International Journal of Emerging Trend in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 2 , Issue 1(Jan-Feb 2015), PP251-256

Efficient Two-Server Password-Only Authenticated Key Exchange in Cross Domain

Kirtee Chaudhari [1], Priya . Chopade [2] ,Veena Dhumal [3], Disha Gawade [4] , Seema Shabadi [5]

[1, 2, 3, 4.] *(Department of Computer,JSPM's Rajarshi Shahu College of Engineering, Savitribai Phule University,India.*

Abstract-Enabling Network Security over internet, firewalls play a major role. It checks all incoming or outgoing packet to decide whether to accept or discard the packet based on its policy. Prior work on firewall optimization focuses on either intra-firewall or inter-firewall optimization within one administrative domain where the privacy of firewall policies is not a concern. The key technical challenge is that firewall policies cannot be shared across domains because a firewall policy contains confidential information and even potential security holes, which can be exploited by attackers. Using Inter-firewall redundant rule which overcomes the prior problem and enables the Inter-firewall optimization across administrative domains. We propose the first cross-domain cooperative firewall (CDCF) policy optimization protocol. The optimization process involves cooperative computation between the two firewalls without any party disclosing its policy to the other. Along with the firewall optimization for secure communication work proposes the Password-authenticated key exchange (PAKE). It is where a client and a server, who share a password, authenticate each other and meanwhile establish a cryptographic key by exchange of messages. Hence this work also presents a symmetric solution for two-server PAKE, where the client can establish different cryptographic keys with the two servers, respectively.

Keywords– cross-domain cooperative firewall (CDCF), Inter-firewall, Intra-firewall, Password-authenticated key exchange (PAKE), policy.

I. INTRODUCTION

The protocol provides explicit authentication in the sense that each party know that other parties have established their secret session keys correctly if the message authentication by the party succeeds. If the client C accepts the messages M4 and M5, the client C is confirmed that the servers S1 and S2 will compute their secret session keys with the client C correctly. If the server S1 accepts the message M6, the server S1 is confirmed that the client C has computed the same secret session key SK1, and the client C and the server S2 have established their secret session key correctly.

Password-authenticated key exchange (PAKE) is where a client and a server, who share a password, authenticate each other and meanwhile establish a cryptographic key by exchange of messages. In this setting, all the passwords necessary to authenticate clients are stored in a single server. If the server is compromised, due to, for example, hacking or even insider attacks, passwords stored in the server are all disclosed. Also optimizing firewall policies is crucial for improving network performance. Prior work on firewall optimization focuses on either intrafirewall or interfirewall optimization within one administrative domain where the privacy of firewall policies is not a concern.

Here we consider a scenario where two servers cooperate to authenticate a client andif one server is compromised, the attacker still cannot pretend to be the client with the information from the compromised server. Current solutions for two-server PAKE are either symmetric in the sense that two peer servers equally contribute to the authentication or asymmetric in the sense that one server authenticates the client with the help of another server. This paper also explores interfirewall optimization across administrative domains for the first time. The key technical challenge is that firewall policies cannot be shared across domains because a firewall policy contains confidential information and even potential security holes, which can be exploited by attackers.

We have proposed the first cross-domain privacy-preserving cooperative firewall policy optimization protocol. Specifically, for any two adjacent firewalls belonging to two different administrative domains, our protocol can identify in each firewall the rules that can be removed because of the other firewall. The optimization process involves cooperative computation between the two firewalls without any party disclosing its policy to the other. Also we present a symmetric solution for two-server PAKE, where the client can establish different cryptographic keys with the two servers, respectively. Our protocol runs in parallel and is more efficient than existing symmetric two-server PAKE protocol, and even more efficient than existing asymmetric two-server PAKE protocols in terms of parallel computation.

II. BACKGROUND

When a password is saved on a single server and if that server is compromised then all the passwords stored on that server are disclosed to the attacker. To solve this problem Ford and Kaliski [1]in 2000 proposed the first PAKE protocol in which n servers cooperate to authenticate the client. As long as n-1 servers or few servers are compromised their protocol remains secure. Joblon[2] removed the requirement for PKI 2001. In 2002, MacKenzie et al [7] give a protocol in the PKI based setting, which requires t out of n servers to cooperate to authenticate a client. It is secure as long as t-1 or fewer servers are compromised. Di Raimondo and Gennaro [5] proposed a protocol in the password-only setting. It require less than 1/3 of the servers to be compromised.

In 2003, Brainard et al.[4] was the first one to develop two server protocol in the PKI based setting. Their protocol assumed a secure channel between the client and the server. In 2005 Katz et al.[9] proposed the first two server password- only authenticated key exchange protocol. It had a proof of security in the standard model.

In this paper, we discuss a new symmetric two server PAKE protocol. In this protocol two servers compute in parallel and meanwhile keep efficiency for practical use. In order to authenticate the client and establish a secret session key the protocol needs only four communication rounds for the client and two servers. The protocol is more efficient than Katz et al.[9] which is existing symmetric two server PAKE protocol. On considering parallel computation the protocol is more efficient than the existing asymmetric two server PAKE protocol, such as Yang et al. protocol [6] and Jin et al.[3] protocol.

III. PRELIMINARIES

3.1 Simple Password Exponential Key Exchange Protocol

One of the older and well known protocol called SPEKE[8] is used for password authenticated key exchange.In 1996 it was first described by David Jablon. SPEKE uses a generator g, were g is calculated as $g=g_q^{\ s}$ with a costant g_q but this value of g was insecure against dictionary attacks.

Here we explain a simple form of SPEKE:

1. Bob and Alice agree to randomly select a number called as safe prime were safe prime (p) can be 2q+1 were q is also a prime number.
2. They also agree on a hash function H().
3. Alice and Bob agree to select a shared password π.
4. They both construct $g=H(\pi)^2 \bmod p$.
5. Alice makes a choice of secret random integer a, then bob sends $g^a \bmod p$.
6. Bob makes a choice of secret random integer b, then sends Alice $g^b \bmod p$.
7. If the received values are not in the range [2,p-2] then Alice and Bob each abort their received values. They do this in order to prevent small subgroups confinement attack.
8. Alice calculates $K=(g^b \bmod p)^a \bmod p$.
9. Bob calculates $K=(g^a \bmod p)^b \bmod p$.

If Alice and Bob use the same value for π then only they arrive at a same value for K. Once the secret key K is computed Alice and Bob can use it in a key confirmation protocol in order to prove each other that they are authenticated users. It means they know the same password π. This can be used to derive a shared secret encryption key for sending secure and authenticated messages to each other.
SPEKE prevents man in m idle attack by incorporation of the password which Diffie Hellman does not prevent. The shared key K cannot be guessed by the attacker who is able to read and modify all messages between Alice and Bob. He cannot make more than one guess for the password in each interaction with a party that knows it.
Therefore SPEKE uses any prime number that is suitable for public key cryptography.

3.2 RC6 (Rivest Cipher 6)

RC6 is derived from RC5.It is a symmetric key block Cipher. It was designed to meet the requirements of the Advanced Encryption Standard (AES) Competition by R.Rivest, M.Robshaw, R.Sydney.RC6 supports 128 bits block size.
RC6 algorithm[8] works as follows :
Input: Plain text stored in r-bit input registers W,X,Y and Z.
w is the number of rounds
r-bit round keys S[0,.....,2r+3]

Output Cipher text stored in W,X,Y and Z
Encryption procedure is as follows:

```
X=X+S[0]
Z=Z+S[1]
for i=1 to w do
{
   t=(X*(2X+1))<<< lg r
   u=(Z*(2Z+1))<<< lg r
   W=((W XOR t)<<< u) + S[2i]
    Y=((Y XOR  u)<<< t) + S[2i+1]
    (W,X,Y,Z)=X,Y,Z,W
}
W=W+S[2]w+2
Y=Y+[2w+3]
```

Decryption procedure is as follows:

```
Y=Y-[2w+3]
W=W-S[2r+2]
for i=w downto 1 do
{
    (W, X, Y, Z)=(Z,W,X,Y)
u=(Z*(2Z+1))<<< lg r
    t=(X*(2X+1))<<< lg r
    Y=((Y-S[2i+1])>>> t) XOR u
    W=((W-S[2i])>>> u) XOR t
}
Z=Z-S[1]
X=X-S[0]
```

Hence, RC6 block cipher can be used for testing , verification, security analysis and encryption efficiency analysis.

IV. DESCRIPTION OF MODULES

Modules:
Module 1: Network Creation
Module 2: Data Communication
Module 3: Authentication and Secure Policy Maintenance in multiple or cross domain server

1. Network Creation: This module has the input as node introduction. It also identifies the node. The output of this module will be secure network creation. Our project promotes the use of shared secret key that can be used for secret communications while exchanging data over a public network. The crucial part of the process is that the two exchanging parties exchange their secret in a mix only. Finally this generates an identical key that is computationally difficult to reverse for another party that might have been listening in on them. Thus to preserve the security of the data, there is a need for our projects implementation.

2. Data Communication:
   The sub modules of this module will be as follows:
   a. Profile Management
- User Registration
- Color Profile Selection
- User Login

It is very necessary to know the complete data of the parties that have agreed to send data over the internet.

Implementation of the above algorithm ensures that the parties are verified and no tampering of data takes

place.

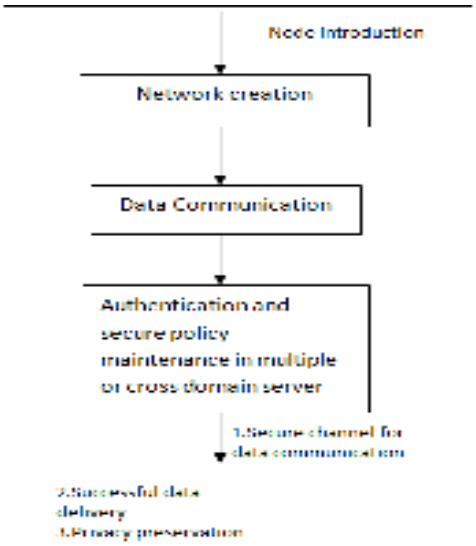

Fig.1 Flow of modules

3. Authentication and secure policy maintenance in multiple or cross domain:
   Authenticated key exchange maintains the data, and prevents its exposure to the attacker.
   It enables the system to confirm the identities of the exchanging parties and assure that the network is a secure network. Our algorithm proves to be very useful.

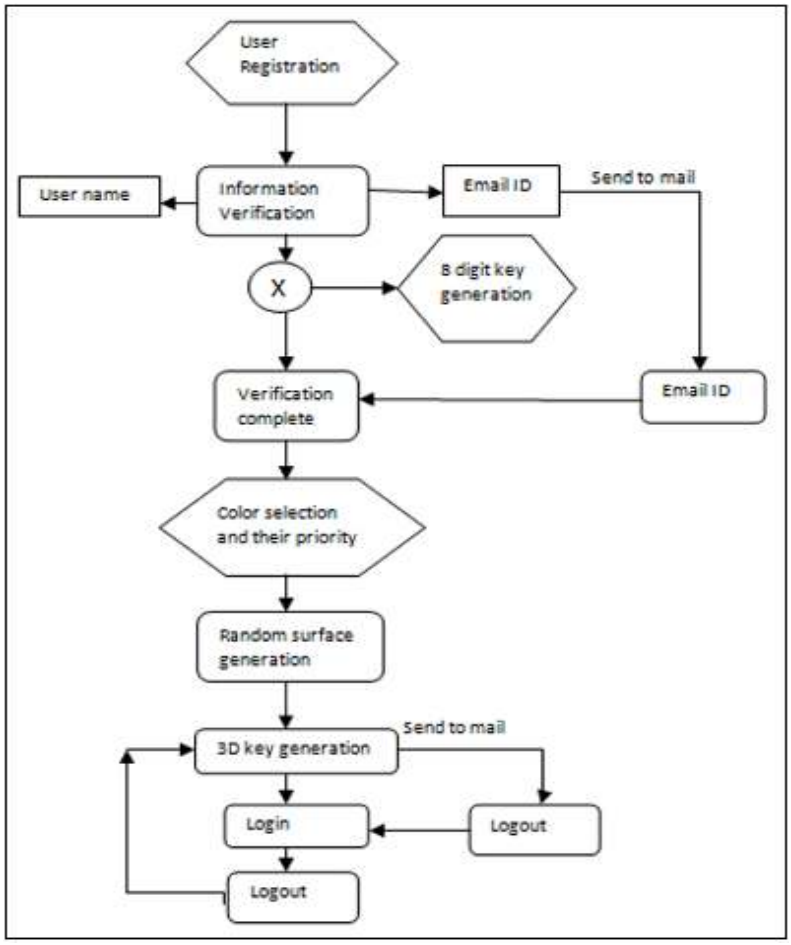

Fig.2 Authentication Process

V. CONCLUSION

In this paper, we have presented a symmetric protocol for two-server password-only authentication and key exchange. Security analysis has shown that our protocol is secure against passive and active attacks in case that one of the two servers is compromised. Performance analysis has shown that our protocol is more efficient than existing symmetric and asymmetric two-server PAKE protocols.

VI. REFERENCES

[1] W.Ford and B.S.Keliski JR.,"Server-Assisted Generation of a strong secret from a password",Proc. IEEE Ninth int'l Workshop Enabling Technologies:Infrastructure for Collaborative Enterprises.
[2] D.Joblon,"Password Authentication Using Multiple Servers"Proc.Conf.Topics in Crytography;The Crytographers track at RSA.
[3] H.Jin,D.S.Wong,and Y.Xu,"An Efficient Password only Two-Server Authenticated Key Exchange System"

[4] J.Brainard,A.Jueles,B.S.Celiski,and M.Szydlo,"A New Two-Server Approach for Authentication with short secret "Proc. 12thConf.USENIX Security Symp.

[5] M. Di Raimondo and R.Gennaro,"Provably Secure Threshold Password Authenticated Key Exchange",Proc. 22nd Int'l Conf.Theory and Applications of Cryptographic Techniques.
[6] Y.Yang,R.H. Deng, and F.Bao,"A Practical Password-Based Two-Server Authentication and key Exchange System",IEEE Trans. Dependable and Secure Computing.
[7]P. Mackenize, T. Shrimptom, and M. Jakobsson, "Threshold Password-Authenticated Exchange", Proc. 22nd Ann. Int'l Crytology Conf. (Crypto '02), pp. 385-400, 2002.
[8] http://en.wikipedia.org/wiki/RC6
[9] J. Katz, P. MacKenzie, G. Taban, and V.Gligor, "Two-Server Password-Only Authenticated Key Exchange", Proc. Applied Crytography and Network Security(ACNS '05), pp. 1-16,2005.