Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.545 – 548

RESEARCH ARTICLE

Secure Key Exchange over Internet

Miss. Pooja P. Taral[1], Prof. Vijay B. Gadicha[2]

[1]CSE Department, PRPCOET, Sant Gadge Baba Amravati University, India
[2]CSE Department, PRPCOET, Sant Gadge Baba Amravati University, India
[1] taralpooja@gmail.com; [2] v_gadicha@rediffmail.com

Abstract- Due to advances in technology and communication, it requires more effort to ensure security. It is essential that every organization has the right level of security. Authentication in security had emerged to be an essential factor in the key establishment over internet. The DIKE (Deniable Internet Key Exchange) protocols add novelty and new value to the IKE standard. In recent communication systems, as there is more and more use of internet, the security services have become essential. Key-exchange in Diffie–Hellman key-exchange (DHKE) is among the core cryptographic mechanisms to ensure network security.

Keywords - Authentication; Key-exchange; DHKE; DIKE; IKE

I. INTRODUCTION

Security is having a great significance over the internet. Key-exchange is a special area of cryptography, in view of its simple yet error prone nature. An authentication protocol allows a sender to send messages to a receiver through an insecure communication channel in such a way that the receiver can be convinced that the messages are indeed coming from the intended sender and them messages have not been modified by any adversary sitting in the middle of the communication channel. In short, the aim of this type of protocols is to establish an authenticated link from the sender to the receiver.

User authentication determines the legitimacy of the intended parties in real time. For example, in a client-server application, a service provider needs to ensure the legitimacy of a user before providing services to the user. Similarly, a user needs to make sure that the service provider is genuine so that the user is willing to send its sensitive information (such as a credit card number) to the service provider. Since communicating parties need a common key to encrypt and decrypt data, shared-key authentication makes sure that the shared common key is known only to the intended parties. In a key-agreement protocol without user authentication, an attacker can misrepresent the identity of an innocent party, leading to attacks such as replay, resource exhaustion and unknown key-share[14].

The IPSec and IKE are intended to protect messages communicated in the IP layer, i.e., “layer 3" of ISO-OSI, that processes the transmission of messages using the network addresses possibly without knowing end-user peers' identities. IKE and IPSec can in turn be used to offer confidentiality, authentication and privacy for communication protocols in the higher layers of ISO-OSI (note that many communication protocols including many authentication protocols which are invoked by end-users with explicit peer's identity information work at “layer 7" of ISO-OSI, i.e., the application layer) [12].

II. LITERATURE REVIEW

A deniability service offered at the IP layer preserves the privacy feature from the upper layers, in particular, the application layer. A deniable authentication protocol is an authentication protocol which prevents the receiver, after receiving the message, from proving to a third party that the message is originated from a particular sender. The security of a communication protocol is usually based on one or more assumptions. For example, a key agreement protocol is built on one or more cryptographic assumptions. A protocol with multiple independent assumptions with a logic OR relationship (OR-related) is like a house with multiple outside doors with different security mechanisms. The more doors a house has, the more ways a thief can break into the house and the weakest security mechanism of all is the easiest to overcome. Similarly, the more independent OR-related assumptions a protocol has, the more ways an attacker can try to attack the protocol and the weakest of all is the easiest to try. In other words, when multiple independent OR-related assumptions are involved, the security of a protocol is typically reduced to that of the weakest one. Therefore, for two protocols A and B, where A is based on multiple independent OR-related cryptographic assumptions and B is based on one of the assumptions in A, B is at least as secure as A. The security of the protocol should be assessed in its entirety, rather than at the level of individual algorithms. Authenticated key establishment is a process of verifying the legitimacy of communicating parties and establishing common secrets among the communicating parties for subsequent use (such as data confidentiality and integrity). Authenticated key establishment is very important for virtually all secure communication systems such as e-commerce, wireless, wired and Internet applications. An authenticated key establishment protocol in general is constructed using multiple cryptographic algorithms which are based on various cryptographic assumptions [14]. In this paper, various features of secure key-exchange are considered as a special feature for key-exchange protocol, Internet key- exchange (IKE), Internet Protocol Security (IPSec).

A. *Deniability*

Deniability is a privacy property that ensures protocol participants can later deny taking part in a particular protocol run. Such a property has been declared as desirable for new protocols proposed to secure the IP (Internet Protocol) level on Internet communications [10]. Traditional deniability only considers the privacy of the honest proven against a possibly malicious verifier, and requires that the interactions between them be computationally simulatable, i.e., computational zero-knowledge (ZK) [11]. A stronger form of deniability can be achieved using shared-key authentication. With a shared-key solution, either user in the protocol run could have produced all the messages in the run. An even stronger form of deniability can be obtained when the shared key is obtained using techniques from identity-based cryptography. Now, any user can simulate runs of the protocol involving any other potential user. Moreover, a user is not required even to reveal if he is registered with the trusted authority in order to take part in runs of the protocol; this is in contrast to schemes which employ certificates and a traditional PKI (including the signature-based schemes), where the existence of a certificate for a user indicates that user has registered, and identifies him as a potential protocol participant amongst all the users in a population [2]. Over the years, many deniable authentication protocols have been proposed but most of them have been proven insecure due to various cryptographic attacks such as the KCI attack [5, 6, 7] and the MITM attack [8].

B. *Internet Key-exchange (IKE)*

One of the basic secure communication technologies is the key establishment protocol that is known as Internet Key Exchange (IKE). It is the standard of Internet protocol Security (IPSec) proposed by the IETF in 1998 [4, 9]. But, people have many criticisms for this protocol, especially for its complexity [9]. The IKE and IPSec used to provide security services and privacy for communication protocols. The standard of IKE has gone through two generations. The first generation IKEv1 [3] uses public-key encryption as the authentication mechanism. The second generation IKEv2 [1] uses signatures as the authentication mechanism, with the SIGMA protocol [13] as the basis.

C. *Internet Protocol Security (IPSec)*

IPSec is the Internet Engineering Task Force (IETF) proposed standard for “layer 3 real-time communication securities.” In a real-time security system, an initiator, say Alice, initiates communication with a responder system, say Bob. They authenticate to each other by proving knowledge of some secret, and then establish a secret key for the protection (integrity and/or privacy) of the remainder of the session. We use the term “real-time” to distinguish it from a system such as secure e-mail, in which Alice can create an encrypted, signed message for Bob without interacting with Bob [4].

By operating below layer 4, IPSec keep away the problem of an active attacker fatally breaking apart a session by injecting a single unpredictable packet. Solutions like SSL, which operate above TCP, are vulnerable to this threat. Although IPSec can be deployed without changes to applications, the power of IPSec cannot be exploited until the API is changed to inform applications of the endpoint identifier, and applications are modified to use the information in the modified API.

III. PROPOSED WORK/METHODOLOGY

In this section, we will check over enhanced ID-based deniable authentication protocol in order to ensure that the security requirements for a deniable authentication protocol are satisfied. For key-exchange protocols, both security and privacy are desired parameters. Actually, providing a certain level of privacy protection serves as one of the major criteria underlying the evolution of a list of important industrial standards of KE protocols, which is particularly witnessed by the evolution of IKE [1]. Deniable key-exchange is that if the key-exchange protocol is deniable, then all the transactions using the session key produced by the key-exchange protocol can be deniable for both the protocol participants. It is advantageous for privacy preservation and proved by Meng-Hui Lim that enhanced ID-based Deniable Authentication Protocol to be capable of preserving all the desired properties of an ID-based deniable authentication protocol.

IV. CONCLUSION

In this paper, we have pointed out various security services used to avail security and privacy features for key-exchange over the internet. Deniability, Internet Key-exchange (IKE), Internet Protocol Security are the basic building blocks that ensure security in accordance with various security services like confidentiality, integrity, authentication and privacy preservation while communication.

REFERENCES

[1] C. Kaufman, “Internet key exchange (IKEv2) protocol,” The Internet Engineering Task Force, London, U.K., Tech. Rep. 4306, Dec. 2005.

[2] Boyd C., Mao, W., Paterson, K.G., “Deniable Authenticated Key Establishment for Internet Protocols, 11th International Workshop on Security Protocols”, LNCS, vol. 3364, pp. 255-271 (2003).

[3] D. Harkins and D. Carreal, “The Internet key-exchange (IKE),” IETF (The Internet Engineering Task Force), New York, NY, USA, Tech. Rep. 2409, Nov. 1998.

[4] R. Perlman and C. Kaufman, “Key exchange in IPSec: Analysis of IKE,”IEEE Internet Computing, (2000)50-56.

[5] Chou, J.S., Chen, Y.L., Huang, J.C., “A ID-Based Deniable Authentication Protocol on Pairings”, Cryptology ePrint Archive: Report, (335) (2006).

[6] Chou, J.S., Chen, Y.L., Yang, M.D., “Weaknesses of the Boyd-Mao Deniable Authenticated Key Establishment for Internet Protocols”, Cryptology ePrint Archive: Report, (451) (2005).

[7] Lim, M.H., Lee, S.G., Park, Y.H., Lee, H.J., “An Enhanced ID-based Deniable Authentication Protocol on Pairings”, Cryptology ePrint Archive: Report, (113) (2007).

[8] Zhu, R.W., Wong, D.S., Lee, C.H., “Cryptanalysis of a Suite of Deniable Authentication Protocols”, IEEE Communications Letters, vol. 10, no. 6, pp. 504-506 (2006).

[9] M.S. Borella, “Methods and protocols for secure key negotiation using IKE,” IEEE Network, (2000), 18-29.

[10] D. Harkins, C. Kaufman, T. Kivinen, S. Kent, and R. Perlman. Design Rationale for IKEv2, February 2002. Internet Draft.

[11] S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of interactive proof-systems,” in *Proc. STOC 1985*, pp. 291–304.

[12] W. Mao. Modern Cryptography: Theory and Practice. Prentice Hall PTR, 2004.

[13] H. Krawczyk, “SIGMA: The ‘SIGn-and-MAc’ approach to authenticated Diffie-Hellman and its use in the IKE-protocols,” in *Proc. CRYPTO 2003*, pp. 400–425.

[14] L. Harn, W.-J. Hsin and M. Mehta, “Authenticated Diffie–Hellman key agreement protocol using a single cryptographic assumption”, IEEE Proc.-Commun., Vol. 152, No. 4, August 2005.