iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Novel Approach for Security Enhancement in IPsec by a New Secured Internet Key Exchange Protocol

Sudhakar K[*1], Sethuraman M[#2], Srikanth S[#3]
[#]*Scientist, AU-KBC Research Centre, Anna University, Chennai, Tamil Nadu, India*
**Research Scholar, AU-KBC Research Centre, Anna University, Chennai, Tamil Nadu, India*

Abstract— IPSec is a network layer security protocol that provides security for internet communications at the IP layer by authenticating and encrypting each IP packet of a communication session. The security properties of IPsec critically depend on the underlying key exchange protocols, known as Internet Key Exchange (IKE). However, IKE is complex and vulnerable due to attacks such as (DOS, replay, etc.). The proposed paper brings a new secured IKE protocol based on one-time password. This protocol uses only the symmetric cryptosystem and is operated in two phases with four messages to accomplish the IPsec SA establishment. It guarantees authenticity of both entities within the same communication session. The proposed protocol ensures secure data transmission between two entities as well as to prevent from the vulnerable attacks.

Keywords— Internet Protocol Security (IPsec), Security Association (SA), Internet Key Exchange (IKE) Protocol, Security Analysis, Internet Protocol (IP), One-Time Password (OTP), Denial of Service (DoS) Attack, Replay Attack, Man-in-the-Middle (MITM) Attack

I. INTRODUCTION

The Internet Protocol (IP) as in [1] & [2], is a data-oriented protocol used for communicating data across a packet switched internetwork. IP provides the service of communicable unique global addressing amongst computers. However, communicating over the Internet involves significant security risks since the Internet is an unprotected network. Therefore, the need for securing the Internet has become a fundamental issue, especially for transmitting confidential data (e.g., electronic commerce, electronic banking, Virtual Private Networks).

For securing the Internet traffic, Internet Protocol Security (IPsec) as in [2] & [3], standard security protocol is used in the IP layer. The IPsec standard extends the IP protocol by securing the IP traffic at the IP level using cryptographic methods. The security properties of IPsec critically depend on the underlying key exchange protocols, known as Internet Key Exchange (IKE) as in [2] & [4]. IPSec has been adopted by all leading vendors and will be the future standard for secure communications on the Internet. It is also rapidly becoming the industry standard for Virtual Private Network (VPN) as in [5] & [6].

In this paper, proposed a new secure IKE protocol, which uses the One-Time Password (OTP) for authentication. It ensures a secure mutual authentication between two entities by requiring both entities to provide a verifiable one-time password to each other. The one-time password would expire after a single use. It guarantees authenticity of both entities within the same communication session. The system achieves mutual authentication by exchanging two one-time password.

The rest of the paper is organized as follows. Section II presents a description of the IPsec. The description of the IKE protocol and its versions are given in section III. The background and related works are presented in section IV. Section V presents the detailed design of the proposed secured IKE protocol. Section VI presents the result and comparison of the proposed protocol with IKE. The security analysis of the proposed IKE protocol with respect to the known vulnerable attacks are presented in section VII. Section VIII concludes the paper.

II. INTERNET PROTOCOL SECURITY

IPSec is a collection of protocols designed by the Internet Engineering Task Force (IETF) to provide security for a packet at the network level as in [2]. IPsec can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). The Security framework of IPsec is shown in Fig. 1. IPSec combines three main protocols, Internet Key Exchange (IKE) as in [2] & [4], Encapsulating Security Payloads (ESP) as in [2] & [7] and Authentication Headers (AH) as in [2] & [8] to form a security framework. IKE is used for establishing mutual authentication between peers at the beginning of the session, negotiation of cryptographic key to be used during the session. AH provides authentication, without any encryption whereas ESP provides both authentication and

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

payload encryption, and consequently is the most commonly used of the two protocols, as ESP extends the capabilities of AH. Both AH and ESP can be used either in transport or tunnel mode as in [2].

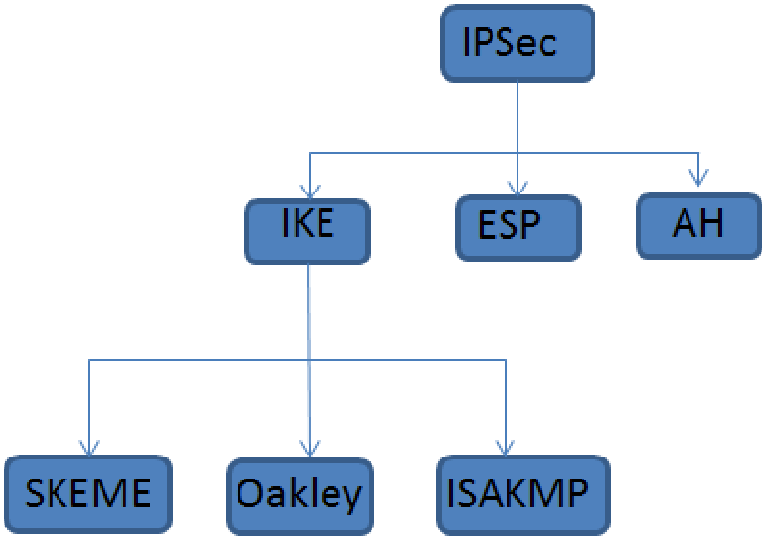


Fig. 1 Security framework of IPsec

The structure of the tunnel mode packet is shown in Fig. 2. Tunnel mode protects the entire original IP packet and is typically used to implement VPN as in [6]. IPsec VPN can be configured to provide a secure gateway to host, host to host, and gateway to gateway communications. The structure of the transport mode packet is shown in Fig. 3. Transport mode protects only the transport layer payload and is used for end-to-end communications between hosts.

New IP Header	IPSec Header	Original IP	TCP Header	Data

Fig. 2 Structure of the tunnel mode packet

IP Header	IPSec Header	TCP Header	Data

Fig. 3 Structure of the transport mode packet

IPsec implements the security mechanisms by setting up for each communication known as a security association [1] & [2]. It essentially targets to establishing a session key, which is used to provide the three main security properties for the subsequently transmitted messages. Establishing such a session key in IPsec, is an involved process with a large amount of options to choose from, such as various sub-protocols, cryptographic methods, and optional fields. The protocol suite responsible for this key establishment phase is IKE.

III.IKE PROTOCOL

The IKE protocol as in [1], [2], & [4], is a key management protocol standard which is used in conjunction with the IPSec standard. The main purpose of IKE within IPsec is to establish a security association, more specifically the IPsec SA, between two authenticated IPsec peers. The IPsec SA includes traffic keys that can be used for a secure IPsec tunnel. The IKE Phases and Modes is shown in Fig. 4. The IKE works in two phases. The first phase establishes an authenticated communication channel between the peers, by using algorithms like the Diffie-Hellman (D-H) key exchange as in [9] & [10], which generates a shared key to further encrypt IKE communications. The communication channel formed as a result of the algorithm is a bi-directional channel. The authentication of the channel is achieved by using a shared key, signatures, or public key encryption.
There are two modes of operation for the first phase: main mode, which is utilized to protect the identity of the peers, and aggressive mode, which is used when the security of the identity of the peers is not an important issue. During the second phase, the peers use the secure communication channel to set up security negotiations on behalf of other services like IPSec. These

negotiation procedures give rise to two unidirectional channels of which one is inbound and the other outbound. The mode of operation for the second phase is the Quick mode. IKE provides three different methods for peer authentication: authentication using a pre-shared secret, authentication using RSA encrypted nonce, and authentication using RSA signatures. IKE uses the HMAC functions to guarantee the integrity of an IKE session. When an IKE session lifetime expires, a new Diffie-Hellman exchange is performed and the IKE SA is re-established

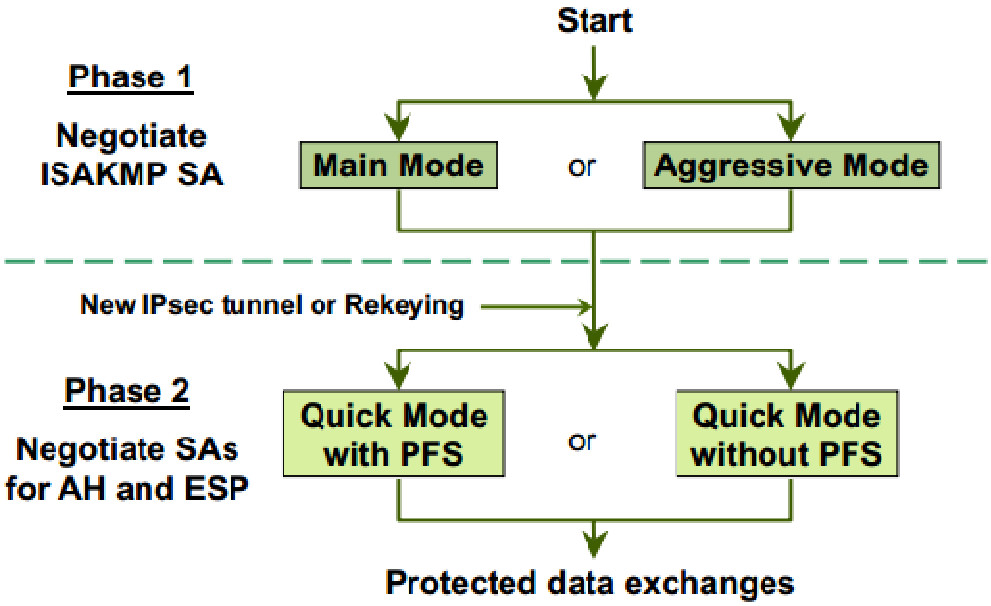


Fig. 4 IKE phases and modes

Currently, there are two versions of IKE such as IKEv1 and IKEv2 as in [4] & [11]. The design of IKEv1 is based on the Oakley protocol as in [12] and ISAKMP as in [13]. The protocol is essentially an authenticated key exchange protocol with additional payloads that supports multiple cryptographic algorithms and which is split into two distinct phases. In phase 1, an ISAKMP SA is established and that is used in phase 2 to set up an IPsec SA.

IKEv2 [11] was designed to add new features, address some weaknesses in IKEv1 and, at the same time, provides a cleaner design. In case of IKEv2, there are three sub-protocols in phase 1 which are based on digital signatures, MAC's, and Extensible Authentication Protocol (EAP) as in [14]. Similar to IKEv1, Diffie-Hellman exponents and nonce are exchanged and used to compute several shared secret keys.

IV. BACKGROUND AND RELATED WORKS

The security properties of IPsec critically depend on the underlying IKE, there exist two versions of IKE such as IKEv1 and IKEv2. From the literature survey, many of the researchers analysed the security aspects of IKE and inferred that the IKEv1 was criticized for its complexity and lot of options. Its successor, IKEv2 is significantly simpler and seems to provide the same level of security, but still offers a lot of options as in [15]. Although various techniques have been proposed to improve the security of IPsec such as a dynamic pre-shared key generation method, a modified IKE with authentication server and uses three round-trip messages, password-based authentication, etc., still it offers large amount of options and complexity.

A new IKE protocol based on D-H. It uses authentication server which generate the random numbers for generation of authentication message and three round-trips exchange message. The first four messages are used to establish IKE SA and the next two messages (protected by shared session key) are used to establish IPSec SA as in [16].Analysed the security of IPSec, introduced a dynamic pre-shared key generation method to improve the security of IPSec as in [17].Two simple password-based encrypted key exchange protocols based on that of Bellovin and Merritt. While one protocol is more suitable to scenarios in which the password is shared across several servers, the other enjoys better security properties as in [18]. A new IKE protocol is proposed, which uses the public encryption key and the public signature key to overcome the limitations of the Public Encryption key, Main Mode, and revised protocol as in [19]. The solution to the strength of RSA authentication is suggested, that is additions to the currently unspecified parts of IKEv2 related to the RSA authentication based on X509 Certificate - Signature, and Hash and URL of the X509 Certificate types as in [20].

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

V. THE PROPOSED PROTOCOL

The proposed new IKE with IPSec is shown in Fig. 5. The proposed protocol ensures a secure mutual authentication between IPSec peers by requiring both peers to provide a verifiable OTP to each other. The OTP would expire after a single use. The proposed protocol is operated in two phases and is composed of four messages (two round trips). The first two messages are used in phase 1 to authenticate the two entities and at the same time derives the session keys (inbound/outbound encryption key) from the Initialization Vector (IV) and the next two messages (protected by session key) are used in phase 2 to establish IPSec SAs. This protocol uses only the symmetric cryptosystem and it can resist the various attack types such as DoS, Man-in-the-Middle, replay, etc.

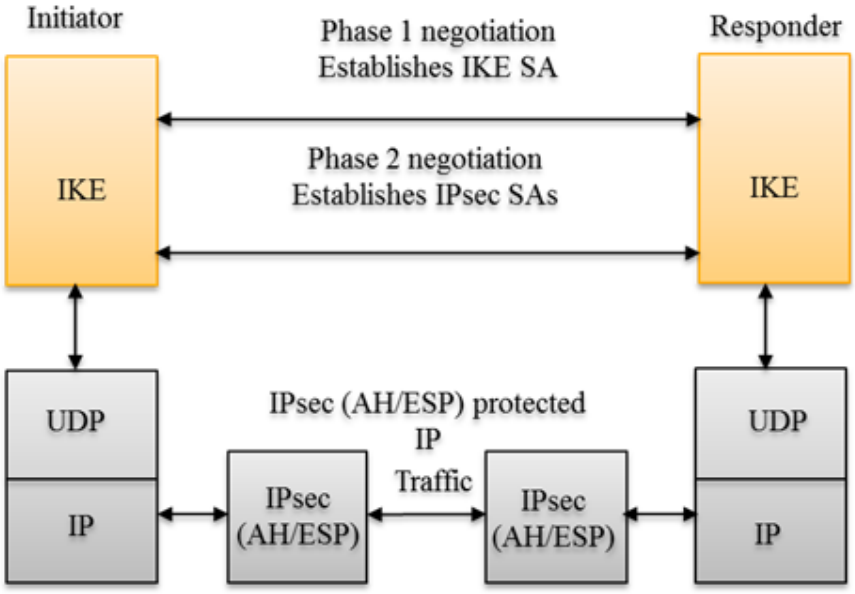


Fig. 5 The Proposed New IKE with IPSec

A. Notations Used

1) HDR: ISAKMP Header
2) Ni, Nr = Nonce (of Initiator, Responder)
3) OTP_i: One-Time Password of initiator.
4) OTP_r: One-Time Password of responder.
5) ||: Concatenation.
6) IV_i: Random Initialization Vector of initiator.
7) IV_r: Random Initialization Vector of responder.
8) $IPSec_{SA_i}$: A list of cryptographic proposals of the initiator (SA proposals of IPSec).
9) $IPSec_{SA_r}$: Cryptographic proposals selected by the responder from the list sent by the initiator (selected SA of IPSec).
10) HOTP (.): Hash based one-time password generate function.
11) SA_i , SA_r : Security Association (of Initiator, Responder).
12) K_i, K_r: The derived session key of Initiator and Responder.
13) MAC_i, MAC_r: Message Authentication Code (of Initiator, Responder).
14) $E_{K_i}(IPSec_{SA_i}, MAC_i), E_{K_r}(IPSec_{SA_r}, MAC_r)$: Encryption of IPSec SAs and its MAC using a symmetric cryptosystem with session key.

B. Protocol Descriptions

Phase 1: The phase 1 of the proposed IKE protocol between Initiator and responder is shown in Fig. 6. It consists of two steps:
Step 1: Initiator → Responder: *HDR*,SA_i,IV_i,N_i, OTP_i

The Initiator computes the One-Time Password (OTP_i), Initialization Vector (IV_i), Nonce (N_i) and sends it along with Security

Association (SA_i) to the responder. Initiator performs the following for one-time password generation

1) Compute: a random initialization vector IV_i
2) Compute: Nonce value (N_i)
3) Computes: OTP_i = HOTP (N_i || IV_i ||SA_i)

Step 2: Responder → Initiator: $HDR, SA_r, IV_r, N_r, OTP_r$

Upon receiving initiator message, responder performs the following operations to authenticate the initiator:

The responder computes the OTP

OTP = HOTP (N_i || IV_i ||SA_i)

Then the responder verifies whether the received OTP_i and computed OTP are same, if the verification fails, responder terminates the execution.

Otherwise, the responder selects the Security Association (SA_r) from SA_i according to its preference and computes the one-time password (OTP_r), Initialization Vector (IV_r), and sends it along with selected Security Association (SA_r) to the initiator. Then computes the outbound encryption key from IV_i and inbound encryption key from IV_r .If the responder does not agree for a SA_i , it can reject the entire list of SA_i and sends back an error in the second message.

Responder performs the following for OTP_r generation

Compute: a random initialization vector IV_r

Compute: Nonce value (N_r)

Computes: OTP_r = HOTP (N_r || IV_r || SA_r)

Upon receiving responder message, Initiator performs the following operations to authenticate the responder:

The initiator computes the OTP

OTP = HOTP (N_r || IV_r ||SA_r)

Then the initiator verifies whether the received OTP_r and computed OTP are same, computes the outbound encryption key from IV_i and inbound encryption key from IV_r , if the verification fails, initiator terminates the execution.

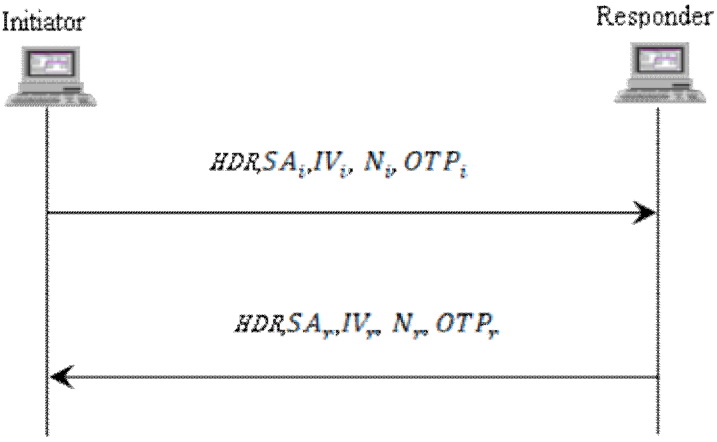


Fig. 6 Phase 1 of New IKE

Phase 2

The phase 2 of the proposed IKE protocol between Initiator and responder is shown in Fig. 7. It consists of two steps

Step 1: Initiator → Responder: $E_{K_i}(IPSec_{SA_i}, MAC_i)$

The initiator Computes the MAC from $IPSec_{SA_i}$

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

encrypts the $IPSec_{SA_i}, MAC_i$ using the outbound encryption key K_i

Sends the $E_{K_i}(IPSec_{SA_i}, MAC_i)$ to the responder.

Step 2: Responder → Initiator: $E_{K_r}(IPSec_{SA_r}, MAC_r)$

Upon receiving initiator message, responder performs the following operations:

Decrypts the received encrypted message using the inbound key K_i.

Computes the MAC from $IPSec_{SA_i}$ and then verifies whether the received MAC_i and the computed MAC are same, if the verification fails, responder discards the packet and terminates the execution.

Otherwise selects the $IPSec_{SA_r}$ from $IPSec_{SA_i}$ according to its preference.

Computes the MAC from $IPSec_{SA_r}$

Encrypts the selected $IPSec_{SA_r}, MAC_r$ using the outbound encryption key K_r.

Sends the $E_{K_r}(IPSec_{SA_r}, MAC_r)$ to the initiator.

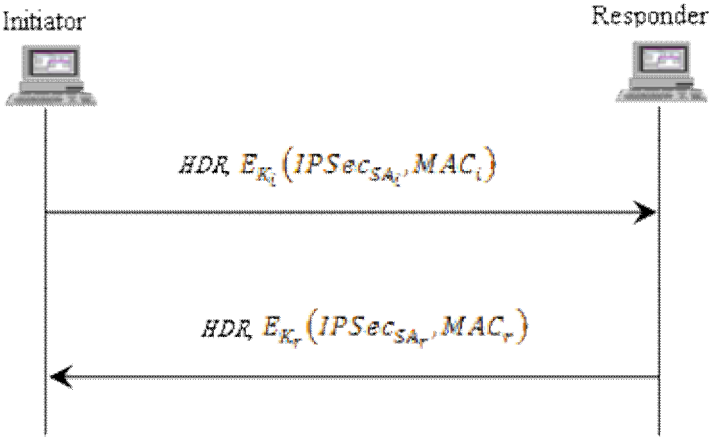


Fig. 7 Phase 2 of New IKE

C. Hash based OTP Generation

The HMAC OTP generation is shown in Fig. 8. The proposed protocol uses HMAC-based One-Time Password (HOTP) algorithm as in [21] to compute the otp. A cryptographic hash is a one-way function that maps an arbitrary length message to a fixed-length digest. Thus, a hash-based otp starts with the inputs, runs them through the one-way function, and produces the fixed-length password.

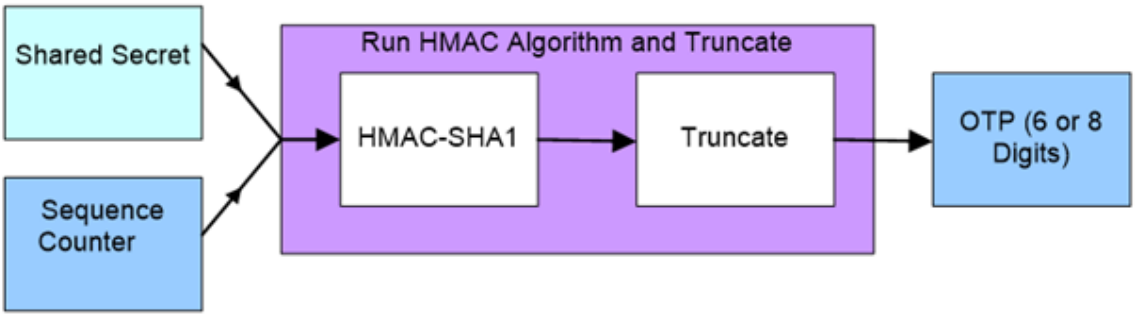


Fig. 8 HMAC OTP Generation

HOTP (K, C) = Truncate (HMAC-SHA-1(K, C))

Where Truncate represents the function that converts an HMAC-SHA-1 value into an HOTP value and the shared secret (K), the

counter (C), and Data values are hashed high-order byte first.

K= Initialization Vector (IV) + Nonce (N) + Security Association (SA)
C= Time stamp (Ts) + Nonce (N)

VI. RESULT AND COMPARISON

The proposed protocol is compared with the IKEv1 and IKEv2 protocols and is shown in Table 1.

TABLE I
COMPARISON OF PROPOSED PROTOCOL WITH IKE

	IKEv1	IKEv2	New IKE
Phase 1- Main Mode	**6**	**4**	**2**
Phase 1- Aggressive Mode	**3**	**-**	**-**
Phase 2- Quick Mode	**3**	**3**	**2**

In phase 1, IKEv1 uses 6 messages for main mode, three messages for aggressive mode and IKEv2 uses four messages whereas the proposed IKE uses only two messages to establish the IKE SAs. In phase 2, IKEv1 uses three messages and IKEv2 uses three messages whereas the proposed IKE uses only two messages to establish the IPsec SAs. So the proposed protocol offers less complexity with better efficiency.

VII. SECURITY ANALYSIS OF PROPOSED PROTOCOL

The proposed protocol prevents many of vulnerable attacks and few of them are discussed here.

A. Known-key security: In proposed protocol, the session keys are dynamically generated based on time and are cryptographically independent of each other, so the compromise of one shared session key should not compromise keys in other sessions.
B. DoS attack: In proposed protocol, a DoS attack would not find it too easy to totally exhaust the responder's CPU time unless such attack lasts for a fairly long period of time.
C. Replay attacks: Proposed protocol can resist replay attack, random IV and one-time password assures that the response is fresh and has not been replied by an opponent.
D. Man-in-the-Middle attack: In proposed protocol, the use of OTP can be effective to authenticate the two parties and resilience to MITM attack.
E. Eavesdropping and Forged attacks: In proposed protocol, since session keys, IV, and OTP are used only once and are cryptographically independent of each other, even if a malicious user acquires a view of all the session keys used so far, user cannot get any advantage from the observation of previous sessions.

VIII. CONCLUSIONS

The proposed new secured IKE protocol achieves mutual authentication by exchanging two OTPs. It operates in two phases with four messages and uses only symmetric cryptosystem to establish the IPSec SAs. Therefore, there are several advantages which make the proposed protocol better than existing IKE protocols. First, it enables secure mutual authentication between two entities, moreover, it guarantees authenticity of both entities within the same communication session. Finally, the proposed protocol ensures a high level of security, robustness, flexibility, extensibility, and secure data transmission between two entities as well as to prevent from known attacks.

IX. ACKNOWLEDGMENT

This work is supported by the Cryptography and Network Security Lab in AU-KBC Research Centre, MIT Campus of Anna University.

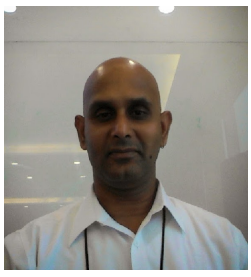
REFERENCES

[1] Behrouz A. Forouzan, "Data communications and networking," Fourth Edition, Publication Year: 2007, Page(s): 549 – 1004.

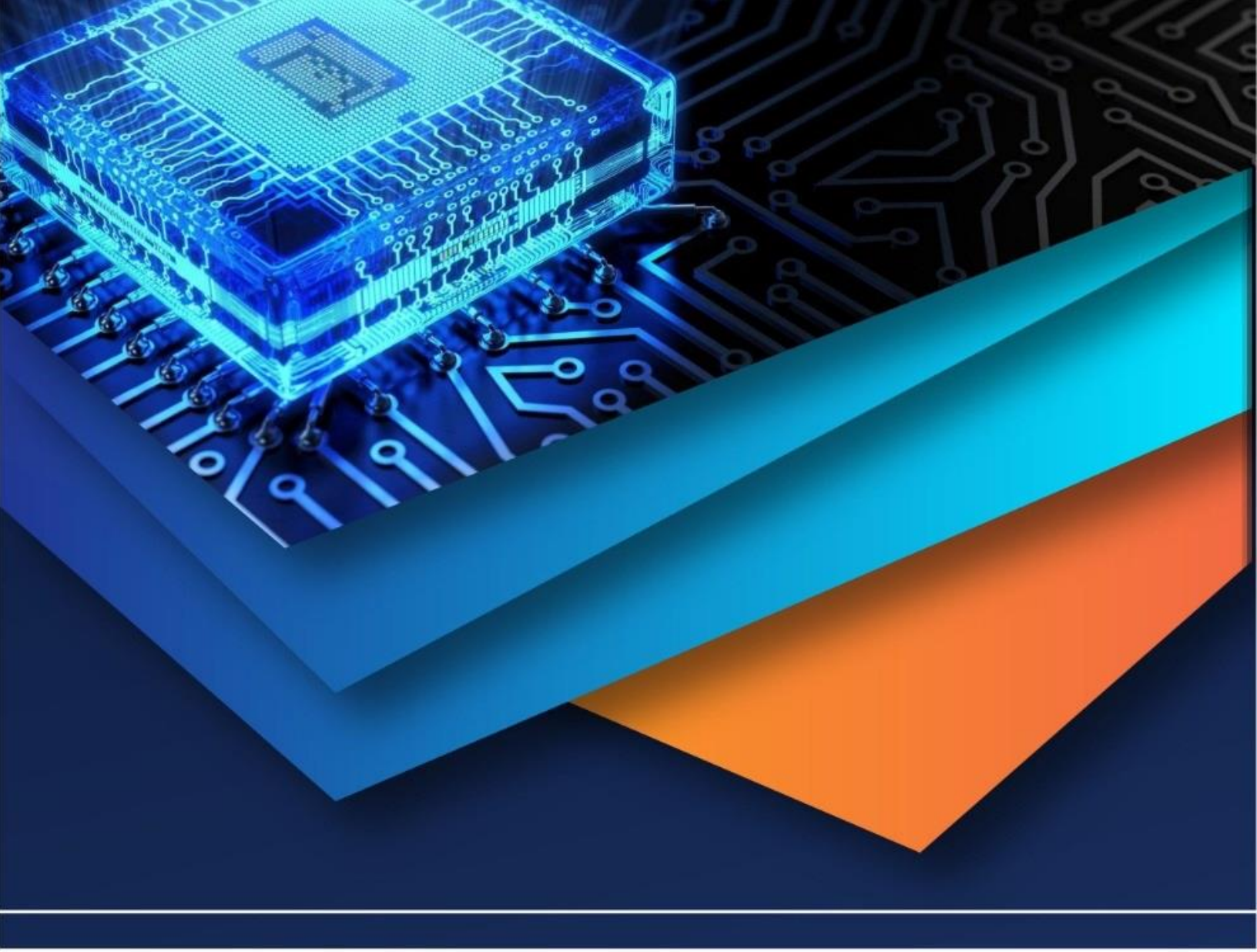
[2] Behrouz Forouzan, Firouz Mosharraf, “Computer networks: a top down approach,” 5th Edition, Publication Year: 2010, Page(s): 241 – 791.
[3] Atkinson R, Kent S, “Security architecture for the internet protocol,” RFC 2401, Internet Engineering Taskforce (IETF), November 1998.
[4] Harkins D, Carrel D, “The internet key exchange (IKE),” RFC 2409, IETF, November 1998.
[5] SSH IPSEC Express, http://www.ipsec.com/Products/Protocol-Security-Toolkits.
[6] Fowler D, “Virtual private networks making the right connection,” Morgan Kaufmann Publishers, Inc., San Francisco, California, 1999.
[7] Atkinson R, Kent S, “IP authentication header (AH),” RFC 2402, IETF, November 1998.
[8] Atkinson R, Kent S, “IP encapsulating security payload (ESP),” RFC 2406, IETF, 1998.
[9] Maryam Ahmed, Baharan Sanjabi, Difo Aldiaz, Amirhossein Rezaei, Habeeb Omotunde, “Diffie-Hellman and Its Application in Security Protocols,” International Journal of Engineering Science and Innovative Technology, Vol. 1, no. 2, November 2012.
[10] Francois J, Raymond A, “Security issues in the diffie-hellman key agreement protocol,” IEEE Trans.on Information Theory, pages 1–17, 1998.
[11] Kaufman C, Hoffman P, Nir Y, Eronen P, “Internet key exchange protocol version 2 (IKEv2),” RFC 5996, IETF, September 2010.
[12] Orman H, “the OAKLEY key determination protocol,” RFC 2412, IETF, November 1998.
[13] Maughan D, Schertler M, Schneider M, Turner J, “Internet security association and key management protocol (ISAKMP),” RFC 2408, IETF, November 1998.
[14] B. Aboba, L. Blunk, “Extensible Authentication Protocol,” RFC 3748, IETF, June 2004.
[15] C. Cremers, "Key exchange in IPsec revisited: formal analysis of IKEv1 and IKEv2," in European conference on research in computer security (ESORICS), Leuven, Belgium, Sep. 2011.
[16] Ahmim marwa, Babes malika, Ghoualmi nacira, “Contribution to enhance IPSec security by a safe and efficient internet key exchange protocol,” Computer and Information Technology (WCCIT), 2013.
[17] Liangbin Zheng, Yongbin Zhang, “An enhanced IPSec security strategy,” IEEE International Forum on Information Technology and Applications, 2009.
[18] Michel Abdalla, David Pointcheval, “Simple password-based encrypted key exchange protocols,” Springer Berlin Heidelberg, vol. 3376, pp 191-208, 2005.
[19] NagaLakshmi V, Rameshbabu I, “A protocol for internet key exchange (IKE) using public encryption key and public signature key,” International Journal of Computer Science and Network Security (IJCSNS), vol.7 no.7, July 2007.
[20] Ana Kukec, Stjepan Gros, Vlado Glavinic, “Implementation of certificate based authentication in IKEv2 protocol,” IEEE information Technology Interfaces, 2007. [29th International Conference].
[21] D. M'Raihi, M. Bellare, F. Hoornaert, “HMAC-Based One-Time Password Algorithm,” RFC 4226, IETF, December 2005.

K. Sudhakar is working presently as Project Engineer in AU-KBC Research Centre, Chennai, TN, INDIA. He is currently pursuing M.S (By Research) in Information and Communication (I&C) Faculty from Anna University, TN, India. His area of interest include Cryptography and Network security, Wireless Communication.

M. Sethuraman is working presently as Scientist in KBC Research Foundation Pvt. Ltd., Chennai, TN, INDIA. He received his M. Tech (EE, Communications) from IIT, Kanpur, India in 1985. He has 35+ years of Crypto design experience. His research areas includes Cryptography and Network security.



Dr. S. Srikanth is working presently as Member Research Staff, AU-KBC Research Centre, Chennai, TN, INDIA. He received his Ph.D. award (Electrical Engineering) from University of Victoria, Canada in 1997. He has 25+ years of wireless communication experience. His research areas includes physical and medium access control layers of wireless communication systems.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY