A NOVEL PASSWORD BASED MULTI PARTY KEY AGREEMENT PROTOCOL ON ELLIPTIC CURVE

Daniyal M. Alghazzawi

Faculty of Computing and Information Technology
Department of Information Systems,
King Abdulaziz University, Kingdom of Saudi Arabia
dghazzawi@kau.edu.sa

ABSTRACT

Key agreement protocol a number of parties involved and communicate over a open public network to generate a common secret key called session key. This paper proposes an efficient password based multiparty Key Agreement Protocol. Security of the protocol is based difficulty of breaking Elliptic Curve Discrete Logarithm Problem and one way hash function. This is resistant against different attack. The security analysis have been discuss and proved in this aticle.

KEYWORDS *secure communication ,man-in middle attack, Password based, ECDLP, off-line dictionary attack, ECDLP.*

1. INTRODUCTION

By reviewing various articles on group key exchange protocol, it is found that not all of them achieve all security requirement and efficiency simultaneously. Group key exchange protocol is an important cryptographic technique in public network where the entities can share secure information may be human-memorable password with a trusted server and establish a session key [6]. The advantages of the proposed protocol are that it does not require any server's public key in the establishment of session key. This is resistant against off-line dictionary attack and man-in middle attack.

The ability to compute security functions with limited computing resources has become increasingly precious. In mobile devices such as smart card , PDA and multimedia cell phones, the processing resources, memory and power are all very constraints, but these need for secure transmission of information may increase due to the vulnerability to attackers of the publicly accessible wireless transmission channel [1][10]. New smaller and faster probabilistic polynomial solvable security algorithms provide part of the solution. Elliptic curve cryptography (ECC) provides the require security for all these low processor devices in much smaller key lengths as compared to the other public key or symmetric key cryptosystem.

DOI : 10.5121/ijcsit.2012.4106

2. BACKGROUNDS

This section gives the preliminary ideas about Finite filed and Elliptic Curve over finite field, Elliptic Curve Discrete Logarithm Problem, Elliptic Curve Diffie-Hellman (ECDH) and group key agreement.

2.1 The finite field F_P

Let p be a prime number. The finite field F_P is comprised of the set of integers $0,1,2.....p-1$ with the following arithmetic operations [5] [6] [7]:

Addition: Let $a,b \in F_p$ then the sum $a+b=r$, where r is the remainder when $a+b$ is divided by p and $0 \le r \le p-1.$

Multiplication: If $a,b \in F_p$ then $a.b=s$, where s is the remainder when $a.b$ is divided by p and $0 \le s \le p-1.$.

Inversion: If a is a non-zero element in F_P, the inverse of a modulo p, denoted a^{-1}, is the unique integer $c \in F_p$ for which $a.c=1$.

2.2 Elliptic Curve over F_P

Let $p \ge 3$ be a prime number. Let $a,b \in F_p$ be such that $4a^3+27b^2 \ne 0$ in F_P. Let E be the elliptic curve define over F_P .Set of all solutions $(x,y), x, y \in F_p$, to the equation $y^2 = x^3 + ax + b$, together with an extra point O is called point at infinity. The set of points $E(F_p)$ forms an abelian group with the following addition rules [9]:

Identity: $P+O=O+P=P$, for all $P \in E(F_p)$.

Negative : if $P(x,y) \in E(F_p)$ then $(x,y)+(x,-y)=O$, The point $(x,-y)$

is dented as $-P$ called negative of P.

Point addition: Let $P(x_1,y_1), Q(x_2,y_2) \in E(F_p)$, then $P+Q=R \in E(F_p)$ and coordinate (x_3,y_3) of R is given by $x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ where $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

Point doubling : Let $P(x_1, y_1) \in E(F_p)$ where $P \neq -P$ then $2P = (x_3, y_3)$ where $x_3 = (\frac{3x_1^{\ 2} + a}{2y_1})^2 - 2x_1$ and $y_3 = (\frac{3x_1^{\ 2} + a}{2y_1})(x_1 - x_3) - y_1$

2.3 Elliptic Curve Discrete Logarithm Problem (ECDLP)

Given an elliptic curve E defined over a finite field F_p ,a point $P \in E(F_p)$ of order n, and a point $Q \in (P)$, find the integer $l \in [0, n-1]$ such that $Q = l.P$. The integer l is called discrete logarithm of Q to base P, denoted $l = \log_p Q$ [9].

2.4 Key exchange

It is a protocols consists of polynomial time algorithms involved between allow two parties to establish a secret shared secret session key. The session key can used for further encryption of a long message. The first protocol was proposed by Diffie-Hellman. Whose security is based on the difficulty of Diffie-Hellman Problem. Elliptic curve Diffie-Hellman key exchange protocol is on Elliptic curve and its security is based on Elliptic Curve Diffie-Hellman Problem (ECDHP).

2.5 Elliptic Curve Diffie-Helman

Elliptic curve Diffie-Helman protocol (ECDH) is one of the key exchange protocols used to establishes a shared key between two parties. ECDH protocol is based on the additive elliptic curve group. ECDH begin by selecting the underlying field F_p or $GF(2^k)$, the curve E with parameters a,b and the base point P . The order of the base point P is equal to n. The standards often suggest that we select an elliptic curve with prime order and therefore any element of the group would be selected and their order will be the prime number n [5][6]. At the end of the protocol, the communicating parties end up with the same value K which is a point on the curve.

Group Key Agreement Protocol

In dynamic scenario, entities' may join or leave a multicast group at any given time. As a result of the increased popularity of multi-party or group key agreement protocol. In the article Ingemerson et al. [13], Burmester and Desmedt [10], Steiner et al. [12] and Becker and Willie [11]. The two party and three party key exchange is converted to multi party protocol under passive (eavesdropping) adversary, These three provide rigorous proofs of security. In a dynamic group, a group key agreement scheme must ensure that the session key is updated upon every participants change so that subsequent communication sessions are protected from leaving members and previous communication sessions are protected from joining members[6].

3. Proposed Protocol

The protocol participants consist of a single authenticated server S and multi clients $C_1, C_2 .....C_m$ who wish to establish a session key. All clients have registered their respective password $pw_1, pw_2 ....pw_m$. Then the multiparty protocol runs among all the clients with the following parameters established:

Let the elliptic curve E defined over a finite field F_P two field elements $a, b \in F_p$, which defined the equation of the elliptic curve E over F_P i.e. $y^2 = x^3 + ax + b$ in the case $p \geq 3$, where $4a^3 + 27b^2 \neq 0$.

Let $M_1, M_2 .....M_m$ be m number of group elements in $E(F_p)$.

Two one-way hash functions G and H , where the output are the elements of F_P.

The proposed protocol computes the following steps.

- **Step -I**: Let each client C_i for $i = 1.2.....m$ selects random numbers $t_i \in [1, n-1]$ and computes the point $P_i = t_i.Q$ and $P_i' = P_i \oplus pw_i.M_i$ and broad cast P_i' to rest of the group.

- **Step -II:** Clients send $(C_1 \| P_1^{'}) \| (C_2 \| P_2') ..... (C_m \| P'_m)$ to S .

- **Step-III:** Upon receiving, S first recovers P_i by computing $P_i = P_i' \oplus pw_i.M_i$. Next S and R by computing $P = P^{'} \oplus M.pw_A$ and $R = R^{'} \oplus N.pw_B$. Next S select random number u from $[1, n-1]$ and computes $\tilde{P}_i = u.P_i$ for all $i = 1,2.....m$ and then compute the following

$pw_i' = pw_i.G(C_i \| S \| P_i)$ for all $i = 1.2.....m$

Then computes $\tilde{P}'_i = pw_j'.P_i', j = 1,2.....m$ and $i \neq j$ and sends $\tilde{P}'_1 \| \tilde{P}'_2 \| .....\tilde{P}_m^{'}$ to rest of the group.

- **Step -IV:** After having received $\tilde{P}'_1 \| \tilde{P}'_2 \| .....\tilde{P}_m^{'}$, C_i computes the pair wise key as $K_j = t_j.\tilde{pw}'^{-1}_j.(\tilde{P}'_i)$, where $i, j = 1,2.....m$ and $i \neq j$.

Computes $\alpha = G(C_1 \| C_2 \| ..... \| C_m \| K)$, where $K = K_i = K_j$ for $i, j = 1,2.....m$ and $i \neq j$.

Client C_j sends $\tilde{P}'_i \| \alpha$ to C_i for $i, j = 1,2.....m$ and $i \neq j$.

- **Step-V:** With $\tilde{P}'_i \| \alpha$ from C_j, C_i computes $pw'_i = pw_i . G(C_i \| S \| P_i)$, $K_i = t_i . (pw'_i)^{-1} . \tilde{P}'_j$ and verifies by computing $\alpha = G(C_1 \| C_2 \| ..... \| C_m \| K)$ if the verification fails, then C_i aborts the protocol. Otherwise C_i computes the session key SK as

$$SK = H(C_1 \| C_2 \| ..... \| C_m \| K)$$

and sends β, where $\beta = G(C_1 \| C_2 \| .....C_m \| K)$.

- **Step-VI:** Each client C_i verifies the correctness of β is equal to β_c by checking the equation $\beta_1 = G(C_1 \| C_2 \| ..... \| C_m \| K)$ $\beta_2 = G(\beta_1) \ldots \beta_c = G(\beta_{c-1})$. If it holds, then each client C_i computes the session key as

$SK = H(C_1 \| C_2 \| \ldots \| C_m \| \ldots \| K)$, otherwise, C_i abort the protocol.

3.1 Verification of Correctness of the protocol

The proof of correctness of the proposed protocol can be verified for each client $C_1, C_2 \cdots C_m$. Let for the client C_1, the key $K_1 = \tilde{P}'_2 . (pw_1')^{-1} . t_1$ can be verified with the client C_2 having the key $K_2 = P_1' . (pw_2')^{-1} . t_2$ by computing as

$$K_1 = \tilde{P}_2' . (pw_1')^{-1} . t_1 = (pw_1')^{-1} . (pw_1') . \tilde{P}_2 . t_1 = u . P_2 . t_1 = u . t_1 . t_2 . Q$$

$$K_2 = \tilde{P}_1' . (pw_2')^{-1} . t_2 = (pw_2')^{-1} . (pw_2') . \tilde{P}_1 . t_2 = u . P_1 . t_2 = u . t_2 . t_1 . Q$$

Similarly for each client $C_3, C_4 .... C_m$ the correctness of the protocol can be verified.

4. Security discussions

Theorem-1: It is computationally infeasible to verify the correctness of password guess.

Proof: In step –IV , One way collisions resistant hash function G is collision resistant is executed and s,u and t are all random numbers, so the protocol does not leak any information that allow the adversary to verify the correctness of password guesses.

Theorem-2: The protocol is resistant against off-line password guessing attacks.

Proof: If the attacker intends to tract out the password, he has to has to solve Elliptic Curve Discrete Logarithm problem (ECDLP) in step- I which is computationally infeasible takes fully exponential time. Therefore it is resistant against off-line password guessing attacks. This have been proved in [10][11]. So that the password will not be leaked.

5. Computational Cost

For each steps of computation of the protocol, the execution time we can calculate. Let the execution time takes for scalar multiplication, XOR operation and inverse operation are denoted T_M , $T_\oplus$ and T_I .

In step-I the protocol takes time = $2T_M + T_\oplus$.

In step-II only concatenation operation has to be performed. It can be ignored. In step-III, the execution time = $5T_M + 2T_\oplus$.

Execution time in step-IV and step- V = $2(T_M + T_I)$.

Total execution time = $9T_M + 3T_\oplus + 2T_I$

6. Off-Line Dictionary Attack

The proposed protocol is resistant against off-line dictionary attacks. This does not leak any information that allows to verify the correctness of password guesses, because G is a one-way function and s,u and t all are random numbers to be taken from $[1, n-1]$. Further the vulnerability of the protocol to the off-line attack can be avoided as

Consider for the client C_i, let $\overline{pw_i} = G(pw_i)$ and $\overline{pw_j} = G(pw_j)$ for $i \neq j$ and for all $i, j = 1,2 \cdots m$. Then C_i computes $P' = P \oplus \overline{pw_i}.M$ in stead of $P' = P \oplus pw_i.M$, and C_j compute as $R' = R \oplus \overline{pw_j}.N$ instead of as $R' = R \oplus pw_j.N$.

Accordingly, the Server S recovers P and R is modified to $P = P' \oplus \overline{pw_i}.M$ and $R = R' \oplus \overline{pw_j}.N$.

7. Conclusion

In this research a secure multi-party key exchange protocol has been proposed. The security of the proposed protocol is based on computational infeasibility of solving ECDLP. This is secure against off-line password guessing attack and also secure against off-line dictionary attack. The adversary cannot tract out the secure information that need to verify the correctness of password guesses. The proposed protocol can be implementing on low processor devices such as smart card, PDA etc. The computational cost is also low, since in all steps of the protocol scalar multiplication and XOR operation have to be executed. As compare to the other public key cryptosystems such as RSA and DSA which based on Integer factorization and simple discrete logarithm problems that take sub-exponential time. Whereas the best algorithm known for solving the ECDLP takes fully exponential time. As compare to the other cryptosystem like RSA and DSA , ECC offers security equivalent to these using far smaller key sizes. Due to this achieves higher-strength per-bit include higher speeds, lower power consumption, bandwidth savings and space complexity. So it can be implemented on low processor mobile devices.

REFERENCES

[1] Murat Fiskiran A and B Ruby Lee "Workload characterization of elliptic curve cryptography and other network security algorithms for constrained environments". Proc. IEEE Intl. Workshop on Workload Characterization, pp:127-137, 2002.

[2] De Win E. and B Preneel "Elliptic curve public-key cryptosystems - an introduction. State of the Art in Applied Cryptography", LNCS 1528, pp: 131-141, 1998.

[3] Aydos M., E Savas and C .K .KoV 1999. "Implementing network security protocols based on elliptic curve cryptography". Proc. fourth Symposium. Computer Networks, pp: 130-139, 1999.

[4] Y.F. Chang "A Practical Three-party Key Exchange Protocol with Round Efficiency". International Journal of Innovative Computing, Information and Control,Vol.4, No.4, April 2008, 953960.

[5] N. Koblitz. "A course in Number Theory and Cryptography", 2nd edition Springer-Verlag-1994.

[6] Jayaprakash Kar & Banshidhar Majhi "An Efficient Password Security of Three Party Key Exchange Protocol based on ECDLP" International Journal of Security & Its Applications Vol.3 (4), pp 25-32, October 2009.

[7] K. H Rosen "Elementary Number Theory in Science and Communication",2nd ed., Springer-Verlag, Berlin, 1986.

[8] A. Menezes, P. C Van Oorschot and S. A Vanstone "Handbook of applied cryptography". CRC Press, 1997.

[9] D. Hankerson, A .Menezes and S.Vanstone. "Guide to Elliptic Curve Cryptography "Springer Verlag, 2004.

[10] Jayaprakash Kar & Banshidhar Majhi "An Efficient Password Security of Multiparty Key Exchange Protocol based on ECDLP" International Journal of Computer Science and Security (IJCSS) Vol.3 (5), pp 405-413, Nov 2009.

[11] Jayaprakash Kar & Banshidhar Majhi "A Secure Two-Party Identity-Based Key Exchange Protocol Based on Elliptic Curve Discrete Logarithm Problem. Journal of Information Security and Assurance.(JISA) Vol.5 (4), pp 473-482, 2010.

[12] "Certicom ECC Challenge and The Elliptic Curve Cryptosystem" available: http://www.certicom.com/index.php.

[13] M. Burmester and Y. Desmedt "A Secure and Efficient Conference Key Distribution System". In proceedings of Eurocrypt 1994, LNCS 950, pp. 275-286, Springer-Verlag, 1995.

Author

Daniyal M. Alghazzawi has completed his Ph.D in Computer Science from University of Kansas in 2007, Master of Science in Teaching & Leadership in 2004 and Master of Science in Computer Science in 2003 from University of Kansas. He has worked as Web Programmer at ALTec (Advanced Learning Technologies) . Dr. Daniyal is currently Chairman of the Information Systems Department, Faculty of Computing and Information Technology, King Abdulaziz University. He has 04 journal papers and conferences to his credit. His research interest includes e-Security and Cryptography. Dr. Daniyal is a member of IEEE (Education Transaction) and ACM-SIGCSE (Special Interest Group in Computer Science Education) .