

IP Security

Lennart Franked ¹

Avdelningen för informations- och kommunikationssystem (IKS),
Mittuniversitetet, Sundsvall.

ipsec.tex 1939 2014-09-01 14:06:04Z danbos

¹ Detta verk är tillgängliggjort under licensen Creative Commons Erkännande-DelaLika 2.5 Sverige (CC BY-SA 2.5 SE). För att se en sammanfattning och kopia av licenstexten besök URL <http://creativecommons.org/licenses/by-sa/2.5/se/>.

Litteratur

The lecture covers chapter 9 “IP Security” in [5]. You should also read section 1 in [3] as a complement to the course literature, to help you grasp the Internet Key Exchange protocol. To check that you have fully understood this chapter, you should solve problems 9.3, 9.6, 9.8 and 9.10.

Översikt

- 1 IPsec
 - IP Security

- 2 Internet Key Exchange
 - IKE

Background

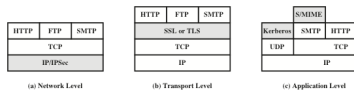
- Lack of security in IP have been discussed since 1994. [1]
- Issue raised by the Internet Architecture Board (IAB).
- Authentication and Encryption features should be included in “Next generation IP”.
- The mechanisms were designed for backwards compatibility.

IPsec usage

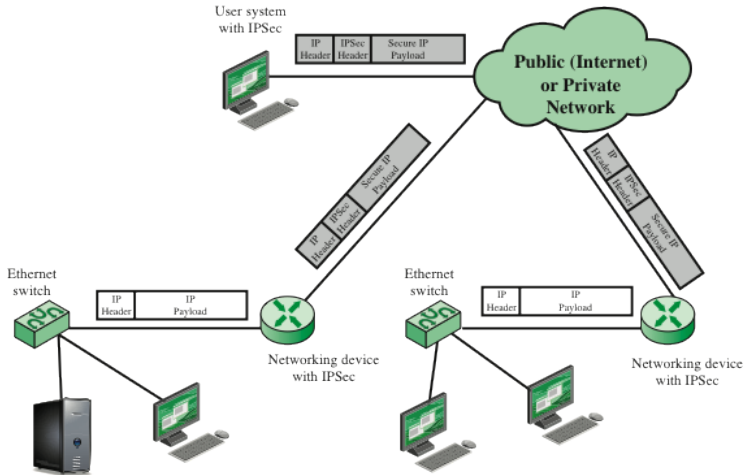
- Secure remote access.
- Secure tunneling.
- Authentication.

IPsec benefits

- Besides the apparent security benefits.
- Transparent to applications.
- Depending on deployment, transparent to users.



Figur : IP security [5]



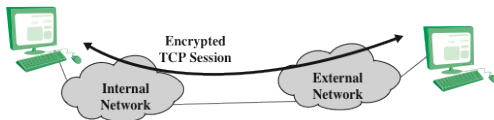
Figur : IPsec deployment scenario [5]

Services provided by IPsec

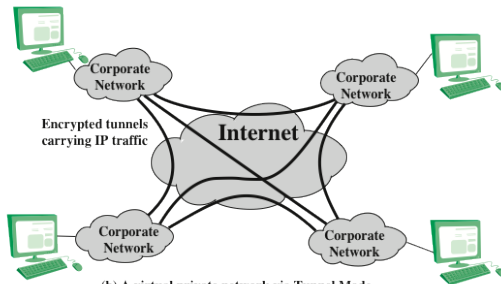
- Access control
- Connectionless integrity
- Data origin Authentication
- Rejection of replayed packets
- Confidentiality
- Limited traffic flow confidentiality

Modes of use

- Transport mode
 - Protects the upper layer protocols.
- Tunnel mode
 - Protects the entire package, including original IP header.

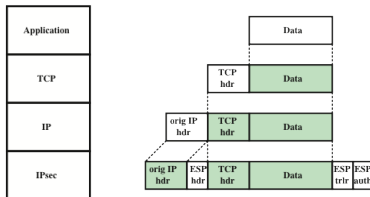


(a) Transport-level security

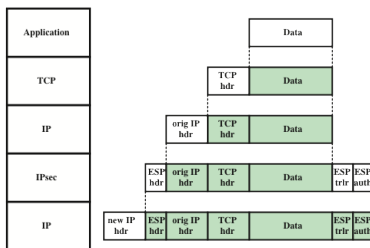


(b) A virtual private network via Tunnel Mode

Figur : Transport vs Tunnel mode[5]

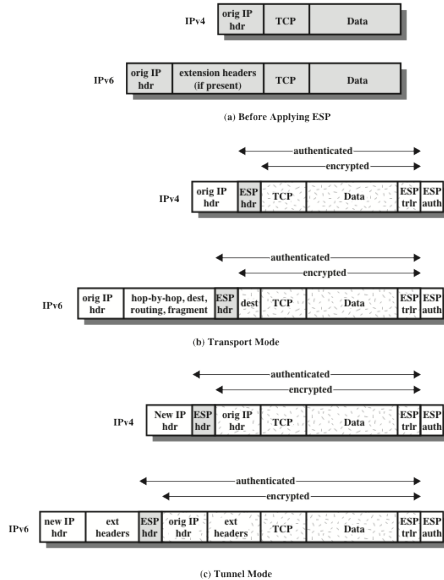


(a) Transport mode



(b) Tunnel mode

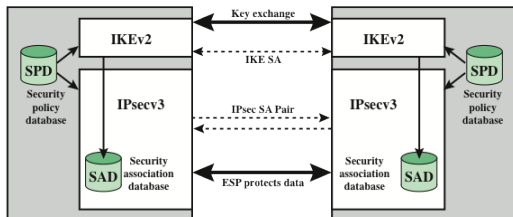
Figur : Transport vs Tunnel mode[5]



Figur : ESP Encapsulation[5]

IPsec policy

- IPsec applies a security policy for each package sent and received.
- Each policy is stored in a Security Policy Database.
- Keeps track of what policy to apply to a package based on Security Associations stored in a SAD.



Figur : IPsec architecture [5]

Security Association

- A one-way logical connection.
- Used to identify a certain connection.
- Identified with three parameters
 - Security Parameter Index – A 32 bit value used as an identifier
 - IP destination address
 - Security Protocol Identifier – AH or ESP

Security Association database

SAD contains the parameters associated with each SA

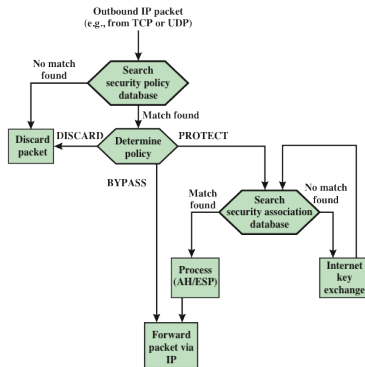
- SPI
- Sequence Number Counter
- Sequence Counter Overflow
- Anti-Replay Window
- AH or ESP information - What algorithms to use
- Lifetime
- Mode of use – Transport/Tunnel
- Path MTU.

Security Policy Database

SPD identifies what IP-traffic should be associated to a SA.
Association is based on:

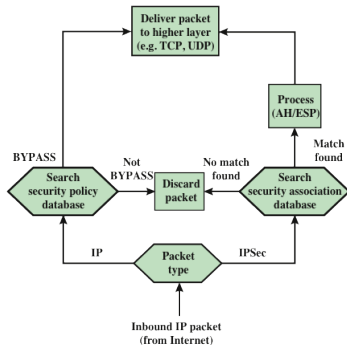
- Remote and local IP address
- Next Layer Protocol
- Name
- Remote and Local Ports

Process outbound packages



Figur : IPsec outbound packages [5]

Process inbound packages



Figur : IPsec inbound packages [5]

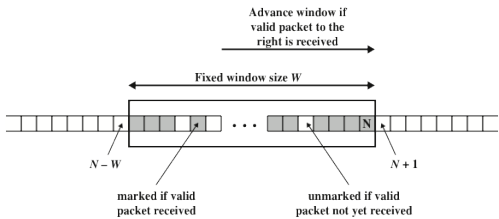
IPsec Anti-Replay

Replay attack

“An attack in which a valid data transmission is maliciously or fraudulently repeated, either by the originator or by a third party who intercepts the data and retransmits it” [4]

- Each SA stores a sequence number counter, that initially is set to 0
- Anti-replay don't allow this counter to exceed $2^{32} - 1$
- if counter is exceeded, a new SA is negotiated.
- Use an anti-replay window to compensate for IPs unreliable and connectionless design.

Anti-Replay Mechanism

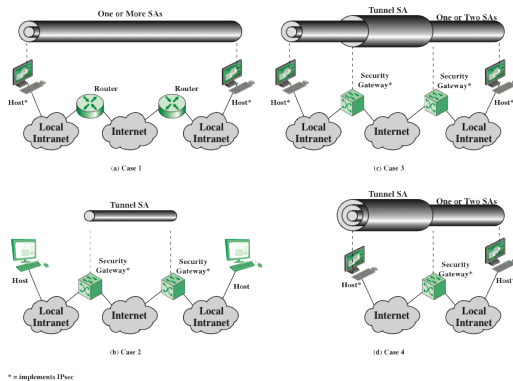


Figur : Anti-Replay window [5]

Combining Security Associations

- A need to combine multiple IPsec services for the same flow.
- Bundles a sequence of SAs
- Each SA might be terminated at a different or the same endpoint.
- Two types of bundles
 - Transport adjacency – Applies multiple security protocols without tunneling.
 - Iterated tunneling – Each security protocol is nested through tunneling.
 - Or a combination of above

Combination of SAs



Figur : Combining Security Associations[5]

Internet Key Exchange

IETF established standard that handles the determination and distribution of the secret keys.

- Two types of key management
 - Manual
 - Automated
 - Oakley – Key exchange protocol based on Diffie-Hellman
 - Internet Security Association and Key Management Protocol (ISAKMP) – A framework for key management. (Same principal as EAP)
 - IKEv2 have implemented a way to use EAP for authentication[2]
- For each IPsec two-way communication, usually four keys need to be created.
 - Two keys for confidentiality
 - Two keys for integrity

IKE Key Determination

Weaknesses in Diffie-Hellman

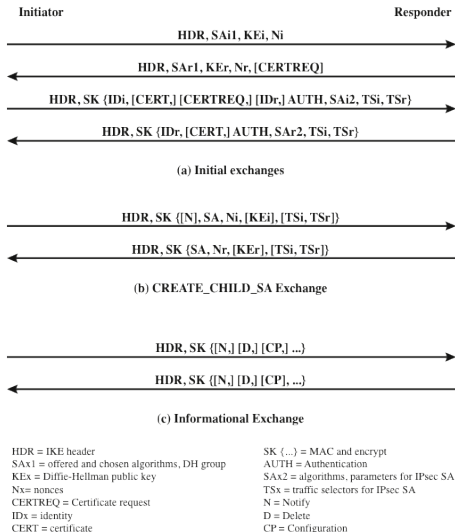
- Doesn't provide any identity information
- Susceptible to a man-in-the-middle attack
- Computationally intensive – clogging attacks.

IKE Key Determination

- Use cookies to counter clogging attacks
- Allows the parties to negotiate the groups to be used for the DH key exchange to increase security.
- Introduce nonces to counter replay attacks.
- Adds authentication to the key-exchange.




IKEv2 consists of four message exchanges [3]

- IKE_SA_INIT – Negotiates security parameters, exchange nonces, cookies and perform DH-key exchange.
- IKE_AUTH – Authenticates previous messages, exchange identities and certificates.
- CREATE_CHILD_SA – Creates an ESP or AH SA for secure communication.
- INFORMATIONAL – Deletes SA, report errors, et cetera.





Figur : IKEv2 Exchanges [5]

Referenser I

-  R. Braden, D. Clark, S. Crocker och C. Huitema. *Report of IAB Workshop on Security in the Internet Architecture - February 8-10, 1994*. RFC 1636 (Informational). Internet Engineering Task Force, juni 1994. URL: <http://www.ietf.org/rfc/rfc1636.txt>.
-  P. Eronen, H. Tschofenig och Y. Sheffer. *An Extension for EAP-Only Authentication in IKEv2*. RFC 5998 (Proposed Standard). Internet Engineering Task Force, sept. 2010. URL: <http://www.ietf.org/rfc/rfc5998.txt>.
-  C. Kaufman, P. Hoffman, Y. Nir och P. Eronen. *Internet Key Exchange Protocol Version 2 (IKEv2)*. RFC 5996 (Proposed Standard). Updated by RFCs 5998, 6989. Internet Engineering Task Force, sept. 2010. URL: <http://www.ietf.org/rfc/rfc5996.txt>.

Referenser II

-  R. Shirey. *Internet Security Glossary, Version 2*. RFC 4949 (Informational). Internet Engineering Task Force, aug. 2007. URL: <http://www.ietf.org/rfc/rfc4949.txt>.
-  William Stallings. *Network security essentials : applications and standards*. 5. utg. International Edition. Pearson Education, 2013. ISBN: 978-0-273-79336-6.