ISSN 2395-1621

Privacy-Preserving Authentication for Identity based Key Exchange over Internet

[#1]Mr. Munde Manoj V., [#2]Mr. Kalbande Hanuman M., [#3]Mr. Khaire Nikhil R.,
[#4]Mr. Kakde Shrikant V., [#5]Prof. Phursule R.N.

[1]manojvmundhe777@gmail.com
[2]kalbandehanuman02@gmail.com
[3]Nikhilkhaire1536@gmail.com
[4]shrikantkakde007@gmail.com

[#1234]Department of Information Technology
[#5]Prof. Department of Information Technology

Jspm's
Imperial College Of Engineering & Research,
Wagholi, Pune-412207.

ABSTRACT

Proposing a New secure channel between user and sender. Both are agree for exchanging his identity at communication time. We develop a family of privacy-preserving authenticated DHKE protocols named deniable Internet key-exchange (DIKE), both in the traditional PKI setting and in the identity-based setting. The newly developed DIKE protocols are of conceptual clarity and practical (online) efficiency. They provide useful privacy protection to both protocol participants, and add novelty and new value to the IKE standard. To the best of our knowledge, our protocols are the first provably secure DHKE protocols that additionally enjoy all the following privacy protection advantages: 1) forward deniability, actually concurrent non-malleable statistical zero-knowledge, for both protocol participants simultaneously; 2) the session transcript and session-key can be generated merely from DH-exponents (together with some public values), which thus cannot be traced to the pair of protocol participants; and 3) exchanged messages do not bear peer's identity, and do not explicitly bear player role information.

ARTICLE INFO

Article History

Received: 8th May 2016

Received in revised form :

8th May 2016

Accepted: 11th May 2016

Published online :

18th May 2016

Keywords: **DHKE, PKI, Key Exchange, Privacy Preserving.**

I. INTRODUCTION

Basic Concept

This Work Represent the detail of check the identity of customer as well as seller for secure communication with using key.

The key exchange (IKE) Protocols, are the core cryptographic protocols to ensure internet security, which specify the key exchange mechanism used to established shared key for use in internet Protocol security standards (Ipsec). The IPSec and IKE are intended to protect message communicated in IP layer i.e layer 3 of ISO-OSI which process the transmission of messages using the network address possibly without knowing end user peers identity. The IKE and IPSec can it turn be used to offer confidentiality, authentication and privacy for communication protocols in the higher layer of ISO-OSI. In this work, develop a family of privacy-preserving (particularly, deniable) authenticated DHKE protocols, named deniable Internet key-exchange (DIKE), in the traditional PKI setting and in the identity-based setting. The newly developed DIKE protocols are of conceptual clarity, practical (online) efficiency, provide useful privacy protection to both protocol participants, and add novelty and new value to the IKE standard and the SIGMA protocol.

Motivation:

Proposing a New secure channel between user and sender. Both are agree for exchanging his identity at communication time.

We develop a family of privacy-preserving authenticated DHKE protocols named deniable Internet key-exchange

(DIKE), both in the traditional PKI setting and in the identity-based setting.

The newly developed DIKE protocols are of conceptual clarity and practical (online) efficiency. They provide useful privacy protection to both protocol participants, and add novelty and new value to the IKE standard. To the best of our knowledge, our protocols are the first provably secure DHKE protocols that additionally enjoy all the following privacy protection advantages: 1) forward deniability, actually concurrent non-malleable statistical zero-knowledge, for both protocol participants simultaneously; 2) the session transcript and session-key can be generated merely from DH-exponents (together with some public values), which thus cannot be traced to the pair of protocol participants; and 3) exchanged messages do not bear peer's identity, and do not explicitly bear player role information.

II. PROBLEM STATEMENT

To design a system for identity based both users and providers by using DHKE protocol and some other family algorithm of key exchange protocols.

III. PROJECT OBJECTIVE

Our system will present the identity based online secure channel for security purpose with using some protocols.

The newly developed DIKE protocols are of conceptual clarity and practical (online) efficiency. They provide useful privacy protection to both protocol participants, and add novelty and new value to the IKE standard.

IV. PROPOSED SYSTEM

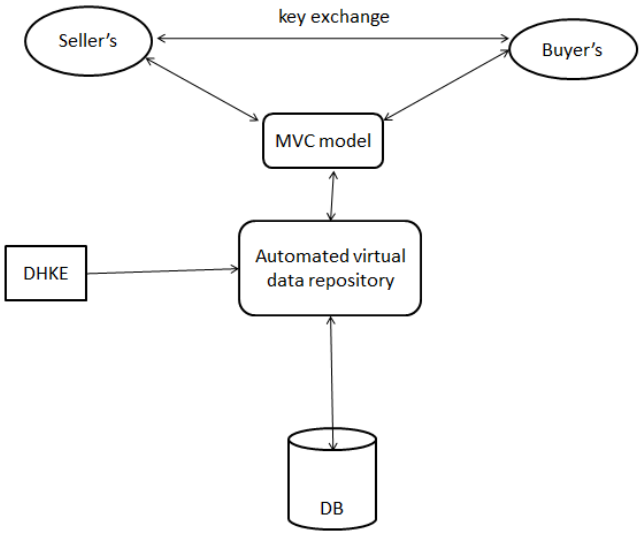

Fig 1. System architecture

We develop a family of privacy-preserving authenticated DHKE protocols named (DIKE).

The newly developed DIKE protocol provides useful privacy protection to both protocol participants, and adds novelty and new value to the IKE standard.

Secure DHKE protocols that additionally enjoy all the following privacy protection advantages:

Forward deniability.

Session key generated which is not traced.

Exchanged messages do not bear peer's identity.

Mathematical Model:

DHIKE Algo:

R-user
S_Seller
Select 2 prime number(key)
R- Select random no a
S- Select random no b
R=q^a mod p
S=q^b mod p
S(k)=R^b mod p
R(k)=S(k)=K
K-"Symmetric key".

V. RESULT

VI. CONCLUSION

We have to conclude Using the deniable Internet key-exchange (DIKE), algorithm can result in efficiency, provide useful privacy protection to both Participants.

REFERENCES

1. H. Krawczyk "SIGMA: The 'Sign-and-Mac' approach to authenticated Diffie-Hellman and its use in the IKE-protocols," in Proc. CRYPTO 2003.

2. C.Kudla and K. Paterson, "Modular security proofs for key agreement protocols," in Proc.Asiacrypt 2005.

3. K.Neupane,R.Steinwandt, and A. S. Corona, "Scalable deniable group key establishment," in Proc. FPS 2012.

4. A.P.Sarr and P. E. Vincent, "A complementary analysis of the (s)YZ and DIKE Protocols," in Proc. Africacrypt 2014.

