International Journal of Pure and Applied Mathematics
Volume 118 No. 7 2018, 381-386
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

Partial Password Authentication using Vector Decomposition

Praveen I
Department of Mathematics,
Amrita School of Engineering, Coimbatore
Amrita Vishwa Vidyapeetham,India.
E-mail: i_praveen@cb.amrita.edu

M Sethumadhavan
TIFAC CORE in Cyber Security,
Amrita School of Engineering, Coimbatore
Amrita Vishwa Vidyapeetham,India.
E-mail: m_sethu@cb.amrita.edu

Abstract– Validation using partial passwords is a mode of authentication which is used in financial sector. This mode of authentication enhances security against attckers attemting to retrieve password by not allowing to realize the full password in a single attempt. Since the studies regarding partial password authentication are available comparatively less in the academic literature, many queries regarding it remain unanswered. In this paper, we propose a scheme for partial password authentication based on vector decomposition problem. The proposed scheme is based on a two-party protocol to securely evaluate 2DNF formula in higher dimensional vector spaces, using vector decomposition problem. The proposed scheme permits the user to select the arbitrary characters of the actual password to be entered, in random order.

Keywords: Vector Decomposition Problem, Partial Passwords, E-Banking

I. INTRODUCTION

Partial password is a mode of password authentication uses a subset of characters from a full password. This method enhances the security on the client side in the sense that it provides comparatively less information to keystroke loggers or shoulder surfers and that the fraudsters cannot provide the full password to their command-and-control (CC) server in a single step. Though partial passwords were introduced in telephonic banking, its significance are extended to other sort of online banking web applications especially in UK as a part of 2-factor authentication method for authenticating users in internet banking.

All type of attacks which are applicable to the password authentication process are also applicable in the case of partial password authentication. But for launching a successful attack, the attacker requires more data. As far as the server side is concerned, the security of partial password authentication can be considered as weak, since the queries regarding the number of observations required for an attacker to learn the complete password is not known explicitly. There exists no formal academic literature which discusses the problem of server side implementation of partial password authentication mechanism, till date, to the best of our knowledge. Just and Aspinall[1] and Mourouzis *et. al.*[7] have done a profound study on various types of possible attacks in the use of partial passwords. According to[1], [7] and several online security related forums, the possible partial password implementations deployed in the industry is as follows:

1. Store the actual password in the form of plaintext and compare the partial entries. It is obvious that this increases the risk from security point of view, since any compromise of database will result in the direct access to the full password to the adversary. Moreover, the administrator is likely to have direct access to the full password which will not match with the policies of password storage.
2. The use of hashed values: Corresponding to each password, store the hash values of all possible combinations of letters per user. This will lead to database issues. The required database storage space will at least quadratic with the length of the password. Hence it will become a requirement to bring restrictions on the length of the password or the size of the character set. These are not advisable from the security point of view.
3. Use symmetric encryption schemes, like AES, for encrypting the full password and store it in the encrypted form. This leads of the requirement of tamper resistant hardware. During the authentication process, the full password is decrypted and there is some chance for the leakage of this decrypted password.
4. Solution based on Secret Sharing schemes, for example, by using Shamir's Secret Sharing Scheme. However, this method is also restricted to the difficulty of finding a number of letters from the full password.

In this paper, we propose a scheme for partial password authentication based on vector decomposition problem (VDP).

The proposed scheme is based on storing a 2-DNF formula corresponding to each password and evaluation of the formula for authentication process. Hence our scheme does not require to store the password neither as plaintext nor in the encrypted form. It is not possible to reconstruct the full password using the stored data. In this manner, the mechanism resembles to that of storing the hash value of the full password. But in the case partial passwords, the usage of hashed values requires to store the digest of each combination of the letters in the full password using hash results, which is not required in the proposed scheme. Since during each authentication process different random numbers are used, any compromise of the previous evaluations does not provide any information about the full or partial password. In this manner the proposed scheme provides forward secrecy. Since each computation depends on the secure 2-DNF formula evaluation, if any of the partial entries are known to the attacker, it will not provide significant advantage in finding the other entries. The proposed work is an extension of [12]. The scheme proposed in [12] does not allow the entry of arbitrary characters where the proposed scheme provides the option.

Vector Decomposition Problem (VDP) was put forward by Yoshida[13],[14] and was introduced as a substitute to discrete logarithm problem (DLP) or computational Diffie-Hellman problem (CDHP). The problem gave an impression that it is a promising candidate in cryptography as an alternative to these assumptions and further studied by Duursma, Kiyavash[3], Duursma, Park[4] and Galbraith, Verheul[5]. In 2008, Okamoto and Takashima generalised the concept of VDP into higher dimensions with an innovative notion called *dual pairing vector spaces*[9]. Using this generalised VDP, they proposed a homomorphic encryption scheme and signature schemes. There are many applications of VDP are available[6],[8],[10],[11]. As an application of the encryption scheme, a two party protocol to securely evaluate a $2DNF$ formula is described[9]. We use a variant of this protocol and propose the scheme for partial password authentication.

Preliminaries are described in Section 2. The scheme for partial password authentication and its correctness are explained in Section 3. The conclusion of the work follows in Section 4.

II. PRELIMINARIES

Bilinear map is a function $e: G_1 \times G_2 \to G_3$ where G_1, G_2, G_3 are groups of finite order such that $e(u^a, v^b) = e(u,v)^{ab}$, for all $u \in G_1$, $v \in G_2$ and integers *a, b*.

Definition 2.1: A bilinear pairing on the finite order groups (G_1, G_2, G') *is an efficiently computable bilinear map* $\rho: G_1 \times G_2 :\to G'$, *with the following properties.*

1. $\rho(x+y,z) = \rho(x,z)\rho(y,z)$, for all $x, y \in G_1, z \in G_2$
2. $\rho(x, y+z) = \rho(x,y)\rho(x,z)$, for all $x \in G_1, y, z \in G_2$,
3. $\rho(x,y) \neq 1$, $\forall x \neq y$.

A. *Vector Decomposition Problem*

For generalising VDP to higher dimensions,the notion of dual pairing vector spaces was introduced by Okamoto and Takashima[9]. The higher dimensional VDP is defined as follows.

Definition 2.2: Generalised Computational Vector Decomposition Problem(gCVDP): For a given basis $\{A_1, A_2, .., A_n\}$ *of a vector space* V *and a vector* $C \in \mathsf{V}$, *VDP with respect to the basis* $\{A_1, A_2, .., A_n\}$ *is to find the element* $P \in \mathsf{V}$ *such that for* $m < n$, $P \in < A_1, A_2, .., A_m >$ *and* $Q \in < A_{m+1}, .., A_n >$ *where* $C = P + Q$.

The $gCVDP_{(m,n)(\lambda)}$ *advantage of* A is

$$Pr\{w = \sum_{i=1}^{m} x_i A_i / v = \sum_{i=1}^{n} x_i (A_i, A_1, A_2, .., A_n) \in \mathsf{V}^n\}$$

where A is a probabilistic polynomial time machine and V is a $n-$dimensional vector space over F_p where λ is the security parameter of the setup algorithm[9].

The gCVDP assumption declares that the $gCVDP_{(m,n)}(\lambda)$ *advantage is insignificant for any polynomial time adversary* A where λ is the security parameter of the setup algorithm.

Definition 2.3: Generalised Computational Diffie Hellman Problem(gCDHP): If $(A_{m+1}, A_{m+2}, .., A_n), (A'_{m+1}, A'_{m+2}, .., A'_n) \in \mathsf{V}^{(n-m)}$ where V is a $n-$dimensional vector space over the field F_p where $m < n$ and if $v = \sum_{i=m+1}^{n} x_i A_i$, $w = \sum_{i=m+1}^{n} x_i A'_i$, where $x_{m+1}, .., x_n \in \mathsf{F}_p$, $gCDHP$ is to find w given v, A_i and A'_i, $i = m+1, .., n$.

The $gCDHP_{(m,n)}$ *advantage of* A

$$Pr\{w = \sum_{i=m+1}^{n} x_i A'_i / v = \sum_{i=m+1}^{n} x_i A_i, A_i, A'_i \in \mathsf{V},$$

for $i = m+1, .., n$ where A is a probabilistic polynomial time machine and V and V is a $n-$dimensional vector space over F_p where λ is the security parameter of the setup algorithm

The gCDHP assumption declares that the $gCDHP_{(m,n)}(\lambda)$ *advantage is insignificant for any polynomial time adversary* A where λ is the security parameter of the setup algorithm.

B. Trapdoor for VDP

The hardness of VDP based schemes demands a trapdoor for its applications in cryptography. This can be achieved by using a distortion eigenvector space proposed by Okamoto and Takashima[9]. Given be a distortion eigenvector basis $(B_1, B_2,.., B_n)$ of be a distortion eigenvector space $\vee$, a change of basis is done using a transformation matrix, say, $X = (x_{ij})$. That is, $A_i = \sum_{j=1}^{n} x_{ij} B_j$. If the basis $(A_1, A_2,.., A_n)$ and $v = \sum_{i=1}^{n} y_i A_i$ are given, our goal find a vector $w = \sum_{i=1}^{m} y_i A_i$, $m < n$. If $X^{-1} = (t_{ij})$, lemma 3 of [9] proves the function

$VDeco(v, < A_j >, X, < A_1, A_2,.., A_n >)$

$= \sum_{i=1}^{n} \sum_{k=1}^{n} t_{ij} x_{jk} \phi_{ki}(Pr_i(v))$

can be used to accomplish this goal.

III. TWO PARTY PROTOCOL TO SECURELY EVALUATE $2DNF$ FORMULA

A. Okamoto and Takshima Protocol

A $2-DNF$ formula ψ over $a_0, a_1,.., a_n$ is of the form $\vee_{i=1}^{n} (\lambda_{i1} \wedge \lambda_{i2})$, where $\lambda_{i1}, \lambda_{i2} \in \{a_0, a_1,.., a_n, \bar{a}_0, \bar{a}_1,.., \bar{a}_n\}$. Okamoto and Takashima proposed a two party protocol to securely evaluate $2DNF$ formula. This is the first protocol to securley evaluate a $2DNF$ formula using prime order subgroups. The arithematization Ψ of ψ is computed by repalcing '$\vee$' by '$+$', '$\wedge$' by '$.$' and $\bar{a}_i$ by $1 - a_i$. Okamoto and Takashima scheme is secure against semi-honest Alice and Bob under $DSP_{(m,n)}$ assumption.

B. Proposed Scheme for Partial Password Athentication

We use a variant of Okamoto and Takashima protocol to attain partial password authentication. In our scheme, Alice(or the Server) holds $2DNF$ formula and Bob(or the User) will enter the input values and at the end of the communication, Alice successfully verifies the entered quantities by evaluating the formula. Further more, the proposed scheme allows the user to choose the arbitarary positions of their password, the number of arbitrary positions to be entered. The proposed scheme is secure in the semi-honest model described in [2]. The following procedure is used for partial password authentication:

- Alice executes $Gen(1^k)$ to compute Sk, Pk and sends $Pk = (A_1, A_2,....A_n)$ to Bob.
- Bob encrypts the password $(m_1, m_2,....m_n)$ using Pk of Alice and sends $C = m_1 A_1 + m_2 A_2 + ... + m_n A_n$.
- Alice use $VDeco(C, < A_i >, X, Pk) = m_i A_i$, for $i = 1,2..,n$. Let x_i be the $x-$coordinate of $m_i A_i$ and let $x_i = x_{i1} x_{i2}..x_{il_2}$, $l_2 < n$
- Alice calculates $\psi(x_1, x_2,.., x_{l_2})$

  $= (\sum_{i=1}^{n} \lambda_{i11}.\lambda_{i21},.., \sum_{i=1}^{n} \lambda_{i1l_2}.\lambda_{i2l_2})$, where

  $\lambda_{i1j}, \lambda_{i2j} \in \{x_{i1}, x_{i2},.., x_{il_2}, 1-x_{i1}, 1-x_{i2},.., 1-x_{il_2}\}$, $for\ j = 1,2,.., l_2$
- When Bob initiates a transaction, Alice generates $c_{i1} = Enc(\lambda_{i11},.., \lambda_{i1l_2})$ and $c_{i2} = Enc(\lambda_{i21},.., \lambda_{i2l_2})$ using Alice's Pk.

  Hence,

  $c_{i1} = \lambda_{i11} A_1 + .. + \lambda_{i1l_2} A_{l_2} + r_{i1l_2+1} A_{l_2+1},.. + r_{i1n} A_n$ and

  $c_{i2} = \lambda_{i21} A_1 + .. + \lambda_{i2l_2} A_{l_2} + r_{i2l_2+1} A_{l_2+1},.. + r_{i2n} A_n$
- Alice sends (c_{i1}, c_{i2}) asks Bob to enter the partial entires of his paasword and the positions of the entered elements, for arbitrary $i = 1,2,.., l_2$.
- Bob enters m_i for some arbitarary $i \in \{1,2,.., l_2\}$.
- When Bob enters m_i, the system generates $m_i A_i$ and generates random numbers $t_{ijk} (i = 1,2,.., n; j = 1,2; k = 1,2,.., l_1)$: system also generates random numbers $u_{\sigma,\mu} (\sigma = 1,2,.., l_2, \mu = 1,2,.., l_1)$.
- System computes $c_{i1}^* = c_{i1} + \sum_{k=1}^{l_2} t_{i1k} A_k$;

  $c_{i2}^* = c_{i2} + \sum_{k=1}^{l_2} t_{i2k} A_k$ and

  $E_k = \{\sum_{i=1}^{n} (t_{i1k} c_{i2} + t_{i2k} c_{i1}) + t_{i1k} t_{i2k} A_k\} + \sum_{\mu \neq k, i=1}^{l_1} u_{i\mu} A_\mu$.

  System also calculates

  $P_S = \sum_{j-entered} j A_{i+1} + \sum_{not entered} \hat{j} A_i$ where j is the position of entries in the actual password and $\hat{j}$ is random and sends $(E_i, c_{i1}^*, c_{i2}^*, P_S)$, for $i = 1,2,.., l_2$ to Alice.
- After getting $(E_i, c_{i1}^*, c_{i2}^*, P_S)$ for $i = 1,2,.., l_2$, Alice

computes

$Z_k = \frac{\Pi_{i=1}^{n} e(VDeco(c_{i1}^*, < A_k >), \rho(e(VDeco(c_{i2}^*, < A_k >)))}{e(VDeco(E_k, < A_k >), \rho(A_k))}$, for $k = 1,2,..,l_2$

Here

$VDeco(c_{ij}^*, < A_k >) = VDeco(c_{ij}^*, < A_k >, X_A, Pk)$.

- Alice computes

$A_k' = VDeco(P_S, < A_k >, X_A, (A_1, A_2, .., A_{l_1}))$ and verifies $A_k' = jA_i$ for $i, j \in \{1,2,..,l_2\}$

- Alice verifies the authentication by checking

$Z_k = e(A_k, \rho(A_k))^{w_k}$, for $k = j$ such that $A_k' = jA_i$ for $i, j \in \{1,2,..,l_2\}$ where

$\psi(x_1, x_2, .., x_{l_2}) = (w_1, w_2, .., w_{l_2})$

$= (\sum_{i=1}^{n} \lambda_{i11}.\lambda_{i21}, .., \sum_{i=1}^{n} \lambda_{i1l_2}.\lambda_{i2l_2})$

C. Correctness of the Scheme

Proposition 3.1: The scheme described in Section 3.2 provides partial password authentication.

Proof

Alice computes

$A_k' = VDeco(P_S, < A_k >, X_A, (A_1, A_2, .., A_{l_1}))$ and verifies $A_k' = jA_i$ for $i, j \in \{1,2,..,l_2\}$ and identifies the values of *j*, the arbitrary positions of the full password.

The server(Alice) stores the 2DNF formula corresponding to every password of length l_2. If $x_1 x_2 .. x_{l_2}$ is the password, then the stored 2DNF formula is

$\psi(x_1, x_2, .., x_{l_2})$

$= (\sum_{i=1}^{n} \lambda_{i11}.\lambda_{i21}, \sum_{i=1}^{n} \lambda_{i12}.\lambda_{i22}, .., \sum_{i=1}^{n} \lambda_{i1l_2}.\lambda_{i2l_2})$

Let us denote $\psi(x_1, x_2, .., x_{l_2}) = (w_1, w_2, .., w_{l_2})$ so that

$\sum_{i=1}^{n} \lambda_{i1j}.\lambda_{i2j} = w_j$

After receiving $(E_i, c_{i1}^*, c_{i2}^*, P_S)$, Alice computes

$VDeco(c_{i1}^*, < A_k >, X_A, (A_1, A_2, .., A_{l_1})) = (\lambda_{i1k} + t_{i1k})A_k$

,

$VDeco(c_{i2}^*, < A_k >, X_A, (A_1, A_2, .., A_{l_1})) = (\lambda_{i2k} + t_{i2k})A_k$

Then the numerator of Z_k can be simplified to

$\Pi_{i=1}^{n} e(VDeco(c_{i1}^*, < A_k >), \rho(e(VDeco(c_{i2}^*, < A_k >))))$

$= e(A_k, \rho(A_k))^{\sum_{i=1}^{n} (\lambda_{i1k}\lambda_{i2k} + t_{i1k}\lambda_{i2k} + t_{i2k}\lambda_{i1k} + t_{i1k}t_{i2k})}$

If $\mu = k$, then

$VDeco(E_k, < A_\mu >, X_A, (A_1, A_2, .., A_{l_1}))$

$= \sum_{i=1}^{n} (t_{i1k}\lambda_{i2k} + t_{i2k}\lambda_{i1k} + t_{i1k}t_{i2k})A_k$

Else if $\mu \neq k$,

$VDeco(E_k, < A_\mu >, X_A, (A_1, A_2, .., A_{l_1})) = u_{i\mu}A_\mu$ Hence

If $\mu = k$, then the denominator is simplified to

$e(VDeco(E_k, < A_k >), \rho(A_k))$

$= e(A_k, \rho(A_k))^{\sum_{i=1}^{n} (t_{i1k}\lambda_{i2k} + t_{i2k}\lambda_{i1k} + t_{i1k}t_{i2k})}$

Else if $\mu \neq k$,then the denominator is simplified to

$e(VDeco(E_k, < A_k >), \rho(A_k))$

$= e(VDeco(E_k, < A_k >), \rho(A_k))^{u_{i\mu}}$

For those values of k for which $A_k' = jA_i$, Z_k simplifies to $Z_k = e(A_k, \rho(A_k))^{\sum_{i=1}^{n} \lambda_{i1k}.\lambda_{i2k}}$

Alice confirms the authentication by checking

$Z_k = e(A_k, \rho(A_k))^{w_k}$.

IV. CONCLUSION

Authentication using partial passwords is a novel method in E-banking. Although this method is already adopted in many countries, the server side security of these implementations is not discussed much in the academic literature. By considering the (informal) discussions of several information security experts in different online forums, we propose a scheme for authentication using partial passwords. The proposed scheme allows the user to choose the arbitrary partial entries to be entered from the original password, in any random order. The scheme is based on the secure evaluation of $2DNF$ formula and is secure in the semi-honest model under decisional subspace assumption. We expect our effort may be a magnet for more attention on the design of schemes for partial passwords authentication and also on the cryptanalysis in this direction.

REFERENCES

[1] David Aspinall and Mike Just. give me letters 2, 3 and 6!: Partial password implementations and attacks. In International Conference on Financial Cryptography and Data Security pages 126–143. Springer, 2013.

[2] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-dnf formulas on ciphertexts. In TCC, volume 3378, pages 325–341. Springer, 2005.

[3] Iwan M Duursma and Negar Kiyavash. The vector decomposition problem for elliptic and hyperelliptic curves. IACR Cryptology ePrint Archive, 2005:31, 2005.

[4] Iwan M Duursma and SeungKook Park. Elgamal type signature schemes for n-dimensional vector spaces.
IACR Cryptology ePrint Archive , 2006:312, 2006.

[5] Steven D Galbraith and Eric R Verheul. An analysis of the vector decomposition problem. In Public Key Cryptography–PKC 2008, pages 308–327. Springer, 2008.

[6] Manoj Kumar and I Praveen. A fully simulatable oblivious transfer scheme using vector decomposition. In
Intelligent Computing, Communication and Devices, pages 131–137.Springer, 2015.

[7] Theodosis Mourouzis, Marcin Wojcik, and Nikos Komninos. On the security evaluation of partial password implementations. arXiv preprint arXiv:1701.00104, 2016.

[8] D Nidhin, I Praveen, and K Praveen. Role-based access control for encrypted data using vector decomposition. In Proceedings of the International Conference on Soft Computing Systems, pages 123–131. Springer, 2016.

[9] Tatsuaki Okamoto and Katsuyuki Takashima. Homomorphic encryption and signatures from vector decomposition. In Pairing-Based Cryptography–Pairing 2008, pages 57–74. Springer, 2008.

[10] Tatsuaki Okamoto and Katsuyuki Takashima. Hierarchical predicate encryption for inner-products. In Advances in Cryptology–ASIACRYPT 2009, pages 214–231. Springer, 2009.

[11] I Praveen, K Rajeev, and M Sethumadhavan. An authenticated key agreement scheme using vector decomposition. Defence Science Journal, 66(6):594, 2016.

[12] M Sreedevi and Praveen I. Password authentication using vector decomposition. Inrternational Journal of Control Theory and Applications:9(10)pp.4639-4645, 2016.

[13] Maki Yoshida. Inseparable multiplex transmission using the pairing on elliptic curves and its application to watermarking. In Proc. Fifth Conference on Algebraic Geometry, Number Theory, Coding Theory and Cryptography, University of Tokyo, 2003.

[14] Maki Yoshida. Vector decomposition problem and the trapdoor inseparable multiplex transmission scheme based the problem. In The 2003 Symposium on Cryptography and Information Security SCIS'2003, 2003