IP Security

Lennart Franked

Department of Information and Communication Systems (ICS), Mid Sweden University, Sundsvall.

13 december 2016



Lennart Franked (MIUN ICS)

< AP

Litterature

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.

Overview







Lennart Franked (MIUN ICS)

イロト イポト イヨト イヨト

Background IP Security

• 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.

- 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.

Image: A matrix

- 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.

Image: A matrix

- 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.

Image: A matrix

• Secure remote access.

- Secure tunneling.
- Authentication.



イロト イロト イヨト イヨト

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



イロト イロト イヨト イヨト

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



イロト イロト イヨト イヨト

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

			HTTP	FTP	SMTP
HTTP	FTP	SMTP	5	SL or TL	3
	TCP			TCP	
	IP/IPSec			IP	

	S/MIME	
Kerberos	SMTP	HTTP
UDP		TCP
		Р

(a) Network Level

(b) Transport Level

(c) Application Level

Figur: IP security [5]



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

HTTP FTP SMTP SSL or TLS TCP TCP					HTTP	FTP	SMTP
	HTTP	FTP	SMTP		5	SL or TL	s
		TCP		1		TCP	
IP/IPSec IP		IP/IPSec		1		IP	

A I >
 A I >
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A

	S/MIME	
Kerberos	SMTP	HTTP
UDP		TCP
		Р

(a) Network Level

(b) Transport Level

(c) Application Level

Figur: IP security [5]



A B M A B M

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

			HTTP	FTP	SMTP	
HTTP	FTP	SMTP	5	SL or TL	3	Ke
	TCP			TCP		
	IP/IPSec			IP		

A I >
 A I >
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A

	S/MIME	
Kerberos	SMTP	HTTP
UDP		TCP
		Р

(a) Network Level

(b) Transport Level

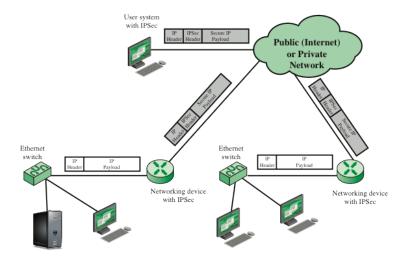
(c) Application Level

Figur: IP security [5]



A B M A B M

IP Sec deployment IP Security



Figur: IPsec deployment scenario [5, Fig. 9-1]



7 / 29

Lennart Franked (MIUN ICS)

IP Security

イロト イポト イヨト イヨト

Access control

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



< AP

Access control

Connectionless integrity

- Data origin Authentication
- Rejection of replayed packets
- Confidentiality
- Limited traffic flow confidentiality



- A 🖓

Access control

• Connectionless integrity

• Data origin Authentication

- Rejection of replayed packets
- Confidentiality
- Limited traffic flow confidentiality



< A

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



- A 🖓

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



< A

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



< A

Transport mode

• Protects the upper layer protocols.

Tunnel mode

• Protects the entire package, including original IP header.



∃ → (∃ →

A I >
 A I >
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A

Transport mode

• Protects the upper layer protocols.

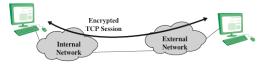
Tunnel mode

• Protects the entire package, including original IP header.

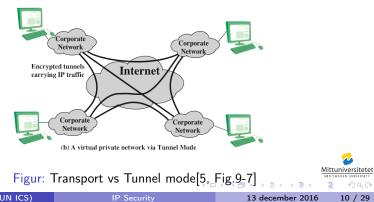


- A - E - N

Transport mode vs. Tunnel mode **IP** Security

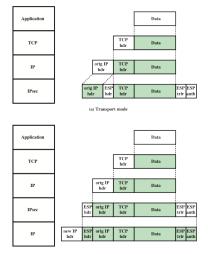


(a) Transport-level security



Lennart Franked (MIUN ICS)

Transport mode vs. Tunnel mode IP Security



(b) Tunnel mode

Figur: Transport vs Tunnel mode[5, Fig. 9-9]



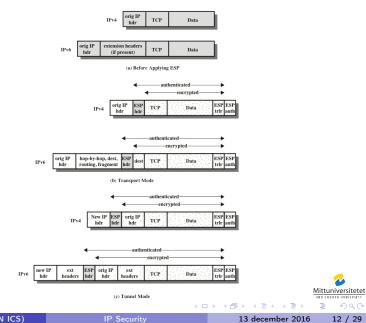
11 / 29

Lennart Franked (MIUN ICS)

IP Security

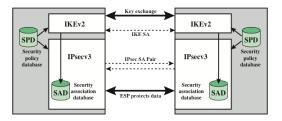
イロト イヨト イヨト イヨト

Transport mode vs. Tunnel mode **IP** Security



IPsec policy IP Security

- 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, Fig. 9-2]



IPsec policy IP Security

- 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, Fig. 9-2]



IPsec policy IP Security

- 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, Fig. 9-2]



• 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

E 5 4 E 5

Mittuniversitetet

• 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

글 > - - - 글 >

Image: Image:

Mittuniversitetet

- 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

E 6 4 E 6

- 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

b 4 To b

- 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

E 6 4 E 6

- 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

E 6 4 E 6

Security Association database IP Security

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 Association database IP Security

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.



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.



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.



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.

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.

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.

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.



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

∃ → (∃ →

Security Policy Database IP Security

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

dittuniversitetet

Security Policy Database IP Security

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

∃ → (∃ →

dittuniversitetet

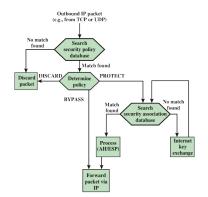
Security Policy Database IP Security

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

Mittuniversitetet

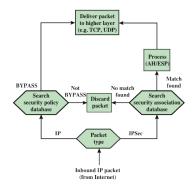
Process outbound packages IP Security



Figur: IPsec outbound packages [5, Fig. 9-3]

Mittuniversitetet

Process inbound packages IP Security



Figur: IPsec inbound packages [5, Fig. 9-4]

Lennart Franked (MIUN ICS)

13 december 2016 18 / 29

イロト イポト イヨト イヨト

Mittuniversitetet

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, page. 249]

- 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.

크 에 관리

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, page. 249]

• 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.

같아. 김 같아

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, page. 249]

- 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.

크 에 관리

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, page. 249]

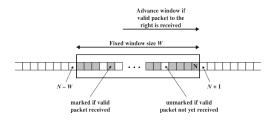
- Each SA stores a sequence number counter, that initially is set to 0
- Anti-replay don't allow this counter to exceed $2^{32}-1$
- if counter is exceeded, a new SA is negotiated.
- Use an anti-replay window to compensate for IPs unreliable and connectionless design.

Image: Image:

토) (토)

13 december 2016

Anti-Replay Mechanism IP Security



Figur: Anti-Replay window [5, Fig. 9-6]



Image: A matrix and a matrix

• 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



• 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



- 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

글 > - - - 글 >

- 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



E 5 4 E 5

- 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

글 > - - - 글 >

- 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

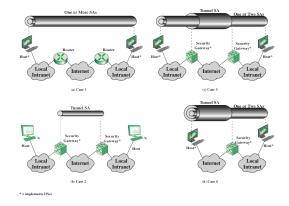
- Transport adjacency Applies multiple security protocols without tunneling.
- Iterated tunneling Each security protocol is nested through tunneling.
- Or a combination of above

- 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 **IP Security**



Figur: Combining Security Associations[5, Fig. 9-10]



Image: A matrix and a matrix

Overview







Lennart Franked (MIUN ICS)

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

Key management

- Manual
- Automated
 - ${\sf Oakley-Key\ exchange\ protocol\ based\ on\ Diffie-Hellman}$
 - 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

E 5 4 E 5

A I >
 A I >
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A

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

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

E 5 4 E 5

A I >
 A I >
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A

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

- 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

E 5 4 E 5

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

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

E 5 4 E 5

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

Key management

- Manual
- Automated
 - Oakley Key exchange protocol based on Diffie-Hellman
 - nternet 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

(B)

A I >
 A I >
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A
 A

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

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

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

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

24 / 29

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

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

24 / 29

IKE Key Determination IKE

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.



IKE Key Determination IKE

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.



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.



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.



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.



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.



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 extra layer for secure communication.
- INFORMATIONAL Deletes SA, report errors, et cetera.



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 extra layer for secure communication.
- INFORMATIONAL Deletes SA, report errors, et cetera.



A B A A B A

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 extra layer for secure communication.
- INFORMATIONAL Deletes SA, report errors, et cetera.



A B F A B F

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 extra layer for secure communication.
- INFORMATIONAL Deletes SA, report errors, et cetera.



IKE Message Exchange II IKE

Initiator	Responder
HDR, SAi1, KEi, Ni	
HDR, SAr1, KEr, Nr, [CERTREQ]	
HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr}	
HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr}	
(a) Initial exchanges	
HDR, SK {[N], SA, Ni, [KEi], [TSi, TSr]}	
HDR, SK {SA, Nr, [KEr], [TSi, TSr]}	
(b) CREATE_CHILD_SA Exchange	
HDR, SK {[N,] [D,] [CP,]}	
HDR, SK {[N,] [D,] [CP],}	
(c) Informational Exchange	
HDR = IKE header SAV1 = offered and chosen algorithms, DH group KEx = DIffice Hellmann public key Nxe nonces CHRTREQ = Certificate request IDx = identity CERT sectificate	SK {} = MAC and encrypt AUTH = Authentication SAx2 = algorithms, parameters for IPsec SA TSx = traffic selectors for IPsec SA N = Notify D = Delete CP = Configuration



27 / 29

Figur: IKEv2 Exchanges [5]

Lennart Franked (MIUN ICS)

IP Security

13 december 2016

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, P. Eronen och T. Kivinen. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 7296 (INTERNET STANDARD). Internet Engineering Task Force, okt. 2014. URL: http://www.ietf.org/rfc/rfc7296.txt.
- R. Shirey. Internet Security Glossary, Version 2. RFC 4949 (Informational). Internet Engineering Task Force, aug. 2007. URL: http://www.ietf.org/rfc/rfc4949.txt.

Referenser II



William Stallings. *Network security essentials : applications and standards.* 5. utg. International Edition. Pearson Education, 2013. ISBN: 978-0-273-79336-6.

