A LITERATURE SURVEY ON COST EFFICIENT RELIABLE AND SECRET DATA SHARING SCHEME

[1] V.Dhinakari,[2].R.NallaKumar, [3]S.Menaka

[1]PG Student, ANNA University Regional centre, Coimbatore
[2]Assistant Professor, ANNA University Regional centre, Coimbatore
[3]PG Student, SNS College Of Engineering, Coimbatore

,

ABSTRACT

This survey proposes an Identity Based forward secure ring signature scheme which works under without random oracles. The special factor of forward security is if a secret key of a corresponding ring member is exposed to the other person means, all previously signed signatures of this member remains valid. If the attacker has stolen the secret key he/she cannot identify any valid signature generated on the past time period by the valid user. This factor is especially useful in the case of ring signature scheme. The exposure of a single secret key to the attacker may make invalidity in thousands or even millions ring signatures which belongs to that particular user. Because most of the ring signature schemes in the literature does not contain forward security. Existing scheme relies on random oracles to prove the security in ring signature scheme. This survey first interest to construct a forward secure ring signature scheme that can be provide secure without using random oracles. In a wireless sensor networks and smart grid system this scheme may be deployed where more number of users is working.

KEY WORDS: Authentication, data sharing, cloud computing, forward security, smart grid

INTRODUCTION

Ring Signature:-

In a Ring signature scheme [18] the member of a group signs a message and sends that message to the all members or special members in the whole group. The verifier or the group member or group member who receives the message does not know who the real signer in the group is. The ring group can be formed dynamic fashion. The member in the group does not need any collaboration.

Public Key Crypto Graphy:-

In conventional public key cryptography system the security of a crypto system is guaranteed under some intractability assumptions that the secret key is kept secret from the adversary/attacker. In the real world however the attacker may use many ways to compromise a secret key. Hackers may steal the secret key if your computer/system is infected with viruses or

ISSN: 2278 – 1323

worms or Trojans. The attacker can get the password when the user uses this ecret key in a phishing website. Therefore, it is very important to the user minimize the damage caused by the attacker even though if the partial/entire secret key is lost by the attacker. If the attacker knows full secret key means, he can sign or decrypt any message on behalf of the injured party. This type of situation is even creating big problem for ring signatures also, because the attacker can forge a message on behalf of the whole group. Moreover the other members in the group may be completely unaware of such type of forgery, since they are also unaware of being conscripted into the group.

Forward Secure Ring Signature:-

For the key exposure problem Forward security for signatures [19] was designed. This secure signature scheme makes the past signature remains secure even though if the current secret key is lost. For the key exposure problem the first solution was designed by Bellare and Miner in 2009 [20]. The main idea of this forward scheme is to divide the lifetime of the public key into T intervals and in each time interval the same public key is used they corresponds to different secret keys. A current secret key can be only used to derive the secret key in the future, but not the past. Therefore the compromised current secret key does not enable the attacker to forge signature stored at the past time.

Forward secure ring signatures were proposed by Liu and Wong in 2012 [21] in order to resolve the key exposure problem in ring signatures for a group of members. The motivation of this technique is to reduce the damage caused by the exposure of any secret key of users in ring signature. Although the secret key is compromised by the attacker the previously/past generated ring signatures remain valid and do not need to be re-generated. This proposed security model provide a concrete construction without the random oracle model

EXISTING SYSTEM:-

In recent years the crypto scientists has drawn much attention in order to deal with the key-exposure problem of digital signatures. In reality, the security of the secret key is especially more important in digital signatures. For example, in a regular signature scheme, if an attacker compromises a single signing key, all the signatures/applications corresponding to this signing key would be untrustworthy even though if they were generated before key exposure to the attacker. In order to deal with this type of problem, several approaches have been proposed.

Threshold Signature [1]

In 1996 R. Gennaro et al proposed "Robust threshold DSS signature. Threshold signature is first proposed scheme which can make key exposure more difficult. In this scheme [1], a secret key is divided into n pieces called shares that will be shared among n users. Only not fewer than t players can cooperate to produce signatures.

ISSN: 2278 – 1323

Forward-secure signature [2-7]

This is another approach that can limit the damage problem created by the key exposure. In which the secrecy of the previous signatures can be preserved when the current secret key is exposed. Therefore, an attacker cannot forge signatures produced at previous time periods even though he/she compromises the current secret key.

Forward- secure signature with encryption[8,9]

In 2011 J. Yu et.al proposed this scheme in [8, 9].Forward-secure threshold signature combines the advantages of previous forward-secure signature and threshold signature, which not only make key exposure difficult but also reduce the damage brought by key exposure. In this paradigm, all the users may update their secret shares to make the corresponding secret key evolve after a regular time period. The public key of the system is remains unchanged during the whole lifetime period like email id of the Gmail. In a forward-secure threshold signature, if an attacker perform attacks fewer than threshold players means he/she cannot forge any signature. Even though if an adversary attacks more players to get their shares in one period he/she cannot forge any signature generated at previous periods.

Forward-Secure Threshold Signature

This scheme was proposed by Abdalla *et al in 2011* [10]. However it had large keys and needed many interactions between those keys. Afterwards, In 2012 W. G. Tzeng et.al proposed another forward-secure threshold signature with proactive property [11] was presented, which had a shorter secret key. In 2012 J. Yu proposed an efficient forward-secure threshold signature from bilinear pairings [12].

Disadvantages:-

From the Observation of all the current forward-secure signature schemes having been proposed there are two weaknesses has been understood.

(1) This scheme either has no security proof or it proves security secure only in the random oracle model.
(2) However, security proofs in the random oracle model are only heuristic as [13].
(3) Furthermore, security proofs in the random oracle model do not always imply the security of the actual scheme in the real world. Therefore, constructing forward-secure threshold signature without random oracles is an attractive issue;
(4) Multiple interactions are needed in update and signing algorithms.

Interactive algorithms

It does not fit in many real-world applications because it is very difficult to build synchronous blocks and communicating channels to complete interactive operations. What is more, interactive operations can bring large burden of bandwidth in some wireless

ISSN: 2278 – 1323

circumstances. Thus, it is desirable to construct a forward-secure threshold signature scheme with non-interactive update and signing algorithms. As far as we are concerned, there has not been any forward-secure threshold signature scheme proven secure without random oracles and not any forward-secure threshold signature scheme with non-interactive update and signing algorithms, either, up to now.

DRAWBACKS

- Costly certificate verification in the traditional forward security signature setting becomes a bottleneck [8].
- Threshold based signatures does not have forward security[2].
- Suppose there are 10,000 users in the ring, the verifier of a traditional public key based ring signature must first validate 10,000 certificates of the corresponding users, after which one can carry out the actual verification on the message and signature pair which is a costly process, saves a great amount of time and computation.
- This saving will be more critical if a higher level of anonymity is needed by increasing the number of users in the ring.
- Diffie-Hellman assumption in the standard model situation is even worse for ring signatures, since the attacker can forge a message on behalf of the whole group.
- Moreover, the other members of the group may be completely unaware of such forgery, since they are unaware of being conscripted into the group.

PROPOSED SYSTEM

This survey proposes ID based forward-secure threshold signature scheme without random oracles which is the first non-interactive forward-secure threshold signature scheme. This scheme is based on the idea of hierarchical ID-based cryptography [14], Waters' signature [15], Yu's forward-secure multi-signature [16] and Shamir's secret sharing [17]. This is one kind of important distributed signatures. In a (t, n) ID based forward-secure threshold signature, if an attacker attacks fewer than t players, she cannot forge any valid signature of the user also even if an adversary attacks t or more players in some time period, he/she cannot forge the signatures generated at previous time periods or past signatures. In a current scenario, all forward-secure threshold schemes are at most proven to be secure in the random oracle model. However, security in the random oracle model does not imply security in the real world. So this work proposed the ID based forward-secure threshold signature scheme that can be proven secure without using random oracles.

ADVANTAGES

- Our proposed scheme does not need any interactions among the participating players and is proved security in the standard model.
- This proposed scheme does not need any interaction among the players in

ISSN: 2278 – 1323

key update and signing algorithms this factor is different from the existing system.

- Therefore, the users belongs to the group can update their shares and sign the message, possibly in a completely decentralized fashion, which is very valuable in ad-hoc circumstances.
- This scheme has constant signing time and signature size.

CONCLUSION

A new ID based forward-secure threshold signature scheme is proposed in this work. The running costs needed for key generation, key updation, signing and verifying algorithms are at most log-squared of the total number of time periods *T which is computationally less compared to the other existing methods*. The big advantage of the proposed scheme over all the previous schemes are that it does not need any interaction among the players and is proved to be secure without using random oracles.

REFERENCES

1. R. Gennaro, S. Jarecki, H. Krawczyk, and T. Rabin, "Robust threshold DSS signatures," in *Proceedings of Cryptology − Eurocrypt*, 1996, pp. 354-371.

2. M. Bellare and S. Miner, "A forward-secure digital signature scheme," in *Proceedings of Cryptology − CRYPTO*, 1999, pp. 431-448.

3. M. Abdalla and L. Reyzin, "A new forward-secure digital signature scheme," in *Proceedings of Cryptology − Asiacrypt*, 2000, pp. 116-129.

4. H. Krawczyk, "Simple forward-secure signatures for any signature scheme," in *Proceedings of the 7th ACM Conference on Computer and Communications Security*, 2000, pp. 108-115.

5. T. Maklin, D. Micciancio, and S. Miner, "Efficient generic forward-secure signatures with an unbounded number of time periods," in *Proceedings of Cryptology − Eurocrypt*, 2002, pp. 400-417.

6. G. Itkis and L. Reyzin, "Forward-secure signatures with optimal signing and verifying," in *Proceedings of Cryptology − CRYPTO*, 2001, pp. 499-514.

7. J. Yu, F. Y. Kong, X. G. Cheng, R. Hao, and J. X. Fan, "New forward-secure signature scheme with uztrusted update," *Journal of Information Science and Engineering*, Vol. 27, 2011, pp. 1435-1448.

8. J. Yu, R. Hao, F. Y. Kong, X. G. Cheng, J. X. Fan, and Y. K. Chen, "Forward-secure identity-based signature: Security notions and construction," *Information Sciences*,Vol. 181, 2011, pp. 648-660.

9. J. Yu, F. Y. Kong, X. G. Cheng, R. Hao, and J. X. Fan, "Forward-secure identitybased public-key encryption without

ISSN: 2278 – 1323

random oracles," *Fundamenta Informaticae*, Vol.110, 2011, pp. 1-16.

10. M. Abdalla, S. Miner, and C. Namprempre, "Forward-secure threshold signature schemes," in *Proceedings of the Cryptographer's Track at RSA Conference*, 2001, pp.441-456.

11. W. G. Tzeng and Z. J. Tzeng, "Robust forward signature schemes with proactive security," in *Proceedings of Public Key Cryptography*, 2001, pp. 264-276.

12. J. Yu, F. Y. Kong, and R. Hao, "Forward secure threshold signature scheme from bilinear pairings," in *Proceedings of the 2nd International Conference on Computational Intelligence and Security*, 2007, pp. 587-597.

13. R. Gennaro, S. Halevi, and T. Rabin, "Secure hash-and-sign signatures without the random oracle," in *Proceedings of Cryptology − Eurocrypt*, 1999, pp. 123-139.

14. D. Boneh, X. Boyen, and E. J. Goh, "Hierarchical identity based encryption with constant Size ciphertext," in *Proceedings of Cryptology − Eurocrypt*, 2005, pp. 440-456.

15. R. Waters, "Efficient identity based encryption without random oracles," in *Proceedings of Cryptology − Eurocrypt*, 2005, pp. 114-127.

16. J. Yu, R. Hao, F. Y. Kong, X. G. Cheng, and X. F. Guo, "Forward-secure multi-signature in the standard model: Security model and construction," *Journal of Software*,Vol. 21, 2010, pp. 2920-2932.

17. A. Shamir, "How to share a secret," *Communications of the ACM*, Vol. 22, 1979, pp. 612-613.

18. R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In ASIACRYPT 2001, volume 2248 of Lecture Notes in Computer Science, pages 552{565. Springer, 2001.

19. R. Anderson. Two remarks on public key cryptology. Technical Report UCAMCL-TR-549, University of Cambridge, Computer Laboratory, Dec. 2002. Relevant material presented by the author in an invited lecture at CCS '97.

20. M. Bellare and S. Miner. A forward-secure digital signature scheme. In M. J.Wiener, editor, Crypto '99, volume 1666 of Lecture Notes in Computer Science, pages 431{448. Springer, 1999.

21. J. K. Liu and D. S. Wong. Solutions to key exposure problem in ring signature. I.J. Network Security, 6(2):170{180, 2008.

ISSN: 2278 – 1323