A New Security Level Oriented Multisignature Scheme

Abulameer Khalaf Hussain, Muthnna Abdulwahid Khudhair

***Abstract*: This paper presents a new multisignature scheme. The idea behind this scheme is that all authenticated users in the system are classified according to their security levels . Each level has its own trusted group manager. To generate the signature, the proposed system selects one of these levels .Each level consists of a group of users . Each user has its own private and public keys. In addition, this scheme implements the cascade encryption for the generated signature, and thus it is necessary to perform the cascade encryption to use a global private key for each level. The system also assigns trustworthiness score for each user to select the proper one to sign on the behalf of his/her group in that level. Finally, the generated multisignure is proved to be more secure and thus it can be used in sensitive applications.**

***Index Terms*: Digital Signature, multisignature system, Security Levels, Multi-level proxy signature.**

I. INTRODUCTION

A multisignature scheme is defined as a digital signature scheme that gives the permission to multiple signers to generate a single signature in a collaborative and simultaneous manner [1,2]. In some applications, there are different roles/ positions associated for co-signers in a signing group and therefore have different management authorization capabilities. Thus, multisignatures generated by the same group of co-signers with different signing orders often imply different meanings. Some workflow management systems have addressed this concern in literature [3,4], in which a multisignature has to be checked against the organizational structure of the signing group.

Different previous studies of structured multisignature schemes such as Mitomi and Miyaji had proposed two schemes that respectively based on discrete logarithm problem and integer factorization [5]. Also in [6], Kotzanikolaou et al. specified an attack against the Mitomi-Miyaji's discrete logarithm based scheme and they proposed a modification for it. However, their modification is not secure as addressed in [7]. Recently, Boneh, Shacham and Lynn proposed a new signature scheme based on the Gap Diffie-Hellman (GDH) problem [8].

Multisignature scheme gives the ability for different signers signing the same document. A verifier person or any entity is convinced that each signer participated in signing by transmitting a multi-signature instead of individual signatures. So multi-signature schemes can greatly save on communication costs. Multisignatures were first introduced by Itakura and Nakamura [9] and have been the topic of muchresearch [10-12]. Micali, Ohta and Reyzin [5] also gave the first strong concept of security of multisignatures. A vaiant of Micali-Ohta-Reyzin model was given by Boldyreva [12] . Multisignatures is related to the aggregate signature. Boneh,Gentry,Lynn and Shacham [13] defined an aggregate signature scheme. Unlike multi-signature, aggregate signature aggregate signature scheme provides a method to aggregate signature by signature on different messages. Alexandra Boldyreva et al. [14] propose a new primitive that they call ordered multi-signatures (OMS) and a formal security model for ordered multi-signatures.

II. RELATED WORKS

Lihua,Wang et al. proposed an ID-based series-parallel multisignature scheme based on pairings . In this scheme, signers in the same subgroup sign the same message, but those in different subgroups sign different messages. This scheme is proven secure against forgery signature attack from parallel insiders under the BDH assumption [15].

A research had been proposed in [16] to propose a new multi-level proxy signature scheme based on q-SDH assumption combining with Wei and Yuen's short signature. The properties of this scheme are non-repudiation, unforgeability, undeniability . Therefore, the proxy signature right can come true step by step under agreement.

In [17] the authors presented a new multisignature scheme which can be used in client-server model of group communication systems to deal with certain problems that arise while implementing safe delivery rule in such systems. The proposed multisignature scheme enables the group communication server to combine all acknowledgements of a certain message from all group members into a single group-acknowledgement message which has a constant size and send it to the sender of the message.

A research was proposed to resist clerk and rogue-key attacks. In the proposed scheme, multiple signers can generate a multisignature for the message with the signers' secret keys, and the specified group of verifiers can cooperate to verify the validity of the multisignature with the signers' public keys and the verifiers' secret key [18].

In [19] , the authors proposed a new efficient identity-based key-insulted multisignature scheme . The aim of this paper is for facilitating group-oriented applications and mitigating the impact of key exposure. Each user ,in this scheme, has the ability to periodically update his private key but the public key remains unchanged. This scheme has the properties of unbounded time periods and random-access key-updates. The scheme is compared with previous works and it is formally proven its security of unforgeability against existential forgery under adaptive chosen-message attacks (EF-CMA) in the random oracle model.

A paper proposed in [20] two structured multisignature algorithms, one based on the RSA scheme and the other on an ElGamal-type scheme. Incorporation of both order-

Revised Version Manuscript Received on December 05, 2016.

Dr. Abdulameer K. Husain, PhD in Computer Science, Computer Security, Presently Working as Assistant. Prof., in Computer Department in Dijlah College University–Iraq-Bagdad.

Muthnna Abdulwahid Khudhair, MSc. In Computer Science Presently Working as Assistant. Prof., in Computer Depament in Dijlah College University–Iraq-Bagdad.

free and order-sensitive multisignature algorithms together is shown to construct a generalized multisignature algorithm.

Another research proposed a multi-signature scheme, in which each signer can express her intention associating with the message to be signed. Signers' intentions mean a kind of information which can be newly attached signature in signers' generating to it. First, the authors considered a multi-signature scheme that realizes the concept of signers' intentions by utilizing existing schemes, and then name it as a primitive method. After that, they introduced the proposed multi-signature scheme which is more efficient than the primitive method in terms of the computational cost for verification and in view of the signature size [21].

In [22] the authors gave the model of ID-based designated verifier proxy multi-signature and presented a new ID-based designated verifier proxy multisignature scheme. The security of this scheme is based on the computational Diffie-Hellman (CDH) problem and it is highly efficient.

III. PROPOSED SYSTEM

The scheme in this paper generates a multisignature of an authenticated group of users. The users are first classified according to their security level in the system. For this purpose, the scheme classifies security levels depending on two types of parameters. The first parameter is the data types, these types are arranged as: classified, secret, and top secret. The second parameter is the degree of trustworthiness of each user within each level (TW).

If we suppose that the level set is DL={C,S,T} , where C denotes classified level , S denotes secret level ,and T denotes top secret level. Suppose also the set of authenticated users of C level is UC={uc1,uc2,….,ucn1} , the set of authenticated users of S level is SU={su1,su2,…,sun2} , and the set of authenticated users of T level is TW={tw1,tw2,….,twn3}.

The multisignature of this group is generated using the RSA scheme. Accordingly, each authenticated user must have a set of private keys, d. These private keys are calculated by choosing two prime numbers ,p and q, for each level and it needs a set of corresponding public keys , e.

Table 1 illustrates these sets of both security levels and authenticated users in each level.

Table1: Security Level Classifications.

Level Number	Level Type	Authenticated Users	public keys(e)	private keys(d)	Trustworthiness Scores
1	Classified(C)	UL11	eL11	dL11	twL11
		UL12	eL12	dL12	twL12
		UL1n	eL1n	dL1n	twL1n
2	Secret (S)	UL21	eL21	dL21	twL21
		UL22	eL22	dL22	twL22
		UL2m	eL2m	dL2m	twL2m
3	Top Secret (T)	UL31	eL31	dL31	twL31
		UL32	eL32	dL32	twL32
		UL3k	eL3k	dL3k	twL33

For each level, there is a global private key (dg) and a corresponding public key (eg).

These keys are used to cascade the encryption process to enhance the security of the signature. Now assume we want to encrypt a message M with a certain private key of a user in one of the levels.

The algorithm below illustrates the steps of generating a secure multisignature :

Algorithm

Sender Side

1: Let Mi be the message for each level , i , Ci the ciphertext of each level.

2: Let Li be the indicated level

3: Select two prime numbers for each level (Li) . Let these prime numbers are pLi and qLi.

4: n(Li)=PLi* qLi

5: ϴLi=(pLi-1)(qLi-1)

6: Choose eLi

7: Calculate the corresponding private key from the following formula:

dLi=inv(eLi)mod ϴLi

8: Generate the group signature for each element in the chosen level as follows :

A: Ci=Mdi mod n

A: Ci=Mdi mod n

B: The group signature is :

CLi=Md1||Md2||…….Mdn

= C1||C2||……..Cn

C: Choose the proper trustworthiness score (TUSLi) to be a candidate signature on the behalf of the group to do the next step.

D: To enhance security we encrypt this signature with the global private key of that level.This is of the general form :

C1=E(M)

C2=E(E(M))=E(C1) then our group signature will take the following form:

Cdouble=(CLi)dgi

=(C1||C2||…….Cn)dgi

This represents the group signature for each level which is performed by the candidate user.

9: The above steps are repeated for each authenticated user in the chosen level.

10: The trusted manager chooses the proper trustworthiness score (TUSLi) to be a candidate signature on the behalf of the group .

Receiver side

Decrypt the ciphertext using the corresponding global public key ,egi :

Mdouble=(CLi)e gi

=(C1||C2||…….Cn)egi

=(C1||C2||…….Cn)

=Me1||Me2||….Men)

Moriginal = M||M||… M

If all M are the same so the signature is authenticated.

IV. RESULTS

Suppose we choose level 1 , L1 . Let pL1=7 and qL1=11. So nL1= 7*11=77 , ϴL1=(pL1-1)((qL1-1)= (7-1)(11-1)=60

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

We choose 3 users from level 1 , namely UL11,UL12,and UL13

Select public keys for these users as , eL11=13,eL12=7,and eL13=11.

The scores assigned to these users are: UL11=60, UL12=30, UL13=50.

Let the message M=18 , calculate the corresponding private keys as following:

dL1=inv(13)mod 60=37

dL2=inv(7) mod 60=43

dL3=inv(11) mod 60= 11

The generation of each ciphertext is explained below:

CL11=18^{37} mod 77= 39

CL12=18^{13} mod 77=46

CL13=18^{11} mod 77=51

The user selected to sign on behalf of this level is UL11 who represents the candidate user , because of his/her high score.

So first we concatenate the above three ciphertext which represent the signature of each user in this level as explained below:

Sig= 3946

Then UL11 again signs this signature with his/her private key,37.

SigK=$(3946)^{37}$ mod 77=68

Then he/she signs this result with the global private key using a global public key which is calculated as follows:

Let the global public key=9

So the global private key= inv(9) mod 60 =7,and the final digital(FSG) signature is :

FSG=(68)7 mod 77 = 40

V. ANALYSIS AND CONCLUSION

This proposed system generates a new scheme secure multisignature. The secrecy of this system is more powerful than other multisignature schemes. It implements the a security level classification and one of them is selected to generate the digital signature so it is considered a general method of security level classification. Each authenticated user had been assigned a trustworthness score depending on his/her experience in dealing with different classes of secret information. The system also uses the cascade encryption to provide more secrecy of the generated signature and thus it assists in increasing secrecy of the message. The system also assume of the message in a strict manner. In addition the proposed system provides properties of a strong muktisignatuthare that enables the system to resist against different attacks such as colluding attack and denial of service . One of these properties is that unforgeablility because only authenticated users of the group can create valid group signatures .The second property is that anonymity since for a given message and its signature, the identity of the individual signer cannot be determined without the group manager's global private key. The applications of this proposed system are: bank funds transfer, military sensitive applications, and marketing.

REFERENCES

1. K. Itakura and K. Nakamura, “A public-key cryptosystem suitable for digital multisignature”, NEC Research and Development, Vol. 71, October 1983, pp. 1-8.
2. S. Micali, K. Ohta and L. Reyzin, Accountable-subgroup multisignatures: extended abstract”, Proceedings of the ACM Conference on Computer and Communications Security 2001 (CCS 2001), ACM press, 2001, pp. 245-254.
3. K.R.P.H. Leung and L.C.K. Hui, “Signature management in workflow systems”, Proceedings of the 23rd Annual International Computer Software and Applications Conference (COMPSAC’99), IEEE, 1999, pp. 424-429.
4. K.R.P.H. Leung and L.C.K. Hui, “Handling signature purposes in workflow systems”, The Journal of Systems and Software, Vol. 55, 2001, pp. 245-259.
5. S. Mitomi and A. Miyaji, “A Multisignature Scheme with Message Flexibility, Order Flexibility and Order Verifiability”, Proceedings of the 5th Australasian Conference on Information Security and Privacy (ACISP 2000), Spring-Verlag, 2000, pp. 298-312.
6. P. Kotzanikolaou, M. Burmester and V. Chrissikopoulos, “Dynamic multi-signatures for secure autonomous agents”, Proceedings 12th International Workshop on Database and Expert Systems Applications (DEXA 2001), IEEE Computer Society, 2001, pp. 587–591.
7. C.J. Mitchell and N. Hur, “On the security of a structural proven signer ordering multisignature scheme”, in: B. Jerman-Blazic and T. Klobucar (eds.), Proceedings of the IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security (CMS 2002), Kluwer Academic Publishers (IFIP Conference Proceedings 228), Boston, 2002, pp.1-8.
8. D. Boneh, H. Shacham and B Lynn, “Short signatures from the Weil pairing”, Advances in Cryptology – AISACRYPT 2001, Springer-Verlag, 2001, pp. 514-532.
9. K. Itankura and K. Nakamura, “A public-key crptosysterm suitable for digital multisignatures”, NEC J. Res. & Dev., vol. 71, (1983).
10. M. Bellare and G. Neven, “Identity-Based Multisignatures from RSA”, In CT-RSA, 2007, LNCS p. 4377, (2007).
11. C. Gentry and Z. Ramzan, “Identity-Based Aggregate Signatures”, In PKC 2006, LNCS, 3958, (2006).
12. D. Boneh, C. Gentry, B. Lynn and H. Shacham, “Aggregate and verifiably encrypted signatures from bilinear maps”, In Proceedings of Euro-crypt 2003, LNCS, 2656, (2003).
13. Haitner, J. J. Hoch, O. Reingold and G. Segev, “Finding Collisions in Interactive Proto-cols - A Tight Lower Bound on the Round Complexity of Statistically-Hiding Commitments”, (2008).
14. K. Ohta and T. Okamoto, “Multisignature schemes secure against active insiderattacks”, IEICE Trans. Fundamentals, E82-A, vol. 1, 1999.
15. W,Lihua , O.Eiji, M.Ying, O.Takeshi,and D.Hiroshi,” ID-Based series-parallel multisignature schemes for multi-messages from bilinear maps” Proceeding of WCC'05 Proceedings of the 2005 international conference on Coding and Cryptography , Pages 291-303 ,Springer-Verlag Berlin, Heidelberg ,2006 .
16. C. WEI , and J. ZHANG, “ Multi-level proxy signature scheme based on strong Diffie-Hellman assumption “, Computer Engineering and Applications, 2008.
17. S. Rahul, R. C. Hansdah , “ Multisignature Scheme for Implementing Safe Delivery Rule in Group Communication Systems “ , Chapter Distributed Computing - IWDC 2004, Volume 3326 of the series Lecture Notes in Computer Science pp 231-239, 2004.
18. T. Jia-lun , W. Tzong ,and T . Kuo-yu ,”A novel multisignature scheme for a special verifier group against clerk and rogue-key attacks” , Journal of Zhejiang University SCIENCE C April 2010, Volume 11, Issue 4, pp 290–295, 2010.
19. Y. Han-u , W. Tzong L. Ming-Lun, and Y. Chi-Kuang ,” New Efficient Identity-Based Key-Insulated Multisignature Scheme”,International Journal of Machine Learning and Computing, Vol. 3, No. 1, February 2013.
20. L. Harn, C.-Y. Lin and T.C. Wu , “ Structured multisignature algorithms”, IEE Proceedings online no. 20040247 , IEE Proc.-Comput. Digit. Tech., Vol. 151, No. 3, May 2004.
21. K. Kei , M. KawauchiHiroshi , and T. MiyajiMitsuru,” A Multi-signature Scheme with Signers' Intentions Secure against Active Attacks”, Proceeding ICISC '01 Proceedings of the 4th International Conference Seoul on Information Security and Cryptology , Pages 328-340 , December 06 - 07, 2001.
22. C. Shenjun , and W. Fengton , “ A New ID-based Designated Verifier Proxy Multi-Signature Scheme” , International Journal of Computer Theory and Engineering, Vol. 3, No. 2, ISSN: 1793-8201, 2011.

AUTHORS PROFILE

Dr. Abdulameer K. Husain, Dijla University College-Iraq. He has completed Master degree in computer science , from university of Sadam , Iraq , in 1993 and his PhD in computer science , computer security from Al-Neelain University ,Sudan . He has total 20 years teaching experience and He got the associate degree from Al-zarqa University-Jordan. He has a long teaching experience in Universities of Lybia and Jordan. He has 7 published books and 25 published papers. He presented in 12 Conferences.

Muthnna Abdulwahid Khudhair, Dijla University College-Iraq. He has completed Master degree in Information technology from Malysia in 2012. He has teaching experience in different topics in computer science.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication