IDENTIFY-BASED ENCRYPTION WITH SERVER REVOCATION AUTHORITY USING PASSWORD AUTHENTICATED KEY EXCHANGE

A.Yugandhara Rao[1], D.Ramya[2], B.Sumana[3], B.Sravani[4], B.Anil Krishna[5]

Abstract: In two-server password-authenticated key exchange (PAKE) protocol, a client splits its password and stores two shares of its password in the two servers, respectively, and the two servers then cooperate to authenticate the client without knowing the password of the client. In case one server is compromised by an adversary, the password of the client is required to remain secure. In this paper, we present two compilers that transform any two-party PAKE protocol to a two-server PAKE protocol on the basis of the identity-based cryptography, called ID2S PAKE protocol. By the compilers, we can construct ID2S PAKE protocols which achieve implicit authentication. As long as the underlying two-party PAKE protocol and identity-based encryption or signature scheme have provable security without random oracles, the ID2S PAKE protocols constructed by the compilers can be proven to be secure without random oracles. Compared with the Katz et al.'s two-server PAKE protocol with provable security without random oracles, our ID2S .PAKE protocol can save from 22% to 66% of computation in each server.

Keywords: password-authenticated key exchange, identity-based encryption and signature, Diffie-Hellman key exchange, decisional Diffie-Hellman problem

I. INTRODUCTION

TO secure communications between two parties, an authenticated encryption key is required to agree on in advance. So far, two models have existed for authenticated key exchange. One model assumes that two parties already share some cryptographically-strong information: either a secret key which can be used for encryption authentication of messages, or a public key which can be used for encryption signing of messages. These keys are random and hard to remember. In practice, a user often keeps his keys in a personal device protected by a password/PIN. Another model assumes that users, without help of personal devices, are only capable of storing "human-memorable" passwords. Bellovin and Merritt [4] were the first to introduce password-based authenticated key exchange (PAKE), where two parties, based only on their knowledge of a password, establish a cryptographic key by exchange of messages. APAKE protocol has to be immune to on-line and off-line dictionary attacks. In an off-line dictionary attack, an adversary exhaustively tries all possible passwords in a dictionary in order to determine the password of the client on the basis of the exchanged messages. In on-line dictionary attack, an adversary simply attempts to login repeatedly, trying each possible password. By cryptographic means only, none of PAKE protocols can prevent on-line dictionary attacks. Button-line attacks can be stopped simply by setting a threshold to the number of login failures.

II. LITERATURE REVIEW

Encrypted key exchange: password-based protocols secure against dictionary attacks
M. Merritt , S.M. Bellovin
Abstract:
Classic cryptographic protocols based on user-chosen keys allow an attacker to mount password-guessing attacks. A combination of asymmetric (public-key) and symmetric (secret-key) cryptography that allow two parties sharing a common password to exchange confidential and authenticated information over an insecure network is introduced. In particular, a protocol relying on the counter-intuitive motion of using a secret key to encrypt a public key is presented. Such protocols are secure against active attacks, and have the property that the password is protected against offline dictionary attacks.
Kerberos: an authentication service for computer networks
B.C. Neuman , T. Ts'o
Abstract:
When using authentication based on cryptography, an attacker listening to the network gains no information that would enable it to falsely claim another's identity. Kerberos is the most commonly used example of this type of authentication technology. The authors concentrate on authentication for real-time, interactive services that are offered on computer networks. They use the term real-time loosely to mean that a client process is waiting for a response to a query or command so that it can display the results to the user, or otherwise continue performing its intended function. This class of services includes remote login, file system reads and writes, and information retrieval for applications like Mosaic.
New directions in cryptography
W.HYPERLINK "http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=%22Authors%22:.QT.W.%20Diffie.QT.&newsearch=true"Diffie ,
M. Hellman
Abstract:
Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

Server-assisted generation of a strong secret from a password
W. Ford , B.S. Kaliski
A roaming user, who accesses a network front different client terminals, can be supported by a credentials server that authenticates the user by password then assists in launching a secure environment for the user. However, traditional credentials server designs are vulnerable to exhaustive password guessing attack at the server. We describe a credentials server model and supporting protocol that overcomes that deficiency. The protocol provides for securely generating a strong secret from a weak secret (password), based on communications exchanges with two or more independent servers. The result can be leveraged in various ways, for example, the strong secret can be used to decrypt an encrypted private key or it can be used in strongly authenticating to an application server. The protocol has the properties that a would-be attacker cannot feasibly complete the strong secret and has only a limited opportunity to guess the password, even if he or she has access to all messages and has control over some, but not all, of the servers.

III. PROPOSED WORK

In this paper, we propose a new compiler for ID2S PAKE protocol based on any identity-based signature scheme (IBS), such as the Paterson et al.'s scheme. The basic idea is: The client splits its password into two shares and each server keeps one share of the password in addition to a private key related to its identity for signing. In key exchange, each server sends the client its public key for encryption with its identity-based signature on it. The signature can be verified by the client on the basis of the identity of the server. If the signature is genuine, the client submits to the server one share of the password encrypted with the public key of the server. With the decryption keys, both servers can derive the same one-time password, by which the two servers can run a two-party PAKE protocol to authenticate the client.

ADVANTAGES OF PROPOSED SYSTEM

We have implemented our ID2S PAKE protocols, it shows that our protocols save from 22% to 66% of computation in each server, compared with the Katz et al.'s protocol. The server performance is critical to the performance of the whole protocol when the servers provide services to a great number of clients concurrently. Our Protocol shows that less than one second is needed for the client to execute our protocols. This is modeled by allowing each user to have unlimited number of instances with which to execute the protocol.

SYSTEM ARCHITECTURE:

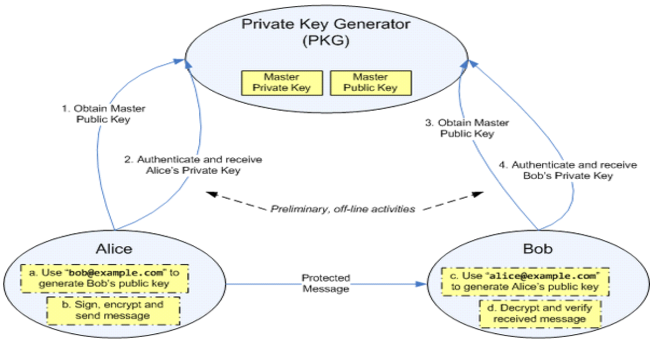
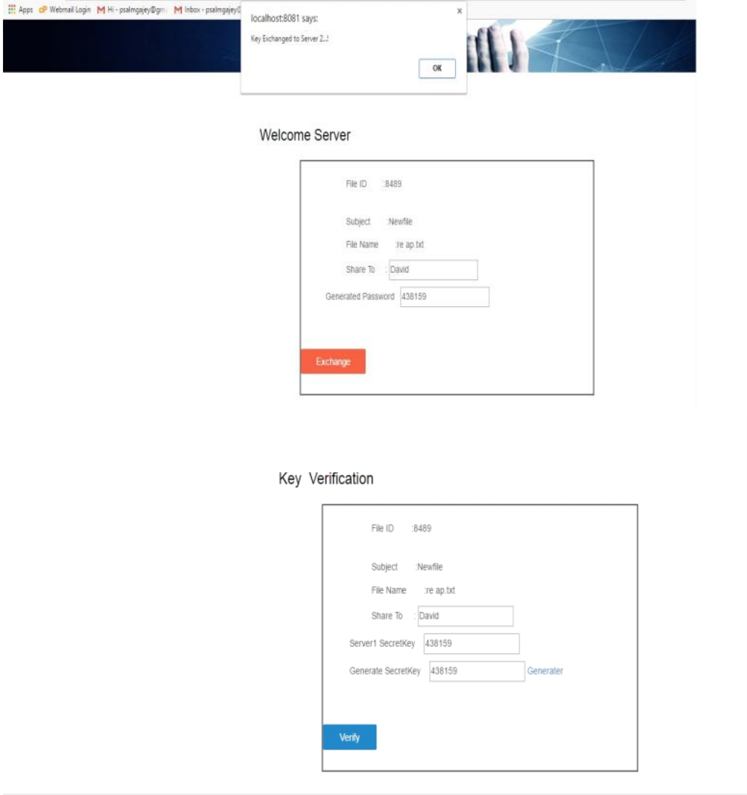

Private Key Generator
(PKG)
Master Private Key
Master Public Key
1. Obtain Master Public Key
2. Authenticate and receive Alice's Private Key
3. Obtain Master Public Key
4. Authenticate and receive Bob's Private Key
Preliminary, off-line activities
Alice
a. Use "bob@example.com" to generate Bob's public key
b. Sign, encrypt and send message
Protected Message
Bob
c. Use "alice@example.com" to generate Alice's public key
d. Decrypt and verify received message

Fig 1:system architecture

STEPS IN THE ALGORITHM:
1.Alice and Bob agree on a prime number p and a base g.
2.Alice chooses a secret number a, and sends Bob (g a mod p).
3.Bob chooses a secret number b, and sends Alicde (g b mod p).
4.Alice computers ((g b mod p)b mod p).
5.Bob computers ((g a mod p) b mod p).Both Alice and Bob can use this number as their key.
Notice that p and g need not be protected.
Example:
1.Alice and Bob agree on p=23 and g=5.
2.Alicechooses a=6 and sends 5 6 mod 23 =8.
3.Bob chooses b =15 and sends 515 mod 23 =19.
4.Alice computers 196 mod 23 =2.
5.Bob computers 815 mod 23 =2.
Sample outputs:-

Fig 2:Home page



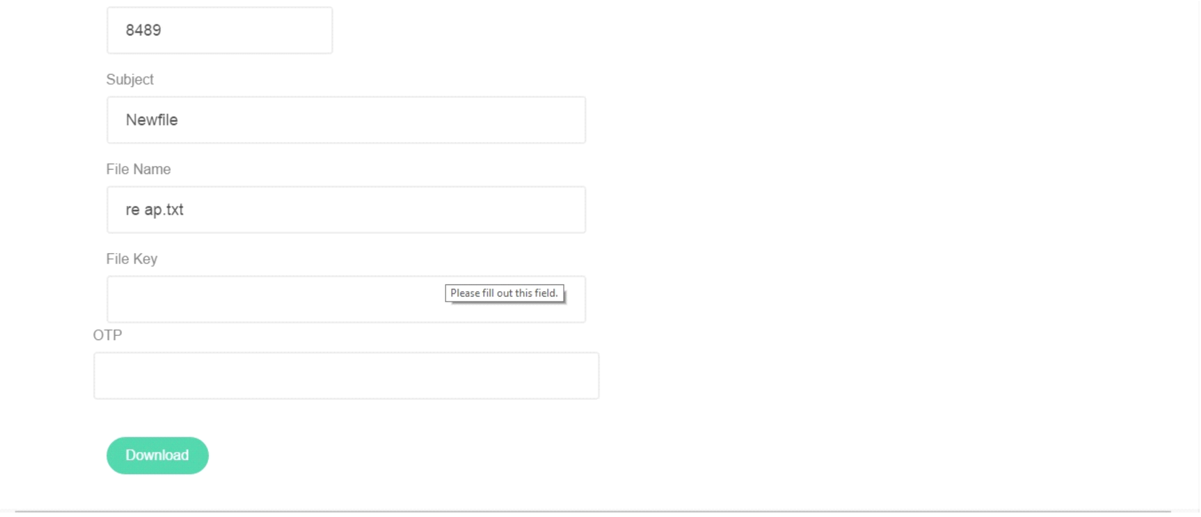
localhost:8081 says:
Key Exchanged to Server 2...!

Welcome Server

File ID :8489
Subject :Newfile
File Name :re ap.txt
Share To : David
Generated Password 438159

Key Verification

File ID :8489
Subject :Newfile
File Name :re ap.txt
Share To : David
Server1 SecretKey 438159
Generate SecretKey 438159



8489

Subject

Newfile

File Name

re ap.txt

File Key

Please fill out this field.

OTP

Fig 3: file download

IV. CONCLUSION

We present two efficient compilers to transform any two-party PAKE protocol to an ID2S PAKE protocol with identity-based cryptography. In addition, we have provided a rigorous proof of security for our compilers without random oracle. Our compilers are in particular suitable for the applications of password-based authentication where an identity-based system has already established. Our future work is to construct an identity-based multiple server PAKE protocol with any two-party PAKE protocol

REFERENCES

[1] M. Abdalla and D. Pointcheval. Simple password-based encrypted key exchange protocols. In Proc. CT-RSA 2005, pages 191-208, 2005.

[2] M. Bellare, D. Pointcheval, and P. Rogaway.Authenticated key exchange secure against dictionary attacks. In Proc. Eurocrypt'00, pages 139-155, 2000.

[3] S. M. Bellovin and M. Merritt.Encrypted key exchange: Passwordbased protocol secure against dictionary attack. In Proc. 1992 IEEE Symposium on Research in Security and Privacy, pages 72-84, 1992.

[4] J. Bender, M. Fischlin, and D. Kugler. Security analysis of the PACE

[5] key-agreement protocol. In Proc. ISC'09, pages 33-48, 2009.

[6] J. Bender, M. Fischlin, and D. Kugler. The PACEjCA protocol for

[7] machine readable travel documents. In INTRUST'13, pages 17-35,2013.

[8] D. Boneh and M. Franklin. Identity based encryption from the Weilpairing. In Proc. Crypto'01, pages 213-229, 2001.

[9] V. Boyko, P. Mackenzie, and S. Patel. Provably secure password authenticated key exchange using Diffie-Hellman. In Proc. Eurocrypt'00, pages 156-171, 2000.