Comparative Analysis of Internet Key Exchange Protocols

Safdar Hussain Shaheen
safdarhussainshaheen@yahoo.com
Riphah International University
Islamabad, Pakistan

Muhammad Yousaf
muhammad.yousaf@riu.edu.pk
Riphah International University
Islamabad, Pakistan

Muhammad Younas Majeed
myounas_m@yahoo.com
Quaid-I-Azam University
Islamabad, Pakistan

***Abstract*—Internet Key Exchange (IKE) protocol is a vibrant component of Internet Security protocol (IPSec). It plays a vital role to accomplish the tasks of negotiation and establishment of security parameters, generation and management of cryptographic keys, mutual authentication of participating peers and establishing security associations. Since the IPSec security relies primarily on secure IKE, therefore the review and analysis of IKE versions is essential prior to their deployment in IPSec. This paper not only reviews the versions 1 and 2 of IKE but also presents a comparative analysis of these key management protocols.**

Keywords- IPSec; IKE; Key Management; Comparative Analysis;

I. INTRODUCTION

The key management is a vivacious component of any modern cryptographic protocol. In IPSec, this task is accomplished through IKE [1]. IKE is used for negotiation and establishment of security parameters, generation and management of cryptographic keys, mutual authentication of participating peers and establishing security associations. As far as IPSec [2, 26] is concern, it is a suite of protocols used to provide security services such as confidentiality, data integrity and authentication on IP layer. The main protocols involved in IPSec are Authentication Header (AH) [3], Encapsulating Security Payload (ESP) [4] and Internet Key Exchange Protocol (IKE). AH is used for assuring authentication and protection of integrity of data whereas the confidentiality along with integrity (optional) is achieved through ESP. The key management in IPSec can be accomplished by using IKE version 1 [5] or 2 [6, 7, 8]. Both of these allow the communicating entities to derive session keys via a series of round trips for secure communication. However, both are incompatible to each other because of their different working scenarios. For example one works in the form of phases and modes whereas other uses request/response mechanism. The number of rounds is also dissimilar between these management protocols. Higher number of rounds, various options and huge specifications in IKE protocol raise its complexity. The other issues include perfect forward security and denial of service (DOS) attack. Therefore, prior to the deployment of any of these versions, their review and comparative analysis is indispensable. This study focuses on both of these versions.

Rest of the article is arranged as follows. Section II gives an overview of the selective related work. Section III illustrates framework of IKEv1 and IKEv2 in detail. Section IV presents the comparative analysis of both versions. Finally, suggestion and concluding remarks are given in Section V.

II. LITERATURE REVIEW

The first analysis about IKE, based on pure mathematics, was performed by R. Canetti and H. Krawczyk [9] in 2001 and 2002. Although, this analysis was conducted systematically, but it has inherited implementation complexity pointed out by many researchers [10] later on. Then a non-mathematical analysis on IKE was performed by Zhou [11]. He suggested some modifications and inclusion of additional payloads in the main phase of IKEv1. However, since the IKEv1 is already considered as a complex [12] protocol, the implementation of proposed suggestions can further lead to higher degree of complexity. Meadow [13] analyzed the security of IKEv1 using Prolog based security tools. The secrecy, authentication and perfect forward secrecy in IKEv1 was also analyzed by her through expert analyzing systems located in Navy Research Labs (NRL). She pointed out some minor obscurities in IKEv1 specification which can become a source of attacks. A manual logical analysis of IKEv1 [10, 20] was conducted by Perlman Kaufman in 2000 and 2001. Many of their suggestions were included in IKEv2 standard. K. Okhee and D. Montgomery [14] conducted various tests based on network simulator NIIST (NIST IPsec and IKE Simulation Tool) to examine the behavior of IKEv1 in a large scale VPN. Resultantly, several routing problems for a VPN simulation of considerable size were indicated. Most of the analysis is made on IKEv1 by the researchers and limited study is available on the latest version of IKEv2. Although, a few analyses are available in the literature about IKEv1 and IKEv2, but hardly a comparative analysis of both is available. Therefore, to investigate, compare and evaluate the better one out of them in terms of security, their review and comparative analysis is vital. The present study not only reviews the versions 1 and 2 of IKE but also constitutes a comparative analysis of these key management protocols.

III. THE INTERNET KEY EXCHANGE

The Internet Key Exchange (IKE) is a fundamental component of Internet Protocol Security (IPSec). For secure communication in IPSec, two types of security associations (SA) termed as IKE SA and IPSec SA are required. Basically, the IKE performs mutual authentication and establishes an IKE SA between two IPSec enabled parties. Furthermore, it is used to exchange security parameters and to generate shared common keys to ensure confidentiality, integrity and authentication between these communication peers. Finally, it negotiates and establishes IPSec SA which is used to attain confidentiality and integrity of data at transient. Additionally it allows IPSec enabled peers to renegotiate SAs and security parameters dynamically at any time for

attaining Perfect Forward Security (PFS). The prominent initiators of IKE protocols are Photuris [15], SKEME [16], Oakley [17] and SIGMA [18]. The existing versions of IKE are 1 and 2. To constitute a comparative analysis, the review of both key management protocols is essential which is outlined here as a first step for further analysis and assessment.

A. IKEv1

The design of IKEv1 [1] is based on Oakley Key Determination Protocol (OKDP) [17] and Internet Security Association and Key Management Protocol (ISAKMP) [19]. ISAKMP protocol provides a framework for exchanging encryption keys and SA payloads. IKE also provides the facility of a key agreement through Diffie-Hellman key exchange protocol [21]. The authentication techniques offered by IKEv1 are; Pre-shared Key [22], Digital Signature [23] and Public key cryptography [24, 25]. It uses same SA for both the inbound and outbound traffic. IKEv1 has been categorized into two phases namely phase1 and phase2. Phase 1 is used to negotiate and establish IKE SA between IPSec enabled peers. The secret common key derivation by using negotiated Diffie-Hellman tokens and peer authentication is also accomplished in this phase. The secret common keys derived in phase 1 are further utilized to protect the traffic in phase 2. Figure 1 shows the hierarchical view of different phases involved in IKEv1 and modes of operation.

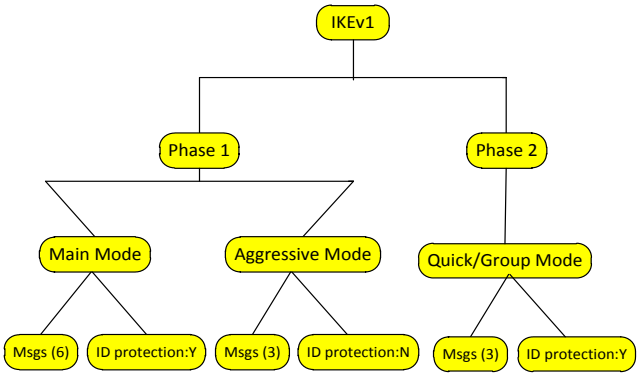

Figure 1: Classification of IKEv1 Resources

The tasks of phase 1 are accomplished through one of the two modes namely Main Mode (MM) or Aggressive Mode (AM). The MM is responsible for exchanging security parameters between authenticated peers. It also supports identity protection of participating peers. This mode comprises of six message round trips to accomplish the key management and security association. Whereas AM requires three message round trips to exchange the security parameters. Although this mode is quicker than MM, however, it does not protect the identity of endpoint peers which makes it less secure than the MM. The round trips involved in MM are shown in Figure 2 and those involved in AM are shown in Figure 3.

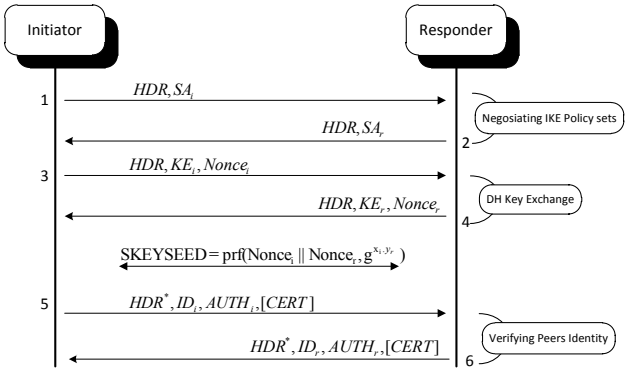

Figure 2: Steps of Messages exchange in Main Mode

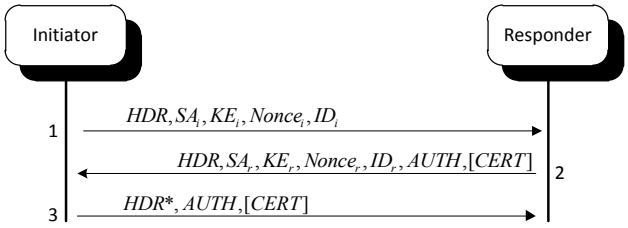

Figure 3: Steps of messages exchange in Aggressive Mode

Phase 2 negotiates the ciphers and authentication algorithms required to establish IPSec SA. Figure 2 and Figure 3 is based on Digital Signature whereas similar procedure can be used for Public Key and Pre-Shared. There is only one mode of operation in phase 2 named as Quick Mode (QM) which is accomplished in three message round trips. It utilizes the shared secret key established in phase 1 to derive several shared secret keys. These keys are used to establish or update the session keys in an IPSec tunnel. QM cannot work independently rather it depends on the secure channel established in phase 1. In this mode, not only the Nonce can be re-exchanged to resist against replay attacks but The Diffie-Hellman key exchange procedure can also be repeated to attain the Perfect Forward Security (PFS). Moreover, the identity protection is also provided by QM. Figure 4 reflects the messages exchanged in QM.

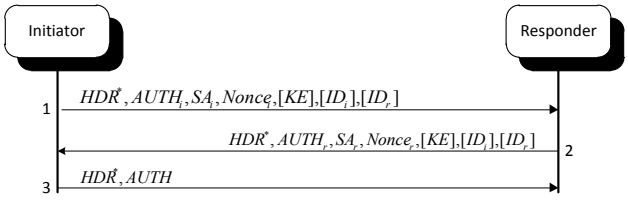

Figure 4: Messages exchange in Quick Mode

B. IKEv2

Various critiques on IKEv1 have led the authors to device IKEv2. It is the latest existing version of IKE [6] with numerous enhanced security features over IKEv1. Instead of modes; it works in the form of request and response scenario. Every request requires a response in this protocol. Also, separate SAs are negotiated and established for inbound and outbound traffic. We have divided IKEv2 into three categories, namely "IKE Initialization Phase", "IPSec SA" and "Re-Configuration

SA", just for the sake of simplicity. Figure 5 illustrates events flow mechanism and categorization in IKEv2.

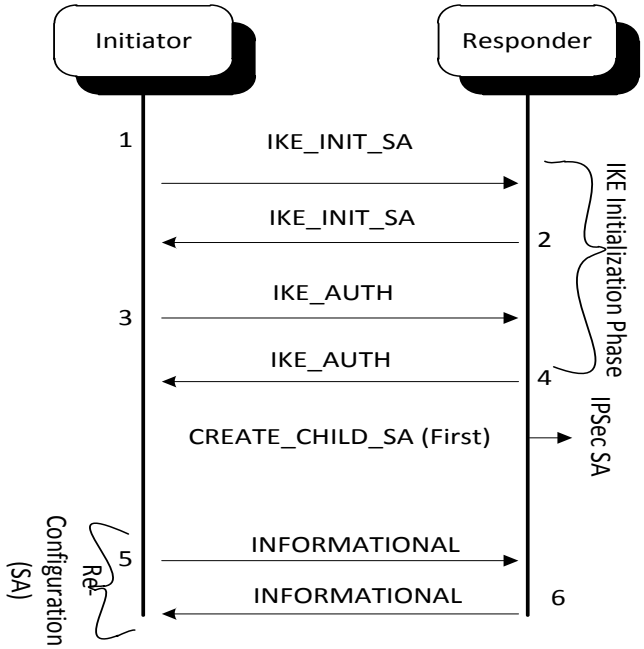

Figure 5: Key management mechanism in IKEv2

1) IKE Initialization Phase

The IKE Initialization phase is used to establish IKE SA and IPSec SA. It is classified into two parts namely IKE_SA_INIT exchange and IKE_AUTH exchange. The tasks to establish IKE SA are accomplished by initiating IKE_SA_INIT exchange. The cryptographic algorithms and security parameters such as Nonce and Diffie-Hellman parameters for key management are negotiated in IKE_SA_INIT exchange through two round trips. After this exchange, the negotiated key material is further used by each peer to derive the shared symmetric keys for authentication and encryption. At this stage, although both the peers agreed on these cryptographic keys but they still require authentication of each other. For this purpose the IKE_AUTH exchange is commenced and two round trips involved in this exchange are masked through these shared symmetric keys. The establishment of IPSec SA as a first Child SA and peer authentication is done through IKE_AUTH exchange. This authentication can be accomplished using digital signatures, Extensible Authentication Protocol (EAP), or pre-shared keys mechanisms. The specification of protocols involved in IKE_SA_INIT exchange phase contains some optional fields. These fields allow initiator and responder to use distinct encryption and authentication techniques. In the case of failure of authentication peers, IKE SA negotiated in IKE_SA_INIT is dismissed. Additional key agreement material may also be exchanged in IKE_AUTH to generate fresh keys for IPSec enabled peers for security enhancement as a PFS. After completion of IKE_AUTH exchange, the first IPSec SA is created through CREATE_CHILD_SA. In case, additional PFS is required, some other security associations can also be established using CREATE_CHILD_SA in two further round trips. IKE Initialization phase is demonstrated in Figure 6.

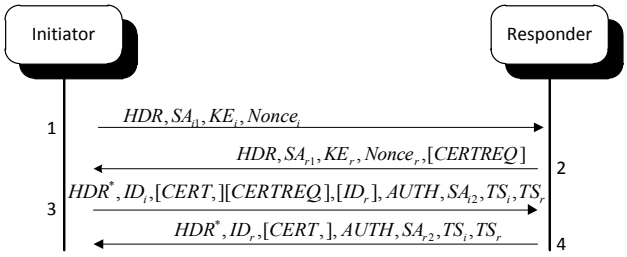

Figure 6: Round trips in IKE SA

2) IPSec SA

On completion of IKE_AUTH exchange, the negotiated SAs and keys are used to create IPSec SA through first CHILD SA for protecting data at transient. For better security, it is necessary to refresh the keys after a certain amount of time. Therefore, the rekeying or fresh security associations can also be established by launching CREATE_CHILD_SA exchange in two further round trips for providing Perfect Forward Security (PFS). The CREATE_CHILD_SA exchange is illustrated in Figure 7.

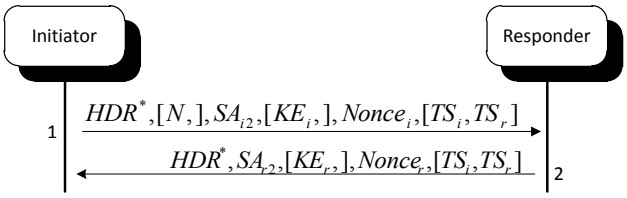

Figure 7: Messages exchange scenario in CREATE_CHILD_SA

3) Re-Configuration SA

The INFORMATIONAL exchange is the last exchange in IKEv2 having two further rounds of messages. Two additional round trips are required for its execution. The primary objective of this exchange is to the check keep alive, the re-configuration of an SA, sending notification about creating new SA, deletion of old SA and errors handling. Figure 8 shows INFORMATIONAL exchange of IKEv2.

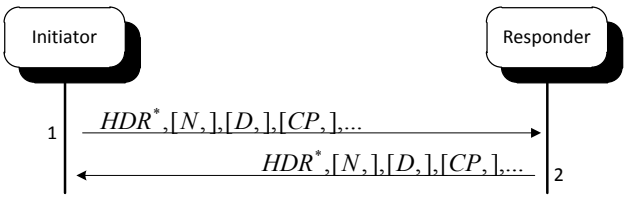

Figure 8: FORMATIONAL Method

C. Derivation of keying material and Hashing Value

In IKEv1, a common secret key named SKEYSEED is derived from the secret material known only to the communicating peers. The secret material contains the pre-shared key, the secret nonce, cookies and Diffie-Hellman secret parameters. Since, the generation of SKEYSEED depends upon authentication methods supported by IKEv1. Therefore, different combinations of key material are fed to Pseudo-Random Function (PRF)

for generating SKEYSEED in accordance with the authentication methods. Following are the SKEYSEED derivation methods with respect to authentication methods;

The secret key derivation through Pre-Shared Key:

$$SKEYSEED = \text{prf}(Pre - SharedKey, Nonce_i || Nonce_r) \quad (1)$$

The secret key derivation using digital signature:

$$SKEYSEED = prf\,(Nonce_i || Nonce_r, g^{x_i y_r}) \quad (2)$$

The secret key derivation through public key technique:

$$SKEYSEED = prf\,((H(Nonce_i || Nonce_r), CKY_i\ || CKY_r) \quad (3)$$

The shared secret SKEYSEED computed from either of the above authentication schemes is used to derive necessary secret keying material for authentication, encryption and computation of fresh keying material for new negotiated SAs. The feedback key expansion function used to derive the keying material is shown in Figure 9.

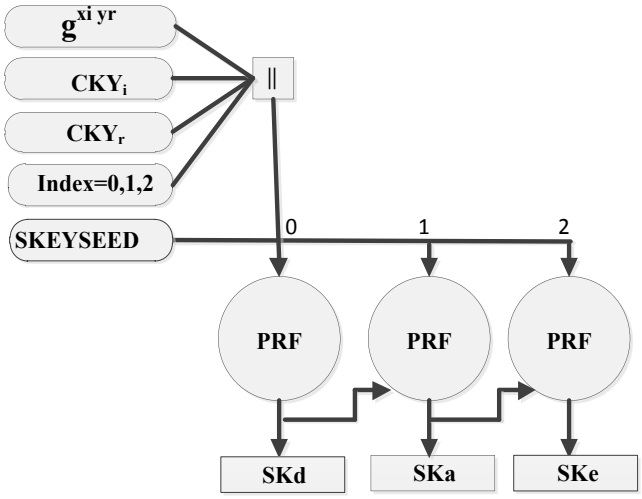

Figure 9: Keying material derivation mechanism

The mathematical representation of this function is:

$$(SK_d, SK_a, SK_e) = \text{prf} + (SKEYSEED, g^{x_i y_r} || CKY_i || CKY_r)$$

whereas,

$$SK_d = \text{prf}(KEYSEED, g^{x_i y_r} || CKY_i || CKY_r || 0)$$

$$SK_a = \text{prf}(KEYSEED, SK_d || g^{x_i y_r} || CKY_i\ || CKY_r || 1)$$

$$SK_e = \text{prf}(KEYSEED, SK_a || g^{x_i y_r} || CKY_i\ || CKY_r || 2)$$

SK_d is used for deriving fresh keying material for new established SAs, SK_a is used for authentication and SK_e is used for encryption in IKEv1. IKEv1 also offers the service of protection integrity. The computation mechanism of hashing value for integrity protection is pictorially shown in Figure 10. Mathematically it can be denoted as

$$AUTH_i = \text{prf}(SKEYSEED, g^{x_i} || g^{y_r} || CKY_i || CKY_r || SA_i || ID_i)$$

$$AUTH_r = \text{prf}(SKEYSEED, g^{y_r} || g^{x_i} || CKY_r || CKY_i || SA_r || ID_r)$$

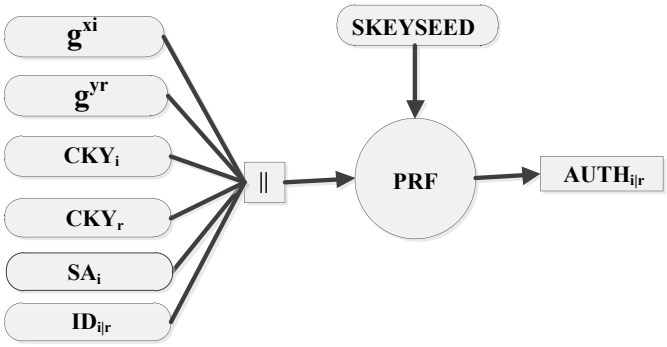

Figure 10: Integrity computation method

The key derivation mechanism in IKEv2 is almost similar as in IKEv1. The only difference is that instead of calculating three keys from SKEYSEED, seven keys are derived in IKEv2. Three of which are used for inbound traffic, three for outbound traffic and one for keys derivation for new SAs. In contrast to IKEv1 which offers three authentication methods, the IKEv2 provides the support of only one authentication method that is Digital Signature. The SKEYSEED in IKEv2 is computed in similar fashion as by IKEv1 using equation (2). The keying material using SKEYSEED are derived as follow:

$$(SK_d, SK_{ai}, SK_{ar}, SK_{ei}, SK_{er}, SK_{pi}, SK_{pr}) = \text{prf} + (SKEYSEED, Nonce_i || Nonce_r || SPI_i || SPI_r)$$

Where the keys SK_{ei} and SK_{er} are used for encrypting Initiator and Responder data in IKEv2; SK_{ai} and SK_{ar} are used for integrity protection; SK_{pi} and SK_{pr} are used in generating IKE_AUTH payload and SK_d is used for deriving fresh keys for CHILD SAs. The session resumption option is also available in IKEv2.

Table 1 sum up some notations along with their description used in IKEv1 and IKEv2:

Table 1: Notations used in IKEv1 and IKE 2

Notations	Description
HDR	ISAKMP header
SA	Security Associations for IKE or IPSec
$Notation_{subscript}$	i in subscript denote Initiator and r Responder
SA_i	SA payload from Initiator contain one or more proposals
SA_r	SA proposal selected by Responder
KE	Diffie-Hellman Key Exchange public value that is g^{xi} or g^{yr}
g^{xi}, g^{yr}	DH parameters for Initiator and Responder
$\|\|$	Concatination operation
$Nonce_i$, $Nonce_r$	Nonce of Initiator and Responder
ID_i, ID_r	Identity of Initiator and Responder
[]	Optional parameters

$AUTH_i$, $AUTH_r$	Authentication payload: Hashes of previous parameters negotiated
*	Encryption must begin after the header
CKY_i , CKY_r	Cookies of Initiator and Responder
$SKEYSEED$	Shared secret key
SK_d	Keys derivation key
SK_a	Integrity protection key
SK_e	Encryption Key
SK_p	Authentication Key
prf (PRF)	Pseudo-Random Function such as HMAC-PRF
$CERT$	Certificate of Initiator or Responder (payload)
$CERTREQ$	Certificate Required
$AUTH$	Authentication payload
TS_i, TS_r	Traffic selector for Initiator, Responder
N	Notify payload
D	Delete payload
CP	Configuration Payload
SPI	Security Parameter Index

IV. COMPARATIVE ANALYSIS

Based on the review c.f. section III and references herein, the main features of IKEv1 and IKEv2 are shown in Table 2.

Table 2: Comparison between IKEv1 and IKEv2

Features	IKEv1	IKEv2
IKE Security Association (SA)	Phase1: Main or Aggressive Modes	IKE Initialization phase
IPSec Security Association (SA)	Phase2: Quick Mode	Child SA (Changed)
Round trips for IKE SA	Main Mode: 4 Aggressive Mode: 3 Quick Mode: 3 Total: 6 or 7	Request/Response IKE_INIT_SA: 2 IKE_AUTH_SA: 2 Total : 4
First CHILD SA	Required 3 messages	No message required
CHILD SAs	3 messages	2 messages
Authentication methods supported	1.Pre-Shared Key (PSK) 2. Digital Signature (RSA-Signature) 3.Public Key Encryption 4. Revised Mode of Public key Encryption	1. Pre-Shared Key (PSK) 2. Digital Signature (RSA-Signature)
Authentication mechanism for Source and Destination peers	Both peers must use the same authentication method	Each peer can use a different authentication method
Categorization	Phases and modes	Only one straight forward exchange procedure
Rekeying	Not defined	Defined for Perfect Forward Security (PFS)
Multi-Homing	Not supported by default	Supported
Attacks	DoS, downgrade, impersonation : protection not supported by default	DoS, downgrade, impersonation: Protection support available by default Replay: Anti-replay function is embedded for replay attack.
Identity protection	Main mode and Quick mode support but Aggressive mode does not support	Identity protection available
Retransmission and acknowledgement	Not supported	Support available
Lifetime for SAs		
Reliability	Less reliable than IKEv2	More reliable than IKEv1
Lifetime for SAs	Explicitly negotiated therefore agreement between peers is required	NOT negotiated. Each peer maintains its own local policy for Security Association lifetime and can be deleted and a rekeying operation is initiated when the lifetime is about to expire by exchanging DELETE payloads
Dead Peer Detection / Keep-alive for SAs	Defined as an extension	Supported by default
Remote Access VPN	NOT defined. Vender-specific implementations are – Mode config – XAUTH	Supported by default: – Extensible Authentication Protocol (EAP) – User authentication over EAP is associated with IKE's authentication. – Configuration payload (CP)
NAT Traversal	Defined as an extension	Supported by default
Traffic selector	Only a combination of a source IP range, a destination IP range, a source port and a destination port is allowed per IPsec SA. Exact agreement of the traffic selector between peers is required	– Multiple combinations of a source IP range, a destination IP range, a source port range and a destination port range are allowed per Child SA. Of course, IPv4 and IPv6 addresses can be configured for the same Child SA.

		– Narrowing traffic selectors between peers is allowed.
Mobile Clients	NOT supported	Supported by MOBIKE
Extensions	Very Poor	Very useful in network environment
Specifications	Many	Few
Security Association	Same for inbound and outbound traffic	Different for inbound and outbound traffic
Framework	Complex	Simpler

IKEv1 has various phases and mode of operations along with the support of many cryptographic algorithms for negotiating and establishing of IKE SA and IPSec SA whereas IKEv2 has only one straight forward procedure to accomplish such tasks. Also, nine round trips are required to establish security associations in IKEv1 in comparison with IKEv2, which needs only four round trips. The higher number of round trips, various modes of operation, bulky specifications, poor extensions and numerous cryptographic options results in an increase in the complexity of IKEv1. Furthermore, it does not resist against DoS, downgrade and impersonation attacks by default. The attacker can exploit these vulnerabilities to break the security of this protocol. It also lacks in multi-homing, retransmission and acknowledgement capabilities. Moreover, Security Association lifetimes require to be explicitly negotiated in IKEv1 whereas it is available as a built-in feature in IKEv2. Each peer in IKEv2 maintains its own local policy for Security Association lifetime. When the lifetime is about to expire, a rekeying operation is initiated. The aforementioned issues in IKEv1 remain a major hurdle for its wide spread implementation. Consequently, the IKEv2 is simpler, easier, straight forward, flexible, secure and versatile than IKEv1.

V. CONCLUSION AND FUTURE WORK

In this paper, initially we reviewed IKEv1 and IKEv2 in terms of security. Afterwards, a comparative analysis of both is carried out. This analysis shows that IKE2 is simpler, more reliable and less complex than IKEv1. It also evaluates that IKEv2 requires less round trips for messages exchange to establish IKE SA and IPSec SA as compared to IKEv1. Moreover IKEv2 offers rekeying, aliveness detection, NAT traversal, remote access VPN, multi-hosting and multi-homing services by default. On the other hand the IKEv1 offers it only as an extension. The IKEv2 also protects against DoS, replay and impersonation attacks as built-in features along with the functionality of retransmission and acknowledgement. The IKEv1 is generic whereas IKEv2 is specific for IPSec. Moreover, the IKEv2 is more flexible, scalable and have significantly less weaknesses than IKEv1. Resultantly, it should certainly be preferred over IKEv1 in IPSec for security association and key negotiation. We are interested to extend IKEv2 for secure multicasting as a future work.

REFERENCES

[1] S. Kent, K. Seo, “Security Architecture for Internet Protocol,” IETF RFC 4301, November 1998.

[2] S. Kent, R. Atkinson, “IP Encapsulating Security Payload (ESP),” IETF RFC 2406, November 1998.

[3] S. Kent," IP Authentication Header," IETF RFC 4302, December 2005

[4] S. Kent, R. Atkinson," IP Authentication Header," IETF RFC 2402, November 1998

[5] P. Hoffman, " Algorithms for Internet Key Exchange version 1 (IKEv1),” IETF RFC 4109, May 2005.

[6] C. Kaufman, P. Hoffman, Y. Nir , P. Eronen," Internet Key Exchange Protocol Version 2 (IKEv2)," IETF RFC 5996 , September 2010.

[7] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen, " Internet Key Exchange Protocol Version 2 (IKEv2)," IETF RFC 7296, October 2014.

[8] T. Kivinen, J. Snyder Signature Authentication in the Internet Key Exchange Version 2 (IKEv2) ," RFC 7427, January 2015.

[9] Ran Canetti and Hugo Krawczyk, " Security Analysis of KE's Signature based Key- Exchange Protocol," Crypto'03 (LNCS Series, Vol. 2729).

[10] Perlman, R. and Kaufman, C.," Key Exchange in IPSec: Analysis of IKE," IEEE Internet Computing, Nov/Dec 2000.

[11] J Zhou, Kent Ridge " Further analysis of the Internet key exchange protocol", Computer Communications 23 (2000) 1606–1612

[12] Ferguson, Niels, and Schneier, Bruce," A Cryptographic Evaluation of IPSec ", April 1999.

[13] Catherine Meadows," Analysis of the Internet Key Exchange Protocol Using the NRL Protocol Analyzer 1999", Naval Research Laboratory Washington, DC 20375 Code 5543

[14] K. Okhee, D. Montgomery," Behavioral and Performance Characteristics of IPsec/IKE in Large-Scale VPNs", www.antd.nist.gov/niist

[15] P. Karn and W.A. Simpson, “The Photuris Session Key Management Protocol”, draft-ietf-ipsec-photuris-03.txt, Sept., 1995.

[16] H. Krawczyk, "SKEME: a Versatile Secure Key Exchange Mechanism for Internet", In proc. of 1996 IEEE Symposium on Network and Distributed System Security (SNDSS'96), pages 114-127.

[17] H. Orman, “The OAKLEY Key Determination Protocol”, RFC 2412, Nov., 1998.

[18] H. Krawczyk, "SIGMA: the SIGn-and-MAc" Approach to Authenticated Diffie-Hellman Protocols ", In Crypto 2000.

[19] D. Maughan, M. Schertler, M. Schneider and J. Turner, " Internet Security Association and Key Management Protocol (ISAKMP)", IETF RFC 2408, November 1998

[20] Perlman, R. and Kaufman, C.," Analysis of the IPSec Key Exchange standard,"IEEE Computer Society, June 2001.

[21] E.Barker, D.Johnson, M. Smid,” Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)“, Computer Security, NIST Special Publication 800-56A, March 2007.

[22] D. Harkins,” Secure Pre-Shared Key (PSK) Authentication for the Internet Key Exchange Protocol (IKE)“, IETF RFC 6617, June 2012.

[23] T. Kivinen, J. Snyder, “Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)“, IETF RFC 7427, January 2015.

[24] D.R. Kuhn, V. C. Hu, W. T. Polk, S. Chang, “Introduction to Public Key Technology and the Federal PKI Infrastructure“,NIST SP 800-32, 26 February 2001.

[25] E. Barker, W. Barker, W. Burr,W. Polk, and M. Smid, “Recommendation for Key Management – Part 1: General (Revision 3)“, Computer Security, NIST Special Publication 800-57,July 2012

[26] Kenneth G. Paterson, “A cryptographic tour of the IPsec standards “,Elsevier, Information security technical report II, 2006.