

A remote attestation for enhanced privacy id

Ms.R.Anitha¹
II yr ME CSE¹
Srinivasan Engineering College
Perambalur

Mr.S.Saravana Kumar²,
Asst.Prof, Department of CSE²,
Srinivasan Engineering College,
Perambalur

anu.karan12@gmail.com¹

saravana.coolya@gmail.com²

Abstract- Direct anonymous attestation (DAA) is a scheme developed for remote authentication of a hardware module and trusted platform module (TPM), while preserving the privacy of the user of the platform that contains the module. In Previous technique, a TPM can be revoked only if the DAA private key in the hardware has been extracted so that if the TPM is found to be compromised after the DAA issuing has occurred. The proposed present a EPID Scheme (Enhanced Privacy ID) builds on top of the DAA scheme and applies Camenisch-Lysyanskaya (CL) signature scheme. EPID is efficient and provably secure in the random oracle model to provide high security scheme a concept of DRAFT has to check the integrity status of the intermediate node to gain the attestation.

Keywords: Security and protection, privacy, trusted computing, cryptographic protocols, Remote Attestation.

1.INTRODUCTION

The project is about Signature scheme for group communication which comes under Network Security. It involves the authorization of access to data in a network, which is controlled by the network administrator. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting

transactions and communications among businesses, government agencies and individuals.

The networks are computer networks, both public and private, that are used every day to conduct transactions and communications among businesses, government agencies and individuals. The networks are comprised of "nodes", which are "client" terminals (individual user PCs) and one or more "servers" and/or "host" computers. They are linked by communication systems, some of which might be private, such as within a company, and others which might be open to public access. The obvious example of a network system that is open to public access is the Internet, but many private networks also utilize publicly-accessible communications. Today, most companies' host computers can be accessed by their employees whether in their offices over a private communications network, or from their homes or hotel rooms while on the road through normal telephone lines.

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

2. RELATED WORK

The EPID scheme differs from the DAA scheme in that it adds additional revocation capabilities. However, the credentials in that system are linkable for multiple display,

whereas the signatures in the EPID scheme are unlinkable. Camenisch and Lysyanskaya proposed a revocation mechanism. Their scheme takes constant time in revocation check for both the prover and the verifier. However, their scheme requires every group member to update his membership private key each time a join or a revoke operation takes place. The unique property that EPID has that none of the above have, is the capability to revoke a membership private key that generated a signature, without being able to open the signature.

To describe and maintain the integrity status of a system, there exist various information flow-based integrity models. With existing integrity models, there is a gap between concrete measurements of a system's components and the verification of its integrity status. We believe an application oriented and domain-centric approach accommodates the requirements of attestation evaluation better than directly adopting an abstract model.

3. PROBLEM DEFINITION

Signature generated by TPM are unlinkable, but revocation only works if the corrupted TPM's private key has been revealed to the public. If the TPM has been compromised but its private key has not been distributed to the verifiers, the corrupted TPM cannot be revoked.

If the verifier determines that a membership private key that was used in signature has been compromised, that verifier can revoke that key locally without knowing the compromised membership private key.

4. EXISTING SYSTEM

4.1 DIRECT ANONYMOUS ATTESTATION

The Direct Anonymous Attestation is a scheme that enables remote authentication of a TPM, while preserving the privacy of the user of the platform that contains the TPM. In the DAA protocol, there are an issuer, a platform who has a membership certificate issued by the issuer, and a verifier who wants to get convinced by the platform has a membership certificate.

The TPM can then forward this certificate to the verifier and authenticate itself with this AIK. There are two possibilities to detect a rogue TPM: 1) If the EK secret key was extracted from a TPM, distributed, and then detected and announced as a rogue secret key, the Privacy CA can compute the corresponding public key and remove it from its list of valid Endorsement Keys. 2) If the Privacy CA gets many requests that are authorized using the same Endorsement Key, it might want to reject these requests. The exact threshold on requests that are allowed before a TPM is tagged rogue depends of course on the actual environment and applications, and will in practice probably be determined by some risk-management policy.

DAA allows for pseudonyms, i.e., for each signature a user can decide whether or not the signature should be linkable to another signature. The user wants her privacy protected and therefore requires that the verifier only learns that the user uses a TPM but not which particular one otherwise all the transactions would become linkable to each other.

4.2 REMOTE ATTESTATION

TCG specifications define mechanisms for a TPM enabled platform to report its current hardware and software configuration status to a remote challenger. A TCG attestation process is composed of two steps:

- 1) an atteste platform measures hardware and software components starting from BIOS block and generates a hash value. The hash value is then stored into a TPM Platform Configuration Register (PCR). Recursively, it measures BIOS loader and operating system (OS) in the same way and stores them into TPM PCRs;
- 2) an attester obtains the attestee's digital certificate with an attestation identity key (AIK), AIK-signed PCR values, and a measurement log file from the attestee which is used to reconstruct the attestee platform configuration, and verifies whether this configuration is acceptable.

From these steps, it is noticed that TCG measurement process is composed of a set of sequential steps including the bootstrap loader. Thus, TCG does not provide effective mechanisms for measuring a system's integrity beyond the

system boot, especially considering the randomness of executable contents loaded by a running OS.

5. PROPOSED WORK

5.1 Enhanced Privacy ID

An EPID scheme has the following four procedures:

Setup: In this procedure, the issuer creates a group public key and a group issuing private key. The issuer publishes the group public key. **Join:** This is a protocol between the issuer and 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 a verifier to convince the verifier that he is a member of the group in good standing (i.e., without being revoked). 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 m based on his membership private key, and
- 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 signatures created by the user, and 3) issuer-based revocation in which the revocation manager revokes a user based on the recommendation from the issuer.

5.2 Security parameters

The security parameter controlling the statistical zero-knowledge property is the output length of the hash function used for Fiat-Shamir heuristic. The security parameter needed for the reduction in the proof of security, is the size of the modulus, and is the size of the order of the subgroup of that is used for revocation checking.

5.3 Network model setup full

The host platform is trusted for performing its portion of computation correctly. However, the host is not allowed to learn the private key of the prover or to forge a signature without the principal prover's involvement. The network is accessible only by the authenticated person and only those have keys based on the network id.

In addition to generating the group public key and groupissuing private key, the issuer generates also a long-term public/private key pair. The issuer publishes the public key. This key is used for authentication between the issuer and any user who wants to become a group member. Analogously, the revocation manager has a long term public/private key pair. The revocation manager uses its key to sign the revocation list.

5.4 Verification of the issuer's public key

The revocation manager publishes the revocation list RL and signs using his private key(pR), everyone can verify the authenticity of this revocation list using the revocation manager's public key (KR). In our project the revocation manager is trusted. Then, the verifiers trust the revocation manager to construct the revocation list in a correct manner. In the model where the revocation manager is not completely trusted, the revocation manager also needs to publish a compromised private key for each item in priv-RL.

6. DRAFT TECHNOLOGY

Framework is based on a domain-based integrity model to describe the integrity status of a system with information flow control. With this property, the high integrity processes of a system are first measured and verified, and these processes are then protected from accesses initiated by low integrity processes during runtime. In other words, the protection of high integrity process is verified by analyzing security policies and ensuring that the policies are correctly enforced.

Having this principle in place, DR@FT enables us to verify whether certain applications (domains) in the attestee satisfy integrity requirements without verifying all components of the system. To accommodate the dynamic nature of a system, DR@FT only verifies the latest changes in a system

state, instead of considering the entire system information for each attestation inquiry.

Through these two tactics, our framework is able to achieve an efficient attestation to the target system. Also, DR@FT adopts a graph-based information flow analysis mechanism to examine security policy violations based on our integrity model, which helps cognitively identify suspicious information flows in the attestee. To further improve the efficiency of security violation resolution, it propose a ranking scheme for prioritizing policy violations, which provides a method for describing the trustworthiness of different system states with risk levels

7. PERFORMANCE EVALUATION

In this study document collection is used to evaluate the proposed approach. Various common measures are applied for performance evaluation. This evaluation compares and defines the following parameters such as setup, join, Proof of membership and revocation which combines TPM and DAA with the existing system. The proposed system is more security and scalable for complex applications. and it shows better results in proposed work than the existing work by evaluating the parameters setup, revocation and join protocol

8. CONCLUSION

The main aim is to provide direct anonymous attestation in order to preserve the privacy. If the trusted platform module itself is being compromised then revocation will be a big problem. So to overcome this, enhanced privacy id scheme has been proposed. This scheme provides a method to revoke trusted platform module even if the trusted platform module private key is unknown. The join protocol is used to ensure system security. The issuer runs the protocol concurrently with the different trusted platform module. The scheme needs to be analyzed in terms of following metrics: efficiency, security, scalability.

REFERENCES

- [1] Boneh. D and shacham. H, "Group Signatures with Verifier-Local Revocation," Proc. 11th ACM Conf. Computer and Comm. Security, pp. 168-177, Oct. 2004.
- [2] Brickell. E, Camenisch. J, and Chen. J, "Direct Anonymous Attestation," Proc. 11th ACM Conf. Computer and Comm. Security, pp. 132-145, 2004.
- [3] Canetti. R, "Security and Composition of Multiparty Cryptographic Protocols," J. Cryptology, vol. 13, no. 1, pp. 143-202, 2000.
- [4] Camenisch. J and Lysyanskaya.A, "A Signature Scheme with Efficient Protocols," Proc. Third Conf. Security in Comm. Networks, pp. 268-289, 2002.
- [5] Camenisch.j and Shoup.v, "Practical Verifiable Encryption and Decryption of Discrete Logarithms," Proc. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO '03), pp. 126-144, 2003.
- [6] Damgaird.I and Fujisaki.E, "An Integer Commitment Scheme Based on Groups with Hidden Order," Int'l Cryptology Conf.Advances in Cryptology (ASIACRYPT '02), pp. 125-142, Dec. 2002.
- [7] Fabrice Boudot France - CNET "Efficient Proofs that a Committed Number Lies in an Interval.
- [8] Fiat.A and Shamir.A, "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '86), pp. 186-194, 2006.
- [9] Lenstra. A.K and Verheul. E.R, "Selecting Cryptographic Key Sizes," J. Cryptology, vol. 14, no. 4, pp. 255-293, 2001.
- [10] Pointcheval. D and Stern. J, "Security Proofs for Signature Schemes," Proc. Ann. Int'l Conf. Theory and Application of Cryptographic Techniques: Advances in Cryptology (EUROCRYPT '), pp. 387-398.