A Secure Key Issuing Protocol for Peer-to-Peer Network

Nirmala Jagadale
Computer Science Dept.
Sinhgad Institute of Technology,
Lonavala, India

Thaksen Parvat
Computer Science Dept.
Sinhgad Institute of Technology,
Lonavala, India.

Abstract

A Peer-to-Peer (P_2P) networks is one of the popular network technology as it design the low cost and high availability content distribution systems. So, security is most important issues for p_2p network. The Identity based cryptography(IBC) was introduced into networks for identity verification and authentication purposes whichcould not address some security Problem.In this paper, We present an efficient key issuing protocol which makes the IBC to be more acceptable and applicable.This protocol provides a peer registration service using Shamir's (k, n) secret sharing scheme and which adopts KGC and KPAs to issue private keys to peers very securely. For the security of KPAs,we authenticate KPAs, also remove malicious ones using the BFT(Byzantine fault tolerance) protocol. The theoretical analysis and experimental results show that this protocol performs effectively and efficiently, and is able to support large scale networks and This Protocol secure networks from various attacks.

1.Introduction

Traditional public key cryptography (PKC) uses certificates, issued by a certification authority(CA), to bind the users with their public keys. Although certificates are the best alternative forkey distribution.With its distributed, self-organization and self-maintenance nature, P_2P networks are extremely vulnerable to a large spectrum of attacks, mainly due to the lack of a certification service responsible for peer's identity verification and for authentication purposes.Some of the problems are solved by verifying the authenticity of nodes identities and issuing public key certificate to each node. As the node churn is highly frequent in the P_2P network, many nodes that stored certificates may quickly become invalid, hence PKI based security protocol is difficult to be deployed. Each node requires large amounts of space to store public key certificates, which can be difficult to implement in practice and it needs more dynamic memory space.Identity based (ID-based) cryptography introduced by Shamir in 1984, overcomes these problems by avoiding the use of certificates. Identity based cryptography uses the users identity such as social security number (SSN), passport number as his public key. The private keys of the users are issued by a key generation center (KGC) through a secure channel, after verifying the user's credentials. Thus, the trust over KGC removes the need of certificates in ID based cryptography. Any identity based cryptosystem includes two phases namely Setup and Key extraction/generation and issuing that are carried out by KGC. Even though ID-based cryptography overcomes the problems in the traditional KGC, it suffers from two inherent problems: key escrow and secure channel requirement.

The KGC has the knowledge of the user's private keys and therefore can decrypt any cipher text or forge signature on any message which is known as key escrow problem. Moreover key issuing requires secure channel to avoid eavesdropping. For overcoming this secure channel problem and key escrow problem,we develop an efficient key issuing protocol which enables the identity based cryptosystems to be more applicable in the real world.

The first key issuing protocol was presented by Boneh and Franklin in 2001. Later on, Lee et al. and Gangishetti et al. have proposed key issuing protocols which use one key generation center (KGC which is nothing but PKG) and multiple key privacy authorities (KPAs) for issuing the private keys to the users. In their approach the key escrow problem can be avoided if at least one of the KPAs is honest. However, private keys of all the users have to be reconstructed if the private key of even one of the KPAs is compromised. In this paper, we propose a secure and efficient key issuing protocol which involves one KGC and n KPAs. Our protocol does not require secure channel for key issuing and eliminates the key escrow problem completely. Thus overcoming the problem of KGC impersonation existing in several schemes.We also show that replay, man-in-the-middle and insider attacks are not possible on the proposed protocol.

The rest of the paper is organized as follows: In section 2, we review the various existing key issuing protocols. In section 3,We give the mathematical background concepts and data flow architecture followed by the model for the proposed protocol.In section 4, we discuss about the salient features and security analysis of the proposed protocol.In section 5, conclusion about paper.

2. Related Work

Mikko,vestola, discuss about attacks occurred in p_2p and give some countermeasures which mitigates the effects of identity assignment attacks and Sybil attack. In 2002,Emil sit,Robert, focuses on the attacks those that threaten the liveness of the system,by preventing participants from finding data.In 2005,Hosam,Williamenck presents admission control system for structured p_2p networks. Though IBC overcomes the problems of the traditional PKI, it suffers from some inherent IBC uses the user's identity as his public key.The private keys of the users are issued by a key generate center (KGC) after verifying the users credentials. IBC was introduced in 1984 by Shamir; however, the first practical encryption scheme (IBE) was not available until 2001 which was developed by Boneh and Franklin problems, one of which is the secure channel requirement: key issuing requires secure channel to avoid eavesdropping. In 2001, Boneh, Franklin [4] addressed the problem of key escrow in identity based cryptosystems using distributed PKGs i.e. instead of one PKG issuing the user secret they used n PKGs. User obtains partial private keys from each PKG and combines them to get the private key. Thus, the key escrow problem can be avoided if at least one-out-of-n PKGs is honest. They also suggested that their approach can be extended to threshold key issuing using Shamir secret sharing.In their approach, all the PKGs are at the same level. Therefore, a user has to be registered at each PKG, which is practically difficult to perform. Moreover, the protocol requires secure channel to issue partial private keys.

In 2002, Chen et al. and Paterson have given solutions which are similar to that of Boneh et al. In these schemes,each trusted party has to check and authenticate user identity independently which is not practically feasible.In 2003, Hess [8] proposed a protocol using the concept of multiple trust authorities to avoid the key escrow problem. Gentry proposed a certificate based encryption scheme that provides secure key issuing by embedding user chosen secret information in the private key. Later, Al-Riyami and Paterson proposed certificateless public key cryptography. They also used the user chosen information for eliminating the key escrow problem. Though the schemes are successful in removing the key escrow problem, they loose the advantages of ID based cryptosystems.

In 2004, Sui et al. proposed a separable and anonymous key issuing protocol without secure channel. However, Kim et al. have shown that their protocol suffers from impersonation attack by KGC.

Thus the scheme obtains only trust level I and the problem of key escrow still remains.In the same year, Lee et al. [3] proposed a key issuing protocol, addressing the key escrow problem and secure channel requirement. In this protocol, a users private key is issued by a key generation center, and its privacy is protected by multiple key privacy authorities (KPAs). These authorities work in a sequential mode. Only one authority (the KGC) has to authenticate the user and thus it greatly reduces the cost of user authentication. The scheme also makes use of user-chosen secret information for constructing a secure channel for a user to retrieve his partial private key securely.However, the scheme suffers from the following attacks as pointed out by Gangishetti et al. [5]: (i) impersonation attack (can be done by any user) (ii) insider attack (can be done by any of the KPAs) (iii) Incompetency of KPAs. Moreover, Chunxiang et al. have shown that a malicious KGC can successfully attack the Lee etals protocol to obtain users private keys. Thus, this scheme attains trust level I. In 2005, Gangishetti et al. [5] proposed a new key issuing protocol, which involves one KGC and n KPAs. According to the protocol, KGC gives a registration identity, r_{ID} to the user during the registration. User uses this r_{ID} as blinding factor while collecting the partial private keys.

3. Programmer's Design

There are three terms present namely Key Generation Center, Key Privacy Authorities and peer in our protocol.

I.Key Generation Center: KGC is the main entity for peer registration. At first it checks the peer identity and then it gives a proof of registration for the registered peer. The registration process is done offline. KGC also maintains a database for the registered peers. This database is modified by KGC only which is publicly available. It also gives a partial private keys to the registered peers.

II. Key Privacy Authorities: Here, in this system number of KPAs are used to provide the key privacy service. On accepting a request from a peer, these KPAs checks that the peer has been registered or not, using this database. If the peer is registered, KPAs calculate the partial private key for registered peer and gives this partial private key to the peer. Each KPA maintains its own database for the received requests, which is not be kept secret for theavoiding KGC impersonation attack.

III. Peers: At first, Peer is registered at KGC.Then it gets partial private key from KGC and after that Peer selects any

a + 1 out of n KPAs and gets the partial private keys from the selected KPAs. At last, Peer combines all these partial private keys which is gots from KGC and KPAs to get its main private key. A Peer with identity ID is denoted by P_{ID} and Q_{ID}, D_{ID} are its public and private keys respectively.

3.1. Notation

Below table 3.1 gives detail information about notation which is used in the protocol.

Table 3.1. Notation used in system.

ID_A :	Peer A's identity (ID)
K_A :	Peer A's private key
$Proof_A$:	Peer A's proof of the registration
.	Concatenation
$SS(x,k)$	Secret share of secret x in Shamir's (k,n) threshold secret sharing scheme
$MAC(x,K)$	Keyed message authentication code of data x and key K
$\{X\}K_A$	A string X signed by peer A
$Thres_{KPA}$	Minimum number of KPAs system possesses
$PK_A(ID)$	Partial key of peer ID issued by A
$Pzl(x)$	A puzzle generated using Seed x
$Sln(x)$	Solution of Puzzle x

3.2. Mathematical Model

In this Section, we discuss the basic concepts and mathematical background which is used for the implementing this protocol .In this, We also discuss about the BILINEAR PAIRING and ID-BASED CRYPTOGRAPHY.

I. BILINEAR PAIRINGS:

Consider, H_1 is an additive group of prime order p and H_2 is a multiplicative group of the same order. Also, consider k is nothing but generator of H_1.A bilinear pairing is a map m : $H_1 * H_1 \rightarrow H_2$ [3] which have some properties gives as below:

a) Bilinear property:

In this, $m(a*h_1,b*h_2) = m(h_1,h_2)*ab$, where h_1,h_2 belongs to H_1 and a, b € X*q [3]

b) Non-degenerate Property:

Here, m(k; k) is not equal to 1 and therefore it is a generator of H_2. [3]

c) Computable property:

There is an efficient algorithm for computing i.em(h_1,h_2) for all h_1,h_2 € H_1.[3]

II.We write H_1 with an additive notation and H_2 with a multiplicative notation, since for general implementation H_1 will be the group of points on an elliptic curve and H_2 will be a multiplicative subgroup of a finite field.The map m will be derived from either the Weil pairing on an elliptic curve over a finite field. Now,we discuss about some mathematical problems.

a) DISCRETE LOGARITHM PROBLEM (DLP):-

Here, two group elements p and h in H_1 is Given, and find an integer n, such that h = n*k [3].

b)COMPUTATIONAL DIFFIEHELLMAN PROBLEM (CDHP):

Here (k,a_k,b_k) is given then compute abk , for any a,b€ Z_k * .[3]

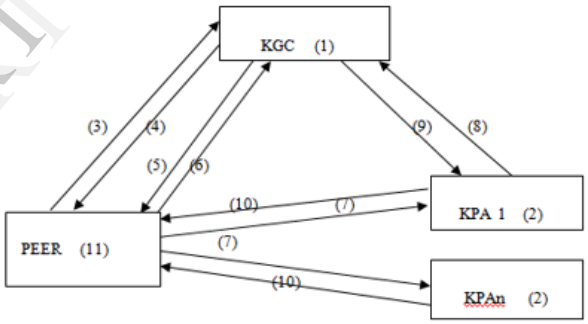
c) DECISIONAL DIFFIEHELLMAN PROBLEM (DDHP):

Here, (k, a_k, b_k, c_k) is given then decide whether c ≡ab mod p,for any a ,b €Z_k *.[3]

d) BILINEAR DIFFIEHELLMAN PROBLEM (BDHP):

Here, (k, a_k, b_k, c_k) is given then calculate m(k; k)*abc € H_2,for any a ,b € Z_k *. [3]

3.3. Data Independence And Data Flow Architecture



1. Publish master public key & system parameter
2. Publish public key of all KPAs
3. Send registration request to KGC
4. Proof of registration
5. Request for partial private key
6. Response of partial private key
7. Blind partial key request to no. of KPAs
8. Check authentication of peer
9. Proof of authentication
10. Send partial private key
11. Collect all partial private key & generate new private key

Figure 1. Data Flow Architecture

3.4. Phases of the proposed protocol

Here, in the proposed key issuing protocol consists of two phases first phase is SETUP and second one is KEY GENERATION AND ISSUING. The first phase is done at start only, by the KGC and KPAs. The second phase is done combinly by all the terms whenever a new peer joins the system. Description of all these phases can be given as below:

(i) SETUP:

In this phase, two sub phasesoccurred (a) SYSTEM SETUP and (b) SYSTEM KEY GERERATION AND DISTRIBUTION.

(a) SYSTEM SETUP: At start, the KGC selects its private key and then it gives the system parameters params which is used for further steps.
(b) SYSTEM KEY GENERATION AND DISTRIBUTION : In this phase all KPA combinly calculate the system key and then distribute that key. Each KPA calculates its parameters and gives this public parameters to the KGC.
(ii) KEY GENERATION AND ISSUING: This phase gives information about how a new Peer joins the system and calculate the private key for that peer securely from the KGC and KPAs. In this phase, there are six sub phasesoccurred which is given as follows:
(a) REGISTERATION: In this sub phase, Peer gives his important information and some parameters to KGC for its registration at KGC. The KGC maintains its own database for the registered peers and gives a proof of registration to the registered peers. This database is publicly available but modified by the KGC.
(b) KGC REQUEST: In this, Peer sends the request to the KGC to obtain the partial private key.
(c) KGC RESPONES: After receiving the peer request, At first, KGC checks whether peer has been registered or not and if peer is registered already then it issues the blinded partial private key to that peer. If peer is not registered then it does not issues the partial private key.
(d) KPA REQUEST: In this sub phase, Peer selects some KPAs and send requests to all selected KPA in parallel to provide key privacy service by sending a request.
(e) KPA RESPONES : Each KPA checks that requested peer is already registered or not to the KGC. If it registered to the KGC then KPA authenticates the peer and issues a partial private key to the authenticated peer. This phase is done by the KPA which is selected by peer.
(f) KEY RETRIEVAL: At last, On accepting all the partial private keys from number of KPA,peer combines the all partial private key and then it calculate its own main private key.

4. Result And Discussion

In this section,we discuss about some features occurred in our protocol and after that we discuss about security analysis.

4.1. Features

We give some features that our protocol enjoys:

- Achieves high trust:
  It is clear that KGC issues a part of the private key and does not know the complete private key of the user. However, KGC may try to impersonate a peer and obtain partial private keys to construct the private key. We have designed our protocol such that malicious KGC can be identified if it tries to impersonate a peer and also we identify malicious KPAs and replace by new KPAs by using BFT protocol. Thus, our protocol achieves high trust.
- Fault tolerance:
  a or less than a KPAs will not be able to generate the user private key in the protocol. Moreover, the protocol is fault tolerant if n = at+1 i.e. key issuing is possible even in the presence of t malicious KPAs.
- Avoids secure channels:
  In general, a secure channel is required to transmit the partialprivate keys to avoid eavesdropping. We overcome the need for secure channel using the blinding factor r_{ID}.
- Robust authentication:
  The private key of each user is issued after the following two authentications. (a) User first authenticates with the KGC in off-line mode (b) User uses the r_{ID} in KGC Request and blind KPA request to authenticate itself which is online.
- Open database:
  The databases maintained by the KGC and KPAs need not be kept secret,but their integrity must be guaranteed.
- Key revocation:
  Key revocation is possible in our protocol if we include the private key expiry time in public key.

4.2. Security Analysis

The security of the proposed key issuing protocol relies on the hardness of solving DLP in elliptic curve groups and is secure against the following attacks.

- Unforgeability:
  It is not possible to forge the KGC request and Blind KPA request tuples, since r_{ID} is required to compute these tuples which is known only to the peer U_{ID}. The security of proposed protocol relies on the hardness of solving DLP.
- Replay attacks:
  Since r_{ID} is required to unblind the partial private keys, an adversary cannot obtain private key of the user even if he replays the request tuples.
- Man-in-the-middle attacks:
  The distributed key generation protocol used in the Setup phase is secure against man-in-the-middle attacks. Further in Key Issuing phase, if an adversary alters the KGC or KPA response tuples i.e. the partial private keys, then it can be detected in the subsequent phases as the user checks the correctness of the received terms.
- Insider attacks:

In the proposed protocol a KPA cannot cheat the other KPAs since they work in parallel and it does not know the other t KPAs that the user has selected. Moreover, a malicious KGC will be detected if it tries to impersonate a user to obtain partial private keys from the KPAs.

- DoS attack:
  Malicious peers in P_2P network can simply drop the messages between KPAs and the requesting peer, which makes the requesting peer difficult to collect sufficient secret shares.we will gives solution for this attack also.
- Collusion attack:
  An adversary can launch a collusion attack by compromising many paths between KPAs and the requesting peer, then compute peers ID and the proof of registration. It is mitigated by this protocol.

5. Conclusion

We have to propose a secure key issuing protocol for peer to peer networks using identity based cryptosystems. A secure key issuing protocol provides a peer registration service using Shamir's (k,n) secret sharing scheme. We develop a secure key issuing protocol, which adopts KGC and KPAs to issue private keys to peer securely. To maintain the security of KPAs, we will develop a scheme to authenticate KPAs, remove malicious ones and find out alternate ones to join in the system using the Byzantine Fault Tolerance Protocol.

A secure key issuing protocol avoids many attacks or this protocol protects the peer to peer networks from various types of attack like man-in-the middle, Replay attack, Insider attack, Dos attack, Collusion attack. Also this protocol avoids Key escrow problem. And also theoretical analysis results may be show that a secure key issuing protocol performs effectively and efficiently, and is able to support large scale networks.

6. References

[1] Cong Tang, Ruichuan Chen, Zhuhua Cai, Anming Xie, Jianbin Hu , Liyong Tang, Zhong Chen "SKIP: A Secure Key Issuing Scheme for Peer-to-Peer Networks"Institute of Software, School of EECS, Peking University, China,2009.

[2]] E. Sit and R. Morris, "Security considerations for peer-to-peer distributed hash tables," in IPTPS, 2002, pp. 261–269.

[3] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo, "Secure key issuing in id based cryptography," in ACSW Frontiers, 2004, pp. 69–74.

[4] D. Boneh, M. Franklin, Identity-based Encryption from the Weil pairing, In J. Kilian, editor, Advances in Cryptology-Crypto'01, Springer-Verlag, LNCS 2139, pp. 213-229, 2001.

[5] R. Gangishetti, M. C. Gorantla, M. L. Das, A. Saxena and V. P. Gulati, An Efficient Secure Key Issuing Protocol in ID-Based Cryptosystems, In Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC'05), Volume-1, IEEE Computer Society, pp. 674-678, 2005.

[6] Hongmei Deng, Annindo Mukherjee, and Dharma P. Agrawal " Threshold and Identity-based Key Management and Authentication for Wireless Ad Hoc Networks" OBR Center for Distributed and Mobile Computing, Dept of ECECS, 2004.

[7] Hosam Rowaihy, William Enck, Patrick McDaniel, and Thomas La Porta "Limiting Sybil Attacks in Structured P2P Networks" Department of Computer Science and Engineering Pennsylvania State University University Park, PA 16802,2006.

[8] F. Hess, Efficient Identity Based Signature Schemes Based on Pairings, Selected Areas in Cryptography-SAC 02, Springer- Verlag, LNCS 2595, pp.310-324, 2003.

[9] Shane Balfe, Amit D. Lakhani and Kenneth G. Paterson, "Trusted Computing: Providing Security for Peer-to-Peer Networks" Information Security Group, Royal Holloway, University of London, United Kingdom.2004.

[10] Dan S.Wallach "A Survey of Peer-to-Peer Security Issues" Rice University, Houston, tx 77005, USA, 2002.