International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 4 Issue 8 ǁ August. 2016 ǁ PP. 68-72

A Mutual Authentication Protocol Which Uses Id for Security from Privileged – Insider Attacks

[1]Aashima Sood, Under the Guidance of [2]Shivi Sharma
[Associate Professor] H.P.T.U (Hamirpur) M. Tech Computer Science

Abstract: In the modern era, IT and e- commerce are developing at a rapid pace. As, with the help of smartphones ,we do internet banking ,online shopping etc from anywhere we want. Hence, we need a secure protocol for communication. So, this study introduces an id based mutual authentication protocol also known as Elliptic Curve Cryptography protocol for security purposes. Elliptic Curve Cryptography is better than RSA protocol which was used before this. ECC is a good development in terms of security protocol as it uses less memory and provides effective computation. Its been proposed to solve the problem of insider attack. This scheme defends against many attacks.

Keywords: mutual authentication; key agreement; bilinear maps; elliptic curve cryptography; discrete logarithm problem; computational Diffie-Hellman problem

I. INTRODUCTION

E-commerce is a the new buzz ward in the society and why not as by sitting at home we can shop online, pay our electricity bills online, transfer money online an can do whatever a human brain can think of. So, as the use of internet is increasing so is the demand of security increases. Therefore , for security purposes elliptic curve cryptography protocol has been proposed as it provide security from privileged insider attack. Basically ,attacks are of two types- active attack and passive attack. This protocol help us to overcome these attacks and provide a secure environment for the user who is accessing the internet.

In case, if users are increasing the issue of heavy certificate management can occur. To resolve this problem, Shamir presented a protocol which is depending on ID [1]. Then, frank presented a encryption approach which is based on the ECC [2]. One the researcher yang also explained an ID based authentication [3]. Yoo and Yoon proposed perfect secrecy and vulnerability for impersonation attack [4]. Later, Islam an Biswas propsed a protocol , followed by it Qi et al , further kim et al all proposed protocol based on the same concept.

ECC is a public key cryptography protocol which focuses on finding a point on elliptic curve which is a very tedious task for an attacker to break security of a protocol. In elliptic curve cryptography, point multiplication ,point addition and point doubling is used. Point addition and point multiplication used here are not like normal point multiplication and point addition. So breaking these points in elliptic curves requires a lot of time which is not possible. Hence, provides an immediate security against the various insider attacks. Here ,we study three different stages between the client and the server. First phase is the connection phase, second phase is the registration phase and third phase is the mutual authentication phase. We have tried to implement the changes in the mutual authentication phase which will discuss here in this paper.

The paper organized as follows: in section II preliminaries has been discussed. Section III discussed the review of previous protocols. In section IV proposed methodology is presented. Section V explained the analysis of security. In section VI conclusion is presented

II. PRELIMINARIES

In this section, preliminaries of presented protocol have been discussed below:

A. Bilinear maps

Suppose that G_1 and G_2 are two cyclic groups of any prime order p. assume the 'g' be any arbitrary generator of $G_{1.}$ Hence bilinear map between these two groups will be given as

$$: * \rightarrow$$

The bilinear map should satisfy the three significant properties ie.Bilinearity,non-degenerate and computability.

B. ECC

An imaginary hyper elliptic curve of genus 'g' over a field 'K' is given by the equation

$$C: +hy = f \in K[x, y]$$

Where $h(x) \in K[x]$ is a polynomial of degree not larger than 'g' and $f(x) \in K[x]$ is a monic polynomial of degree '$2g + 1$'. It can be concluded from the above equation that elliptic curves are of genus 1. 'K' is said to be a finite field. The Jacobian of 'C' is a quotient group and it is, denotedas $J(C)$. The elements of the Jacobian are equivalence classes of divisors of degree 0 under the relation of linear equivalence. And these elements of jacobian are not points. These have the same opinion with the elliptic curve case, because it could be indicate that the Jacobian of an elliptic curve is isomorphic with the group of points on the elliptic curve.

III. REVIEW OF PREVIOUS PROTOCOL

Arshad, Hamed*et al.[7]* proposed An proficient authentication and key agreement scheme for session initiation protocol using ECC. This work proposed a secure authentication and key agreement approach for session initiation protocol. This approach is relied on the elliptical cryptograph curve. Its security analyses indicate that proposed approach is secure against attacks of different types.

Mohammad Sabzinejad*et al.[8]* This paper presented a enhanced password-based authenticated key agreement protocol in order to overcome security problem. The result indicates that its gives low computational cost, better efficiency and performance as compared with other protocol. This proposed protocol is analyzed in random oracle model.

Shuenn-Shyang Wang *et al. [9]*In this paper, a authentication scheme has been presented which is secured and used for multi-server environment. These schemes achieve user's anonymity and also help to manage the secret key table which is associated with users. The entire requirement can satisfy with this novel approach. This approach uses hashing functions in order to implement mutual verification and session key agreement. This scheme is well suited to the smart card's applications.

Sghaier, Anissa*et al. [10]*This paper presented an implementation of arithmetic operation for HECC. The implementation has been done on FPGA. Hyper elliptic curves cryptosystems can easily be used in embedded environment where speed, energy, power, chip and area are constrained. The performance of HECC is relying on the speed constraint. Arithmetic operations are depends on the complexity of a mathematical issues and in order to have an optimized architecture, optimize arithmetic operations are necessary. In this work, high performance, area efficient implementation of arithmetic operations in HECC has been discussed over real field and a new design methodology is presented.

Chen, Tien-Ho *et. al.* Password protection scheme rely on the dynamic id based mechanism has been presented in this paper. This proposed model is secured mutual authentication and also gives ID - based authentication with higher security.

Kim et al.proposed an id based mutual authentication key agreement protocol with the help of bilinear mapping operation and elliptic curve cryptography. Here bilinear maps has been used for the verification of one if the messages sent by the client but it has not mention about the calculation of $=$. In actual such calculation is not possible in elliptic curve cryptography. Ifit is possible then one can easily calculate the randomly generated private values at both ends.

IV. THE PROPOSED MODIFIED MUTUAL AUTHENTICATION KEY AGREEMENT PROTOCOL

This paper presents an ID-based modified mutual authentication key agreement protocol based on elliptic curve cryptography. In this protocol, two entities which are a client C and a server Sauthenticate mutually and exchange a session key. And the IDof C is n-bits string. This protocol consists of three phases:system initialization phase, client registration phase, and modified mutual authentication with key agreement phase.

A. System Initialization Phase:

- Server S selects group of elliptic curve (G) of order (p) on E.
- S selects random master key,$x \in$, then computes$X = xP$, which is public key.
- S chooses three hash function $,, and$ where $: \rightarrow, : G \rightarrow \ and \ : \rightarrow$
- S keep x as private key and publishes .

B. Client Registration Phase:

- C randomly selects $\in$ and computes$= P$ and sends$I,)$ to the server.
- S verifies the identity of C. After successful verification S calculates and computes $= P$ and$s = x +$, then sends $(, s)$ to C.
- After receiving$(, s)$, C verifies $sP = X + Rs$ then computes $s = s +$ as secret key.

Whole procedure for client registration phase is shown in figure 1.

C.Modified Mutual Authentication Key Agreement Phase:

- C selects $\in$ and computes $= P\ , = X, = ID \oplus\ , M2 = sP\ and\ = (ID,,)$ and sends $(,,,)$
- S receives $(,,,)$, and compute $= x$ and $ID = \oplus H2$, then verifies $= sP +$ and also verifies $=$ from computed values.
- After successful verification S chooses $\in$and computes$= P, = x = xsP,\ = (ID,,„\ )$ and send to C
- C computes $= sX$ and verifies $= (ID,,,,)$. After successful verification C computes $=, S =, =$ and sends to S
- After receiving by S, it computes $=\ , S = (I\ ,,,,,,)$ and $=$ and verifies $=$ if yes then S accept that c has session key S.

Whole procedure of modified mutual authentication key agreement phase is show in figure 2.

$Client$	$Server\ (x \in, X = xP)$
$chooses\ \in, computes\ = P$ $(I,)$	
	$checks\ identity\ of\ C$ $chooses\ \in, computes\ = P, s = +$ $(s,)$
$verifies\ sP = X + Rs$ $computes\ s = s +$ $s\ is\ client's\ secret\ key$	

Figure 1 Registration phase of client

$Client\ (I)$	$Server\ (x \in, X = xP)$
chooses $\in$ $computes\ = P$ $= X, = sP$ $= I\oplus$ $=$ $(,,,)$	
	Computes $=$ x $= \oplus$ $Verifies\ = sP +$ $=$ $chooses\ \in$ $computes\ = P$ $= x = sxP$ $=$
$computes = sX$ $verifies =$ $computes =$ $S =$ $=$ ()	
	$compute =$ $S = (I\ ,,,,,,)$ $=$ $If\ = , acceptsSKassessionkey$

Figure 2 Modified Mutual authentication key agreement phase

C. Efficiency

The efficiency of proposed algorithm has been compared with various previously proposed protocol in islam and biswas[6], Qi et al [12] and kim et al [11]. From the table shown in Table 1 it is already proved that kim et al is better than in islam and biswas and Qi et al in terms of security with tradeoff between cost. But in our protocol cost has been reduced as compared to Kim et al with same security coverage. In Kim et al total cost for authentication is $12H + 1 + 14 + 3B$ and in our modified protocol total cost is coming out to be $12H + 2 +$

14, the only difference is $3B\ and\ 1$. Now let's assume the cost of Bilinear computation is half of the computation of Point addition in elliptic curve i.e.
$B = 0.5$
Then the overall difference between the total cost of Kim et al and our protocol is coming out to be
$=Total\ cost\ of\ kim\ et\ al - total\ cost\ of\ \ Our\ protocol$
$= -$
$= 3 \times 0.5\ -$
$=\ 0.5$
On assuming that the computation cost of bilinear map w.r.t. point addition in elliptic curve is equal i.e.

$$B =$$

Then the overall difference between the costs of the two protocols is coming out to be
$= Total\ cost\ of\ kim\ et\ al - total\ cost\ of\ \ Our\ protocol$
$= -$
$= 3 \times -$
$=\ 2$
Hence in both the cases the proposed modified mutual authentication protocol has less cost of computation than previously proposed protocol with security against almost all attacks covered in kim et al.

Table 1 Efficiency Comparison Against Protocol

	Protocols				
	islam and biswas		*Qi et al*	*kim et al*	*our protocol*
Security against Insider-Attack	NO		NO	YES	YES
Security against other -Attack	YES		YES	YES	YES
Registration phase	C	$1H + 1A + 3M$	$1M$	$1H + 1A + 3M$	$1H + 1A + 3M$
	S	$1H + 2A + 2M$	$2H + 1A + 3M$	$1H + 1M$	$1H + 1M$
Mutual Authentication Phase	C	$5H + 6M$	$5H + 3E$	$5H + 5M$	$5H + 5M$
	S	$6H + 1A + 5M$	$5H + 1A + 4M$	$5H + 5M + 3B$	$4H + 5M + 1A$
Total Cost		$13H + 4A + 16M$	$12H + 2A + 11M$	$12H + 1A + 14M$ $+ 3B$	$12H + 2A + 14M$

C: *The Client*, S: *The Server*, H: *Hash function computation*, B: *Bilinear Map computation*
: *Point addition computation*, : *Point multiplication computation*

V. SECURITY ANALYSIS

In the analysis of security, it can be seen that the presented protocol is secure against the following attacks: Privileged insider attack.

This type of attack utilized to verify that the server be familiar with all user's private key. If the server obtain a secret key, then it will create a valid session key while the user did not desire to make sessions. In our protocol will be verified at server end without knowing client's secret key which was also done in kim et al
Logged in user attack
This type of attack is that in which various people simultaneously access to the target with the aim of DoS attack. But the proposed protocol is developed to connect with single client by utilizing status bit.
Known session-specific temporary information attack In this type of attack user knows the session short-term secrets and an attacker desires to know the session key ofclient for acting as a client. Even though the attacker already knew the session short-term secrets but this session key can only be calculated by the server and client.

User anonymity

In this attack, attacker will not able to see the client information like client ID's. if any third party tries to discover the client's ID then the client will be vulnerable to attack. The proposed protocol gives user anonymity using hash function so that any third party is not able to view the client information.

Replay attack

The attacker tries to confirm with key agreement by information of client as an original client. The client and the server of the protocol always choose random values, thus the attacker will not use the client information again and our protocol is protected against replay attack.

Known session key security

In this type of attack, the third party will try to obtain the latest session key by using former session key. But, in the proposed protocol, when the client calculate the session key then client is using cryptographic one way hash function. Due to this function, no value is exposed thus, attacker could not able to get the current session key and our protocol is safe against this type of attack.

Perfect forward secrecy

In this attack, security of previous session key should be kept secret, even though the attacker knows of secret key of the client and of secret key of the server.

VI. CONCLUSION

As a matter of fact, network communication is of no use if it does not provide security and authentication or we can say internet is nothing without security as every user as his/her requirements for security first of all as priority. We have tried t make changes in the mutual authentication phase and have successfully implemented those changes and hence ended up reducing the cost of the protocol proposed before. Thus, made a successful completions of the ECC protocol.

REFERENCES

[1]. A. Shamir, “Identity-based cryptosystems and signature protocols,”Proceedings of the Advances in Cryptology-Crypto84, Santa Barbara,USA, pp.47-53, 1984.

[2]. D. Boneh, M. Franklin, “Identity-based encryption from the WeilPairing,” Advances in Cryptology-Crypto01, Springer Berlin Heidelberg,

[3]. pp.213-229, 2001.

[4]. J. Yang, C. Chang, “An ID-based remote mutual authentication with keyagreement protocol for mobile devices on elliptic curve cryptosystem,”Computers & Security vol. 28, no.1, pp.138-143, 2009.

[5]. E. Yoon, K. Yoo, “Robust ID-based remote mutual authentication withkey agreement protocol for mobile devices on ECC,” International

[6]. Conference on Computational Science and Engineering, Vancouver,Canada, vol.2, pp.633-640, 2009.

[7]. H. Debiao, C. Jianhua and H. Jin, “An ID-based client authenticationwith key agreement protocol for mobile client-server environment on

[8]. ECC with provable security,” Information Fusion, vol.13, no.3, pp.223-230, 2011.

[9]. S. H. Islam, G. P. Biswas, “An improved ID-based client authenticationwith key agreement protocol on ECC for mobile client-sercer

[10]. environments,” Theoretical and Applied Informatics. vol.24, no.4,pp.293-312, 2012.

[11]. Arshad, Hamed, and MortezaNikooghadam. "." *Multimedia Tools and Applications* 75, no. 1 (2016): 181-197.

[12]. Mohammad Sabzinejad, and Mahmoud AhmadianAttari. "A provably secure and efficient authentication scheme for access control in mobile pay-TV systems." *Multimedia Tools and Applications* 75, no. 1 (2016): 405-424.

[13]. Shuenn-Shyang Wang. "A secure dynamic ID based remote user authentication scheme for multi-server environment." Computer Standards & Interfaces 31.1 (2009): 24-29.

[14]. Sghaier, Anissa, MedienZghid, and Mohsen Machhout. "Proposed efficient arithmetic operations architectures for Hyperelliptic Curves Cryptosystems (HECC)."Systems, Signals & Devices (SSD), 2015 12th International Multi-Conference on.IEEE, 2015.

[15]. Kim, Song Yi, Hyoseung Kim, and Dong Hoon Lee. "An Efficient ID-Based Mutual Authentication Secure against Privileged-Insider Attack." IT Convergence and Security (ICITCS), 2015 5th International Conference on. IEEE, 2015.

[16]. Y. Qi, C. Tang, M. Xu and B. Guo, “An Identity-based mutual authentication with key agreement protocol for mobile client-server environment,” Communications Security Conference, pp.29, 2014.