ISSN: 0976-3031

Available Online at http://www.recentscientific.com

CODEN: IJRSFP (USA)

International Journal of Recent Scientific Research
Vol. 8, Issue, 11, pp. 21946-21952, November, 2017

International Journal of Recent Scientific Research

DOI: 10.24327/IJRSR

Research Article

VPA-3P-EKE: A VERIFIER-BASED PASSWORD-AUTHENTICATED 3P-EKE PROTOCOL AND ITS ANALYSIS

Archana Raghuvamshi[1]* and Premchand Parvataneni[2]

[1]Department of CSE, Adikavi Nannaya University, Rajamahendravaram, India
[2]Department of CSE, Osmania University, Hyderabad, India

DOI: http://dx.doi.org/10.24327/ijrsr.2017.0811.1168

ARTICLE INFO

Article History:

Received 17th August, 2017
Received in revised form 12th September, 2017
Accepted 04th October, 2017
Published online 28th November, 2017

Key Words:

Public-key Cryptosystem based on Logarithmic Approach(PCLA), Asymmetric Model, Verifier-based, Three-Party Encrypted Key Exchange (3P-EKE), Security Analysis, Performance Analysis.

ABSTRACT

This paper attempts to probe a new model for the standard structure of a Verifier-Based Password-Authenticated Three-Party Encrypted Key Exchange (VPA-3P-EKE) protocol which concedes more efficient model. A previous model presented by Archana *et al*. [1], is more secured against all types of attacks like password guessing, replay, pre-play, man-in-the-middle attack, etc., but unfortunately, this protocol does not solve the problem of a server compromise completely, because it is defined in a symmetric model. These drawbacks help as inspiration to search for another standard model which overcomes the existing problems in a smart way. The model which we design yields discerning explanation about the existing attacks that are not solved in our previous model. Further, it lets straight transformation from a group of approach private-key encryption to a hybrid (symmetric & Asymmetric) one without major hassle. This paper endeavors to probe a novel framework for establishing a secure session key based on an asymmetric model by using PCLA keys [2]. PCLA is a novel Public-key Cryptosystem based on the Logarithmic Approach proposed by Archana *et al*. in 2012[2].

INTRODUCTION

An Ideal password authenticated key exchange protocol should satisfy the security necessities like, Resistant to password guessing attacks , Mutual Authentication, Session Key (SK) security, Known-Key Security, Resistant to Trivial Attack, Perfect forward secrecy, Resistant to Pre-play Attack, Resistant to Replay Attack, backward secrecy, Server spoofing security, Resistant to Man-in-the-middle Attack, etc. A protocol proposed by Archana *et al*. [1] satisfies all the security requirements except one. That is if the server is compromised it reveals all the direct passwords of the clients, further which gives the scope for an attacker to attack.

Henceforth, the design of a novel framework which is smart in establishing a secure session key with less computational overhead; which proves to be secure against the attacks like Password Guessing Attacks (Online and Offline), Direct Server Compromise Attack, Trivial Attack, Pre-play Attack, Replay Attack, Man-in-the-middle Attack, and provides Mutual Authentication, Backward Secrecy, Forward Secrecy, Session Key Secrecy, Known-Key Security is the need of the hour.

This paper attempts to probe a new model for the standard structure of a Verifier-Based Password-Authenticated Three-Party Encrypted Key Exchange (VPA-3P-EKE) protocol which concedes more efficient model. A previous model presented by Archana *et al*. [1], is more secured against all types of attacks like password guessing, replay, pre-play, man-in-the-middle attack, etc., but unfortunately, this protocol does not solve the problem of a server compromise completely, because it is defined in a symmetric model. These drawbacks help as inspiration to search for another standard model which overcomes the existing problems in a smart way. The model which we design yields discerning explanation about the existing attacks that are not solved in our previous model. Further, it lets straight transformation from a group of approach private-key encryption to a hybrid (symmetric & Asymmetric) one without major hassle. This paper endeavors to propose a novel framework for establishing a secure session key based on an asymmetric model by using PCLA keys [2]**.** PCLA is a novel Public-key Cryptosystem based on the Logarithmic Approach proposed by Archana *et al*. in 2012[2]**.**

Corresponding author:* **Archana Raghuvamshi
Department of CSE, Adikavi Nannaya University, Rajamahendravaram, India

Further, the rest of the paper is planned as follows: The history and state of the art are discussed in section 2. A framework for the newVPA-3P-EKE Protocol based on PCLA Keys [2] is given in section 3. The security analysis by considering all possible types of attack are done in section 4and performance analysis with some of the existing protocols is done in section 5. Concluding remarks are given in section 6.

HISTORY AND STATE-OF-ART

Due to the lack of authentication, a Diffie-Hellman (1976) [9] key exchange protocol is suffered from a man-in-the-middle attack. To assure good access control, many applications require a robust client authentication. In such scenario, password-authenticated key exchange (PAKE) protocols [10, 11, 12, 13, 14, 15, 16, 17, 18, 19] have their own identity.

Bellovin and Merritt (1992) [20] have first proposed password-based authenticated encrypted key exchange protocol for the two-party network, but, due to the server compromise[21], (server hacking: e.g., In 2012, more than million LinkedIn passwords are stolen) this protocol no longer proved to be secure. Hence, to eliminate such a problem he proposed an improved protocol, known as Augmented EKE protocol (1993) [22], where a server instead of storing actual passwords, it stores the verifiers of the passwords which prevents from a server compromise [21] but it does not solve the problem of off-line dictionary attacks.

Subsequently, Gong *et al.*(1993) [23], proposed three-party password-based authenticated key exchange protocol using a server's public key, where the clients are given a risk to verify and keep the public key safely. Many improvements proposed by various researchers in terms of security and computational efficiency [24, 25, 26].

Abdalla *et al*. (2005) [3], proposed a 'provable secure' one-time password-based authentication and key exchange (OPKeyX) technology for grid computing; where a user changes the password from one session to another session to eliminate the problem of password sniffing. Lin *et al*. (2008) [6], proposed an efficient verifier-based password-authenticated key exchange protocol by using elliptic curve cryptography. Unfortunately, Yang *et al*. (2011) [7], showed the flaws of Lin *et al*. protocol [6]and proposed an improvement over the Efficient verifier-based password-authentication key exchange protocol via elliptic curves.

Also, Kulkarni *et al*., (2007) [27] proposed novel key exchange protocol based on verifier-based password authentication for three parties [3, 4, 5, 6, 7]; where each client instead of storing the direct password itself it computes a one-way hash function on each password and stores the corresponding result in a server's password table. Subsequently, Shaban *et al.*(2008) [88], proposed an improvement over the Kulkarni *et al.*'s protocol [27] in terms of computational complexity, by showing the reduced rounds from 7 to 4 without using symmetric encryption/decryption. But unfortunately, Archana *et al*. [28] cryptanalyzed Shaban *et al.*'s protocol [9] and proved that it suffers from a detectable online password guessing attack. Kulkarni *et al*.'s protocol [27]is proved as secure against the dictionary attacks, but it is computationally more expensive thanVPA-3P-EKE Protocol. Notations along with their description are listed in Table 1.

Table 1 List of Notations

Alice-A, Bob-B	Clients
Catherine-C	An Attacker or Malicious Client
Trusted Server-TS	Authentication Server (Trusted Third-Party)
id_a, id_b ,id_{ts}	Identities of Alice-A, Bob-B and Trusted Server-TS
PW_a, PW_b	Low Entropy Passwords of Alice-A and Bob-B
DV_a, DV_b	Derived Verifiers of Alice-A and Bob-B
NewPW	New Password for Backward Secrecy
PS_{puk}, PS_{prk}	PCLA Public & Private keys of Trusted Server-TS
$SE_{PW}()$	A symmetric Encryption scheme with a password PW
$SD_{PW}()$	A symmetric Decryption scheme with a password PW
$AE_{Key}()$	An Asymmetric Encryption scheme with a PCLA keys
$AD_{Key}()$	An Asymmetric Decryption scheme with a PCLA keys
p_n	A large prime number
g	A generator in GF(Group Field)
RN_a, RN_b	Random Numbers are chosen by Alice-A, Bob-B respectively.
RE_a, RE_b ,RE_{ts}	Random Exponents of Alice-A, Bob-B, and Trusted Server-TS respectively
N_a , N_b	$N_a=g^{REa} \bmod p_n$, $N_b=g^{REb} \bmod p_n$
K_{ats} , K_{bts}	One-time strong keys computed by Alice-A and Bob-B respectively.
$f_t()$	A one-way trapdoor function, where only Trusted Server-TS knows the trapdoor 't'
$PHF_K()$	A pseudo-random hash function indexed by a key K
K	Session Key
H()	Message Digest Algorithm or One-way Hash Function

VPA-3P-EKE PROTOCOL

Notations along with their description are listed in Table 1.

Building Blocks of a Scheme

Building blocks of the scheme are:

- Preliminary Phase
- Key Agreement Phase
- Key Computation Phase

Preliminary Phase

Initially, all the parties who may communicate in future have to register with the Trusted Server TS in advance. Suppose Alice-A and Bob-B want to register with the Trusted Server-TS, then they have to go through the following step.

Step PP: Alice and Bob choose their low entropy passwords PW_a ,PW_b respectively and derive the verifier from theses password as follows:

Alice-A: $DV_a=H(id_a, id_{ts}, PW_a)$ and
Bob-B: $DV_b=H(id_a, id_{ts}, PW_b)$ where H is any Message Digest Algorithm (or Hash Function).
Now, Alice-A and Bob-B sends these derived verifiers to Trusted Server-TS through a secure channel.
i.e., Alice-A→ Trusted Server-TS: $\{id_a, DV_a\}$ and
Bob-B→Trusted Server-TS: $\{id_b, DV_b\}$.

Upon receiving the derived verifiers from the clients, the Trusted Server-TS stores (secure) these derived verifiers of passwords in its Password Verifiers Table. The Preliminary Phase of VPA-3P-EKE Protocol is also clearly depicted in Fig 1.

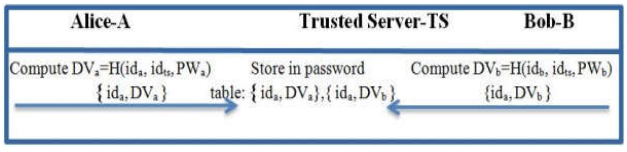

Fig 1 Preliminary Phase

Key Agreement Phase

As soon, if any one of the parties decides to establish a secure communication with any other party then it has to go through the *Key Agreement Phase* of VPA-3P-EKE Protocol. Say, Alice-A wants to communicate with Bob-B then the VPA-3P-EKE Protocol executes the following steps of the key agreement phase.

Step AP1: Alice-A selects a random number and random exponent $RN_a, RE_a \in_R Z_R$. Now, she computes $K_{ats} = N_a^{RNa} \bmod p_n$ where $N_a = g^{REa} \bmod p_n$ and encrypts her low entropy password PW_a with PCLA public key of Trusted Server-TS and sends the computed credentials $\{id_a, id_b, id_{ts}, \{AEPS_{puk}(PW_a), DV_a\}, SE_{PWa}(N_a \oplus RN_a), f_t(PW_a \oplus N_a), PRF_{Kats}(N_a)\}$ to Trusted Server-TS.

i.e.,Alice-A→Trusted Server-TS: $\{id_a, id_b, id_{ts}, \{AEPS_{puk}(PW_a), DV_a\}, SE_{PWa}(N_a \oplus RN_a), f_t(PW_a \oplus N_a), PRF_{Kats}(N_a)\}$

Similarly, Bob-B selects a random number and random exponent $RN_b, RE_b \in_R Z_R$. Now, he computes $K_{bts} = N_b^{RNb} \bmod p_n$ where $N_b = g^{REb} \bmod p_n$ and encrypts his low entropy password PW_b with PCLA public key PS_{puk} of Trusted Server-TS and sends the computed credentials $\{id_a, id_b, id_{ts}, \{AEPS_{puk}(PW_b), DV_b\}, SE_{PWb}(N_b \oplus RN_b), f_t(PW_b \oplus N_b), PRF_{Kbts}(N_b)\}$ to Trusted Server-TS.

i.e., Bob-B→ Trusted Server-TS: id_a, id_b, id_{ts} $\{AEPS_{puk}(PW_b), DV_b\}, SE_{PWb}(N_b \oplus RN_b), f_t(PW_b \oplus N_b), PRF_{Kbts}(N_b)\}$

Step AP2: Aftergetting the messages from Alice-A and Bob-B, Trusted Server-TS decrypts $AEPS_{puk}(PW_a)$ &$AEPS_{puk}(PW_b)$ by using its PCLA private key PS_{prk} and obtains the passwords of Alice-A and Bob-B respectively.
i.e., $PW_a = AEPS_{puk}(ADPS_{prk}(PW_a))$ and $PW_b = ADPS_{prk}(AEPS_{puk}(PW_b))$.

With these retrieved passwords a Trusted Server-TScomputes$DV_a = H(id_a, id_{ts}, PW_a)$&$DV_b = H(id_b, id_{ts}, PW_b)$ and gets the password verifiers DV_a&DV_b from its *password verifiers table* to check whether both the values are identical. If both values are not identical, then it terminates the VPA-3P-EKE Protocol at the present session.

If both the values are identical, then it implies that both the parties are verified and authenticated successfully at first level. Hence Trusted Server-TS continues with the rest of the procedure of VPA-3P-EKE Protocol. That is, by using its trapdoor 't', it retrieves $Pwd_a \oplus N_a$ &$Pwd_b \oplus N_b$ from $f_t(PW_a \oplus N_a)$ &$f_t(PW_b \oplus N_b)$ respectively. Next, TS computes $N_a = (PW_a \oplus N_a) \oplus PW_a$&$N_b = (PW_b \oplus N_b) \oplus PW_b$ and also retrieves $N_a \oplus RN_a$&$N_b \oplus RN_b$ from $SE_{PWa}(N_a \oplus RN_a)$ &$SE_{PWb}(N_b \oplus RN_b)$ by decrypting it using low entropy password (PW_a, PW_b) of Alice-A and Bob-B respectively. Now, trusted server computes$K_{atp} = N_a^{RNa} \bmod p_n$&$K_{btp} = N_b^{RNb} \bmod p_n$ and performs second level verification by computing and comparing $PRF_{Kats}(N_a)$ &$PRF_{Kbts}(N_b)$ with the received values. If both the values are equal, then it selects a random exponent $RE_{ts} \in_R Z_P$ to compute $N_b^{REts} \bmod p_n$ and $N_a^{REts} \bmod p_n$ and encrypts these values by using PCLA Private Key PS_{prk}. Now it sends $\{AEPS_{prk}(N_b^{REts} \bmod p_n)\}$ to Alice and $\{AEPS_{prk}(N_a^{REts} \bmod p_n)\}$ to Bob.

i.e., Trusted Server-TS→ Alice: $\{AEPS_{prk}(N_b^{REts} \bmod p_n)\}$ and

Trusted Server-TS→ Bob: $\{AEPS_{prk}(N_a^{REts} \bmod p_n)\}$.

Alternatively, if both the values are not equal, then it terminates the VPA-3P-EKE Protocol. The details of *Key Agreement Phase* arealso illustrated in Fig 2.

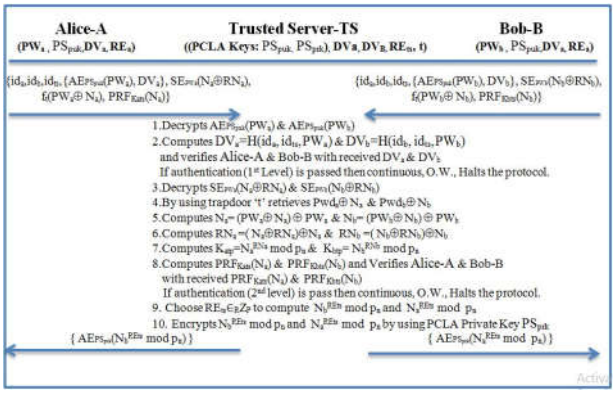

Fig 2 Key Agreement Stage

Key Computation Phase

Once key agreement phase is over i.e., both the parties are authenticated, the actual key computation phase begins. Here, in this phase initially trusted server is authenticated by both the parties individually before computing a common session key in a smart way.

Step CP1: Alice-A decrypts $AEPS_{prk}(N_b^{REts} \bmod p_n)$ with the PCLA public key PS_{puk} of Trusted Server-TS to authenticated it.

i.e., DE $PS_{puk}(AEPS_{prk}(N_b^{REts} \bmod p_n)) = N_b^{REts} \bmod p_n$.

Similarly, Bob-B decrypts $AEPS_{prk}(N_a^{REts} \bmod p_n)$ with the PCLA public key PS_{puk} of Trusted Server-TS to authenticated it.

i.e., DE $PS_{puk}(AEPS_{prk}(N_a^{REts} \bmod p_n)) = N_a^{REts} \bmod p_n$.

Step CP2: In this step, Alice & Bob compute a common session key K and pseudo-random function (PRF) index with K as follows:

Alice-A: $K = (N_b^{REts})^{REa} \bmod p = ((g^{REb})^{REts})^{REa} \bmod p$ and $PRF_K(id_a, K)$
Bob-B: $K = (N_a^{REts})^{REb} \bmod p = ((g^{REa})^{REts})^{REb} \bmod p$ and $PRF_K(id_b, K)$
Now, Alice sends $PRF_K(id_a, K)$ to Bob and Bob sends $PRF_K(id_b, K)$ to Alice for final verification of generated session key .

i.e.,Alice-A→Bob-B: $\{PRF_K(id_a, K)\}$
Bob-B→Alice-A: $\{PRF_K(id_b, K)\}$

Upon receiving the incoming credentials $PRF_K(id_b, K)$ and $PRF_K(id_a, K)$ from Alice-A and Bob-B respectively, they verify each other and can confirm that the common session key is $K = (N_b^{REts})^{REa} \pmod p = K = (N_a^{REts})^{REb} \pmod p$. The detail of a *Key Computation Phase* is also depicted in Fig 3.

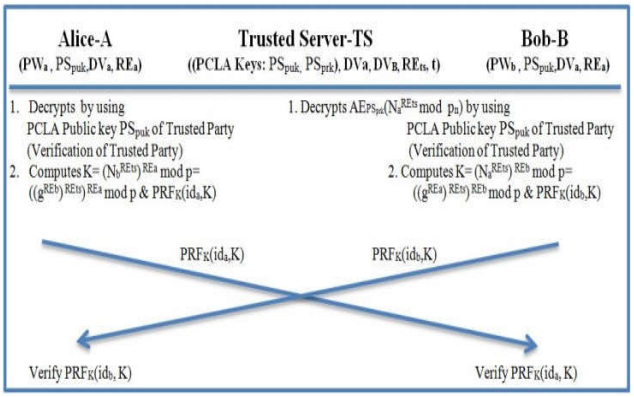

Fig 3 Key Computation Stage

Password Change Mechanism

If any party suspects a 'leak of information' then VPA-3P-EKE Protocol supports p*assword change mechanism*which is supportive in forward secrecy, known-key secrecy, and backward secrecy. The steps involved in this mechanism are as follows:

Step PCM1: Alice-A retains the session key K from the earlier session.

Step PCM2: Now, Alice-Aencrypts the session key K by using PCLA public key PS_{puk} of a Trusted Server-TS. Next, shework out$H(id_a, id_{ts}, PW_a) \oplus H(Id_a, Id_{ts}, NewPW_a) \oplus K$ and finally sends the credentials $\{Id_a, Id_{ts}, AEPS_{puk}(K), H(id_a, id_{ts}, PW_a) \oplus H(id_a, id_{ts}, NewPW_a) \oplus K, f_t(H(Id_a, Id_{ts}, NewPW_a))\}$ to Trusted Server-TS to reset the new password verifier.

i.e., Alice-A→Trusted Server-TS: $\{Id_a, Id_{ts}, AEPS_{puk}(K), H(id_a, id_{ts}, PW_a) \oplus H(id_a, id_{ts}, NewPW_a) \oplus K, f_t(H(Id_a, Id_{ts}, NewPwd_a))\}$

Step PCM3: After getting the credentials from Alice-A, Trusted Server-TS retrieves K by using the PCLA private key PS_{prk}, i.e., $ADPS_{prk}(AEPS_{puk}(K))$ and also gets the *old derived verifier* from the password table and computes the new derived verifier from the new password as follows: $H(Id_a, Id_{ts}, NewPwd_a) = (H(id_a, id_{ts}, PW_a) \oplus H(id_a, id_{ts}, NewPW_a) \oplus K) \oplus H(Id_a, Id_{ts}, PW_a) \oplus K$. Now, The Trusted Server-TS verifies the new password verifier by retrieving $H(Id_a, Id_{ts}, NewPW_a)$ using a trapdoor 't' from the received one i.e., $f_t(H(Id_a, Id_{ts}, NewPwd_a))$; if both the values are identical then

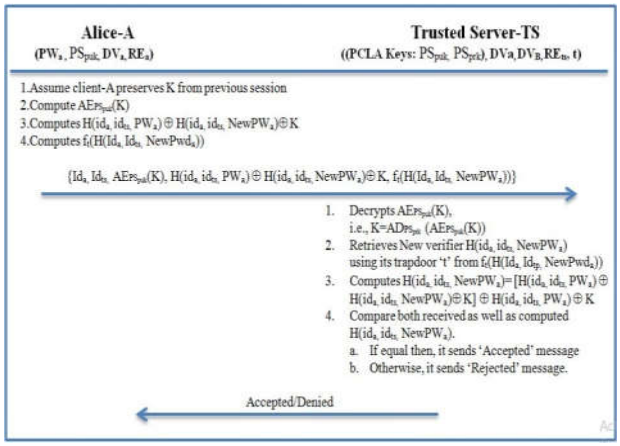

Fig 4 Password Change Mechanism

Trusted Server-TS updates the password verifier table accordingly and sends 'Accepted' message to Alice-A. Otherwise, Trusted Server-TS rejects the request by sending the 'Denied' message to a particular client.
i.e., Trusted Party-TP: Accepted/Denied

The details of a *Password Change Mechanism* also depicted in Fig 4.

SECURITY ANALYSIS

The VPA-3P-EKE protocol satisfies the following security requirements, which implies that the VPA-3P-EKE Protocol is not only secure but also efficient.

Resistant to an Offline Password Guessing Attack
Let us assume an intruder Catherine-C wants to mount an *Off-line Password Guessing Attack* on client Alice-A. Hence, she intercepts $\{id_a, id_b, id_{ts}, \{AEPS_{puk}(PW_a), DV_a\}, SE_{PWa}(N_a \oplus RN_a), f_t(PW_a \oplus N_a), PRF_{Kats}(N_a)\}$ and may guess a password of Alice-A as PW_a but it is not feasible for her to retrieves $N_a$because she needs a trapdoor 't' which is known only to a Trusted Server-TS.

Hence, *Offline Password Guessing Attack* is not possible on the proposed VPA-3P-EKE Protocol.

Resistant to a Direct Server Compromise Attack
Let us assume Catherine-C succeeded in obtaining a *derived passwords table* of Trusted Server-TS. Even though she cannot succeed in obtaining a common session key K because the *derived passwords table* stores only the derived verifiers DVs, not the passwords.

Hence, a *Direct Server Compromise Attack*is eliminated from the VPA-3P-EKE Protocol.

Provides the Mutual Authentication

First: Both the parties use PCLA public key PS_{puk} of Trusted Server-TS to hide their passwords so that only Trusted Server-TS who possesses the PCLA private key PS_{prk} can retrieve the passwords. Hence, for intruder it is not possible to get the passwords of parties.

Second: Random exponents of the clients and their passwords are hidden in a one-way trapdoor function where the trap door 't' is known only to a Trusted Server-TS. Hence, Trusted Server-TS very well authenticate the clients as shown in *Step AP1* of the VPA-3P-EKE Protocol.

Third: The message send in *Step KA2* of the VPA-3P-EKE Protocol i.e., $\{AEPS_{prk}(N_b^{REts} \bmod p_n)\}$ and $\{AEPS_{prk}(N_a^{REts} \bmod p_n)\}$ is used to authenticate the Trusted Server-TS by both the clients.

Fourth: Both the clients derives a common session key K from the received credentials $N_b^{REts} \bmod p_n$ and $N_a^{REts} \bmod p_n$ as shown in *Step CP1.* As mentioned in Step CP2, both the clients can authenticate each other by crosschecking the credentials (i.e., $PRF_K(id_a,K)$, $PRF_K(id_b,K)$).

Hence, the VPA-3P-EKE Protocol provides the *Mutual Authentication* in ways.

Provides Backward Secrecy

Backward Secrecy ensures that a compromise of old session keys should not lead to the compromise of new session keys. Let us say somehow a current session key K is revealed and hence a client Alice-A sensed this. As soon Alice-A invokes the *Password Change Mechanism* of VPA-3P-EKE Protocol. However, say an intruder Catherine-C intercepts the request message sent by Alice-A. But she cannot obtain the new password $NewPW_a$ from the intercepted message. Hence she cannot succeed in getting the new session key even though she knows the old session key K.
Hence, the VPA-3P-EKE Protocol provides the *Backward Secrecy*.

Provides the Forward Secrecy

Forward Secrecy ensures that compromise of long-term session keys should not lead to a compromise of old session keys. Let us assume, an intruder Catherine-C gets success in obtaining the current session key K_i. However, in order to obtain the old session keys K_{i-1}, K_{i-2},...from the current intercepted credentials $AEPS_{prk}(N_b^{REts} \bmod p_n)$ and $AEPS_{prk}(N_a^{REts} \bmod p_n)$, she should know the random exponents of the previous session (RE_a and RE_b) which are independent in each session. Hence, she cannot succeed in getting the old session keys even though she possess current session key K_i.

In this way, the *Forward Secrecy* is provided by VPA-3P-EKE Protocol.

Provides Session-Key Secrecy

Session-Key Security ensures that compromise of any session key should not lead to the compromise of previous or later session keys. It is already proved that VPA-3P-EKE Protocol provides *Backward* as well as *Forward Secrecy* which implies that VPA-3P-EKE Protocol provides *Know-Key Secrecy*. Hence, it is proved.

Resistant to Man-in-the-Middle Attack

It is not possible for an intruder to mount *Man-in-the-Middle Attack* because in *key agreement phase* itself we are providing two-level authentication by Trusted Server-TS and in *key computation phase* Trusted Server-TS is authenticated by both the parties.

Hence, VPA-3P-EKE Protocol is perfectly resistant to *Man-in-the-Middle Attack*.

Resistant to Trivial Attack

Due to the Pseudo Random Functions indexed by a one-time strong key and intractability of Discrete Logarithmic Problem (DLP) it impossible to compute Session Key K directly from the intercepted credentials.

Hence it is impossible to mount *Trivial Attack* on VPA-3P-EKE Protocol.

Resistant to Pre-play Attack

Due to the intractability of Discrete Logarithmic Problem (DLP) and randomness (e.g., RE_a , $RN_a \in_R Z_p$) in generating the Session Key K, it is impossible for an intruder to mount a *Pre-play Attack*.

Hence, *Pre-play Attack* is also rolled out from VPA-3P-EKE Protocol.

Resistant to Replay Attack

Let us assume, an intruder sends an intercepted message $\{id_a, id_b, id_{ts}, \{AEPS_{puk}(PW_a), DV_a\}, SE_{PWa}(N_a \oplus RN_a), f_t(PW_a \oplus N_a), PRF_{Kats}(N_a)\}$ to Trusted Server-TS.But, Trusted Server-TS will detect the attack easily, since RN_avaries for each session.

Hence,*Replay Attack* is also rolled out from VPA-3P-EKE Protocol.

Resistant to an Online Password Guessing Attacks
Because of the same reasons mentioned above i.e., Random Numbers and Random Exponents are independent in each session one cannot mount a*Detectable or Undetectable Online Password Guessing Attacks.*

Hence, VPA-3P-EKE Protocol is resistant to an *Online Password Guessing Attacks*.

PERFORMANCE ANALYSIS

Table 2 list the performance analysis of some well-known verifier-based 3P-EKE protocols with the Verifier-Based Password-Authenticated 3P-EKE protocol, where ($T_E + T_H + T_R$) is the total computational time for executing modular exponentiation, hash operation(it may be hash function or/and pseudo-random hash function indexed by a key or/and trapdoor hash function) and generating a random numbers; time for executing a modular exponentiation is denoted by T_E; time for executing a hash function is denoted by T_H and time for generating a random number is denoted by T_R; assume time for executing any type of hash function (hash function, pseudo-random hash function indexed by a key, trapdoor hash function) is approximately same for consistency.

From the Table 2, it is concluded that the verifier-based 3P-EKE protocol takes very fewer computations of modular exponentiations comparing with the other protocols. A second computational component is *required messages* and *rounds in transmission*. The verifier-based 3P-EKE protocol requires 8 messages & 5 rounds including the initial message, whereas, Wang-Mo [4], Chien [5], Lin-Lee [16] and Shaban *et al*. [9] protocols need 5 rounds, 6 messages & 6 rounds, 6 messages & 4 rounds and 10 messages & 5 rounds respectively.

Table 2 Performance Comparison with related Verifier - Based Password-authenticated 3P-EKE Protocols

Verifier-based 3P-EKE Protocols ⇨ Computation types & Attack types ⇩	Wang-Mo Protocol	Chien Protocol	Lin-Lee Protocol	Shaban et al. Protocol	The VPA-3P-EKE Protocol
Computational Cost ($T_E + T_H + T_R$)	$14T_E + 10T_H + 4T_R$	$15T_E + 14T_H + 5T_R$	$14T_E + 12T_H + 4T_R$	$12T_E + 12T_H + 4T_R$	$10T_E + 14T_H + 6T_R$
Transmission Messages/ Round	-/5R	6M/6R	6M/4R	10M/5R	8M/5R
Provides Mutual Exclusion	YES	YES	YES	YES	YES
Provides Session Key Security	YES	YES	YES	YES	YES
Resists Stolen Verifier Attacks	YES	YES	YES	YES	YES
Resists Key Confirmation	NO	YES	YES	NO	YES
Resists Undetectable Online Password Guessing attack	YES	NO	YES	NO	YES
Resists Detectable On-line Password Guessing Attack	YES	No	YES	No	YES
Resists Offline Password Guessing Attack	YES	No	YES	No	YES

The following comparison elements are security requirements, viz., Mutual Authentication, Session Key Security, Password Guessing Attacks, Stolen Verifier Attacks, and Key

Confirmation. The Wang-Mo [4] verifier-based 3P-EKE protocol, the Lin and Lee's [16] verifier-based 3P-EKE protocol and the verifier-based 3P-EKE protocol provide more security requirements than other verifier-based 3P-EKE protocols. Therefore, the verifier-based 3P-EKE protocol preserves robustness, computation-efficient and provides efficient transmission and higher security than other related verified-based 3P-EKE protocol schemes.

CONCLUSION

This paper attempts to probe a new verifier-based password-authenticated three-party encrypted key exchange protocol. A verifier-based password authenticated 3P-EKE protocol using PCLA keys [2], provides perceptive justification about the existing attacks that do not solve in the previous framework. That is, thisVPA-3P-EKE Protocol is proved to be secure against the attacks like Password Guessing Attacks (Online and Offline), Direct Server Compromise Attack, Trivial Attack, Pre-play Attack, Replay Attack, Man-in-the-middle Attack, Session Key Secrecy, and Known-Key Security.

Further, it is also proved that the VPA-3P-EKE Protocol provides mutual authentication, backward secrecy and also forward secrecy. Finally, the performance analysis of well-known verifier-based 3P-EKE protocols, viz., Wang-Mo [4], Chien [5], Lin-Lee [16] and Shaban *et al*. [9] 3P-EKE protocols with the new verifier-based 3P-EKE is done and proved that the new verifier-based 3P-EKE protocol provide more security requirements than other verifier-based 3P-EKE protocols.

References

1. Archana Raghuvamshi, Premchand Parvataneni,*Design of a Robust, Computation-Efficient and Secure 3P-EKE Protocol using Analogous Message Transmission, International Journal of Computer Network and Information Security*(IJCNIS), MECS Publishers,2016,5, DOI:10.5815/ijcnis.2016.05.02, pages 9-17.
2. Archana Raghuvamshi, Premchand Parvataneni, *PCLA: A New Public-key Cryptosystem Based On Logarithmic Approach*, IJCSI *International Journal of Computer Science* Issues, Vol.9, Issue.2, No.1, March 2012, pages 355-359.
3. Abdalla M, Chevassut O, and Pointcheval D, *One-time verifier-based encrypted key exchange*, In PKC 2005, LNCS 3386, Springer, January 2005, pages 47-64.
4. Wang R.C., Mo K.R., Security enhancement on efficient verifier-based key agreement protocol for three parties without server's public key, *Int. Math. Forum* 1 (20) (2006), pages 965–972.
5. Chien H.Y., Secure verifier-based three-party key exchange in the random oracle model, *J. Inf. Sci. Eng.* 27 (4) (2011)1487–1501.
6. Lin T.H., Lee T.F., Secure verifier-based three-party authentication schemes without server public keys for data exchange in telecare medicine information systems, *J. Med. Syst.* 38 (2014), http://dx.doi.org/10.1007/ s10916-014-0030-4.
7. Yang J and Cao T,*A* Verifier-based Password-Authenticated Key Exchange Protocol via Elliptic Curves, *Journal of Computational Information Systems, Binary Information* Press,2011, pages 548-553.
8. Shaban Dina Nabil, Ibrahim Maged H, and Nossair Zaki B, Enhanced Verifier-Based Password Authenticated Key Agreement Protocol for Three-Parties, *Journal of Engineering Sciences,* Vol. 36, No. 6, November 2008, pages 1513- 1522.
9. Shaban Dina Nabil, Ibrahim Maged H, and Nossair Zaki B, Enhanced Verifier-Based Password Authenticated Key Agreement Protocol for Three-Parties, *Journal of Engineering Sciences,* Vol. 36, No. 6, November 2008, pages 1513- 1522.
10. Diffie W, Hellman M E, New directions in cryptography, IEEE Trans Inform Theory, Vol.22, 1976, pages 644-654.
11. AngGao, Provable Password-Authenticated Key Exchange Protocol against Imposter Attack on Ad Hoc Networks, *JDCTA*, Vol.4, No.8, 2010, pages 150–163.
12. Benhamouda F, Blazy O, Chevalier C, Pointcheval D, and Vergnaud D, New techniques for smooth projective hash functions and efficient one-round PAKE protocols, In CRYPTO 2013, Part I, LNCS 8042, Springer, August 2013, pages 449-475.
13. Choi S B and Yoon E J, Cryptanalysis of Guo et al's three-party password-based authenticated key exchange *(G-3PAKE) protocol*, Procedia Engineering, Vol.24, 2011, pages 187-191.
14. Gennaro R and Lindell Y, A framework for password-based authenticated key exchange, In EUROCRYPT 2003, LNCS 2656, Springer, May 2003, pages 524–543.
15. Gennaro R and Lindell Y, A framework for password-based authenticated key exchange, ACM Transactions on Information and System Security, Vol.9, No.2, 2006, 181-234.
16. Groce A and Katz J, A new framework for efficient password-based authenticated key exchange, In ACM CCS 10, ACM Press, October 2010, pages 516-525.
17. Katz J, Ostrovsky R, and Yung M, Efficient password-authenticated key exchange using human-memorable passwords, In EUROCRYPT 2001, LNCS 2045, Springer, May 2001, pages 475-494.
18. Katz J and Vaikuntanathan V, *Round-optimal password-based authenticated key exchange*, In TCC 2011, LNCS 6597, Springer, March 2011, pages 293-310.
19. Lee C, Li C, and Hsu C, A three-party password-based authenticated key exchange protocol with user anonymity using extended chaotic maps, Nonlinear Dynamics,Vol.73, pages 125–132.
20. Weijia Wang, Lei Hu, and Yong Li, How to construct secure and efficient three-party password-based authenticated key exchange protocols, In proceedings of Information Security and Cryptology, 2011, pages 218-235.
21. Bellovin S M and Merritt M, Encrypted key exchange: password-based protocols secure against password guessing attacks, In Proceedings of 1992 IEEE Symposium on Research in Security and Privacy, 1992, pages 72–84.
22. Gentry C, MacKenzie P, and Ramzan Z, *A method for making password-based key exchange resilient to server*

compromise, In CRYPTO 2006, LNCS 4117, Springer, August 2006, pages 142-159.
23. Bellovin S M and Merritt M, Augmented encrypted key exchange: A password-based protocol secure against dictionary attacks and password file compromise, In ACM CCS 93, ACM Press, November 1993, pages 244-250.
24. Gong L, Lomas M, Needham R, and Saltzer J, Protecting poorly chosen secrets from guessing attacks, IEEE Journal on Selected Areas in Communications, Vol.11, No.5, 1993, pages 648-656.
25. Yang J and Cao T,*A* Verifier-based Password-Authenticated Key Exchange Protocol via Elliptic Curves, *Journal of Computational Information Systems, Binary Information* Press,2011, pages 548-553.
26. Yoon E J and Yoo K Y, Improving the novel three-party encrypted key exchange protocol, Computer Standards & Interfaces, Vol. 30, No.5, 2008, pages 309-314.
27. Zeng, Yong, Ma, Jianfeng, An improvement on a password authentication scheme over insecure networks, *Journal of Computational Information Systems*, Vol.5, No.4, 2009, pages 1331-1336.
28. Kulkarni S, Jena D, and Jena S K, A Novel Secure Key Agreement Protocol using Trusted Third Party, *Computer Science and Security Journals, IJCSS*, Vol.1, Issue.1, 2007, pages 11 – 18.
29. Archana Raghuvamshi, Premchand Parvataneni, Cryptanalysis of Verifier-Based Password Authenticated Key Agreement Protocol for Three Parties, *Research Journal of Recent Sciences,* Vol.4 (ISC-2014), Feb 2015, pages 5-8.

How to cite this article:

Archana Raghuvamshi and Premchand Parvataneni.2017, Vpa-3p-Eke: A Verifier-Based Password-Authenticated 3p-Eke Protocol And Its Analysis. *Int J Recent Sci Res.* 8(11), pp. 21946-21952. DOI: http://dx.doi.org/10.24327/ijrsr.2017.0811.1168

****