IJCSC International Journal of Computer Science and Communication Vol. 2, No. 2, July-December 2011, pp. 419-422

TWO-STAGE AUTHENTICATION FOR WIRELESS NETWORKS USING DUAL SIGNATURE AND SYMMETRIC KEY PROTOCOL

Sushma Yalamanchili[1] and K. V. Sambasiva Rao[2]

[1]Research Scholar, Department of Computer Science & Engineering,
Acharya Nagarjuna University, Nagarjuna Nagar, India.
E-mail: sushma_yalamanchili@yahoo.co.in
[2]Principal, M.V.R. College of Engineering and Technology, Paritala, Vijayawada, India
E-mail: kvsambasivarao@rediffmail.com

ABSTRACT

Wired networks differ from wireless networks in that they can support computationally intensive security protocols, have high bandwidth and offer high reliability. Strong authentication schemes can be applied to wired networks. Wireless networks on the other hand suffer from packet losses and bit errors, often have low bandwidth and have resource constraints such as computation overhead and storage. In the present work, we present a two-stage authentication scheme for wireless networks that uses a computationally intensive but highly secure strong authentication in Stage 1 and a lightweight symmetric key based protocol in Stage 2. The cost of the strong authentication adopted in Stage 1 is amortized over N sessions thus reducing the overall cost of the scheme. We adapt the Dual-signature based IKE authentication that we proposed in our earlier work and employ it as Stage 1 authentication. The Symmetric key protocol in Stage 2 authentication that we propose uses the symmetric keys that are generated in Stage 1.

Keywords: Mutual Authentication, Wireless Networks, Symmetric Key Encryption, IKE Strong Authentication.

1. INTRODUCTION

Internet Key Exchange (IKE) [1,2] is a key generation and authentication protocol for Internet Security protocol (IPSec) [3]. Adaptations have been proposed in the literature for IKE authentication [4,5]. We proposed an authentication scheme [4] for use in IKE main mode methods that relies on private keys and public key certificates to achieve mutual authentication between a pair of parties. A concept called Dual Signature is employed in that authentication scheme which involves a signed hash value of the concatenated hash values of the private key and the public key certificate of the sender. Sender authentication is completed when the remote party is able to open the Dual Signature with the sender's public key as this is proof that the sender possesses the corresponding private key. In this manner, receiver authentication and thus mutual authentication is achieved. Establishment of Security Associations (SAs) follow with session key generation. This is a strong authentication scheme that is readily applicable to wired networks. In the current work, we extend the Dual-signature based IKE authentication and supplement it with a proposed symmetric key based authentication scheme for two party communication that renders it highly suitable for Wired-Wireless and Wireless networks [6].

2. LITERATURE SURVEY

Commonly used authentication techniques are based on hash functions [7], digital signatures [8,9], time stamps [10], biometrics [11] and identity [12]. Hash algorithms take a finite length message or string as input and generate a fixed length string which is much smaller. Keyed hash functions are often used for message authentication. Lee et al. propose a light weight user authentication scheme for mobile communication based on one-way hash functions and smart cards [13]. Hoffman discusses the vulnerabilities of MD5 and SHA-1 hash algorithms and suggests the use of stronger hash algorithms such as the SHA-2 family. He suggests that certificates should be signed by SHA-256, SHA-384 and SHA-512 hash algorithms [7].

Homomorphism is used when an algebraic function on one form of input is the equivalent of another algebraic function on the equivalent ciphertext [14]. Homomorphism functions can be used to map identities to the equivalent cryptographic keys in our current work.

Caldera et al. [15] discuss the performance and limitations of IPSec and IKE when used in wireless and mobile networks. Bezawada et al. [16] describe constructs using symmetric key encryption that amortize the cost of session key establishment over N sessions.

3. MOTIVATION

Wireless networks are constrained by battery power and computational resources. They suffer from packet losses and bit errors leading to abortion of many cryptographic protocols. Hence there is a need to devise an Authentication mechanism that is strong in security and lightweight in operation. The Dual Signature based Authentication scheme proposed in our earlier work [4] is highly secure and the cost of this authentication needs to be lowered without reducing the degree of security provided. As public key encryption involves high computational overhead [17], a lightweight authentication scheme that uses Symmetric key encryption is needed for the two-party wireless scenario.

4. PRESENT WORK

A two-stage authentication scheme for two parties in wireless networks is proposed and the details of the Symmetric key protocol for Stage 2 along with the session key generation procedure and message formats are discussed below.

4.1 Two Party Wireless Authentication

The Authentication model that is being proposed for Wireless setting involves two stages. Stage 1 is an altered Dual signature based authentication in IKE setting [4] where the two wireless nodes achieve strong security and operate using a reliable communication method to generate the Symmetric keys needed for Stage 2 authentication protocol. If the number of sessions is N, then 2 log N symmetric keys are generated in Stage 1 authentication. In Stage 2, if the same two nodes wish to establish a different session then they will not re-run the Stage 1 Dual Signature based Authentication protocol but will use a Symmetric key-based protocol.

Table1
Two Party Wireless Authentication

S.No.	*Action*
Step 1	Strong authentication at Initialization based on Dual signature and generation of 2 log N symmetric keys
Step 2	Assuming N sessions, Session key establishment to maintain key freshness through Symmetric key protocol
Step 3	Mutual Authentication
Step 4	After expiry of current 2 log N symmetric keys, goto Step 1

The purpose of this model is that the initial stage guarantees a highly secure key establishment with sender authentication. The subsequent phases also enable sender authentication but use only symmetric key methods thereby amortizing the cost of strong authentication and session key establishment. The wireless authentication scheme for two-party scenario is described in Table 1.

4.2 Sender, Receiver and Mutual Authentication

For every session, a unique non-repeating log N size subset of symmetric keys is chosen and the session key is computed by using XOR operation on them. The hash value of the past session key (if any) and the current session key is sent along with the homomorphism function that identifies the identities corresponding to the current session key. It is essential that the sender prove to the receiver that it is in possession of the corresponding XOR. If the receiver is able to compute and match the appropriate hash value based on its values of symmetric keys then the sender is authenticated. This process is repeated with a new set of identities for every session. Each time a different and unique subset of symmetric keys is chosen. Further more, Step 2 does not require a reliable communication channel and can be re-run as many times as required till the goals of authentication and session key establishment have been met. The session key that is actually established is never even exchanged. It is only verified over the wire through hash values.

Table 2
Session Keys and Message Formats for Sessions

S.No	*Scenario*	*Session Key / Message*
1	First session	**Session_key**=h(XOR(randomly_ chosen_subset_of_ keys)) **Message** = f(key_ids_chosen), h(XOR (randomly_chosen_subset_of_keys))
2	In between sessions with no packet loss	**Session_key** = h(prev_session_key || XOR(current_subset_of_keys_chosen)) **Message** = f(ids_of_current_subset_of_ keys_chosen), h(prev_session_key || XOR(current_subset_of_keys_chosen))
3	In between sessions with packet loss	**Session_key** = h(XOR(randomly_ chosen_subset_of_keys) XOR(current_subset_of_keys_chosen)) **Message**=f(ids_of_current_ subset_of_ keys_chosen), f(ids_of_randomly_ chosen_subset_of_keys), h(XOR (randomly_chosen_subset_of_keys)|| XOR(current_subset_of_ keys_chosen))

Our protocol addresses the fact that packet losses are frequent and a characteristic of wireless networks. In this work, we only consider loss of packets that are bearing session keys. We assume that the sender and the receiver share a couple of homomorphism functions. The session key is computed as XOR ($s_1, s_2, .., s_{\log N}$) where ($s_1,\ldots,s_{\log N}$) is a unique non-repeating subset of 2log$N$ symmetric keys. The homomorphism function is executed with an n-tuple of identity numbers that

correspond to the log$N$ symmetric keys that constitute the session key. Three scenarios are possible for session key generation and message sent by the sender. The session key computation and message format used in each of the three cases is detailed clearly in Table 2. In the following discussion, f represents a homomorphism function [14] shared by the sender and the receiver that hides the value of the key identities from the attacker and h represents a hash function. || denotes the concatenation operation.

The receiver can follow the same procedure to generate Session keys resulting in *receiver authentication* and subsequent *mutual authentication* which is unique to this authentication scheme.

4.3 Experimental Work

In the discussion that follows, p represents the probability of loss of a packet bearing a session key in a wireless network and N represents the number of sessions. The number of symmetric keys currently used is represented by m which takes on an initial value of 2log N. The final value of m for given values of N and p indicates the actual number of symmetric keys required to complete N sessions in a lossy network. The value of p ranges from 0.1 to 0.9 and is incremented in steps of 0.1. The number of sessions, N, takes on the values 32, 64, 128, 256, 512 and 1024.

The experimental work is performed in Java. Each experiment is averaged over 100 runs for a specific value of N, p and m. During the experiment, successful transmission of packets bearing a session key uses up only one session key. However, packets bearing session keys are lost randomly based on the probability of packet loss requiring additional session keys for that particular session.

Table 3
Adequacy of Session Keys and Session Key Utilization

Number of Sessions	*Initial Symmetric*	*Symmetric keys needed*	*% Session Keys Used*	
(N)	*keys (2logN)*	*(m)*	*p=0.1*	*P=0.9*
32	10	10, 12*	13.9	39.7
64	12	12	7.7	68.5
128	14	14	4.1	36.5
256	16	16	2.2	20.6
512	18	18	1.2	10.4
1024	20	20	0.6	5.5

* m=12 for N=32, p=0.9 and is 10 for all other values of N, p

It can be observed from Table 3 that the proposed Symmetric key protocol results in successful completion of N sessions with the initial 2log N symmetric keys in all cases except for one case with small N (32) and very high p (0.9). Even in this case, the protocol completes successfully by re-running Stage 1 authentication protocol and generating a new set of 2 log N symmetric keys. Further the protocol requires storage for only 10, 12, 14, 16, 18, and 20 symmetric keys for N =32, 64, 128, 256, 512, 1024 session sizes respectively.

5. ANALYSIS

The Stage 1 and Stage 2 authentication for Wireless setting provide for sender authentication, receiver authentication and mutual authentication. The session keys generated using 2 log N symmetric keys ensure confidentiality of user sessions. Replay is easily tackled as each log N symmetric key combination occurs only once by selecting non-repeating subsets from among 2 log N symmetric keys. Performance is better than exclusively using expensive public key cryptography as we use public key cryptography in Stage 1 and symmetric key cryptography in Stage 2. The storage cost associated with the symmetric keys is very small compared to the gains from low computational overhead associated with the symmetric key protocol. It tolerates packet loss as well.

Adequacy of session keys is observed in most of the cases in the experimental work. Even in the case of small N and large p when the session keys are exhausted, the Stage 1 authentication protocol can be re-run generating a new set of 2 log N symmetric keys and the symmetric key protocol can be continued for the remainder of the sessions.

6. CONCLUSION AND SCOPE OF FUTURE WORK

The strong authentication protocol [4] proposed for IKE main mode methods is used for Stage 1 authentication in wireless networks. At the end of Stage 1 authentication, 2 log N symmetric keys are generated between the two peers. Stage 1 authentication scheme using dual signature and digital envelope has high computational overhead but ensures strong security. The cost of computation associated with Stage 1 is spread over N sessions. The symmetric key protocol proposed for Stage 2 wireless network authentication requires low storage and low computational power. It is very efficient and light weight in operation. It also takes into account packet loss which is another characteristic of wireless networks. Further, this Symmetric key encryption based authentication scheme works in conjunction with other authentication schemes for IKE [1,2,5] with the alteration that 2 log N symmetric keys are generated and exchanged between the two negotiating parties at the end of the IKE authentication.

Multicast group based applications for wireless networks are on the rise with group membership changing dynamically. Applications in this area include pay-per-view television, conferencing, stock market updates, distance education and distribution of

government forms and information. Authentication and key management in dynamic groups is of great interest and is being widely studied in the research community. We propose to extend our work to dynamic groups.

REFERENCES

[1] D. Harkins and D. Carrel, The Internet Key Exchange (IKE), RFC 2409, Network Working Group, 1998. Available at http://www.ietf.org/rfc/rfc2409.txt.

[2] C. Kaufman, P. Hoffman, Y. Nir and P. Eronen, Internet Key Exchange Version 2 (IKEV2), RFC 5996, Network Working Group, 2010. Available at http://tools.ietf.org/html/rfc5996.

[3] N. Doraswamy and D. Harkins, IPSec, Prentice Hall PTR, Second Edition, 2003. ISBN: 013046189X.

[4] Sushma Yalamanchili and K.V. Sambasiva Rao, "Authentication and Confidentiality in IKE using Dual Signature, Digital Enveloping and PGP", *To Appear in International Journal of Computational Intelligence and Information Security*, **2**, No. 6, June 30, 2011.

[5] V. NagaLakshmi and I. Rameshbabu, "A Protocol for Internet Key Exchange (IKE) using Public Encryption Key and Public Signature Key", *International Journal of Computer Science and Network Security*, **7**, No. 7, pp. 342-346, July 2007.

[6] Matthew Gast, "802.11 Wireless Networks: The Definitive Guide – Creating and Administering Wireless Networks", O'Reilly Media, April 2002.

[7] P. Hoffman, Use of Hash Algorithms in Internet Key Exchange (IKE) and ipsec, RFC 4894, Network Working Group, May 2007. Available at https://tools.ietf.org/rfc/rfc4894.txt.

[8] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures", *Journal of Cryptology*, **13**, No. 3, pp. 361–396, 2000.

[9] B. Weis, "The use of RSA/SHA-1 Signatures within ESP and AH, RFC 4359", *Internet Engineering Task Force*, 2006. Available at http://tools.ietf.org/html/rfc4359.

[10] K. Elmufti, D. Weerasinghe, M. Rajarajan, V. Rakocevic and S. Khan, "Timestamp Authentication Protocol for Remote Monitoring in eHealth", *CMPC: 1st International ICST Workshop on Connectivity, Mobility and Patients' Comfort, ICST*, 2008. DOI=10.4108/ICST.PERVASIVEHEALTH2008.2542.

[11] A. Bhargav-Spantzel, A. C. Squicciarini, S. Modi, M. Young, E. Bertino and S. J. Elliott, "Privacy Preserving Multi-factor Authentication with Biometrics", *Journal of Computer Security*, **15**, No. 5, pp. 529–560, 2007.

[12] Y. Liao and S. Wang, "A Secure Dynamic Id Based Remote User Authentication Scheme for Multi-server Environment", *Computer Standards & Interfaces*, **31**, pp. 24–29, 2009.

[13] C. Y. Lee, C. H. Lin and C. C. Chang, "An Improved Low Computation Cost User Authentication Scheme for Mobile Communication", *Proceedings of the 19th International Conference on Advanced Information Networking and Applications*, **2**, 2005.

[14] Robert Johnson, David Molnar, Dawn Song and David Wagner, "Homomorphic Signature Schemes", *In CT-RSA*, pp. 244-262, 2002. Springer-Verlag.

[15] J. Caldera, D. De-Niz and J. Nakagawa, "Performance Analysis of ipsec and ike for Mobile ip on Wireless Environments", *Technical Report*, Information Networking Institute, Carnegie Mellon University, 2000. Available at *http://www.cs.cmu.edu/dionisio/personal-publications.html*.

[16] B. Bezawada, K. Kothapalli and S. D. Maddi, "Reducing The Cost of Session Key Establishment", *Proceedings of International Conference on Availability, Reliability and Security*, pp. 369–373, 2009, IEEE Computer Society.

[17] Robert Edward Palma Junior, A Problem with Public Key Encryption and PKI, White paper, KetuFile, 2003. Available at *http://www.ketufile.com/Problem_With_Public_Key_Encryption_and_PKI.pdf*.