Efficient and Secure ID-Based Mutual Authentication for Mobile Devices using ECC

Shubhangi N. Burde
Mtech Scholar
Department of computer science and engineering, G.H.Raisoni Institute of Engineering and technology for Womens Nagpur, India

Prof. Hemlata Dakhore
Asst. Professor
Department of computer science and engineering, G.H.Raisoni Institute of Engineering and Technology for Womens Nagpur, India

Prof. S. P. Chhaware
Asst. Professor
Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, India

Abstract

With the rapid development of mobile devices, people can easily use various electronic services any time everywhere for convenient and modern life. Remote user authentication becomes a very important ingredient procedure for the network system service to verify whether a remote user is legal through any insecure channel. Users can use to access many applications, for example internet banking, online shopping, mobile pay TV, are accomplished on internet or wireless networks. Therefore, secure communications in such wireless environments are more and more important because they protect transactions between users and servers. Especially, users are people vulnerable to attacks and there are many authentication systems proposed to guarantee them. Islam and Biswas have proposed a more efficient and secure ID-based system for mobile devices on ECC to enhance security for authentication with key agreement system. They claimed that their system truly is more secure than previous ones and it can resist various attacks. However, it is true because their system is vulnerable to known session-specific temporary information attack, and the other system is denial of service resulting from leaking server's database. Thus, the paper presents an improvement to their system in order to isolate such problems.

Keywords-Authentication, Password, Dynamic ID, Smart card, Impersonation, Session key, elliptic curve cryptosystem

1. Introduction

Elliptic Curve (EC) systems as applied to cryptography were first proposed in 1985 Independently by Neal Koblitz and Victor Miller. Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create smaller, faster, and more efficient cryptographic keys. Elliptic curve cryptography (ECC) is an approach to public key cryptography (PKC) based on the algebraic structure of elliptic curves over finite fields. The technology can be used in conjunction with most public key encryption methods, such as Diffie-Hellman and RSA. According to some researchers, Elliptic curve cryptography (ECC) can yield a level of security with a 164-bit key than other systems require a 1,024-bit key. Because ECC helps to establish equivalent security with lower computing power and battery resource usage. It is widely used for mobile applications. Elliptic Curve Cryptosystem (ECC) based remote authentication system has been use for mobile devices. Mobile phones are most common way of communication and accessing Internet based services. Currently, mobile phones are used for formal communication, sending and receiving sensitive data. However, the security of mobile communication has topped the list of concerns for mobile phone users. Public key cryptography is effective security solution to provide secure mobile communications. Mobile devices (e.g., cell phone, notebook PC and PDA) have gained increasingly popularity due to their portability nature. Therefore, secure communications in such wireless environments are more and more important because they protect transactions between users and servers from illegal adversaries. Public key cryptography algorithms provide the way to achieve security requirements viz; confidentiality and authentication.

In 2009, Yang [6] proposed a system combining elliptic curve and identity-based cryptosystems to enhance security. They claimed that their system's secure against various attacks, such as replay attack, impersonation attack. But in the same year, Yoon [7] pointed out that Yang's system can't withstand impersonation attack. Furthermore, it doesn't achieve perfect forward secrecy property, which is a very important security in evaluating a strong authentication and key agreement protocol. Then, Yoon proposed another system to fix such problems. In 2010, Chen [5] proposed an advanced

ECC ID-based remote mutual authentication system for mobile devices to improve Yang's system. And they also claimed that their system's more secured to authenticate users and remote servers for mobile devices. However, Islam and Biswas [4] in 2011 have proposed a more efficient and secure ID-based remote mutual authentication with key agreement system for mobile devices on elliptic curve cryptosystem. And they pointed out many new problems in 3 previous systems, for example user's anonymity, many logged-in users, clock synchronization. Then, they claimed that their system's truly efficient and usable for mobile users in many internet applications or wireless networks. Nevertheless, in this paper, we prove that the Islam's system can't resist known session-specific temporary information and denial of service resulting from leaking server's database attacks. Afterward, we propose an improvement of their system to overcome such entanglements. Besides, our system possesses low power consumption and computation cost than previous systems. Our main ideas aren't using point addition operation between a random point and user's authentication key and not letting random value is stored into server's database to fix recommended problems of Islam's system [4].

2. Related works

This paper reviews the basic concepts of elliptic curve cryptosystem & introduces 3 computational problems.

A. Elliptic Curve Cryptosystem

An elliptic curve's a cubic equation of the form y2 + a1xy + a2y = x3 + a3x2 + a4x + a5, where a1, a2, a3, a4, a5 are real numbers. In elliptic curve equation is defined as the form of Ep(a, b): y2 = x3 + ax + b (mod p) over a prime finite field Fp, where a, b $\in$ Fp, p > 3, and 4a3+ 27b2 _= 0 (mod p) (Hankerson et al., 2004). Given an integer s $\in$ F$*p$ and a point P $\in$ Ep(a, b), the point multiplication s.P over Ep(a, b) can be defined as s ・ P = $P + P + ... + P$ _ __ _ *s times* .

B. Computational Problems

Generally, the security of ECC based on the difficulties of the following problems.
1) Given two points P and Q over Ep(a, b), the elliptic curve discrete logarithm problem (ECDLP) is to find an integer s $\in$ F$*$ p such that Q = s ・ P.
2) Given 3 points P, s ・ P, and t ・ P over Ep(a, b) for s, t $\in$ F$*$ p, the computational Diffie-Hellman problem (CDHP) is to find the point (s ・ t) ・ P over Ep(a, b). 3) Given two points P and Q = s ・ P + t ・ P over Ep(a, b) for s, t $\in$ F$*$ p, the elliptic curve factorization problem (ECFP) is to find two points s ・ P and t ・ P over Ep(a, b).

3. ECC for mobile devices and its applications

Although the discrete logarithm problem was first deployed by Diffie and Hellman was defined precisely as the problem of finding logarithms with respect to a generator in the multiplicative group of the integers modulo a prime, this method can be enhanced to arbitrary groups and specially, to elliptic curve groups. The elliptic curve public-key systems provide relatively small block size, high speed, and high security. The primary advantage that elliptic curve systems have over systems based on the multiplicative group of a finite field (and also over systems based on the intractability of integer factorization) is the absence of a sub exponential-time algorithm (such as those of "index-calculus" type) that could find discrete logs in these groups. Consequently, we can use an elliptic curve group which is smaller in size while retaining the same level of security. Also in RSA cryptosystem, the security increases sub exponentially whereas in elliptic curve cryptosystem, the security increases directly exponentially. The consequence is smaller key sizes, bandwidth savings, and faster implementations features which are especially attractive for security applications where computational power and integrated circuit space is limited, such as smart cards, PC (personal computer) cards, and wireless devices.

● In paper [1], author provides the security than previous one. The computation and energy costs of the pairing-based systems are higher than those of ECDLP-based systems. Recently, Yang and Chang pointed out some disadvantages in the previous user authentication systems on ECC. Some of these systems do not provide the mutual authentication or the session key agreement between the user and the server. For some applications, the user and the server need a session key to encrypt the secret information for the subsequent communications after they authenticate with each other. To resolve such problems, YC proposed an ID-based remote mutual authentication with key agreement system on ECC. Based upon ID-based concept, YC system has the following advantages: (1) This system does not require additional computations for certificate; (2) This system is not constructed by bilinear-pairings, which is an expensive operation on EC; (3) This system not only provides mutual authentication but also supports a session key agreement between the user and the server; (4) This system is more efficient and practical than the related works. Nevertheless, YC system not only is vulnerable to an impersonation attack but also does not provide perfect forward secrecy in spite of efforts to perform mutual authentication and session key agreement between the user and the remote server and reduce the computational costs more than the related works. To avoid these security problems, this paper proposes an improved ID-based remote mutual

authentication with key agreement system for mobile devices on ECC. This work explains a cost effective Public-Key Cryptography (PKC) based solution for security services like key-distribution and authentication which are required for wireless sensor networks. The author proposes a custom hardware assisted approach to implement Elliptic Curve Cryptography (ECC) in order to obtain stronger cryptography as well as to minimize the power. Their compact and low-power ECC processor contains a Modular Arithmetic Logic.

4. Proposed Authentication System

The proposed system will result more efficient enhancements for security on mobile devices using ECC. The proposed system not only inherits the advantages of their system, it also enhances the security. The general ideas in the proposed system is more detailed. In registration phase, the main goal is achieving AIDU. Random value X helps to resist reregistration of attackers, with the same identity but various authentication keys at different time. In authentication phases, we use two random value rU and rS for server & user to challenge each other. Furthermore, we don't store random value X into database & don't perform point addition operation for AIDU. This system's divided into the four phases of system initialization, user registration, and mutual authentication with key agreement & leaked key revocation phase.

Figure 1: System Design Model

A. System Initialization Phase

In this phase, three one-way hash functions are used. The system initialization phase includes four steps:

· Step 1: S chooses k-bit prime number p & base point P with order n from the elliptic curve group Gp.

· Step 2: S chooses random number qS from [1, n - 1]

· Step 3: S chooses three one-way hash function H1: {0, 1}* → Gp, H2: Gp x Gp → {0, 1}k and H3: Gp → {0, 1}k

· Step 4: The server publishes (Ep(a, b), P, H1, H2, H3) as system parameters & keeps the master key qS secret.

B. User Registration Phase

There are 3 requirements for a registration phase: secrecy for information transmitted between user & server, difference between keys provided for each time of registration by server & server mustn't store user's information which can be a hazardous risk. Easily, Islam's system achieved first two requirements but not the last. So, to recover this point accomplishes a good registration phase. This system consists of 3 steps illustrates these ones.

Step 1: U chooses identity IDU = {0, 1}k and Submits it to S with some personal information via secure channel.

Step 2: S checks U's IDU. If IDU already exists in the server's database, S asks U for different identity. Otherwise, S chooses a random value X ∈ Z* p. Then, S computes AIDU = qS · H1(IDU _ X). Finally, S stores (IDU, status-bit) of that user U into database (status-bit is similar to Islam's system).

Step 3: S returns AIDU to U via a secure channel

C. Mutual Authentication & Session Key Agreement Phase

Similarly, this phase also proposes 3 requirements that help authentication be more secure: firstly, user & server must use random values to challenge each other. Secondly, user & server share a secret session key. Finally, temporary information mustn't affect negatively to important information such as authentication key. In Islam's system, both user & server use random values to challenge each other. However, their system's easy to leak authentication key AIDU if any random point's known. Thus, this phase'll fix this weak point. In this phase, S and U will have the same session key SK. Figure 4 illustrates the steps that S authenticates U and vice versa.

Step 1: At first, U keys identity IDU & the authentication key AIDU into the mobile device & randomly choose a number rU from [1, n - 1]. Then, mobile device computes R = rU · H1 (IDU _ X), R_ = rU · AIDU, M = H2 (R_ _ AIDU) and CIDU = IDU ⊕ H3 (R_). Mobile device sends (X, CIDU, M, R) to S.

Step 2: On receiving (X, CIDU, M, R) from U, S computes R_ * = qS · R. Then, S extracts user's identity by doing IDU = CIDU ⊕ H3 (R_ *) and then checks the validity of the identity IDU. If IDU is valid, S continue to go next step, otherwise rejects U's login message request.

Step 3: S computes the authentication key AID* U = qS · H1 (IDU _ X) and checks M?= H2(R_ * _ AID* U). If it doesn't hold, S rejects U's login request, otherwise chooses a random number rS from [1, n - 1]. Then, S computes point S = rS · AID* U, T = R_ * + S and HS = H2(S _ AID* U).

Now, S sends (T, HS) to U.

4) Step 4: On receiving (T, HS), U computes S* = T - R_ and checks HS? = H2 (S* _ AIDU). If it holds, U authenticates S and sends the message (HRS) to S, where HRS = H2 (R_ _ S*). U computes session key

SK = H3 (rU ・ S∗). 5) Step 5: On receiving (HRS), S checks HRS? = H2 (R_ ∗ _ S). If it holds, S authenticates U. S computes session key SK = H3 (rS ・ R_ ∗).

D. Leaked Key Revocation Phase

This phase's similar to Islam's system. However, this phase use a secure channel in two ways to protect secret information of user. And Islam's system doesn't mention secure channel in this phase.

5. Security and Efficiency Analysis

This section discusses the 2 aspects i.e. security & efficiency of the proposed system.

A. Security Analysis

In this subsection, the proposed system can resist many kinds of attack. Assume that wireless communications are insecure and that there exists an attacker. He/she has capability to intercept all messages communicated between server & user. Especially, denial of service resulting from leaking server's database in the systems of Yang, Yoon, and Chen isn't problem because these systems don't store anything in server's database.

1) Stolen Verifier Attack: Because S doesn't store any table with information related to U, the proposed system can withstand stolen-verifier attacks. In this system, S generates a random value X for each user. Therefore, when authenticating with S, U only needs to send X to S and S uses master key qS to re-construct AIDU of that user. So, S doesn't need to keep U's password in the storage space when a new user's added in the system.

2) Known Session-Specific Temporary Information Attack: Like definition of Islam's system, the proposed system can resist this kind of attack and also assume that another adversary A knows rU and rS of another past session. However, a still can't know session key SK. We see that SK = rU ・ rS ・ AIDU and A can't know AIDU. So, A can't compute random point R_ or S to know SK.

3) Session Key Perfect Forward Secrecy Attack: Session key perfect forward security means, if the long term secret key of user & server are leaked but the generated session key should be safe from the attacker. In proposed system, if the authentication key AIDU and qS are compromised to an adversary, then he can compute two random points R_ = rU ・ AIDU and S = rS ・ AIDU. However he can't compute session key SK = rU ・ rS ・AIDU because he must face the Diffie-Hellman problem.

4) Known-key Attack: The known-key security means that compromise of another past session key can't derive any further session key. In the proposed system, the session key SK is the result of one-way hash function, which isn't recomputed. Thus, the attacker can't obtain any further session key. At this point, Islam's system also achieves due to using one-way hash function.

5) Denial of Service Resulting from Leaking Server's Database Attack: Denial-of-service attack means that another adversary can update wrong verification information of another legitimate user. Then, that legal user can't login to remote server successfully. In this system, there's no verification table or dangerous risk information stored in the remote server. So, the proposed system can resist this kind of attack successfully.

6) Mutual Authentication: Like Islam's system, the proposed system uses the three-way challenge-response handshake technique to achieve mutual authentication. First, U sends (X, CIDU, M, R) to S. Afterward, S checks M?= H2(R_ _ AIDU) and then resends (T, HS) to U. U will checks HS ?= H2(S _ AIDU) to authenticate S. Then, U sends HRS to S. Finally, S checks HRS?= H2(R _ S) to re-authenticate U.

7) Session-key Agreement: After finishing mutual authentication successfully, both user & server share a session key SK to encrypt message later. So, proposed system not only satisfies mutual authentication but also provides session key to partners. For example, this system can resist various attacks & problems such as replay, insider, and impersonation attacks, clock synchronization, many logged-in users, user's anonymity problems. Also provides session key to partners.

B. Efficiency Analysis

To analyze computational complexity, compare efficiency between proposed system & the previous systems. That is, let H be the hash function operation, PM be the elliptic curve scalar point multiplication, and PA be the elliptic curve scalar point addition or subtraction. Furthermore, slight difference with Islam's system, the proposed system ignore exclusive-or (⊕) and concatenation (_) operation because it requires very few computations. Clearly, proposed system needs less computational amount than previous systems.

6. CONCLUSIONS

With the continuous growth of wireless networks, such as GSM, CDPD, 3G and 4G, remote authentication systems play an important role in communicating between parties. After examining the security, implementation and performance of ECC applications on various mobile devices, we can conclude that ECC is the most suitable PKC system for use in a constrained environment. The efficiency and security makes it an attractive alternative to

conventional cryptosystems. Consequently, we propose an improved system to eliminate some problems. Also provide the actual implementation of ECC based on the proposed paper. Compared with related systems, the proposed system has the following main advantages: It needs less computational cost. It provides secure user's anonymity. It doesn't hold any verification table. It provides mutual authentication with session key agreement. As a result, the proposed system's able to provide greater security & be practical in wireless communication systems.

7. Reference

[1] "Improvement of the more efficient and secure ID-based remote mutual authentication with key agreement system for mobile devices on ECC", Toan-Thinh TRUONG, Minh-Triet TRAN & Anh-Duc DUONG, 2012 IEEE 26th International Conference on Advanced Information Networking and Applications Workshops.

[2] "A secure and efficiency id-based authenticated key agreement system based on elliptic curve cryptosystem for mobile devices", Eun-jun yoon, Sung-bae choi and Kee-young yoo, international journal of innovative computing, information and control, April 2012.

[3] "High Performance Scalar Multiplication for ECC", Ravi Kishore Kodali, Harpreet Singh Budwal, 2013 IEEE International Conference on Computer Communication and Informatics (ICCCI -2013), Jan. 04 – 06, 2013, Coimbatore.

[4] "A more efficient and secure id-based remote mutual authentication with key agreement system for mobile devices on elliptic curve cryptosystem", S. H. Islam and G. P. Biswas, Journal of Systems and Software, vol. 84, no.11, 2011.

[5] "An advanced ecc id-based remote mutual authentication system for mobile devices", 2010 Symposia and Workshops on Ubiquitous, T.-H. Chen, Y.-C. Chen and W.-K. Shih, Autonomic and Trusted Computing, pp. 116–120, 2010

[6] "Robust id-based remote mutual authentication with key agreement system for mobile devices on ecc", E.-J. Yoon and K.-Y. Yoo, IEEE International Conference on Computational Science and Engineering, vol. 2, pp. 633–640, 2009.

[7] "Security enhancement for a dynamic id-based remote user authentication system", I.-E. Liao, C.-C. Lee, and M.-S. Hwang, IEEE Transactions on Consumer Electronics, vol. 50, pp. 629–631, 2008.

[8] "A dynamic ID-based remote user authentication system", M.L. Das, A. Saxena, V. P. Gulati, IEEE Transactions on Consumer Electronics, 2009, 629-631.

[9] "Further improvement of an efficient password based remote user authentication system using smart cards", E. J. Yoon, Tian et al, IEEE Transactions on Consumer Electronics, vol. 50, pp. 612-614, May 2004.

[10] "A new remote user authentication system using smart cards", M. S. Hwang and L. H. Li, IEEE Transactions on Consumer Electronics, vol.46, pp. 28-30, Feb 2000.

[11] "A novel remote user authentication system for multi-server environment without using smart cards", K.-H. Yeh and N. W. Lo, International Journal of Innovative Computing and Information Control, vol.6, no.8, pp.3467-3478, 2010.

[12] "Efficient convertible multi-authenticated encryption system without message redundancy or one-way hash functions", J.-L. Tsai, T.-S. Wu, H.-Y. Lin and J.-E. Lee, International Journal of Innovative Computing, Information and Control, 2010.

[13] "An authenticated key exchange protocol for mobile stations from two distinct home networks", H.-L. Wang, T.-H. Chen, L.-S. Li, Y.-T. Wu and J. Chen, International Journal of Innovative Computing Information and Control, 2010.