International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 1, Issue 6, October 2014, PP 19-24
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Implementing a Secure Key Issuing Scheme for Communication in P2P Networks

[1]Veeresh, [2]K. Arjun

[1]P.G student, Dept of CSE, BITS, Adoni, Kurnool
[2]Asst Professor, Dept of CSE, BITS, Adoni, Kurnool

Abstract: *Key issuing scheme focuses on the confidentiality maintained in using the secret key for communication in p2p networks. Identity based cryptography (IBC) was introduced into peer-to-peer (P2P) networks recently for identity verification and authentication purposes. However, current IBC-based solutions were not addressing the problem of secure private key issuing. In this paper we propose a novel secure key issuing scheme for P2P networks using IBC. We present an IBC infrastructure setup phase, a peer registration solution using Shamir's (k, n) secret sharing scheme, and a secure key issuing scheme, which adopts key generate centre (KGC) and key privacy authorities (KPAs) to issue private keys to peers securely. This enables the IBC systems to be more acceptable and applicable in real-world P2P networks.*

1. BACKGROUND

P2P networks are extremely vulnerable to large spectrum of attacks, with its self-organized and self- maintenance nature. This is mainly due to the lack of certification service responsible for identity verification and for authentication purposes. We can solve some of the problems by verifying the authenticated nodes identities and by issusing public keys to the nodes for certification using traditional certificate-based public key infrastructure.PKI based on security protocol is difficult to deployed as many nodes that store certificates to each node may become invalid quickly as node churn is highly frequent in P2P network. Practically it is difficult to implement as each node requires more space to store public key certificates. If overlay nodes have a common shared key for secure communication then secured P2P overlay communication is efficient. In dynamic P2P overlay network achieving such an efficiency is difficult as a new key must be generated every time a node membership changes occurs in order to preserve secrecy.

2. INTRODUCTION

Traditional online social networks (OSNs) are centralized networks. Their service is mainly centralized management, which is not able to provide users with sharing information service among multiple OSNs [1]. If a user is interested in multiple OSNs, he will have to register one after another. It wastes a lot of time of the users, because they are not able to transfer friends' data from one online network to another. Also it leads to serious consequences because the user's personal information is dispersed in multiple OSNs, which is inconvenient for them to manage and protect personal information. Thus, it results in privacy information leakage. Therefore, distributed OSNs privacy protection becomes a hot issue. Traditional public key infrastructure (PKI) based on the certificate is well known. It utilizes digital certificates to verify the authenticity of the user's identity, and issues keys to users. The digital certificates need a central authority to manage access control and keys uniformly. The authority is usually presumed to be reliable, which issues, updates, and revokes keys. However, the authority sometimes is malicious. Then it will bring tremendous challenge to certificate management. In 1984 Shamir put forward an idea [2], until 2001 researchers of Stanford University and University of California, Davis concretely realized the IBE privacy protection scheme on its basis [3]. IBE encryption scheme, to a certain degree, improves the traditional public key encryption mechanism: it does not demand digital certificates and provides more facile authentication technique of user ID. But it demands a centralized server and a secure channel, which are difficult to guarantee in real-world networks. In recent years, research on distributed OSNs has emerged. Key management scheme in distributed

OSNs is studied by G. Felix [15]. This research outlines strict requirements and weak constraints for data encryption in distributed OSNs. However, it still requires a detailed security analysis from cryptographic view. Afterwards, a completely distributed approach for group management based on hash tables is designed by H. Olivier [16]. Registering to this system by using the approach is not controlled by any central authority. Any user can create groups, and current applications can share the existing groups' information. While this approach neglects key renewal protocol and adaptation mechanisms to balance load for extremely popular groups. So far, most literatures cannot resolve the following problems, (1) Most of current key issuing schemes are offline, based on traditional PKI schemes or attribute-based encryption (ABE). They all require secure channels. If network users execute the key issuing schemes online, they would sustain replay attacks and insider attacks. In addition, secure channels are difficult to obtain and applied in real-world networks. (2) In current studies, most schemes require a central authority. The central authorities always are served by network service providers. Then it is easy to get the private keys of users for mediators (eg. the social network service providers) in current researches. This can cause middle-man attacks. To address the above problems, this paper presents a novel key issuing scheme based on KPA and PC for IBE-based distributed online social networks. This scheme no longer demands secure channels, and either KPA or PC cannot impersonate the users to get their keys.

2.1 Related Work

IBC uses the user's identity as the public key. The private keys of the users are issued by a key generate centre (KGC) after verifying the user's credentials. IBC was introduced in 1984 by Shamir [2]; however, the first practical encryption scheme (IBE) was not available until 2001 which was developed by Boneh and Franklin [3]. Though IBC overcomes the problems of the traditional PKI, it suffers from some inherent problems, one of which is the secure channel requirement: key issuing requires secure channel to avoid eavesdropping. In 2001, Boneh and Franklin [3] addressed secure key issuing problem using multiple key issuing authorities. After that, many key issuing protocols [4], [5], [6] without secure channels were proposed. So far, several studies have been focused on introducing IBC into P2P security applications. Lu et al. in [7] combined distributed hash tables (DHTs [8]) and identity based encryption (IBE) to defend against man-in-the-middle attacks, however, the scheme assumed that each node has had a pre-assigned unique identifier, and has obtained the corresponding private key through a secure offline channel. This is expensive and difficult to achieve in a large scale P2P overlay network. In [9], Lua proposed a hybrid security protocol using IBE to resist the Sybil attacks, Ryu et al. in [10] proposed ID assignment protocols based on IBC to permit the acquisition of node IDs to be tightly regulated in order to mitigate the Sybil attacks, but these two schemes still suffered from the attack against key issuing phase. Likir [11] presented by Aiello et al.m signs messages with IBS in Kademlia-based P2P networks, however the authors supposed every system user had already obtained a private key and did not consider the key issuing problem.

In real-world P2P networks, it is important to have a key issuing scheme in order to keep in secret whether the private key corresponding to a certain identity has been requested. In this paper, a secure key issuing scheme for P2P networks, which addresses the shortcomings of [7], [9], [10], [11], and makes IBC more applicable in the real world is presented

2.2 Contribution

In this paper, a novel secure key issuing scheme for P2P networks is proposed along with the setup scheme of IBC infrastructure. A peer registration protocol which can register peers adopting Shamir's secret sharing scheme is introduced [12].Finally a secure key issuing protocol which can issue private keys securely without the requirement of secure channels is introduced. The protocol enables IBC more acceptable and applicable in real-world P2P networks.

3. SYSTEM DESIGN

We have four section namely system setup,peer registration, secure keying and system maintenance. In system setup phase we describe how KGC and KPA work in the beginning of the system. In Peer Registration phase and secure keying phase we describe how a peer joins the system .In system maintenance phase the maintenance of KPAs takes place

The requirements of the system are :

1) Secure peer registration:

It must be able to a methodology to mitigate attacks such as man-in-middle attack, collusion attacks during peer registration phase.

2) Robust system maintenance :

The system must provide a online method to add new substitution of KPAs remove, identify malicious KPAs.

3) Secure key issuing :

The key that is being issued must be secure that will secure the keys without secure channel and defend attacks of all types. The software requirements analysis (SRA) step of a software development process yields specifications that are used in software engineering. If the software is "semi automated" or user centered, software design may involve user experience design yielding a story board to help determine those specifications. If the software is completely automated (meaning no user or user interface), a software design may be as simple as a flow chart or text describing a planned sequence of events. There are also semi-standard methods like Unified Modeling Language and Fundamental modeling concepts. In either case some documentation of the plan is usually the product of the design. A software design may be platform-independent or platform-specific, depending on the availability of the technology called for by the design

Design Considerations

There are many aspects to consider in the design of a piece of software. The importance of each should reflect the goals the software is trying to achieve. Some of these aspects are:

 Compatibility –The software is able to operate with other products that are designed for interoperability with another product. Since our software is developed on java it is compatible with other products.

 Packaging - In java many packages are available. Thus we have used various packages which made coding simpler.

 Reliability - The software is able to perform a required function under stated conditions for a specified period of time. Hence the software reliable.

 Reusability -The modular components designed capture the essence of the functionality expected out of them and hence the modules are reusable.

 Robustness - The software is able to tolerate unpredictable or invalid input.

 Usability - The software has user friendly interface which makes its usability easy.

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

4. IMPLEMENTATION

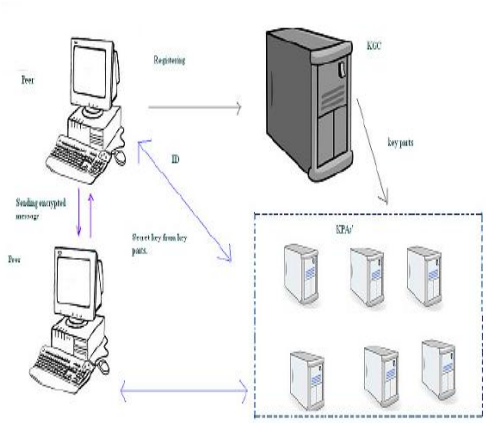

Figure 1: System architecture

The implementation of the key issuing scheme can be as shown by the system architecture in figure 1. The scheme is implemented with six KPAs. The detailed design of our work can be described by following UML design diagrams, which are documented below in Figure 2-5.

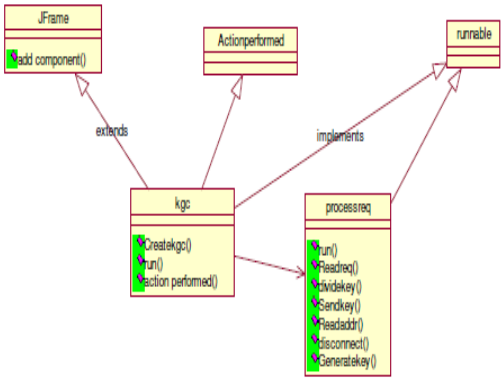

Figure 2: Class diagram for KGC

This is the Key Generation Center (KGC), central node operating in the network.This implements a form of location transparency.The nodes added to the network are unaware of actual location of this central node.This is possible with a level of abstraction provided by the underlying framework. KGC runs as thread on a peer and services the incoming requests by other nodes for registration .It also performs the key generation with the prerequistes of underlying algorithm.It also performs the part of look up work for synthesizing the whole key into parts and back parts into the whole with the mathematical background running over it.

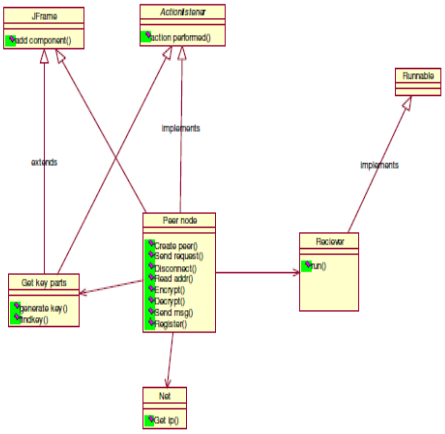

Figure 3: Class diagram for peer node

This is the peer node, a regular node seeking to enter the network and establish the communication with other peer in the network. The peer runs as a thread with different roles. The first form sends a request for registration of node for the communication and awaits the reply token for acquiring the parts of key. The second form is receiver, which involves rendering the message sent it to it by another peer in the network after unwrapping up of the scrambled data.

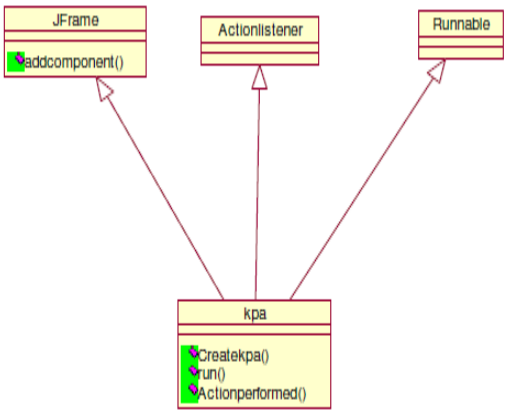

Figure 4: Class diagram for KPA

This is the Key Privacy Authority (KPA).This also runs as a thread. This involves a node in a network, which actually conceals a part of key after it is broken by KGC. The existence of KPAs is solely known to KGC with degree of location transparency and authentication involved. The other peers are unaware of the KPAs. KGC interacts with KPAs after breaking the key. And its upto the peers to render these parts (not all, but subset) with the usage of reference given by KGC. Even if peers come to know the keyparts directly, there is no way of rendering the key without the synthesis process involving the KGC references[2].

5. CONCLUSION

We have developed a secure key issuing scheme for P2P networks using IBC, SKIP. SKIP 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 peers securely. Our future work includes developing a scheme to authenticate KPAs, remove malicious ones and finding out alternate ones to join in the system using the BFT protocol.

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", in Institute of Software, Peking University, China,2010,

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

[3]. Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO, 1984, pp.47–53.

[4]. D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in CRYPTO, 2001, pp. 213–229.

[5]. 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.

[6]. R. Gangishetti, M. C. Gorantla, M. L. Das, A. Saxena, and V. P. Gulati, "An efficient secure key issuing protocol in idbased cryptosystems," in ITCC (1), 2005, pp. 674–678.

[7]. Saxena, "Threshold ski protocol for id-based cryptosystems," in IAS, 2007, pp. 65–70.

[8]. Z.-L. Lu, G.-H.; Zhang, "Wheel of trust: A secure framework for overlay-based services," ICC, pp. 1148–1153, 2007.

[9]. Stoica, R. Morris, D. R. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in SIGCOMM, 2001, pp. 149–160. [9] E. K. Lua, "Securing peer-to-peer overlay networks from Sybil attack," in ISCIT'07, Sydney, Australia, 2007.

[10]. S. Ryu, K. R. B. Butler, P. Traynor, and P. D. McDaniel, "Leveraging identity-based cryptography for node id assignment in structured p2p systems," in AINA Workshops (1), 2007, pp. 519–524.

[11]. L. M. Aiello, M. Milanesio, G. Ruffo, and R. Schifanella, "Tempering kademlia with a robust identity based system," in Peer-to-Peer Computing, 2008, pp. 30–39.

[12]. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, 1979.