Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 9, September 2016, pg.133 – 139

PREVENTION OF COLLUDING ATTACK USING GROUP SIGNATURE STRATEGY

Falgun Shah[1], Hitul Patel[2]
[1]M.E in C.E, Swaminarayan College of Engineering &Technology (S.C.E.T., Kalol), India
[2]Asst. Prof. in Swaminarayan College of Engineering & Technology (S.C.E.T., Kalol), India
falgunshah1990@gmail.com; hitulce@gmail.com

ABSTRACT--- An extension to Digital signature is a Group Signature scheme which allows the members of the group to sign messages containing information on behalf of the group, having the feature of hiding the identity of the signer. A single group public key is used to verify the Signatures. In case of any dispute, only a designated group manager, holding their special property, is able to open signatures, and thus reveal the signer's identity. Its applications are used widespread, especially in e-commerce such as e-cash, e-voting and e-auction. This paper incorporate the detailed study of group signature definition, concept and the main contributions in this field such as applications of group signature that tells where we can use this technique. It starts with overview, concept, properties, keys used, application, challenges, and attack of group signature and a comparative analysis of some group signature techniques.

I. INTRODUCTION

A digital signature is a mathematical scheme for providing the authenticity of a digital information or document. A valid digital signature provides a proper reason to the recipient to believe that the information was provided by a known sender, so the sender cannot deny having seen the message, moreover it also checks that the message was not altered in transit.

Digital signatures are computed based on the documents (message/ information) that need to be signed and it is done on some private information held only by the sender. In practice, instead of using the whole message, a hash function is applied to the message to obtain the message digest. A hash function, in this context, takes an arbitrary-sized message as input and produces a fixed-size message digest as output. Among the commonly used hash functions in practice are MD-5 (message digest 5) and SHA (secure hash algorithm).

Digital signatures are basically applied for software distribution, financial transactions, and in cases of disputes where detect forgery or tampering of digital information are very important.

II. INTRODUCTION TO DIGITAL SIGNATURE TECHNOLOGY

Authentication of messages or we say information, protects the party involved in the communication or the process of information exchange from some exterior interference or say the third party. However, it does not protect the two parties against each other. Several forms of dispute between the two are possible. In situations where there is not complete trust between sender and receiver, something more than authentication is needed. The most attractive solution to this problem is the digital signature. It combines a hash with a digital signature algorithm. The digital signature is analogous to the handwritten signature.

A digital signature is said to be valid if it satisfy the following properties.

- It must verify the author and the date and time of the signature.
- It must to authenticate the contents at the time of the signature.
- It must be verifiable by third parties, to resolve disputes

Thus a digital signature must be a bit pattern that depends on the message being signed. It must also have some information that should be unique to the sender to prevent both forgery and denial. It must be easy to produce, recognize and verify a digital signature. It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message. Lastly it must be practical to retain a copy of the digital signature in storage.

A digital signature is a piece of data which is attached to a message and which can be used to find out if the message was tampered with during the conversation. The digital signature for a message is generated in two steps:

1. A *message digest* is generated. A message digest is a 'summary' of the message we are going to transmit, and has two important properties: (a) it is always smaller than the message itself and (b) Even the slightest change in the message produces a different digest. The message digest is generated using a set of hashing algorithms.

2. The message digest is encrypted using the sender's *private* key. The resulting encrypted message digest is the *digital signature*.

The digital signature is attached to the message, and sent to the receiver. The receiver then does the following:

1. Using the sender's public key decrypts the digital signature to obtain the message digest generated by the sender.

2. Uses the same message digest algorithm used by the sender to generate a message digest of the received message.

3. Compares both message digests (the one sent by the sender as a digital signature, and the one generated by the receiver).

If they are not *exactly the same*, the message has been tampered with by a third party. We can be sure that the digital signature was sent by the sender (and not by a malicious user) because *only* the sender's public key can decrypt the digital signature (which was encrypted by the sender's private key; remember that what one key encrypts, the other one decrypts, and vice versa). If decrypting using the public key renders a faulty message digest, this means that either the message or the message digest are not exactly what the sender sent.

The following are the techniques based on Digital signature.

Group Signature: The concept of group signatures allows a group member to sign messages anonymously on behalf of the group. However, in the case of a dispute, the identity of a signature's originator can be revealed by a designated entity.

Ring Signature: A similar system that excludes the requirement of a group manager and provides true anonymity for signers.

Threshold Signature: A threshold signature involves a fixed-size quorum (threshold) of signers. Each signer must be a genuine group member with a share of a group secret signing key. A (t,n) threshold signature scheme supports n potential signers, any t of which can on behalf of the group. Threshold signatures reveal nothing about the t signers; no one can trace the identity of the signers (not even a trusted center who have set up the system).

Multi signature: A multi signature represents a certain number of signers signing a given message. Number of signers is not fixed and signers' identities are evident from a given multi-signature. A multisignature is much shorter (sometimes constant) than the simple collection of individual signatures.

Proxy Signature: A proxy signature allows a delegator to give partial signing rights to other parties called proxy signers. Proxy signatures do not offer Anonymity.

Blind Signature: A signer can sign messages for users. The signer does not know the message he is signing. The signer should not be able to recognize the message nor the signature he has produced. The user is anonymous w.r.t all other users. Blind Signature implemented based on Schnorr Signature. It is lot faster than group signature.

III. DETAIL INTRODUCTION TO GROUP SIGNATURE

A technique of signing the documents or any relevant information anonymously on behalf of group is known as Group Signature scheme, where group consist of manager and various designated members. The designated verifier verifies the integrity of sign, and where the verifier is aware of the correctness of the sign not the identity of member who signed the documents.

There are three participants in this scheme which are as follows:

Group Manager: The manager of group for managing the memberships and generating the membership keys of group members (Signers). Group Manager enabling signers to sign on behalf of the group, and revealing the identity of the signature's originator when dispute.

Group Member: The group member, he/she have his/her membership key, and he/she can using the membership key to sign message on behalf of the group.

Verifier: Receiver of group signature or anyone can check the validity of the group signature by the public key of group.

A group signature scheme consists of the following four procedures:

Setup: a probabilistic interactive protocol between a designated group manager and the members of the group. Its result consists of the group's public key Y, the individual secret keys x of the group members, and a secret administration key for the group manager.

Sign: a probabilistic algorithm which, on input a message m and a group member's secret key x, returns a signature s on m.

Verify: an algorithm which, on input a message m, a signature s, and the group's public key Y, returns whether the signature is correct.

Open: on input a signature s and the group manager's secret administration key this algorithm returns the identity of the group member who issued the signature s together with a proof of this fact.

It is assumed that all communications between the group members and the group manager are secure.

For a group Signature to be valid needs to satisfy the following properties:

- Only group members are able to correctly sign messages **(unforgeability)**.
- It is neither possible to find out which group member signed a message **(anonymity)** nor to decide whether two signatures have been issued by the same group member **(unlinkability)**.
- Group members can neither circumvent the opening of a signature nor sign on behalf of other group members; even the group manager cannot do so **(security against framing attacks)**.

A consequence of the last property is that the group manager must not know the secret keys of the group members.

There are three types of key are used in this scheme as:

- **Master Public Key:** anyone who knows this key can verify that some group member has signed the message..
- **Master Secret Key:** given to all group members for signing of messages.
- **Administrative Key:** only known to manager to identify that which group member has signed the message.

IV. PROPOSED METHOD

Colluding Attack:

The act of cooperation between two person or set of person for the sake of achieving mainly the illegal benefits is known as Collusion. It is a very common and risky problem to be faced in every field which cannot be controlled easily as the unpredictable nature of attack can observed in figure below.

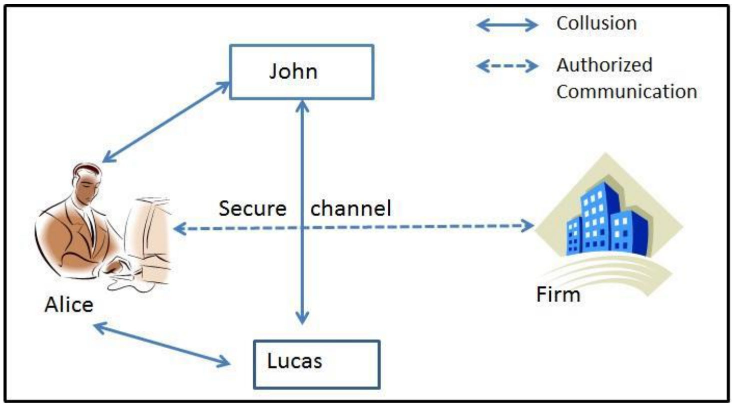

Fig.1 Scenario of collusion attack

The Colluding attack has another flavor with small variation ie stated as coalition. The coalition can be thought of subpart of collusion where a set of member collide to achieve the respective objective. Basically with respect to the group coalition is another security threat. The Colluding attack has another flavor with small variation ie stated as coalition. The coalition can be thought of subpart of collusion where a set of member collide to achieve the respective objective. In general, the group manager is responsible in distributing many security parameters between members, which is a very critical role where collusion is possible, secondly the group member who are responsible in signing the documents can also collude which makes the member very critical issue and finally the verifier who is responsible for verifying the signature in the document can also collude which can create a threat to the integrity of the document. Above all discussed roles were involved in the system; huge threat to the real time system is that a non-group member or a set of non-group members can also collude with the group member. Means to avoid or to resist the colluding attack one have to consider all possible roles in the system. The trust and security parameters used in the system is the actual whole strength of secure system, so considering the consequences of colluding attack, if collusion is possible then the signature can be easily forged crashing whole system of signing the document thus a threat to the security of digital information or message.

Proposed Method:

Here group signature scheme provides full anonymity of signer, full traceability of the signature, resistant to colluding attack and forgery attack. A trusted third party (TTP) is an entity involved in the proposed scheme who manages all critical communications among the group members and group manager.

The scheme consisting of following five stages.

1) Setup stage

Manager selects a prime p as public key which is large enough that the discrete log problem is intractable in $Z\ p*$. He selects another public key q such that $(q - 1) = 0 \bmod p$ and also chooses a random private key Y . Manager also computes group key as $gk = (y - 1)\delta$, where the δ is a randomly chosen parameter.

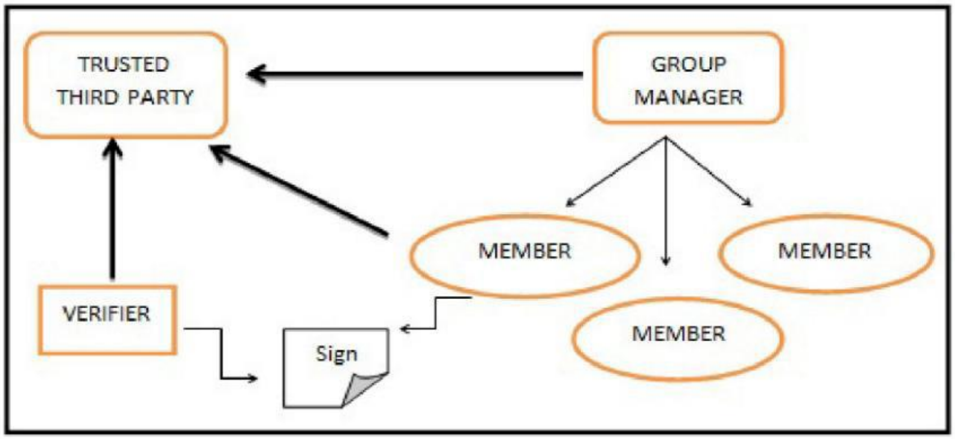

Fig.2 Layout of the proposed scheme

2) Joining Stage

Member who wants to joining the group gets registered through the certificate authority and authority ensures the registration of member to the manager. Manager computes the secret d for the member such that d = yα mod p where α is randomly chosen by the group manager.

Then the manager splits the secret key d into two parts as d1 and d2 . The key division can be done through any method which is appropriate to the manager.

Here the manager has a flexibility to decide the splitting method but one important concern regarding the splitting is that the division should be lossless.

The secret keys d and d1 are sent to each member in encrypted form using the member0 s public key. The key d2 is send to the trusted third party (TTP) which manages keys of each member. Each member chooses a primitive element e0 in zp , and computes

$$e_1 = e_0^{\frac{p-1}{q}} \ mod\, p$$

The Member chooses a secret key x and computes

$$e_2 = e_1^{xd} \, mod\, p$$

The Member chooses Members are organized according to a structure as shown in. Here we have two structures namely QA, QB which are divided into many slots with respect to the member who will sign the document. Each member is assigned with the binary counter (0/1), where 0 represents that the member is not signing any document and 1 represents that the member is reserved with the signing of document.

We have members organized initially in QA and when a member completes the signing of the document then the member is send to the QB similarly a member completing signing of document or message in QB is send back to the QA. The trusted third party has database maintained for the member according to the slot and structure defined.

3) Signature generation stage

In this stage, a member Xi chooses a random number β from 1 to q and com- putes the signature as:

$$s_1 = h(M|e_1^{\beta} \, mod\, P)$$

$$s_2 = \beta + x \times (id + d_2) \times s_1 \, mod\, q$$

Where M is the required message to be signed, h represents the hash for the signature and id represents the slot id that maps the key from trusted third party with the respective member. The parameter e1, e2 are encrypted using verifiers public key and finally the message, signature with hash M, s1, s2 along with the hash of key h(d2) encrypted via manager's public key are finally encrypted using group key and send to the verifier. The value of β will vary with respect to each message

4) Verification Stage

The verifier gets the encrypted data which he decrypts using the group key and verifier's private key accordingly. And now computes

The following to check the validity of signature.

$$s0 = h(M | e1^{s2} \times e2^{-s1} \bmod p)$$

If the value of S0 satisfies the following, s1 = S0 mod p ,then signature is accepted otherwise rejected.

5) Opening Stage

The encrypted signature can be decrypted by manager with the group key and can check the hash value that is encrypted with the manager's key. As manager has the key hashed with respect to each member so can say who has generated the signature.

V. CONCLUSION

The proposed scheme satisfies standard security features like anonymity, unforgeability and unlinkability. The proposed scheme is member independent such that any member leaving or joining would not affect the signature generation scheme. The size of signature is still needed to be considered. Though the cost of signature verification is more as compared to other standard signature scheme but on the security aspect this would be efficient scheme where this scheme is very much safe against many active attacks can be very much useful in an organization, where the group manager can be equivalent to the chief executive officer, the signers can be employees of the organization and the verifier may be a specific customer. This scheme can also be applicable in e-voting system, e-cash system and e-commerce applications.

References

[1] J. J. . Chen and Y. Liu. A traceable group signature scheme. Mathematical and Computer Modelling, 31(2-3):147–160, 2000.

[2] T. Isshiki, K. Mori, K. Sako, I. Teranishi, and S. Yonezawa. Using group signatures for identity management and its implementation. In Proceedings of the Second ACM Workshop on Digital Identity Management, DIM 2006. Co-located with the 13th ACM Conference on Computer and Communications Security, CCS'06, pages 73–78, 2006.

[3] Y. Geng, G. Shao, M. Zheng, and G. Cui. An improved efficient group signature scheme for large groups. HuazhongKejiDaxueXuebao (ZiranKexue Ban)/Journal of Huazhong Uni- versity of Science and Technology (Natural Science Edition), 37(7):66–69, 2009.

[4] L. Chen and T. P. Pedersen. New group signature schemes. In A. De Santis, editor, Advances in Cryptology- EUROCRYPT'94, pages 171–181. Springer, Berlin,, 1994.

[5] Mihir Bellare and Sara K. Miner. A forward-secure digital signature scheme. pages 431–448. Springer-Verlag, 1999.

[6] W.B. Lee and C.C. Chang. Efficient group signature scheme based on the discrete logarithm. volume 145, pages 15–18. IEE, 1998.

[7] Dan Boneh and Hovav Shacham. Group signatures with verifier-local revocation. In ACM Conference on Computer and Communications Security, pages 168–177, 2004.

[8] Fengyin Li, Jiguo Yu, and Hongwei Ju. A new threshold group signature scheme based on discrete logarithm problem. In Proceedings of the Eighth ACIS International Confer- ence on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing - Volume 03, SNPD '07, pages 1176–1182, Washington, DC, USA, 2007. IEEE Computer Society.

[9] Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: formal definitions, simplified requirements, and a construction based on general assump- tions. In Proceedings of the 22nd international conference on Theory and applications of cryptographic techniques, EUROCRYPT'03, pages 614–629. Springer-Verlag, 2003.
[10] Steven D. Galbraith and Mark Holmes. A non-uniform birthday problem with applications to discrete logarithms. Discrete Applied Mathematics, 160(10-11):1547–1560, 2012.
[11] Jeffrey Hoffstein, Jill Pipher, and J.H. Silverman. An Introduction to Mathematical Cryp- tography. Springer Publishing Company, Incorporated, 1 edition, 2008.
[12] Henk C. A. van Tilborg and Sushil Jajodia, editors. Encyclopedia of Cryptography and Security, 2nd Ed. Springer, 2011.
[13] Behrouz A. Forouzan. Cryptography & Network Security. McGraw-Hill, Inc., 1 edition,2008.
[14] G. Tsudik and G. Ateniese, "Quasi-efficient revocation of group signatures", in To Appear in Financial Cryptography, 2002.
[15] M. Harkavy, H. Kikuch and J.D. Tygar, "Electronic auction with private commerce", in Proceedings of the 3rd USENLX Workshop on Electronic Commerce, August 1998.
[16] L. Harn and Y.Xu, "Design of generalized ElGamal type digital signature schemes based on discrete logarithm", Electronics Letters, 1994.
[17] W.H. He, "Digital signature scheme based on factoring and discrete logarithms", Electronics Letters, 2001.
[18] Fangguo Zhang and Kwangjo Kim, "Security of A New Group Signature Scheme", IEEE TENCON'02