message (before padding). This allows messages of length up to 2^{64} bits.

MD5



Overview of Message Digest operation

MD5

- It transforms the 512 bits of message at a time with the 128 bit digest and outputs the a new 128 bit digest. Then this new digest is the input to the next 512 bit chunk in the message
- Possible number of outputs are 2^{128} ,these outputs should be randomly distributed , as it requires to compute the digest of about 2^{64} to find that the two are same. (Birthday Attack Problem)

Security Threats

Active Attacks:

- **Replay Attack**:- Involves the passive capture of data unit and its subsequent retransmission to produce an unauthorized effect.
- **Denial of service (DOS) Attack**:- Disruption of the entire network by disabling the network or by overloading the network by flooding messages to degrade the performance (SYN-Attack in TCP).

  Can be protected through firewalls.

KEYS

Two Types are keys are identified:-

- Session key:- When the two end systems wish to communicate, they establishes a logical connection. For the duration of that logical connection, all user data are encrypted with a one-time session key. It is destroyed at the end of session.
- Permanent key:- A permanent key is used between entities for the purpose of distributing session keys.

Authentication Protocol

The three common protocols for implementing authentication are:-

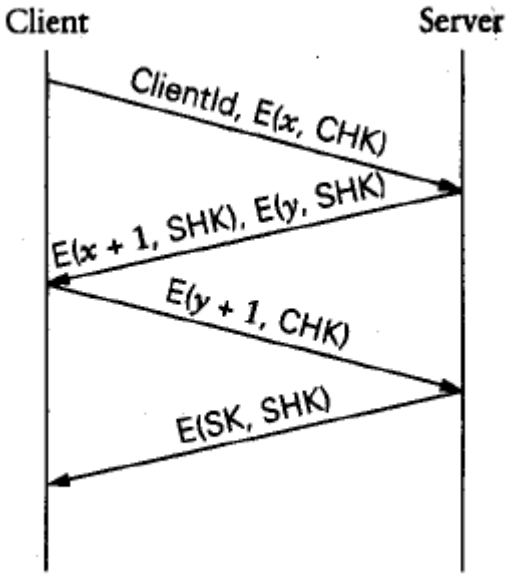
- Simple Three-Way Handshake.
- Trusted Third Party (Used in Kerberos).
- Public Key Authentication.

Simple Three-Way Handshake

- The client sends encrypted random number

  E (x, CHK) along with its ClientId.
- The server uses the same key as SHK corresponding to that client. It decrypts that random number and adds 1 to it and send back to the client after encrypting it. It also send another random number “y” to the client.
- The client authenticate the server and sends “y” after adding one to it, after receiving the message the server also authenticate the client and sends a session key to the client which is encrypted using SHK.

Simple Three-Way Handshake



Three-way handshake protocol for authentication.

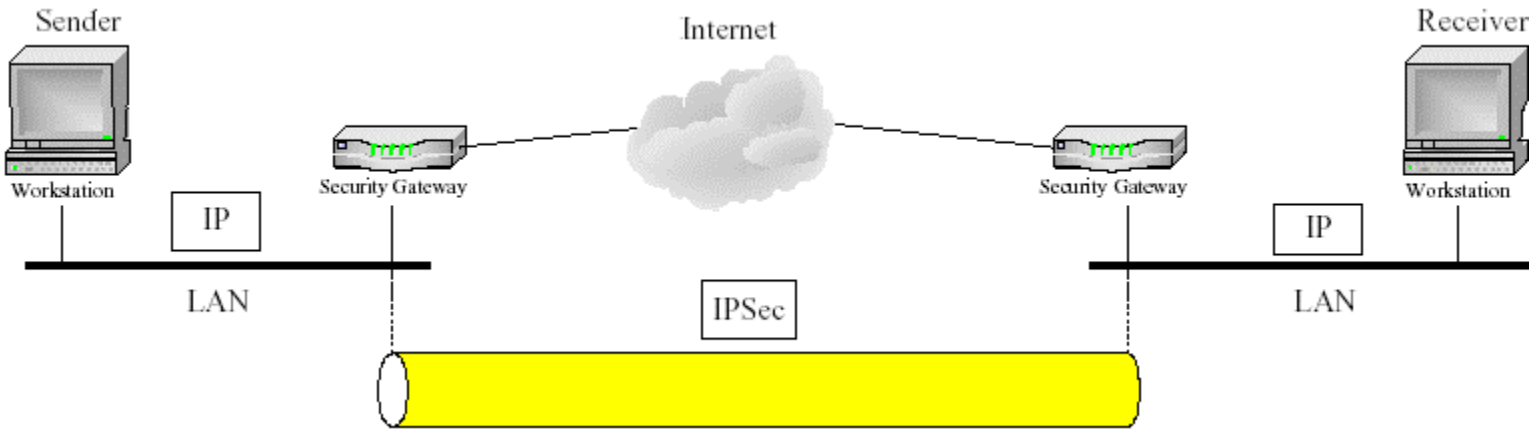
IPSec

IPSec has two modes of operation:

- Transport Mode: Transport mode encrypts only the data portion (*payload*) of each packet, but leaves the header untouched. It is more efficient and the end points are obvious.

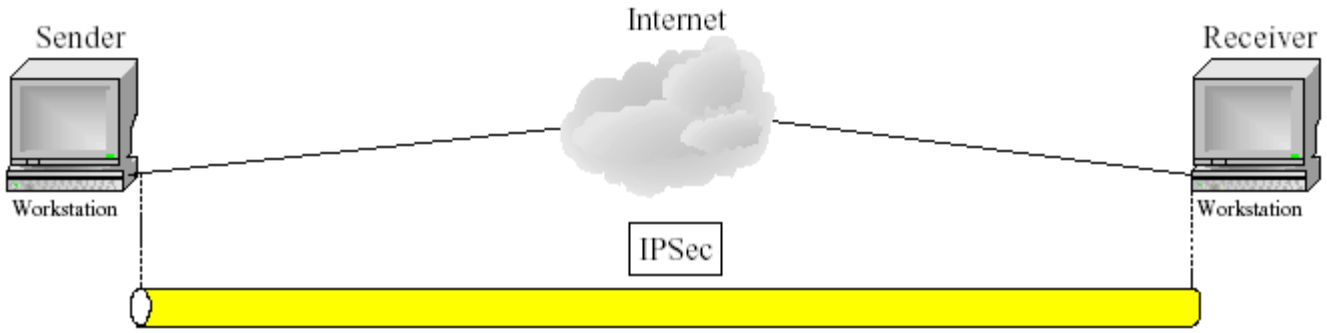
- Tunnel Mode: is the way Mobile-IP works or the VPN are constructed. It is less efficient but hides the network behind the security gateways. the traffic of the several networks can be concealed in one tunnel making traffic analysis difficult. It encrypts both the data and the header.

Tunnel Mode



IPSec implemented between security gateways.

Transport Mode



IPSec implementation in end-to-end communication scheme

IPsec: Protocols Types

IPSec consists of 2 pieces

1) Protocols:

- Authentication Header (AH):- Provides access control, connectionless message integrity, authentication, and anti-replay protection.
- Encapsulating Security Payload (ESP):- Provides all the above services plus confidentiality (Encryption).

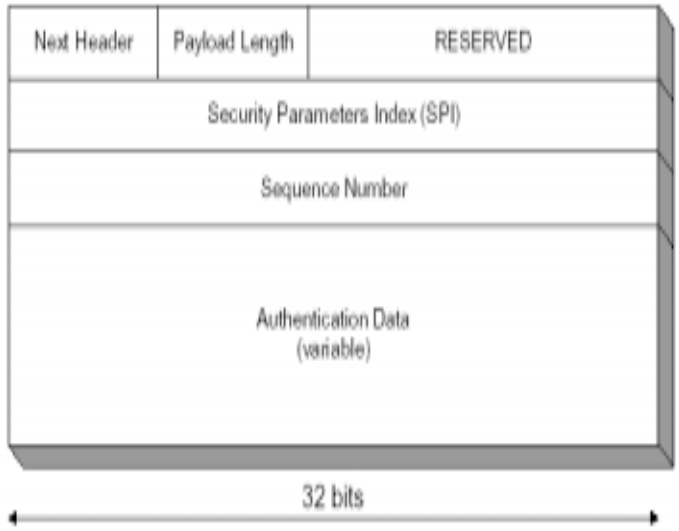
2) Key Management:

- ISAKMP: defines procedures and packet formats to establish, negotiate, modify and delete security associations.

Security Association (SA): An SA is a simplex (one-way) connection that is protected by one or more available security services.

Authentication Header (AH)

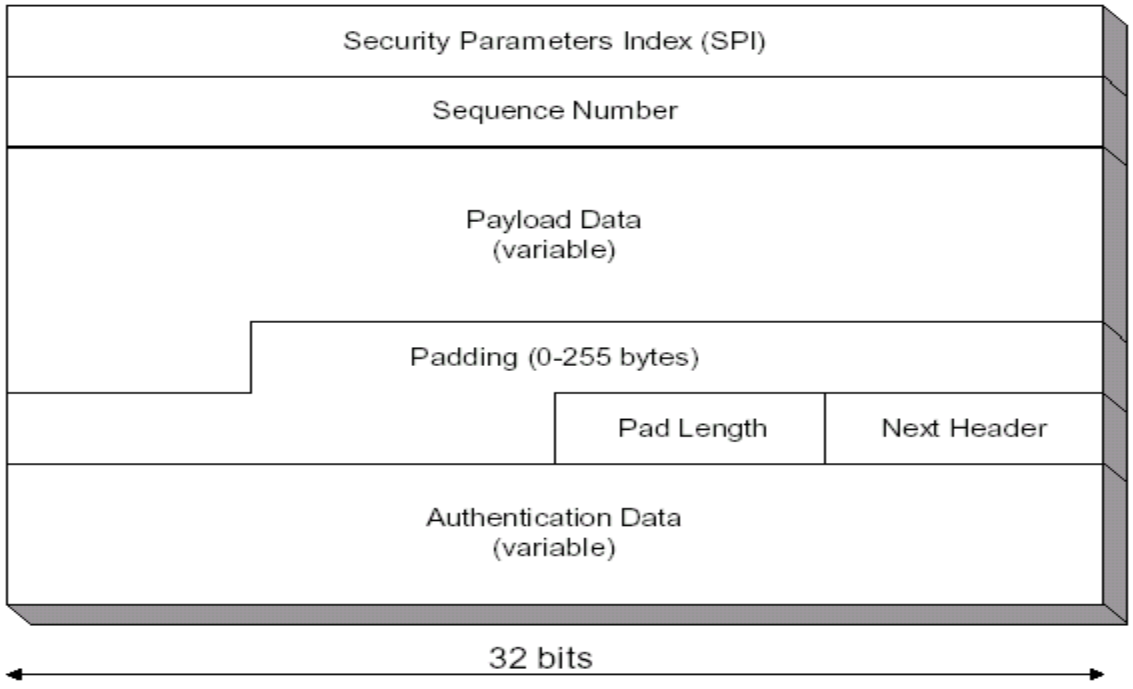
- **AH provides authentication of the payload and also of the packet header.**
- **It also provides protection against replay attack.**
- **NextHdr field identifies the type of the next payload.**
- **Payload Length field specifies the length of AH in 32 bit words.**
- **SPI uniquely identifies the SA in combination with the destination IP address.**
- **SeqNum field contains a monotonically increasing counter to provide anti-replay service.**
- **A session is expired after 2^{32} packets are transmitted.**



AH format

Encapsulating Security Payload (ESP)

- ESP provides authentication and encryption of the payload



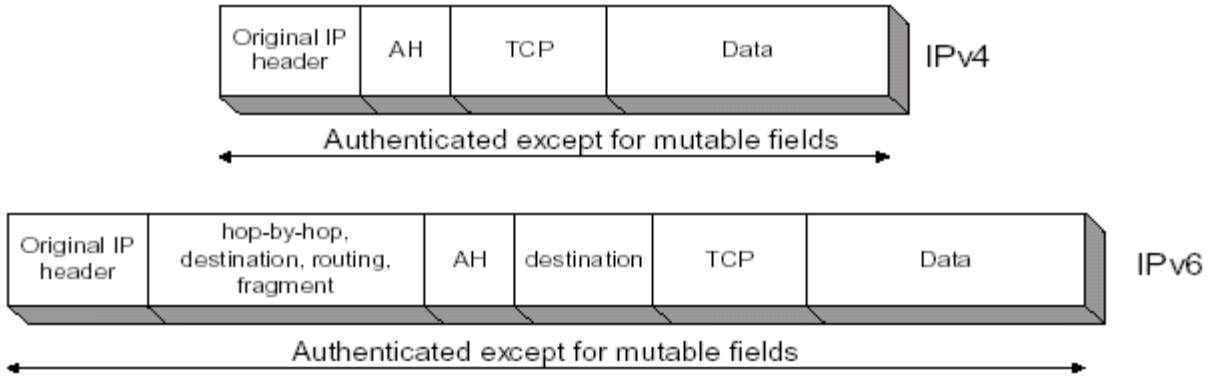
ESP header format

ESP

- SPI , SeqNum provides the same function as in AH.
- PaylaodData contains the data described by the NextHdr field.
- Padding is required as the encryption algorithm requires the plaintext to be multiple of some number or bytes.
- Authentication Data contains the Message Integrity code (MIC) for this packet.

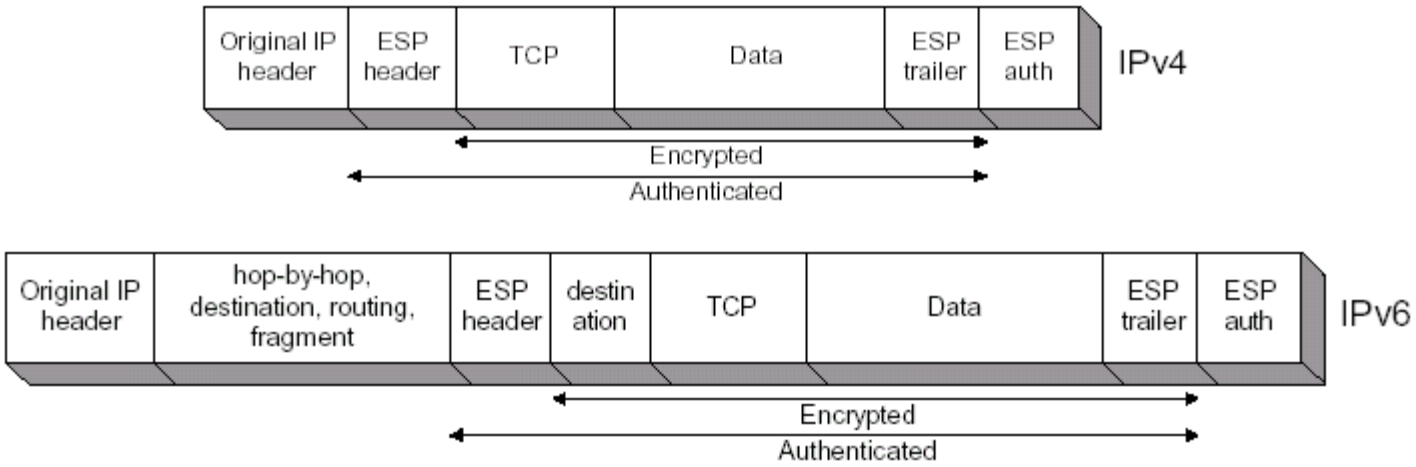
Transport Mode AH

- AH is stronger in this mode as it also authenticates the IP header fields.



Transport Mode AH using IPv4 and IPv6.

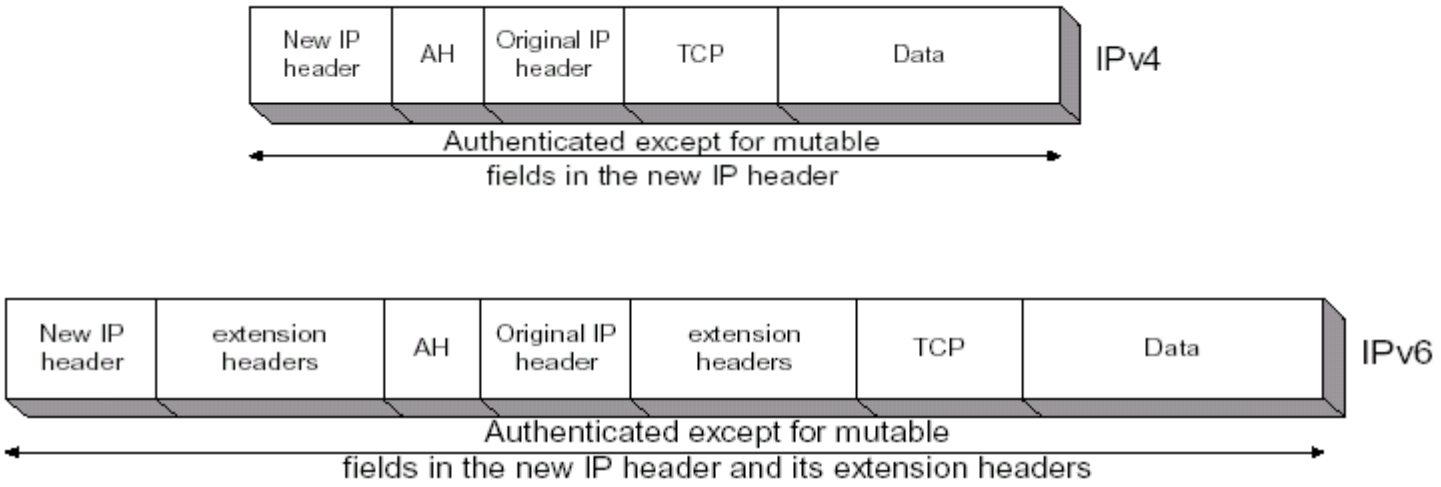
Transport Mode ESP



Transport Mode ESP using IPv4 and IPv6.

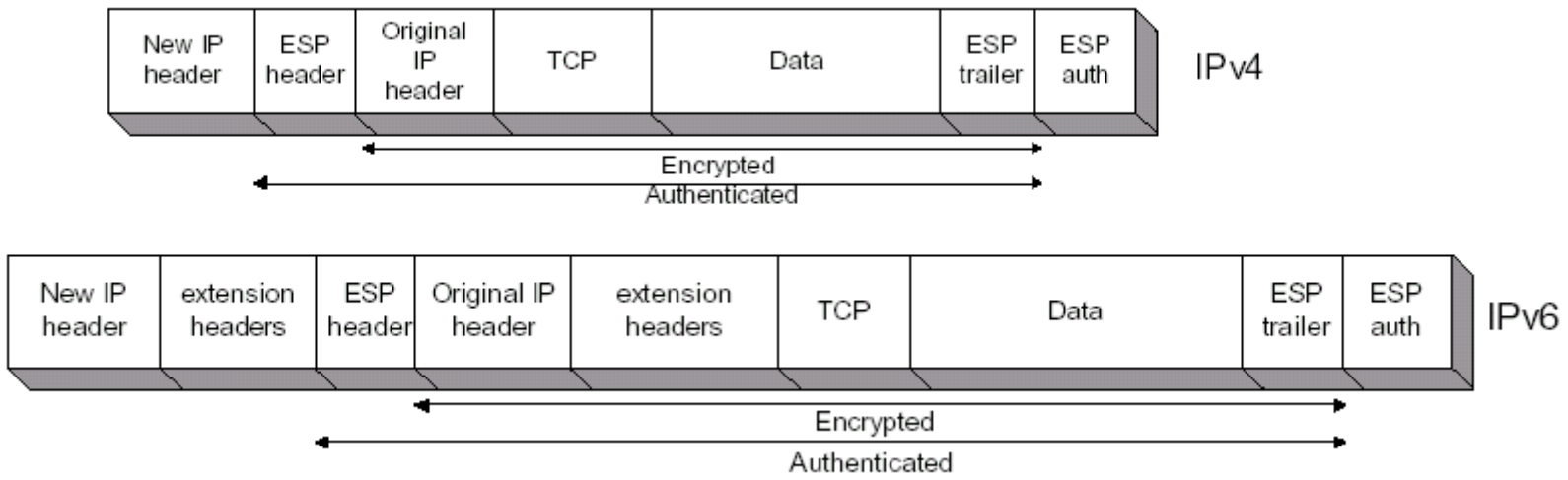
ESP trailer is used for adding the padding and the NextHdr fields.ESP Authentication is used when authentication is carried by ESP

Tunnel Mode AH



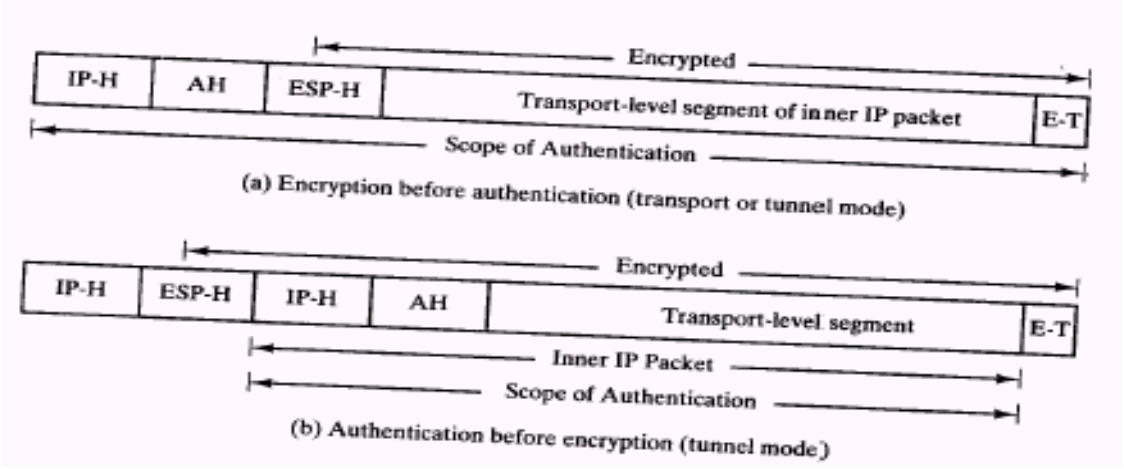
In tunnel mode the payload includes the original IP header.

Tunnel Mode ESP



Tunnel mode ESP using IPv4 and IPv6

Encryption before/after Authentication.



Advantage of applying Authentication before Encryption

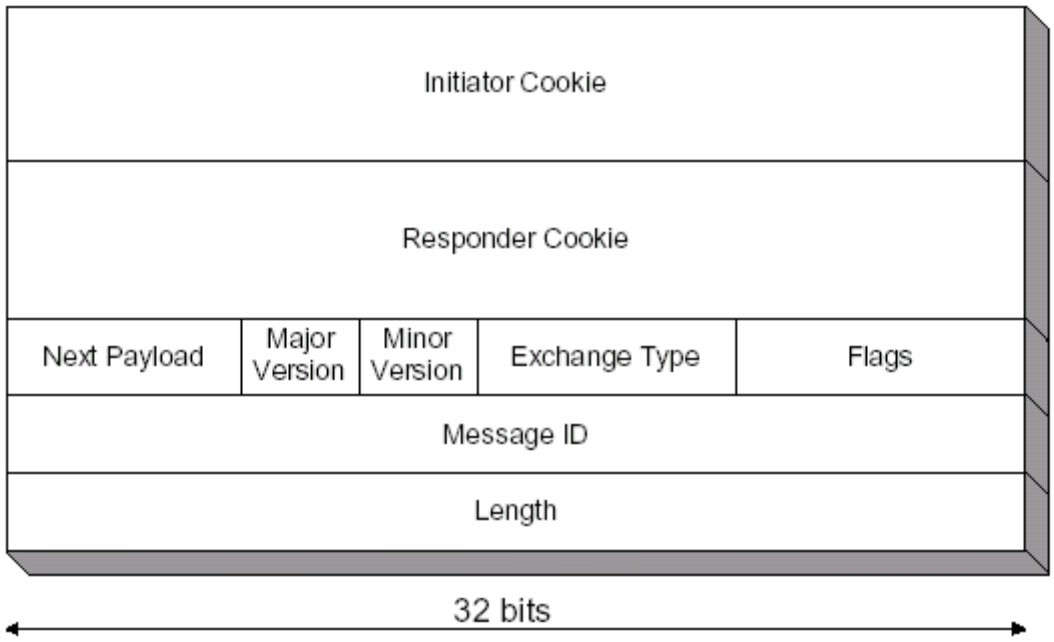
- **Since AH is protected by ESP it is impossible for anyone to intercept the messages and alter the AH without detection.**

- **If it is required to store the Authentication Information is it beneficial as the authentication information applies to the plaintext message and not cipher-text message**

Internet Security Association and Key Management Protocol (ISAKMP)

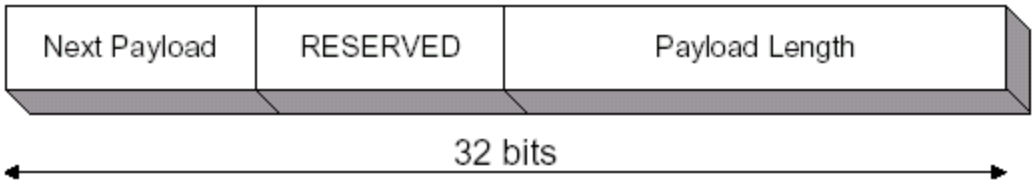
- It's role is to define the procedures and packet formats to establish, negotiate, modify, and delete security associations.
- It defines packet formats for exchanging key (IKE) generation and authentication data.
- It does not specify any specific protocol but provides building blocks for various Domains of Interpretations and Key-Exchange protocols.

ISAKMP



ISAKMP Header Format

ISAKMP



Generic Payload Header.

•The initiator cookie field is cookie that initiated the SA process.

•The responder cookie field contains the cookie of the responding identity.

• A "cookie" or anti-clogging token (ACT) is aimed at protecting the computing resources from attack without spending excessive CPU resources to determine its authenticity. An exchange prior to CPU-intensive public key operations can thwart some denial of service attempts (e.g. simple flooding with bogus IP source addresses).

ISAKMP

- The major and minor version fields indicates the corresponding version of the ISAKMP in use.
- The conventional Payloads are:-

  Security Association (SA), Proposal (P), Transform (T), Key Exchange (KE), Identification (ID), Certificate (CERT), Certificate Request (CR), Hash (HASH), Signature (SIG), Nonce (NONCE), Notification (N), Delete (D).
- There are five types of exchanges

  Base, Identity Protection, Authentication Only, Aggressive and Informational.

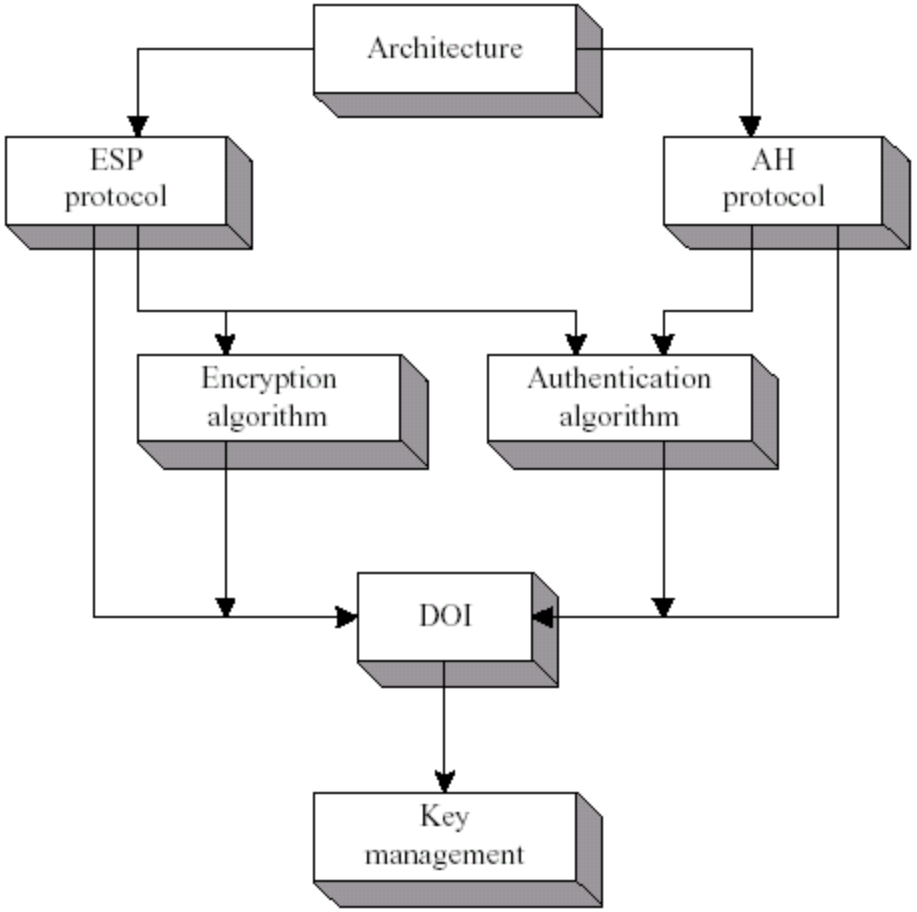
ISAKMP

Base Exchange	
(1) I → R (2) R → I (3) I → R (4) R → I	SA; NONCE SA; NONCE KE; ID(I); AUTH KE; ID(R); AUTH
Identity Protection Exchange	
(1) I → R (2) R → I (3) I → R (4) R → I (5)* I → R (6)* R → I	SA SA KE; NONCE KE; NONCE ID(I); AUTH ID(R); AUTH
Authentication Only Exchange	
(1) I → R (2) R → I (3) I → R	SA; NONCE SA; NONCE; ID(R); AUTH ID(I); AUTH
Aggressive Exchange	
(1) I → R (2) R → I (3)* I → R	SA; KE; NONCE; ID(I) SA; KE; NONCE; ID(R); AUTH AUTH
Informational Exchange	
(1)* I → R	N/D

ISAKMP

- DOI:- Domain of Interpretation: A Domain of Interpretation (DOI) defines payload formats, exchange types, and conventions for naming security-relevant information such as security policies or cryptographic algorithms and modes.
- A Domain of Interpretation (DOI) identifier is used to interpret the payloads of ISAKMP payloads. A system SHOULD support multiple Domains of Interpretation simultaneously.

IPSec Overview.



From the Authors

- Lesson 1: Cryptographic protocols Should not be developed by a committee.

  Benefit is shown by the development of AES.
- Security systems should be simple to test through security reviews.The difficulty of performing security evaluations also increases with increasing complexity.
- Lesson 2:The documentation of a system should include introductory material, an overview for first time readers, states goals, rationale, etc.

From the Authors

- Lesson 3: Authenticate not just the message, but everything that is used to determine the meaning of the message.
- Lesson 4: The properties required of each of the primitive functions used in the system should be clearly documented.

From the Authors

Recommendation 1: Eliminate Transport mode.

Recommendation 2: Eliminate the AH protocol.

Recommendation 3: Modify ESP to always provide authentication; only encryption should be optional.

Recommendation 4: Modify the ESP protocol to ensure that it authenticates all data used in the deciphering of the payload.

Recommendation 5: Encryption Algorithm that have large classes of weak keys that introduce security weakness should simply not be used.

From the Authors

- Recommendation 6: Fix the derivation formulas for SKEYID and associated values.
- Recommendation 7: Fix the definition of HASH values so that it provides proper authentication.
- Recommendation 8: Change the KETMAT derivation in phase 2 to avoid generating the same keys for the two negotiated SA's

Conclusion

- IPSec is too complex, and this leads to large numbers of ambiguities, contradictions and weakness.
- IPSec in its current form is not 100% secure.
- It is either required to decrease the complexity of IPSec and improving the modularization or another alternative is required.

THANK YOU