PRIVACY ID BASED SECRET ATTESTATION SCHEME WITH REPUDIATION CAPABILITIES

Emal Dyana .M .V
Department of Computer Science & Engineering,
Saveetha Engineering College,
Chennai

Abstract---*The Secret Attestation Scheme is a method for preserving the privacy of users providing authentication of a Trusted Hardware Platform. A TPM can prove to a remote party that it is a valid TPM without revealing its identity. In the DAA scheme, a TPM can be revoked only if the DAA private key in the hardware has been extracted and published widely so that verifiers obtain the corrupted private key. This scheme allows each user generating the signature to decide or not the signature should be linkable to another signature. This expanded revocation property makes the scheme useful for other applications such as for driver's license. Using the EPID scheme the verifier can prove the prover that the user is a non revoked user by maintaining a database to retrieve the details of a user who frequently accesses other users data. The EPID scheme is efficient and provably secure in the security model as DAA with a new Privacy ID scheme with repudiation capabilities is proposed to run the join protocol concurrently with different users.*

Index Terms— Trusted Platform module, Secret Attestation Scheme, Trusted Computing Group, Enhanced Privacy Identity.

I INTRODUCTION

The Secret Attestation Scheme is a signature scheme, which offers a zero knowledge proof of a key certificate and provides a variety of balances between security and privacy by choosing a random base – for privacy sensitive cases, named base – for non privacy-sensitive cases and a combination of both of random and named base.

1.1 Trusted Platform

A TPM can prove to a remote party that it is a valid TPM without revealing its identity and without likability. In the SAS scheme, a TPM can be revoked only if the SAS private key in the hardware has been extracted and published widely so that verifiers obtain the corrupted private key.

If the unlinkability requirement is relaxed, a TPM suspected of being compromised can be revoked even if the private key is not known. However, with the full unlinkability requirement intact, if a TPM has been compromised but its private key has not been distributed to verifiers, the TPM cannot be revoked. Furthermore, a TPM cannot be revoked from the issuer, if the TPM is found to be compromised after the SAS issuing has occurred. This scheme provides an outline of a certificate issuer, a trusted platform module and an external partner. It also enables the signature to provide user-control link that can be used to link some selected signatures from the same signer for the same verifier EPID scheme is efficient and provably secure in the same security model as SAS and has a security proof in the random oracle model based on the strong RSA assumption and the DDH assumption.

1.2 Secret Attestation Scheme

Attestation is a trusted computing technology that permits a computer to measure properties of a remote system in such a way that the remote system will be detected if it is lying. SAS was adopted by TCG and specified in TCG TPM. A SAS signature has flexible-traceability and flexible likability. There is no identity-disclosure authority. The SAS signature provides the user-control link that can be used to link some selected signatures from the same signer for the same verifier. TCG requires a TPM to have an embedded “endorsement key (EK)”, to prove that a TPM is a particular genuine TPM. EK is not a platform identity. TCG lets a TPM control “multiple pseudonymous attestation identities” by using “attestation identity key (AIK)”. AIK is a platform identity, to attest to platform properties. A user of a platform communicates with a verifier who wants to be assure that the platform of the user contains a certified TPM. The user wants the privacy to protected. Each TPM obtains a membership private key from the user. When the verifier suspects that a TPM has been compromised, but not obtained the membership private key of the compromised TPM, the verifier can reject any further signatures from the suspected TPM using the revocation method.

During the issuing of a DAA private key, the issuer obtains the identity of the TPM, but does not learn the DAA membership private key. If sometime after issuing, the issuer discovers that the TPM has been compromised, the issuer cannot revoke the DAA private key that has been issued to that compromised TPM.

II OBJECTIVES

The ultimate goal is to enable users to propose a new scheme with enhanced revocation capabilities, a protocol that must be unforgeable where only non revoked group members are able to generate valid signatures, a protocol that must be anonymous where the verifier cannot identify the actual signer given a valid signature, a protocol that must be unlinkable, where it is computationally infeasible to determine whether two different signatures were computed by the same group member.

III PRELIMINARIES

In this paper, a scheme called Enhanced Privacy ID(EPID) that can be seen as a new SAS scheme with enhanced revocation capabilities. With this enhanced revocatioin capability, the new scheme will have broader capability beyond attestation and the TCG application. In a EPID scheme, there are four types of entities: an issuer, a revocation manager, users and verifiers. The user could be the same entity as the revocation manager.

SETUP:

The issuer issues a group public key and a private key. The issuer publishes the group public key.

JOIN:

This involves interaction between the issuer and a user a user that results in the user becoming a new group member. At the end of this protocol, the user obtains a membership private key from the issuer.

PROOF OF MEMBERSHIP:

In this protocol, a prover interacts with the verifier to convince the verifier that he is a member of the group in a good standing. During the signing phase, it takes input as group public key, a private key and a message M and returns a signature. The verifier takes input as group public key and a set of revocation tokens along with a signature on a message. The response from verifier returns either valid or invalid. It has the following steps:

- The prover sends a request to the verifier,
- The verifier responds with a message m;
- The prover generates a signature on the message m based on his membership private key,
- The verifier verifies the signature using the group public key.

REVOCATION:

The revocation manager puts a group member into the revocation list. There are three types of revocations:

1. Private key based revocation in which the revocation manager revokes a user based on the user's membership private key,
2. Signature-based revocation in which the revocation manager revokes a user based on the signature created by the user, and
3. Issuer-based revocation in which the revocation manager revokes a user based on the recommendation from the issuer.

IV RELATED WORK

Zero-Knowledge Proof

Zero-Knowledge Proof describes much more efficient implementations on Group Signature Schemes. A SAS scheme is a cryptographic scheme for providing an anonymous signature. EPID is an extension of Direct Anonymous Attestation. It involves additional revocation capabilities with flexible key Generation and signature options. EPID (enhanced privacy identity scheme). Issuer need not know how to know member private key as the EPID scheme are anonymous and untraceable.

Secret Attestation Scheme

Both the SAS and EPID scheme are unlikable and it depends upon the base. The signature includes a pseudonym B^f where B is the base chosen for signature and revealed during the signature. f is unique per member and private. Revocation in EPID scheme Verifier Local Revocation using Name Base where revocation check is performed by verifier. Signature based revocation defines a Signature revocation list where the issuer and the verifier decide that they no longer want to accept signatures from a signed "revoked" message with pseudonym B^f.Member proves his signature with base B and not with

$$K: = B^f \bmod p$$

It retains same anonymity with unlinkability properties.

Verifier Group Signature

An additional argument of Revocation list is provided to the signature algorithm. Every revoked user contains a token maintained in a revocation list. The verifier accepts the signatures generated by unrevoked users and reveals no information about which unrevoked user issued the signature. If the user is a revoked user , the signatures from that user is no longer accepted. In the VLR group signatures, the revocation tokens are placed in the left half of the private key. However, the private key can be added to the RL and can be revoked. To test whether the two signatures are issued by the same revoked user, then verify the signatures once using the RL before the user is revoked and once using the RL after. This eliminates the need for a trusted revocation authority. The VLR group signatures uses a hash function. In tis case, the security of the signatures depends on two problems namely Diffe-Hellman problem and Decision Linear Problem.

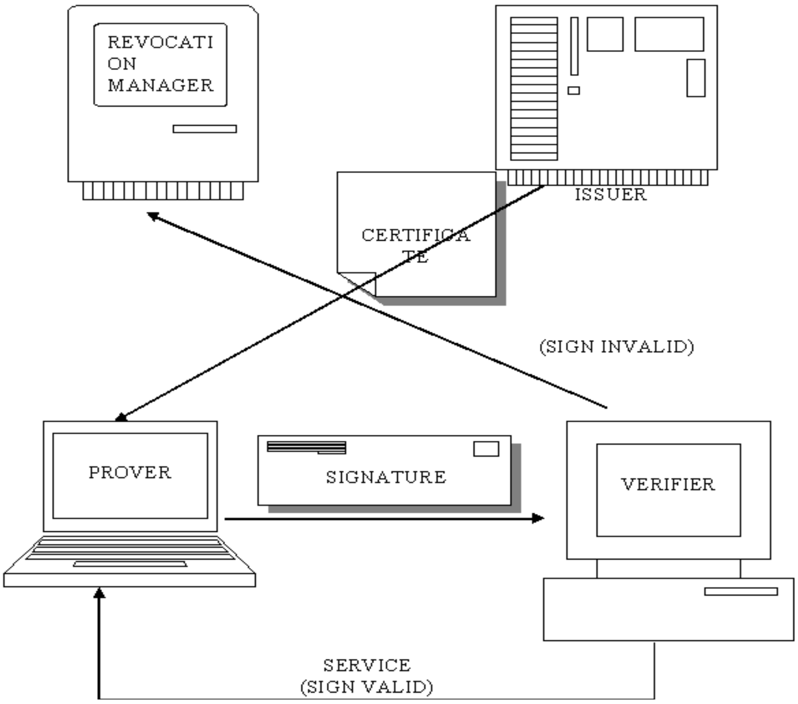

FIG 1. PROPOSED ARCHITECTURE

V PROPOSED SYSTEM

In this paper, the signature generated in the proof of membership protocol must be

(i) Unforgeable
(ii) Anonymous
(iii) Unlinkable.

The EPID scheme chooses not to have traceability from the revocation manager because to provide maximum privacy to users. Traceability provides the capability that the revocation manager can determine which user generates which signature without any acknowledgment from the user that is being traced. Trusted hardware device for EPID enables to have more efficient revocation. In EPID scheme, there are few cases where the user can be revoked.

The users's membership private key was removed from the trusted hardware device and was published widely so that everyone knows this compromised private key.

- The users membership private key was extracted from the trusted hardware device by the adversary. The issuer suspects that the user's hardware device was compromised, but has not obtained the user's private key .
- The user's membership private key was extracted from the hardware device by the adversary.The revocation manager suspects that the hardware device was corrupted. The revocation manager obtains a signature from the corrupted device but has not obtained the private key.
- The issuer revokes the user for some management reason,eg., the user left the group or the user's group membership expired.
- The user is revoked from transactions. More specifically, the user abuses the group privilege and is revoked by the revocation manager after the user conducted the proof of membership.

To handle the above revocations using the EPID scheme, one can use private key based revocation to revoke users of case1, issuer-based revocation to revoke user's of case2 and case4, and signature based revocation to revoke users case3 and case5.

An extension to the EPID scheme is to improve the join protocol in such a way that the user can run the join protocol concurrently with different users. This can be achieved using secure multiparty computation using multiparty cryptographic protocols. The cost of proof of membership protocol is linear to the size of the revocation list and could be quite expensive if the revocation list becomes large. There are two ways to control the size of the revocation list .

- Divide to smaller groups. If the group size is too big, the list may become large as well. One way to control the size of the evocation list is have multiple smaller groups.
- Issue a new group if the list grows too big. If the size of the revocation list is above a certain threshold, then the issuer can "rekey" process as follows: The issuer first creates a new group. Then, each user in the old group proves to the issuer that he is a legitimate member of the old group and has not been revoked, then obtains anew membership private key for the new group.

Efficient Revocation

In the VLR group signature, the signature verification time increases linearly with the revked users. It is applicable to have Verifier-Location Revocation system where verification time is constant. Consider users are connected to a web site. A private attestation is performed at each site using group signatures provided by tamper-resistant chip. In this case, during the revocation check, the parameters such as *u* and *v* generated as,

$$(u, v) \leftarrow H_o \text{ (gpk ,S , r)}$$

where r is a random range{1,…..,k} and k is a security parameter, *u* and *v* does not depend on the message beind signed. Therefore ther can be only *K* possible values at a given site for a given site. There are cases where a site *S* is given a revocation list. Inorder to verify the signature $\sigma = (r , T_1 , T_2 ,c ,s_\alpha , s_x , s_\delta)$ was not issued by a revoked user, the site uses the same procedure.

1. Compute $(u , v) \leftarrow H_o$ (gpk ,S ,r), and
2. For i = 1,…,b , then check that, $e (T_1 ,v) e (A_i ,u) \neq e (T_2 ,u)$.

To check revocation, it simply checks look-up table to test whether the value $e (T_2 ,u) / e (T_1 ,v)$ lies in the *r*th row of the table, else the signature was not issued by a revoked user. However, the revocation check take time that is independent of the size of the revocation list.

Conclusion

The notion of EPID gave an efficient construction to SAS scheme under the RSA assumption and the decisional Diffie-Hellman assumption in order to improve the join protocol in such a way that the user can run the join protocol concurrently with different users. To prove membership, both the prover and the verifier need to perform computations linear to the size of the revocation list.

References

[1] Ernie Brickell and Jiangtao Li, "Enhanced Privacy ID: A Direct Anonymous Attestation Scheme With Enhanced Revocation Capabilities", IEEE Transactions on Dependable and Secure Computing, 2012.

[2] J. Camenisch and M. Stadler, "Efficient Group Signature Schemes for Large Groups," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '97), pp. 410-424, 1997.

[3] J. Kalian and E. Petrank, "Identity Escrow," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '98), pp. 169-185,1998.

[4] D. Boneh and H. Shacham, "Group Signatures with Verifier-Local Revocation," Proc. 11th ACM Conf. Computer and Comm. Security, pp. 168-177, Oct. 2004.

[5] E. Brickell, J. Camenisch, and L. Chen, "Direct Anonymous Attestation," Proc. 11th ACM Conf. Computer and Comm. Security, pp. 132-145, 2004.

[6] D. Chaum and E. van Heyst, "Group Signatures," Proc. Ann. Int'l Conf. Theory and Application of cryptographic Techniques: Advances in Cryptology (EUROCRYPT '91), pp. 257-265, 1991.

[7] R.Canetti, " Studies in Secure Multiparty Computation and Applications, " PhD dissertation, Weizmann Inst. of Science, Rehovot, Israel,1995.

[8] R.Canetti, " Security and Composition of Multiparty Cryptographic Protocols," J.Cryptography, vol. 13, no. 1, pp. 143-202, 2000.

[9] J.Camenisch and M.Michels, "Proving in Zero-Knowledge that the number is two Safe Primes," Proc.Int'l Conf.Theory and Application of Cryptoraphic Techniques: Advances in Cryptology,1994.

[10] D.Pointcheval and J.Stern, ," Security Proofs for Signature Schemes," Proc Ann.Int'l Conf.Theory and Application of Cryptographic Techniques:Advances in Cryptology (EUROCRYPT '96),PP.387-398,1996.

[11] J.Camenisch and M.Michels," Separability and efficiency for Generic Group Signature Schemes," Proc.Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '99),PP.413-430,1999.

[12] M. Bellare, J.A. Garay, and T. Rabin, " Fast Batch Verification for Modular Exponentiation and Digest Signatures, " Proc.Int'l Conf. Theory and Application of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '98), pp.236-250, 1998.

[13] E .Bresson and J. Stern, "Efficient Revocation in Group Signatures" Theory in Public Key Cryptography, pp. 190-206, 2001.

[14] P.P. Tsang, M.H. Au, A. kapadi, and S.W. Smith,"Black listable Anonymous Credentials: Blocking Misbehaving Users without T.T.Ps," Proc. ACM Conf. Computer and Comm. Security, pp. 72-81, 2007.

[15] Trusted Computing Group, "TCG TPM Specification 1.2," http://www.trustedcomputinggroup.org, 2003.

[16] J. Camenisch and A. Lysyankanya, "An Efficient System for Non-Transferable Anonymous Credentials with Optional Anonymity Revocation," Proc.Int'l Conf. Theory and Application of Cryptographic Techniques: Advances in Cryptography (EUROCRYPT '01), pp 93-118, 2001.

[17] J. Camenisch and V. Shoup, "Practical Verifiable Encryption and Decryption of Discrete Logarithms," Proc.Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '03), pp. 126-144, 2003.