ISSN:0975-9646

Review on Credential Systems in Anonymizing Networks

Snehal Pise , Prof. Ratnaraj Kumar

G.S.Moze College of Engineering, Balewadi, Pune-45.
University Of Pune, Pune, India.

Abstract-A credential system is a system in which users can obtain credentials from organizations and reveal possession of these credentials. This system is called anonymous when transactions carried out by the same user cannot be linked. In this paper we are describing few such credential systems. Nymble is a credential system in which servers themselves can blacklist misbehaving users, and thus blocks users but keeps their anonymity intact. Pseudonym systems permit users to communicate with many organizations secretly with the use of pseudonyms. An anonymous credential system is based on the strong RSA assumption and the decisional Diffie-Hellman assumption. It allows a user to unlinkably demonstrate possession of a credential as many times as necessary without involving the issuing organization. Traceable signatures extend group signatures to address various basic traceability issues beyond merely identifying the anonymous signer of a rogue signature. Dynamic accumulators allow capable membership revocation in anonymous setting. Verifier local revocation is the approach of membership revocation in the group signatures. In this revocation method only verifiers are concerned, and signers have no involvement.

Keywords– ***Credential Systems, Pseudonymous system, Nymble, Anonymous credential system, Dynamic accumulator, Traceable Signature, Verifier local revocation.***

1. INTRODUCTION

Data anonymization is the procedure of destroying the electronic trail or tracts, on the data that would show the way to an eavesdropper to its origins. Anonymizing networks for example Tor or I2P provides a strong way to anonymize Internet communications, so that is will be very hard to link communication parties.

There are several forms of credential systems evolved over the time in anonymizing networks. Anonymous communications networks facilitate to resolve the actual and important problem of permitting users to communicate privately over the Internet. The credential system play important role to authenticate, control or block the users as needed.

2. LITERATURE SURVEY OF CREDENTIAL SYSTEMS

There are following existing credential systems in anonymizing network.

2.1. Pseudonymous Credential Systems

Pseudonymity technology is technology that allows individuals to disclose or prove information about themselves to others, but revealing the full identity. A credential system is the system where users of it can obtain credentials from organizations and shows possession of these credentials. The idea of Pseudonymous credential systems was initially put by “Anna Lysyanskaya”, “R.L.Rivest” and “A.Sahai” [2] when anonymous networks were not even developed. In pseudonymous credential systems, users can login the websites using these pseudonyms. Pseudonyms are the false names used to hide users actual identities and maintains anonymity. Pseudonyms are generated by Tor client program itself and they are used to log into websites. Server maintains the blacklist of mischievous users by using pseudonyms provided by the users.

Pseudonym systems allow users to interact with multiple organizations anonymously, using pseudonym. The pseudonym cannot be linked but are formed in such a way that a user can prove a statement about his relationship with another to one organization. Such a statement is called credential. Previous work in this area did not protect this system against dishonest users who collectively use their pseudonym and credentials. Previous schemes were depend heavily on participation on trusted center. In their paper they gave a formal definition of pseudonym system where users are motivated not to share their identity and in which trusted center’s involvement is minimal.

Pseudonym system was introduced by Chaum [8] as a way of allowing a user to work effectively, but anonymously with multiple organizations. He suggests that each organization may know the user by different pseudonym or nym. These pseudonyms or nyms are unlinkable. Nonetheless user can obtain a credential from one organization using one of his nyms, and demonstrate possession of the credentials to another organization, without revealing his first nym to second organization.

Chaum and Evertse [9] develop a model for pseudonym system, and present an RSA based implementation. While pseudonyms are information-theoretically unlinkable, the scheme relies on a trusted center who must sigh all credentials.

Damgard [11] suggests a scheme based on multiparty computations and bit commitments that provably protects organizations from credentials forgery by malicious users and the central authority and protects secrecy of users identities information. Central authority’s role is limited to ensure that each pseudonym belongs to some valid user.

Chen [10] presents a discrete logarithm based scheme where a trusted center has to validate the entire pseudonym, but does not participate in credential transfer. Chen’s scheme relies heavily on the honest behaviour of the trusted center as malicious trusted center can also transfer credentials between users.

These schemes have a common weakness there is little to motivate or prevent a user from sharing his pseudonyms or credentials with other users. Proposed scheme on the presumption that each user has a master public key whose corresponding secret key the user is highly motivated to keep secret. This master key might be registered as his legal digital signature key so that disclosure of his master secret key would allow others to forge signatures on important legal or financial documents in his name. Our proposed scheme then has the property that a user can not share his credential with a friend without sharing his master secret key with the friend that is without identity sharing.

A certification authority is needed only to enable a user to prove to an organization that his pseudonym actually corresponds to a master public key of a real user with some stake in the secrecy of the corresponding master secret key such that the user can only share a credential issued to that pseudonym by sharing his master secret key [12]. As long as the CA does not refuse service a cheating CA can do no harm other than introduce invalid users into the system ie users who have nothing to lose in the outside world. In their model, each user has to first register with the CA, showing his true identity and his master public key and showing possession of the corresponding master secret key.

Sometimes it is not required that a user should be motivated not to share his identity. In those cases the CA is not needed altogether. After registration the user may open accounts with many different organizations using different unlinkable pseudonyms [13]. However all pseudonyms are related to each other-there exists an identity extractor that can compute a user's public and secret master keys given a rewindable user who can authenticate himself as the holder of the pseudonym.

Advantages:

- Pseudonym Credential System is practical and easy to implement.
- It is overall less computational.

Drawbacks:

- It gives pseudonymity to all users.
- Weakens the anonymity
- These schemes have a common weakness there is little to motivate or prevent a user from sharing his pseudonyms or credentials with other users.

2.2. Anonymous credential systems

Anonymous credential system consists of users nothing but clients and respective organizations. These organizations know the users only by their pseudonyms. The basic system contains protocols. These protocols are used by user to join the system, and then to register with an organization and after that, obtain multiple show credentials, and show such credentials.

"J.Camenisch" and "Anna Lysyanskaya" put their innovation in Anonymous credential system [3]. In this specially the concept of "Group signatures" is used to make the system more capable and anonymous. Anonymous credential system consists of 3 parties; those are users, authority, and verifiers. These systems make use of group signatures which allow servers to revoke i.e. cancel a misbehaving user's anonymity by complaining it to a group manager [4]. Unfortunately servers must have to query the group manager for each and every authentication and hence this system considerably lacks scalability.

This is a practical anonymous credential system that is based on the strong RSA assumption and the decisional Diffie-Hellman assumption modulo a safe prime product and is considerably superior to existing ones.

Advantages:

- Digital signatures ensure the security of system to some extent.
- It allows a user to unlinkably demonstrate possession of a credential as many times as necessary, without involving the issuing organization.
- It offers optional anonymity revocation for particular transactions that is can prevent misuse of anonymity
- It provides separability; all organizations can choose their cryptographic keys independently of each other.

Drawbacks:

- This system lacks scalability.
- In this system, the backward unlinkability is not possible.
- There is a constraint that servers can easily find users' IP addresses with the use of traceable Signature.

2.3. Traceable signatures

Traceable signatures allow the group manager to release a trapdoor that allows all signatures generated by a particular user to be traced [5]. This approach does not provide the backward unlinkability that they desire, where a user's accesses before the complaint remain anonymous. Backward unlinkability permits subjective blacklisting, where servers can blacklist users for whatever reason since the privacy of the blacklisted user is not at risk. In contrast, those approaches which are without backward unlinkability requires paying watchful attention to when, why a user must have all their connections linked. Users must concern about whether their behaviours will be judged fairly or not. Subjective blacklisting is suitable to the servers like Wikipedia where misbehaviours like questionable edits to a Webpage are difficult to define in mathematical terms. In some systems it is possible to define misbehavior accurately. For example, as given in [5], in anonymous e-cash systems double spending of an "e-coin" is considered as misbehavior, after which the responsible user is deanonymized. But in reality such systems work for only contracted i.e. few definitions of misbehavior. So mapping of such complex ideas of misbehaver to double spending is difficult task.

Traceable signatures (TS), suggested by Kiayias, Tsiounis and Yung, extend group signatures to address various basic traceability issues beyond merely identifying the anonymous signer of a rogue signature. Specifically they facilitate the efficient tracing of all signatures produced by a misbehaving party without revealing identity of other parties. They also permit users to claim a possession of a previously signed anonymous signature. Currently known traceable signatures systems are depend on the random oracle model.

Advantages:

- Traceable signatures support an extended set of fairness mechanisms when compared with the traditional group signature mechanism.

- Extended functionality of traceable signature is needed for proper operation and adequate level of privacy in various settings and applications.

2.4. Dynamic accumulators

Benaloh, de Mare, Baric´ and Ptzmann studied the scheme called an accumulator. Accumulator is an algorithm that hash large set of input values into a short value such a way that there is a witness of incorporation of given value into the accumulator. Therefore it is impractical to find a witness for a value that was not even accumulated.

Further study of Jan Camenisch, Anna Lysyanskaya stated a dynamic accumulator is an accumulator that permits dynamically add and or delete inputs in a way that the cost of add or delete is independent of the number of accumulated values. They accomplish this with the use of the strong RSA assumption. For this construction, they also show an efficient zero-knowledge protocol for proving that a committed value is in the accumulator.

Dynamic accumulators allow competent and cap able membership revocation in the anonymous setting. Their construction is especially suitable for membership revocation in group signature and identity escrow schemes, such as the one due to Ateniese et al. It is also suitable in efficient revocation of credentials in anonymous credential systems for example in the case of Camenisch and Lysyanskaya. Application of their method to these schemes enables membership revocation and does not even significantly increase the complications in operations. There is increase in the cost of a membership or credential verification but it is nominal which less than 2. All previously known methods incur an increase in these costs that is linear in the number of members [6].

2.5. Verifier-local revocation (VLR)

In order to overcome the problem of lack of backward unlinkability VLR is proposed in 2004 by “Dan Boneh” and “Hovav Shacham”. Verifier local revocation is an approach of membership revocation in the group signatures [7]. In this approach, only verifiers are involved in the revocation mechanism, while signers have no involvement. Because of no load to signers this approach is good for mobile environments. Such a system satisfies backward unlinkability to some extent.

The backward unlinkability means that even after a member is revoked, signatures produced by the member before the revocation remains anonymous. Verifier local revocation needs the server nothing but verifier to do only local updates while doing revocation. As a result lot of load will be on servers [7].

Advantages:

- Local updating is in reach.
- Backward unlinkability is possible to some extent.

Drawbacks:

- There is a need of an efficient VLR group signature scheme where signature verification time is sub-linear in the number of revoked users, without compromising user privacy.
- There is heavy computational work at server side.
- It is time consuming and is less secure.

2.6. Nymble System

Anonymizing network are the networks where users of it can access internet services but this anonymizing network hides Client's IP address from servers. Through this, anonymizing network keeps identity of users hidden from server giving full privacy to them.

But few clients misuse this privacy and misbehave defacing popular websites. Nymble system is the system which blacklists such users and blocks its access but can still keeps their anonymity.

Patrick P. Tsang, Apu Kapadia and Sean W. Smith makes following contribution [1]

- Blacklisting anonymous users. In this servers can now blacklist users of an anonymizing network and also maintains their privacy.
- Practical performance. Protocol uses inexpensive symmetric cryptographic operations to significantly outperform the alternatives.
- Open-source implementation. With the goal of contributing a workable system, they have built an open-source implementation of Nymble, which is publicly available. They also provide performance statistics to show that their system is practical.

Advantages:

- Servers can blacklist misbehaving users.
- Privacy of blacklisted users is maintained by still keeping their anonymity.
- System is practical, efficient, and sensitive to the needs of both users and services.

Drawbacks:

- If a user can obtain multiple addresses, she can circumvent both nymble-based and regular IP-address blocking.
- IP address is used for blocking of misbehaving users in anonymizing network.
- It cannot closely intimate Sybil attack as user can change identity.
- If pseudonym manager and nymble manager collude, user identity may reveal.
- Cannot avoid side channel attack
- System is totally centralized to nymble manager, so if nymble manager failed whole system in trouble.
- Lacks scalability
- Servers can find users’ IP addresses by using traceable Signature.

3. CONCLUSIONS

In conclusion, maintaining anonymity of users in anonymizing network remains essential. Nymble system is practical, efficient system, can be used to add a layer of accountability to any publicly known anonymizing network where servers can blacklist misbehaving users while maintaining their privacy. Anonymous credential system is considerably superior to existing ones and is to prevent misuse of anonymity. Traceable signature enables the efficient tracing of all signatures produced by a misbehaving party without opening the identity of other parties. Dynamic accumulator’s construction is especially suitable for membership revocation in group signature and identity escrow schemes.

REFERENCES

[1] Patrick P. Tsang, Apu Kapadia, Member, IEEE, Cory Cornelius, and Sean W. Smith, "Nymble:Blocking Misbehaving Users in Anonymizing Networks" IEEE Transactions on dependable and secure computing, vol. 8, No. 2, March-April 2011.

[2] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf. "Pseudonym Systems. In Selected Areas in Cryptography", LNCS 1758, pages 184– 199. Springer, 1999.

[3] J. Camenisch and A. Lysyanskaya, "An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation," Proc. Int'l Conf. Application and Theory of Cryptographic Techniques (EUROCRYPT), Springer, pp. 93-118, 2001.

[4] J. Camenisch and A. Lysyanskaya, "Signature Schemes and Anonymous Credentials from Bilinear Maps," Proc. Ann. Int'l Cryptology Conf. (CRYPTO), Springer, pp. 56-72, 2004.

[5] A. Kiayias, Y. Tsiounis, and M. Yung, "Traceable Signatures," Proc. Int'l Conf. Theory and Application of Cryptographic Techniques (EUROCRYPT), Springer, pp. 571-589, 2004.

[6] J. Camenisch and A. Lysyanskaya. "Application and Dynamic Accumulators to Efficient Revocation of Anonymous Credentials". In CRYPTO, LNCS 2442, pages 61–76. Springer, 2002.

[7] D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," Proc. ACM Conf. Computer and Comm. Security, pp. 168-177, 2004.

[8] David Chaum. "Security without identification: transaction systems to make Big Brother obsolete". Communications of the ACM,28(10),1985.

[9] David Chaum and Jan-Hendrik Evertse. "A secure and privacy protecting protocol for transmitting personal information between organizations". In Advances in Cryptology CRYPTO '86 pages 118-167,Springer-Verlag 1986

[10] Lidong Chen. "Access with pseudonyms". In Ed Dawson and Jovan Golic editors Cryptography: Policy and Algorithms pages 223-243. Springer-Verlag 1995 Lecture Notes in Computer Science No. 1029

[11] Ivan Bjerre Damgard. "Payment systems and credential mechanisms with provable security against abuse by individuals extended abstract". In Advances in Cryptology CRYPTO '88, pages 328-335. Springer-Verlag,

[12] Chunling Cheng, Bingzhen Gao, Dengyin Zhang, "A Double Pseudonyms Authentication for Distributed P2P Systems" Computer Modeling and Simulation, 2010. ICCMS '10.

[13] Ji Won Yoon, Hyoungshick Kim. "A Perfect Collision-Free Pseudonym System", Page(s): 686 - 688, IEEE 2011.