An Improved Two-factor Authenticated Key exchange Protocol in Public Wireless LANs

AJIT SINGH
Assistant Professor
Department of Computer Engineering
TIT&S, Bhiwani, India
Email: ajit713@gmail.com

RAHUL RISHI
Professor
Department of Computer Engineering
U.I.E.T, M.D.University, Rohtak, India
Email: rahulrishi@rediffmail.com

Abstract:- Recently, Lee et. al. carried out the cryptanalysis of Juang et. al. two-factor authentication key exchange protocol in Public wireless LANs. It was shown that Juang et.al. protocol is vulnerable to the stolen verifier attack and doesn't satisfy the user anonymity. Apart from the, high computational overhead of the server. This paper, proposes an improved protocol towards authentication and key exchange based on Elliptic Curve Decision Diffie-Hellman(DDH) problem which ensures their strong resistance towards the existing weaknesses. Besides this, their security and performance analysis shows that the proposed protocol is more secure and efficient.

Keywords- Public wireless LANs (PWLANs), Elliptic Curve, Decision Diffie-Hellman (DDH), Authentication.

I. INTRODUCTION

Remote authentication is an inevitable task in many networking application areas like transaction, net banking, and PWLANs services. The authenticated users might have to login to the system remotely. One of the major challenging problems faced by this field is to ensure robust security while using an insecure channel. There are a number of ways to authenticate a user remotely by using one, two or more factors but two factor authentication mechanism become most familiar among them due to high level of authentication and low computational overheads. Numerous works have been addressed regarding this issue from different perspective but nonetheless, many of the works were not suitable for the PWLANs services. As PWLANs services includes billing, roaming, transactions and security. So security is an essential issue and the system which could claims the authentication in PWLANs must satisfy these three security requirements. First, it should ensure the user anonymity. Second, a mutual authentication between a user and a server. Third, it must satisfies the forward secrecy.

One of the two-factor authentication key exchange protocol proposed earlier is Juang et. al. protocol [8] which is based on authenticated key exchange protocol proposed by Park et. al. [7]. In this paper, an improved authenticated key exchange protocol is proposed which is adapted from Juang et. al. protocol. We eliminate the weaknesses and vulnerabilities of Juang et.al protocol carried by cryptanalysis of Lee et. al.[9] to provide enhanced security for remote authentication in networking applications.

The rest of the paper is organized as follows: Section 2 states the related works, Section 3 contains the details of our proposed protocol, and finally Section 4 and 5 presents the security and performance analysis.

II. RELATED WORK

In 1981, Lamport [1] first proposed the user authentication protocol using password. Besides that, numerous work has been addressed [1]-[7] regarding this issue from different perspective but nonetheless, many of the works which dealt with this issue are sufficiently not able to provide mutual authentication and user anonymity. In 2003, Park et. al. proposed an authentication and key exchange protocol which could ensure the above requirements. But, later in 2008 Juang et. al [8] showed that, [7] wouldn't ensure the user anonymity and also proposed an enhanced protocol which could withstand against the existing weaknesses of [7]. Unfortunately, later in

978-0-7695-4941-5/13 $26.00 © 2013 IEEE
DOI 10.1109/ACCT.2013.58

2009 Hee et. al. [9] cryptanalysis showed that, Juang et.al. protocol was still insecure, not able to ensure user anonymity, vulnerable to stolen verifier attack and have high computational overheads.

The proposed protocol is based on elliptic curve DDH problem that is totally different than all of the mentioned protocols and overcomes the drawbacks of the existing protocols.

III. PROPOSED PROTOCOL

Like the Juang et. al.'s, our proposed protocol has three distinct but interrelated phases as registration phase, pre-computational phase and mutual authentication phase. We keep the pre-computational same as [8] and modify the other two phases to countermeasure the vulnerabilities mentioned earlier in [8]. Beside the different concept involved in these phases, our proposed protocol is totally based on elliptic curve DDH problem. Elliptic curve cryptography offers efficient security solution requiring fewer bits than the discrete logarithm based cryptography for a similar level of security. With 160 bit moduli, an elliptic curve logarithm based DDH system offers the same level of cryptographic security as discrete logarithm based DDH with 1024 bit moduli. The smaller the key sizes result in smaller system parameters, bandwidth savings, faster implementation, low power requirement and smaller hardware. In the proposed protocol an elliptic curve E is taken which is defined over GF(Z_n), having a point g that lie on curve of order n, where n is a large prime number. It is assumed that A and B share the parameters of elliptic curve, point and its order.

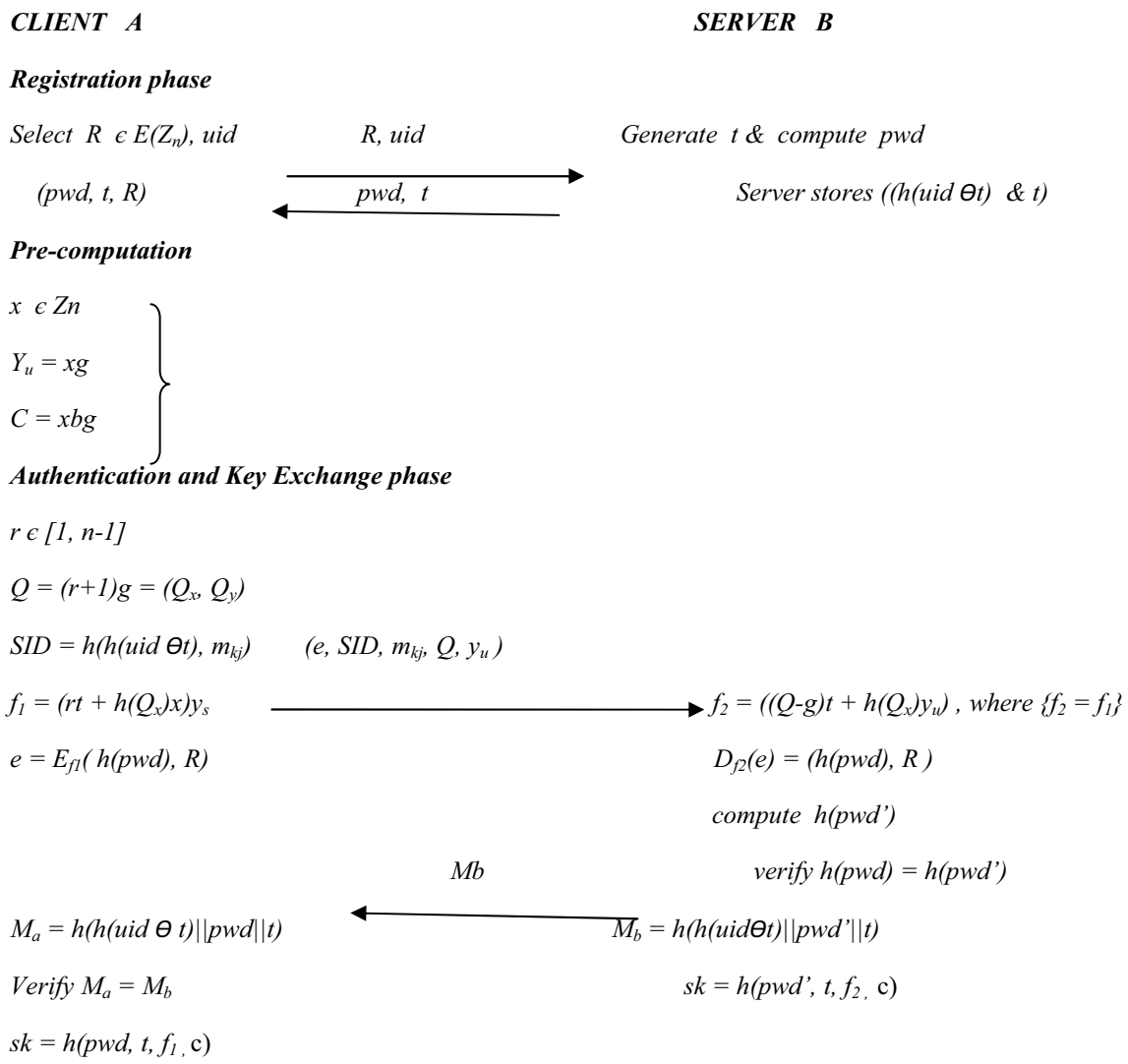
REGISTRATION PHASE

In the registration phase, user A submits his identity *uid* and a randomly chosen point R on elliptic curve to the server B to register himself. After checking the validity of *uid* and *R*, B chooses a symmetric key *t* and using all these parameters, it will compute the password *pwd* by using these steps:

1. B computes $a = h(uid \oplus t)$
2. Then B computes $d = a.R$, where d is the point which lie on elliptic curve and have a coordinate (d_x, d_y).
3. On generating (d_x, d_y) in step 2, B also compute variable password $vpwd = h(f(d_x, d_y))$, where $f()$ is an arbitrary complex function .
4. Finally, B computes a human mind retainable password *pwd = (m most significant bit of vpwd)* $\oplus$ *(m least significant bit of vpwd).*
5. After computing pwd, B send the (pwd, t, M_{ij}) to the user A, while server B only stores the indirect user identity $h(uid \oplus t)$ and *t* in its j^{th} index database file. Note that, B neither store the direct user identity *uid* nor the *pwd* in its storage system to defend itself against the stolen-verifier attack and to preserve the user anonymity. Also note that, M_{ij} is a special encoded server database character, in which M_i denotes a large prime integer range through which we have to randomly select a prime number m_k during the *SID* generation and *j* indicates that indirect user identity will be stored in j^{th} index database file to reduce the searching time and to overcome high computational overhead problem.
6. Upon receiving (pwd, t, M_{ij}), A remembers *pwd* and stores $(t \text{ and } M_{ij})$ in his smart card.
7. Beside this, B also chooses a random number $b \varepsilon Z_n$ and set it as a private key, B also computes $y_s = bg$ and set it as a public key.

PRE-COMPUTATION PHASE

A selects a random value x ε Z_n and computes $y_u = xg$. After that, to reduce the computational overhead in the authentication and key exchange stage, A computes $c = xbg$ and store it.



(Where ⊖ *is EX-OR operation)*

AUTHENTICATION and KEY EXCHANGE PHASE

In this phase, a mutual authentication between A and B is performed and the session key is established, which consists of the following steps:

1. Initially A computes Q = (r+1)g = (Q_x, Q_y), where r ε [1, n-1].
2. A also computes SID = h(h(uid ⊖t), mkj), f = (rt + h(Q_x)x)y_s, e = E_f(h(pwd), R) and sends (e, SID, m_{kj}, Q, y_u) to B, where m_{kj} signifies as m_k is a large prime no belongs to M_{ij} and j indicating the j^{th} server database file.
3. Upon receiving these parameters, B first search its j^{th} index database file corresponding to the m_{kj}. Then B replaces h(uid⊖t)' stored in the database to SID' = h(h(uid⊖t)', mkj) and finds that value of SID sent by A matches with B or not. After finding right h(uid⊖ t), B acquires t. Then B computes f_2 = ((Q-g)t + h(Q_x)y_u)b and extracts h(pwd), R by decrypting D_{f2}(e). After decrypting, B computes password pwd' corresponding to the h(uid⊖t) using same procedure as in registration phase. Then B compares h(pwd') with h(pwd). If so, B authenticates A as a legitimate client. Finally, B compute

M_b = h(h(uid ⊖t)||pwd'||t) and send it to A.

4. A computes M_a = h(h(uid ⊖ t)||pwd||t) and compare it with the M_b send by B. If so, A authenticates B as a legitimate server. So a mutual authentication between A and B take place.

IV. SECURITY ANALYSIS

In this section, this paper demonstrates that the proposed protocol can withstand against the existing weaknesses in Juang et. al [8].

Provision of user anonymity:- User anonymity means that not only a user identity should be protected from being exposed to an attacker , but also to the server. That is because there are chances that a server may abuse the user information. The proposed protocol doesn't expose the direct user identity during communication and even also server intentionally can't abuse them because server only stores the indirect uid and t not pwd , and pwd can't be generated without knowing the proper value of R. So, proposed protocol provides user anonymity.

Resistance to the stolen verifier attack:- In stolen verifier attack, the attacker can get the verifier maintained by the server database. But in proposed one, server only stores the indirect uid and t in its database and compute the password when user login. So, stolen verifier attack in this protocol will be useless as server database will not provide any information regarding R and pwd. Without knowing R and pwd, attacker can't impersonate.

Server has low computational overhead:- In the proposed protocol, server provide a special encoded server database character M_{ij}, in which M_i denotes a large prime integer range through which we have to randomly select a prime number m_k during the SID generation and pass this m_{kj} to the server side during login phase, where j indicates to the server that indirect user identity will be stored in j^{th} index database file to reduce the searching time and to overcome high computational overhead problem.

V. PERFORMANCE ANALYSIS

In this section, We summarize security features and performance analysis of our proposed protocol and compare it security and robustness with the Park and Park [7], and Juang and Wu [8] protocols. Table 1 shows that our protocol is more secure and robust than the protocol [7] and [8].

Security features	**Proposed protocol**	**Juang and wu [8]**	**Park and Park [7]**
Protection against user identity	Yes	No	No
Protection against user anonymity	Yes	No	No
Protection against dictionary attack	Yes	Yes	No
Protection against stolen verifier attack	Yes	No	No
No. of message exchanged during authentication phase	2	3	4
No. of searching operation in server database	Very Low	High	Low
Computational operation in registration phase	2 Hash	No	No
Computational operation in mutual authentication phase	13 Hash	8 Hash	9 Hash

Table 1. Efficiency comparisons of the proposed protocol with Juang [8] and Park [7].

Table 1 demonstrates that proposed protocol require 13 hash operations as compared to [7] and [8], which require only 8 and 9 hash operation respectively. No doubt few more hash operation will provide a robust and enhanced security features to this authentication system. Beside this, number of message exchanged

between client and server during authentication phase is 2 as compared to 3 and 4 of [7] and [8], so low messages will be helpful for achieving network resource efficiency and minimum latency.

REFERENCES

[1] Lamport L. "Password authentication with insecure communication," Communications of the ACM, 1981;24(11):770–.2.

[2] Juang W. "Efficient password authenticated key agreement using smart card", Computers & Security, 2004; 23:167-.73.

[3] Park Y, Park S. "Two factor authenticated key exchange protocol in public wireless LANs", IEICE Trans. Communication 2004; E87-B(5): 1382-.5.

[4] Sun H. "An efficient use authentication scheme using smart cards", IEEE Trans. Consumer Electronic, 2000; 46(4): 958-61.

[5] Yang C, Wang R. "Cryptanalysis of a user friendly remote authentication scheme with smart cards", Computer Society, 2004; 23:425-.7.

[6] Kumar M. "New remote user authentication scheme using smart cards", IEEE Trans. Consumer Electronic, 2004; 50(2): 597-600.

[7] Y Park, S Park, "Two factor authenticated key exchange protocol in PWLANs", IEICE Trans. Communications, 2004, E87-B(5), pp. 1382-1385.

[8] Wen-Shenq, Juang, Jing-Lin Wu, "Two factor authenticated key exchange protocol in PWLANs", Computers and Electrical Engineering, 2008, Vol.10, pp 1-8.

[9] H. Lee, D Choi, Y Lee,D Won,S Kim, "Cryptanalysis of two-factor authenticated key exchange protocol in PWLANS", World Academy of Science, Engineering and Technology,2009, pp.194-197.