Modern Credential Access Control Approach Based On Pseudonymous Signature

Faiz Ahmad, Rajesh Jalnekar

Department of Computer Engineering, Faculty of Engineering , Bharati Vidyapeeth University , Pune-411043(India)
Department of Electronic and Telecommunications, Vishwakarma Institute of Technology, Pune-411037(India)

Summary
This paper proposes a modern credential access control approach which allows the organizations to provide their resources/services on the internet and grant access rights to users by employing Cryptographic Pseudonymous Signature. The concepts of Modern Credentials and Pseudonymous Signature are proposed with respect to Pseudonymous Identification Scheme to facilitate pseudonymity in access control service. These mechanisms highly protect the privacy rights of users and organizations and resolve the problem of scalability in identity and key-based access control systems: The prover keeps anonymous to verifier by informing the pseudonyms to receiver, and the receiver can not identify the sender from his pseudonym, but upon verifying the pseudonymous signature he can be ensured that the pseudonym belong to a trusted anonymous user from the trusted domain .

Key words :

Modern Credential, Access Control, Pseudonymous Certificates, Privacy.

1. Introduction

The protection of individual privacy is an important factor when accessing online applications like e-commerce, online banking, or e-government and so on. Individuals will find it unacceptable to establish extensive profiles about their daily online activities and tracing their identities unconditionally [20]. Actually it happens when the individuals use their identities as explicit identifiers.

Pseudonymity technology is a technology that allows individuals to reveal or prove information about themselves to others, without revealing their full identity. Pseudonymity is therefore more suitable when accessing online applications. In normal case, a pseudonymous transaction is one that is identified by a pseudonym and it cannot be associated with a particular individual. If a specific piece of additional data is available, then the transaction data can be linked to that party[19].

In fact, the pseudonymous transaction to access services and applications can be followed in a credential-based system with the help of credentials while it is not possible in traditional access control.

Traditional access control adopts the framework of subjects, objects and access rights. While authentication establishes the identities of the subjects (individuals), authorisation provides individuals with certain rights to access objects (services and applications). Recently, the term credential-based access control is used for systems that base access control on any kind of digital credential [21]. Digital credentials are a convenient way to ensure that a user possesses particular access rights in a system. Most modern distributed access control systems apply the ideas of cryptographically protected credentials. Based on how credentials are used, distributed access control may be grouped into two categories[11]:

• Identity- oriented approach : One common use of access control credentials is to bind the name of a subject with access rights. The idea is that once the name of a requester is proved by a reliable authentication mechanism, access control credentials with the matched name can then be used to make access decisions. Standards exist for the binding from a public key to a name. Pretty Good Privacy (PGP) and X.509 Public Key Infrastructure (PKIX) are the two most widely used today.

• Key-oriented approach: Another possible use of access control credentials is to directly bind a public key with authorizations, thus avoiding the use of names completely. With this approach, the public key in an access control credential effectively identifies a subject, There are currently two major access control systems based on the key-oriented approach: Simple Public Key Infrastructure (SPKI) and KeyNote.

In this paper, a modern credentials access control framework is proposed that integrates identity and key oriented approaches in one novel approach. With this approach, the cryptographic pseudonyms in

an access control credentials effectively identifies a subjects(e.g. users and organisations). The user share his cryptographic pseudonym with cryptographic pseudonym of an organization that provide a service to generate encryption shared secret key. If possession of the corresponding decryption shared secret key can be proved a service accepting this credential can be anonymously sure of the identity of the subject and make access decision simply by examining the access rights in the credential.

1.1 Our Contributions

The underlying cryptographic primitive called a Pseudonymous identification scheme based on strong assumptions of combined public key cryptosystem is described. In such scheme every user registered with a trust third party (TTP) is assigned two Pseudo-identities, one is a private identity and other is a public identity and the sum of both identities constitute a global identity(unitary identity) of a user. The Pseudonymous identification scheme offer two tier of pseudonymity and capture the desired requirements for designing a pseudonymous certificate. The pseudonymous certificate uniquely identifies by public identity (public pseudonym) and it contains no binding between a public pseudonym and the name of it's holder.

A modern credential access control framework is described. It is built with respect to a new proposed pseudonymous digital signature (PDS) between a prover (user) and a verifier (organization) during communication session to make access control decision. The framework captures security properties for organisations and users both in terms of credential unforgeability and non-transferability.

The rest of this paper is organized as follows: The next section describes the pseudonymous identification scheme. Subsequently, Section 3 explains the whole modern credential access control architecture including pseudonymous digital signature. Sections 4 and 5 describe the notion of modern credentials and the system security analysis respectively. Finally, the paper concludes in Section 6.

2. Cryptographic Pseudonymous Identification Scheme

In a digital world, individuals may use a distinct pseudonym for access to every system they use on a regular basis, thereby preventing the linking of transactional data accumulated in each system. A pseudonymous transaction is one that can only be linked to a pseudonym but not to a particular individual. With respect to the way in which they are created and their relation to the pseudonym user's identity the pseudonyms can be classified into [18]:

• Self-generated Pseudonym: Generated by the owner. Only the owner can translate the pseudonym into a real-world identity.

• Reference Pseudonym: A pseudonym that can be translated into a real-world identity with the help of a reference list that is typically kept by a trusted third party. E.g. Social security numbers.

• Cryptographic Pseudonym: Generated by applying a cryptographic function to identifying data.

A digital pseudonym could be realized as a public key to test digital signatures where the holder of the pseudonym can prove holdership by forming a digital signature which is created using the corresponding private key. Pseudonymous identification scheme explained here offers a two-tier of cryptographic pseudonyms and it based on the following assumptions:

Asumption1. *for any trusted center with an integrated RSA modulus* $n \in Z_n^* : n = p \cdot q \cdot f$ *(p, q and f are three prime numbers with approximately of k-bits length each) and the related integrated Euler's totient function* $\phi(n)$ *=(p-1)(q-1)(f-1), maching public and secret keys can be generated using the public algorithm* $(pk, sk) \xleftarrow{R} K_g(1^k)$ *,where* $\exists\, g \in Z_n^*$ *and the following conditions must be hold:*

$$\phi(n)^{\phi(n)} \equiv 1 \bmod n \text{ and } g^{\phi(n)} \equiv 1 \bmod n \qquad (1)$$

Assumption2 . *If there exist a random secret integer* $r \xleftarrow{R} Z_{\phi(n)}$, where r : 2 < r < ϕ *(n), then the related public integer* $d \in Z_{\phi(n)}$ *and d=* ϕ *(n)-r. The sum of public and secret integers r , d should always be equal to value of* ϕ *(n).*

With respect to above assumptions every user registered with certification authority (CA) will obtains pseudonymous certificate uniquely identified by *public integer d* as a cryptographic public pseudonym, while the *secret integer r* considered as a cryptographic private pseudonym. The sum of public and private pseudonyms combine a global user pseudonym. We assume that no two user registered with a trusted third party have the same public or private pseudonyms .

3. New Modern Credential Access Control Framework

For centralised, closed systems the traditional process of access control is used. It employ basic mechanisms (username and password) for identifying legitimate users before granting services by providers. This authorisation mechanism is simple and works well in relatively small and closed systems. In open, distributed settings, the traditional approach to access control is inadequate. In a large-scale system such as the internet, the set of users is not known a priori. Furthermore, subjects and resources often belong to different security domains administered by different organisations. In decentralised settings, the traditional approach to access control is replaced by the process of trust establishment (or trust management) [22]. This approach bases authorisation decisions on digital credentials.

For building trust in our framework , a trusted third party (TTP) issues access pseudonymous certificates (i.e. credentials) to authorize access to services provided by an organization. An access certificate is signed with the trusted authority's secret key and access control decision made upon completing verification phase of pseudonymous digital signature (PDS). A user or organization holding an access certificate can't freely delegate its access rights to other users or organizations(credential non-transferability). An important contribution of this credential-based system is allowing the authentication and access control to be performed in a single step. Figure 1, shows the architecture of modern credential access control system.

3.1 Parameter Generation

let G be a finite cyclic group, and let *g* be the generator of prime order *n* in *G* , a trusted authority (CA) generates an *integrated RSA modulus* $n \in Z_n^*$ (chooses L_n = 2048 bits or above) and the related *Euler's totient function* $\phi(n)$. After computing values of n and $\phi(n)$ a trusted authority chooses a generator $g \xleftarrow{R} G^*$, then checks if $\phi(n)$ and generator *g* are satisfying the conditions (1). If they do then it considers *(n,* $\phi(n)$ *, g)* as a system wide parameters.

3.2 Access Certificates based Multitask Cryptographic unique Pseudonym

As it is known, the access control systems focuses on authorisation rather than user authentication in most business to customer e-commerce and other applications on the internet. For privacy and security reasons customers prefer to remain anonymous and untraceable. There are situations where it is desirable for certain transactions to be unambiguously linked[12]. In an electronic cash scheme, for example, all withdrawals of a particular user should be capable of being linked to that user's bank account. To capable with various kinds of anonymous online transactions the mechanism of the pseudonymous access certificate is proposed to provide authorisation services relying on the players (e.g. users and organisations) multitask cryptographic unique pseudonyms in a diversified and distributed environment. A pseudonymous certificates for the players are issued by the trusted authority in the following manner:

(i) Every player p_i registered with a trusted authority is granted a random public number $d_i \xleftarrow{R} Z_{\phi(n)}$, where d_i : 2 < d_i < ϕ *(n),* and d_i is selected as a public identity (public pseudonym) of a player denoted by ID_p .

(ii) The trusted authority computes user 's secret exponent r_i = ϕ (n)- d_i , where r_i is selected as a private identity(secret pseudonym) denoted by ID_v . A player's unitary identity denoted by ID_u *:*

$$ID_u = ID_p + ID_v = \phi(n)$$

(iii) The registered player upon completion of registration phase will obtains a pseudonymous certificate uniquely identified by multi-task public pseudonym ID_p with no linking to the player name. Basically, it is similar to the X.509 attribute certificate except that the holder field is replaced by a multi-task public unique pseudonym field and a new field, named peudonymity revocable, is added to indicate that a third party can unveil a subject's identity under well specified Conditions. The certificate is signed by issuer's private key (TTP).

(iv) The certificate intended for multi-show with different purposes in the sense that several uses of the same pseudonymous certificate by the same player cannot be linked together. In addition to pseudonymous certificate the player grants a secret 3-tuple($\phi(n)$, r_i ,*g*).

3.3 Pseudonymous Digital Signature(PDS)

Consider a pseudonym system to involve three types of player: subjects, issuers and verifiers. We refer to issuers and verifiers, collectively, as `organisations'. The system security parameters $\phi(n)$ and g are owned by players and it is assumed that the player has ability to assign for himself whenever needed a new unitary pseudonymous identity with respect to value :

$$ID_{u,i} = k \cdot \phi(n) \quad (2)$$

Where *k*-random integer number.

The corresponding new secret pseudonym then calculated by formula:

$$r_{i,new} = k \cdot \phi(n) - d_i \quad (3)$$

where the multi-task unique pseudonym d_i for any player in the system remains unchangeable. For the purpose of untraceability and unforgeability it is proposed that for every session the player has ability to select a different secret pseudonym to generate different signature values .

3.3.1 Signing Algorithm

Consider the protocol is a session between a user U wants to access some service with an organization O.

Sign(r_U , d_O ,g ,m)**.** This algorithm takes as input a signer's secret pseudonym(user) r_U , a destination's public pseudonym(organization) d_O , generator *g*, and a message $m \in \{0,1\}^*$ and proceeds as follow:

(i) The user computes the sum of his secret pseudonym r_U and organization's public pseudonym d_O and generates what we called *encryption shared secret key* S_j :

$$S_j = g^{r_U + d_O} \bmod n \quad (4)$$

(ii) A user then encrypts hash function of the message *m* by S_j and sends it to organization that provides such service :

$$S_U(m) = H(m).\ S_j \quad (5)$$

3.3.2 Verification Algorithm

Verify(S_U *(m),* r_O , g , d_U). The verification algorithm takes as input signer's public pseudonym d_U , a verifier's secret pseudonym r_O ,generator *g*, and a purported signature S_U *(m),* and proceeds as follow :

(iii) The organization computes the sum of its secret pseudonym r_O and user's public pseudonym d_U , then generates *a decryption shared secret key* V_j :

$$V_j = g^{r_O + d_U} \bmod n \quad (6)$$

(iv) The organization decrypts the signature using V_j :

$$H(m) = S_U \cdot V_j \bmod n \quad (7)$$

The organization generates hash function for the message *m* and compares it to decrypted one . If the generated hash code for the message *m* equal to decrypted one the signature is accepted and the organization ensured that the signer belongs to trusted anonymous user from the same trusted domain, then the user is granted access to the intended service.

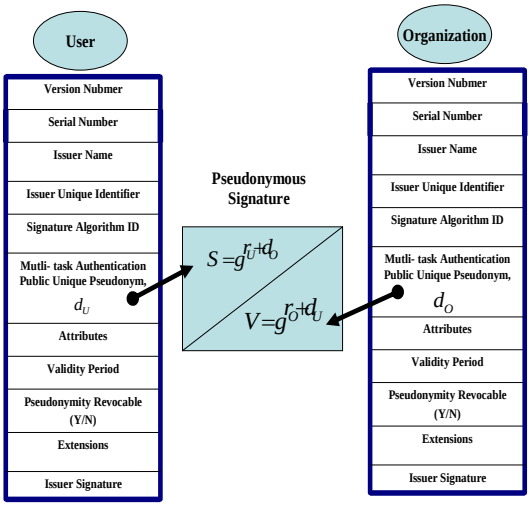

Fig.1 Pseudonymous certificates for access control framework

4. Modern Credential Concept

The pseudonymous access certificates that has been issued under a proposed pseudonymous identification scheme , and it is shown to a verifier under the Pseudonymous Digital Signature(PDS) to make access control decision we called a *Modern Credentials*. Different actions involving the same modern credential can be linked, on the basis of the unique pseudonymous identifier, but they cannot be traced to the modern credential holder. In addition, even multitask public unique pseudonyms are used by the same user and verifier many times , there are always a different encryption/decryption shared secret keys could be available for each communication session.

5. Security Analysis

5.1 Correctness

The correctness of the Pseudonymous Digital Signature(PDS) and furthermore the reliability of access control framework can be provided starting from equation (7) as follow :

$$H(m) = S_U \cdot V_j \bmod n$$

$$= H(m) \cdot g^{r_U + d_O} \cdot g^{r_O + d_U} \bmod n$$

$$= H(m) \cdot g^{r_O} \cdot g^{r_U} \cdot g^{d_O} \cdot g^{d_U} \bmod n$$

$$= H(m) \cdot g^{r_O + d_O} \cdot g^{r_U + d_U} \bmod n$$

$$= H(m) \cdot g^{2\phi(n)} \bmod n$$

$$= H(m)$$

The result ensure that only intended organization able to make verification to the signature and grants access rights to signer.

5.2 Unforgeability and Untraceability

The credential access control approach is secure if the underlying pseudonymous signature scheme is secure against various an adversary attacks. In order for an adversary to forge a successful PDS signature, he must therefore learn the secret pseudonym of the verifier. From the hardness condition, we know that the adversary cannot compute secret pseudonym for legitimate player in the system from publicly available information. Furthermore, the shared secret keys, which are not publicly known in the activities, are different for every task, and the player's multitask public pseudonym is could be anonymously linkable but can't be traced to it is holder. In this way, the properties of unforgeability and untraceability are achieved.

As a comparison to other existing signatures in the literature like RSA and DSA algorithms, the PDS algorithm seems very secure. In addition , the encryption/ decryption operations very fast in spite of the large key size.

5.3 Pseudonymity Revocation

In our access control system the major pseudonymity revocation refers to the possibility to discover the secret pseudonym of a player. The system supports two kinds of pseudonymity revocation :

- *Public pseudonymity revocation*, where the Player's pseudonymous certificate with the related multitask public pseudonym are revoked by a trusted authority to issue new one.
- *Private pseudonymity revocation*, is made by the player itself whenever needed. It is performed by assigning a new unitary identity with respect to equation(2), then a new secret pseudonym calculated by deducing the value of unique public pseudonym from the value of new unitary identity according to equation(3). The public pseudonym in this revocation mechanism remains unchangeable.

6. Conclusion and Future Work

In this paper a new access control framework for open distributed systems has been developed. Fast and secure pseudonymous digital signature(PDS) based on pseudonymous identification scheme is proposed to support pseudonymity and enhance the scalability of access control systems. The access control scheme assures that the user receives the required service with his privacy protected from the service provider. The system offers the higher degree of protection against credential sharing, i.e. the only intended destination able to make anonymous verification and prove the signer's pseudonymity. The system is suitable for applications in open environments, such as e-commerce ,online banking, or e-government and so on.

References

[1] R.L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp 120-126, February 1978.

[2] T. ElGamal, "A public-key cryptosystem and signature scheme based on discrete logarithms," In Crypto '84, volume 196 of LNCS, pp. 10–18, Berlin, Springer-Verlag, 1985

[3] Dan Boneh and Matthew Franklin. ," Efficient Generation of Shared RSA Keys," Journal of the ACM, Vol. 48, No. 4, July 2001.

[4] Gilboa N,"Two party RSA key generation," In *Advances in Cryptology—Crypto '99*. Lecture Notes in Computer Science, vol. 1666. Springer-Verlag, New York, pp. 116–129,1999

[5] Aleksandra Nenadiæ, Ning Zhang, Barry Cheetham, Carole Goble," RSA-based Certified Delivery of E-Goods Using Verifiable and Recoverable Signature Encryption," Journal of Universal Computer Science, vol. 11, no. 1 (2005), 175-192

[6] D. Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, 1985.

[7] J. Camenisch and A. Lysyanskaya. An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In *EUROCRYPT 2001, LNCS 2045*, pages 93–118, 2001.

[8] C. Farkas, G. Ziegler, A. Meretei, and A. Lorincz. Anonymity and Accountability in Self-organising Electronic Communities. In Proceedings of ACM Workshop on Privacy in Electronic Society, pages81–90, 2002.

[9] J. Camenisch and A. Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In *CRYPTO 2002, LNCS 2442*, pages 61–76, 2002.

[10] David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms; Communications of the ACM 24/2 (1981) 84-88

[11] Walt Teh-Ming Yao, Trust Management for Widely Distributed Systems, Ph.d thesis, February 10th, 2003.

[12]A. Pashalidis and C.J. Mitchell, A Security Model for Anonymous Credential Systems, Proceedings of the 3rd Working Conference on Privacy and Anonymity in Networked and Distributed Systems (I-NetSec'04), Kluwer Academic Publishers, pages 183-199, Toulouse, France, August 2004.

[13] I.B. Damgard. Payment systems and credential mechanisms with provable security against abuse by individuals. In S. Goldwasser, editor, *Advances in Cryptology | CRYPTO '88: Proceedings*, number 403 in Lecture Notes in Computer Science, pages 328-335. Springer Verlag, 1990.

[14]S. Brands. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, 2000.

[15] Y. Tao and X. Xiao. Personalized Privacy Preservation. In *Proc. of ACM SIGMOD*, pages 229–240, 2006.

[16] S. Chow, C. Boyd, and J. Gonzalez. Security-mediated certificateless cryptography. In *PKC 2006*, volume 3958 of *Lecture Notes in Computer Science*, pages 508-524. Springer-Verlag, 2006.

[17] Oliver Jorns, Gerald Quirchmayr, Oliver Jung," A Privacy Enhancing Mechanism based on Pseudonyms for Identity Protection in Location-Based Services". Australian Computer Society, Vol. 68, pages 133-142.

[18] NIKLAS AUERBACH. Anonymous Digital Identity in e-Government. Ph.d thesis, June 2004.

[19] Richard Au, Harikrishna Vasanta, Kim Kwang Raymond Choo, Mark Looi. A User Centric Anonymous Authorisation Framework in Ecommerce Environment. ICEC'04, Sixth International Conference on Electronic Commerce, ACM, pages 138-147.

[20] B. Friedman, P.H. Khan, and D.C. Howe. Trust Online. In Communications of the ACM, volume 43, pages 34–40, 2000.

[21] Pierangela Samarati. Enriching Access Control to Support Credential-Based Specification. In Sigrid E. Schubert, Bernd Reusch, and Norbert Jesse, editors, Informatik bewegt: Informatik 2002 - 32. Jahrestagung der Gesellschaft f¨ur Informatik e.V. (GI), volume 19 of Lecture Notes in Informatics, pages 114–119. K¨ollen, Bonn, 2002.

[22] Matt Blaze, Joan Feigenbaum, and John Keromyzis. The Role of Trust Management in Distributed Systems Security. In Jan Vitek and Christian D. Jensen, editors, Secure Internet Programming, volume 1603 of Lecture Notes in Computer Science, pages 185–210. Springer, Berlin, 1999.

F**aiz ahmad** received the B.E. and M.E. degrees in Automation, from Russia in 1997. He received the M.E. degree in computer science and engineering from Pune Univ. in 2004. Since 2005 he is a Ph.D candidate at Bharati Vidyapeeth University. His research interest cryptography and information's security .

Rajesh Jalnekar received the B.E. , M.E. and Ph.D degrees in Electronic and telecommunication engineering from Univ. of Pune. His research interest network security and signal processing . he is working as dean academic development at VIT Pune.