AN APPROACH TO REVOKE BLACKLISTED ANONYMOUS CREDENTIAL USERS THROUGH TTP

1H. Jayasree, Assoc. Prof., Dept. of IT, ATRI, Uppal, Hyderabad, Email: jayahsree@yahoo.com
2Dr. A. Damodaram, Prof. of CSE Dept & Director – Academic Audit Cell, JNTUH, Hyderabad, Email: damodarama@rediff.com

ABSTRACT

Many of us use the Internet on a daily basis for purposes ranging from accessing information to electronic commerce and e-banking to interactions with government bodies. This requires that transactions are securely authenticated, and that we protect privacy by not revealing more about ourselves than necessary. Anonymous credentials promise to address both of these seemingly opposing requirements at the same time. Anonymous authentication can give users the ability to misbehave since there is no fear of retribution. To tackle such misbehaving users several schemes have been proposed that strike different tradeoffs between privacy and accountability. In this paper, we significantly make an attempt to generalize the basic form of revocation amounting to “revoke anybody on the blacklist” immediately through our proposed scheme. Depending on the type of misbehaving action we also consider revocation based on the threshold value of number of negative credits of a user.

Keywords
Pseudonym, Anonymous Credentials, Certification Authority, Blacklist, Revocation

1. INTRODUCTION

As information becomes increasingly accessible, protecting the privacy of individuals becomes a more challenging task. To solve this problem, an application that allows the individual to control the dissemination of personal information is needed. An anonymous credential system (also called pseudonym system), introduced by Chaum[10], is the best known idea for such a system. An anonymous credential system consists of users and organizations. Organizations know the users only by pseudonyms. Different pseudonyms of the same user cannot be linked. Yet, an organization can issue a credential to a pseudonym, and the corresponding user can prove possession of this credential to another organization.
(who knows hereby a different pseudonym), without revealing anything more than the fact that she owns such a credential. Credentials can be for unlimited use (these are called multiple-show credentials) and for one-time use (these are called one-show credentials). Possession of a multi-show credential can be demonstrated an arbitrary number of times; these demonstrations cannot be linked to each other. Pseudonym systems were introduced by Chaum as a way of allowing a user to work effectively but anonymously with multiple organizations. He suggests that each organization may know a user by a different pseudonym or nym. These nyms are unlinked: two organizations cannot combine their databases to build up a dossier on the user. Nonetheless a user can obtain a credential from one organization using one of his nyms and demonstrate possession of the credential to another organization without revealing his first nym to the second organization. For example: Bob may get a credential asserting his good health from his doctor who knows him by one nym and show this to his insurance company who knows him by another nym.

2. RELATED WORK

Anonymous credential systems permit the users to authenticate themselves in a privacy-preserving way. An anonymous credential system is the best means of providing privacy for users. A significant amount of research is available in the literature of about developing the anonymous credential system [1]. Chaum was the first person to propose privacy-enhancing cryptographic protocols that minimize the amount of personal data disclosed on a network. His work put forth the principles of anonymous credentials [8, 10, and 11]. He introduced the pseudonym systems. These concepts have in common that some party issue a digital signatures where the message signed includes information about the user (i.e., attributes). The concept of blind signatures was introduced by Chaum [9] to be able to protect the privacy of users in applications such as electronic payment systems. Two different sets of protocols, one from David Chaum [9], and one from Stefan Brands [12], have the strongest privacy protection of any developed payment system—they use sophisticated cryptographic protocols to guarantee that the payer’s privacy is not compromised by the payment protocol even against a colluding bank and payee.

Patrick P Tsang et al --- in [4] (BLAC) motivated the need for anonymous credential systems that support anonymous blacklisting and subjective judging without relying on trusted third parties that are capable of deanonymizing (or linking) users. They provide the first cryptographic construction that simultaneously provides anonymous blacklisting, subjective judging, and eliminates the reliance on trusted third parties capable of revoking the privacy of users.

Man Ho Au et al in --- [5] makes the first significant effort to extend TTP-free anonymous revocation with subjective blacklisting to more general behavior-based policies. Their approach gives SPs a rich language to characterize acceptable and unacceptable uses of their services while supporting anonymous revocation. They showed that such a scheme can be realized by extending BLAC, which unlike PEREA does not require misbehaviors to be
identified within a “revocation window.” They refer their construction BLACR (BLacklistable Anonymous Credentials with Reputation). While improving on the linear time complexity (in the size of the blacklist) for authentications in BLAC and BLACR remains an open and important problem, through a quantitative analysis they show that BLACR can indeed be used in practical settings to support reputation-based anonymous revocation.

3. OUR APPROACH

3.1 Requirements

Following are the requirements for any Revocation Scheme taken from [7]:

(R1: Anonymity) The revocation scheme must preserve the anonymity of the anonymous certificate holder. The fact that the certificate is to be revoked is not the justification to reveal the holder’s real-world identity, to release information that may later lead to his identification, or to allow linkage of his certificates.

(R2: Authorisation) The revocation scheme must be actionable by authorized parties upon receipt of proper authorization tokens only, in order to prevent a denial-of service type attack.

(R3: Accountability) The revocation scheme must provide accountability of the parties actions. By accountability, we mean the scheme enables an authorized entity, such as a Legal Authority, to collect, collate and interpret evidence of involved parties’ actions from an audit trail. In this way, each party has motivation to comply with the protocol, since any deviation may be detected and attributed to them. In order for parties to be held accountable, the evidence presented must have the property of non-repudiation.

(R4: Non-repudiation) In order to hold each party accountable for their actions, the scheme must have the property of non-repudiation, i.e. no party can falsely deny his/her own actions or claim that such actions were performed by another, when presented with the evidence of the actions.

(R5: Notification) As a courtesy to the User, the scheme is to provide the User with notification of revocation. This notification may take the form of a Revocation Acknowledgement to the User in the case that the User requested the revocation or a Revocation Notice to the User in the case that the revocation was invoked by the CA or a Legal Authority.

The Proposed work provides a better revocation approach by:

• Including Trustee between Initiator & Certification Authority to increase anonymity. Trustee is included as an interface between Initiator and CA to ensure trust for both initiator and CA. To reduce the burden on CA, we propose to include TTP.
• To use a different Communicating Protocol. We propose to include RADIUS protocol for authenticated and authorized communication between the parties.
• To implement a trimming technique at the Initiator to disclose minimum fields to the Responder. We apply a blind signature method to implement trimming technique.
• Automatic Revocation (blocking) with respect to network and individual. Our proposal ensures automatic revocation.
3.2 Including Trustee

- Trustee generates pseudonym ‘P’ for user ‘u’.
- Trustee obtains a Certificate from CA on behalf of user.
- Trustee acts as a trusted third party between Initiator and CA.
- CA can cross verify with Trustee upon any misbehavior.
- Trustee is included to increase anonymity and unlink ability of user even by CA.

3.3 Communication Protocol


RADIUS is a networking protocol that provides a centralized Authentication, Authorization, and Accounting management for computers to connect and use a network service. RADIUS serves 3 functions:

- To authenticate users or devices before granting they access to a network.
- To authorize those users or devices for certain network services and
- To account for usage of those services.

3.4 Trimming Technique

In a given set of 30 attributes in a user Anonymous Credentials, assume we need to disclose only 5 attributes. To achieve this, technique used is to blindly sign all other 25 attributes (encrypt with public key of sender) so that the intended 5 attributes only will be visible to the receiver. Hence we trim all unwanted attributes at the initiator itself, so that only attributes to be disclosed will be delivered to receiver. This will increase the speed of delivery, since packet load is reduced.

3.5 Automatic Revocation

Revocation of the user is done by the CA in many scenarios.

User can himself make request to revoke, because 1) the private key is compromised or 2) certificate has expired or 3) user wishes to update his private key. In all the above cases upon request by the user, CA revokes the user and the revoked certificates are kept in the certificate revocation list (CRL).

On complaint by a responder, CA revokes the user, to verify the misbehavior of the user and block any such misbehavior by proper cross verification with the help of Trustee. CA invalidates the pseudonym assigned to the blacklisted user and his anonymous certificate is made invalid. CA maintains a list of all blacklisted pseudonyms. Pseudonyms are basically assigned either for one-time use or for multi-use. If a pseudonym is issued for one –time show automatically it will be blocked if the user uses the same pseudonym again. We are including a lifetime for a pseudonym so that a pseudonym can be automatically blocked once the lifetime expires.
4. Model

Fig1: our reference model

4.1 Attributes
We denote an attribute $A_i$ as the tuple consisting of name, value and type that is $A_i = \{n_i, v_i, t_i\}$. The name must be unique within its scope (e.g., a credential structure), which will allow us to refer to the attribute using that name and the scope. The value refers to the content of the attribute, which is encoded as defined by the type.

4.2 Credentials
Credentials can have two options either one-show or multi-show credentials. We distinguish attributes contained in credentials depending on which party knows the value of an attribute. More concretely, the owner of a credential always knows all attribute values but the issuer or the verifier might not be aware of certain values. During the issuance of a credential we distinguish two sets of attributes as the issuer might know a value, or the value might be completely hidden to him. Let us denote these sets of attributes by $A_k$ and $A_h$, respectively. When creating a proof of possession of credentials, the user has the possibility to reveal only a selected set of attributes. Therefore, we distinguish the revealed attributes, which will be learned by the verifier, from the unrevealed attributes. Credentials are always issued to a recipient authenticated with a pseudonym, which ensures that the user's master secret gets "blindly" embedded into the credential.

Attributes

```
{  
  Attribute { FirstName, known, type:string }  
  Attribute { LastName, known, type:string }  
  Attribute { Sex, known, type:string }  
  Attribute { Nationality, known, type:string }  
  Attribute { CivilStatus, known, type:enum }  
```
{Marriage, Never Married, Widowed, Legally Separated, Divorced}
Attribute { PassportNumber, known, type:string }
Attribute { DateofBirth, known, type:date1900s }
Attribute{ Profession, known, type:enum} {Student, Scientist, Doctor, Engineer, Lawyer, Teacher, others}
Attribute{ AcademicDegree, known, type:enum} {B.Tech, M.Tech, Ph.D, MCA, M.Sc, M.S., M.D., others}
Attribute{MinorityStatus, known, type:enum} {Blind, Deaf, Hear impaired, Phys impaired, None}
AttributeOrder { FirstName, LastName, Sex, Nationality, CivilStatus, PassportNumber, DateofBirth, Profession, AcademicDegree, Minoritystatus}

4.3 Encoding freshness into credentials
In certain applications, typically those involving short-lived credentials, verifiers need to validate the freshness of credentials [6]. Thus, some indication of freshness has to be encoded into the credentials by their issuers. However this indication constitutes an additional attribute and its value helps determine the type of the credential. If the indication of freshness is unique for each credential (such as a serial number, a counter value, or a nonce), then it becomes trivial for organizations to link pseudonyms, as every credential will have its own, unique, type. It is thus desirable, from a privacy perspective, that the indication of freshness is shared among as many credentials as possible. One possible freshness indication is a timestamp generated using a universal clock, with a sufficiently coarse accuracy. We thus henceforth assume that one of the attributes that present in all credentials is such a timestamp. A question that arises in this context is who decides whether or not a credential has expired. If it is the issuer, it seems more appropriate for the timestamp to indicate the time of expiry. If, on the other hand, it is the verifier, then it makes more sense for the timestamp to indicate the time of issue. Since the latter alternative enables verifiers to have individual policies with respect expiry of credentials, in the sequel we assume that the timestamp indicates the time of credential issue.

5. ARCHITECTURE
5.1 Procedure
At, the TTP we provide an option for the user exclusively to obtain a digital certificate for a general purpose, and a digital certificate for anonymous purpose. Initiator generates his public/private key pair and makes a request to the TTP asking him to issue a pseudonym for anonymous communication. In the request to obtain a Digital Certificate from CA through TTP, the user has to enter some mandatory fields about his profile, say for example, passport number. If a user’s request is for a Digital Certificate for anonymous Communication purpose, then the TTP generates a pseudonym, and on behalf of user TTP makes a request to CA to issue Digital Certificate. And at the same time, TTP maintains in its database, the user details and the pseudonym assigned to him, stands as the basic source, to give details to the
responder upon request to find the details of misbehavior user. TTP obtains a Digital Certificate from CA issued in the name of pseudonym, which is then forwarded to user by TTP.

The notation used is summarized as follows.

\((pk_{i,b}, sk_{i,b})\) is a pair of public and private keys for a user \(U_i\) certified by a CA \(A_b\). \((pk_b, sk_b)\) with a single subscript is a pair of public and private keys owned by a CA \(A_b\). \(Ek(x)\) denotes the cipher text of a data item \(x\) encrypted with a key \(k\). \(h(x)\) is a one-way hash function with the following properties: for any \(x\), it is easy to compute \(h(x)\); given \(h(x)\), it is difficult to compute \(x\); and given \(x\), it is difficult to find \(x'\) (\(x \neq x'\)) such that \(h(x) = h(x')\).

\(C_{i,b}\) is an anonymous certificate of a user \(U_i\) issued by a CA \(A_b\), denoted as \(C_{i,b} = (A_b, P_{i,b}, pk_{i,b}, e_{i,b}, td_{i,b}, S_{i,b})\) where \(S_{i,b} = E_{sk_b}(h(A_b, P_{i,b}, pk_{i,b}, e_{i,b}, td_{i,b}))\) is \(A_b\)'s Signature, and \(P_{i,b}, pk_{i,b}, e_{i,b}, td_{i,b}\) are \(U_i\)'s pseudonym, public key, certificate expiration time, and certificate creation time date stamp, respectively. \(C_{i,b}^R\) is a real-identity certificate of a user \(U_i\) issued by a CA \(A_b\). The only difference between \(C_{i,b}\) and \(C_{i,b}^R\) is that the former uses \(U_i\)'s real identity rather than her pseudonym. We assume that every user knows the public keys of all CAs. For each certificate issued by each individual CA, that CA stores a number of items required for accountability, real identity trace back and revocation.

After receiving the Digital Certificate the user now prepares his profile containing a list of attributes as mentioned above, encrypts them with his public key (blind signature), appends his pseudonym, attaches the Digital Certificate, and requests the CA to sign. Since the pseudonym was already issued by CA, CA blindly signs the document. Initiator has to first authenticate himself to the responder. Now, when a user wants to communicate to a responder and needs to submit some personal data to a responder, he now applies the trimming technique (a blind signature on the remaining items) and discloses only the data needed by the responder. For added security, this data can be encrypted with the public key of the responder, so that the harm of a man in the middle attack can be prevented. Along with the document, he also attaches his Digital Certificate received from CA.

5.2 Anonymous Revocation

When a responder wants to blacklist a user associated with a session, it inserts the ticket for that session in to the blacklist maintained by him. The ticket can be considered as the data structure which holds the details like, username, pseudonym, date and time of logon. It maintains the list of users already blacklisted, containing the details of the ticket of that session and the associated pseudonym of the user, received as the credential from the user. The database also maintains number of positive (merits) and negative (demerits) credits of a user. The user is immediately blocked by the responder in two scenarios: 1) a severe misbehaves, causing harm to the responder or 2) the number of negative points of a user exceeds the threshold value.
When an initiator first authenticates anonymously using his credentials, the responder first cross verifies in the blacklist. If the user is already blacklisted then the responder either blocks the user or allows the user according to the policy mentioned above. If the user misbehaves for example if he defaces the web pages of the responder which may lead to loss of data of the responder or the users negative credits crosses the threshold value( 5) then the responder decides to block the user. If so, then the responder files a complaint to CA and request to revoke the corresponding user. Our scheme is efficient enough to immediately block the user, for any further transactions with the responder. The responder can retrieve the details of the blocked user from TTP. And further the user is also blacklisted at the CA and TTP, so that user will not repeat anonymous misbehave with another responder. Since we use a distributed TTP, the data of blacklisted users will be maintained at every TTP.

Any anonymous authentication scheme will be vulnerable to Sybil attack if users can get new credentials after their issued credential is blacklisted. With our approach if once a user is revoked due to misbehave then at any cost he will not be able to use his anonymous credentials anymore. Because a user cannot reproduce him newly in order to obtain a new pseudonym, may be from a new TTP. Hence our proposal is free from Sybil-attacks.

6. CONCLUSION

Several anonymous authentication schemes with varying degrees of accountable anonymity have been proposed in the past. In our work we focus on the paradigm for anonymous credential systems that support anonymous blacklisting and subjective blacklisting with the support of TTP.

REFERENCES


Authors

Dr Avula Damodaram obtained his B.Tech. Degree in CSE in 1989, M.Tech. in CSE in 1995 and Ph.D in Computer Science in 2000 all from JNTUH, Hyderabad. His areas of interest are Computer Networks, Software Engineering, Data Mining and Image Processing. He has successfully guided 6 Ph.D. and 2 MS Scholars apart from myriad M.Tech projects. He is currently guiding 9 scholars for Ph.D and 1 scholar for MS. He is on the editorial board of 2 International Journals and a number of Course materials. He has organized as many as 30 Workshops, Short Term Courses and other Refresher and Orientation programmes. He has published 35 well researched papers in national and International journals. He has also presented 45 papers at different National and International conferences. On the basis of his scholarly achievements and other multifarious services, He was honored with the award of DISTINGUISHED ACADAMICIAN by Pentagram Research Centre, India, in January 2010.

H. Jayasree obtained her B.E. in CSE from Bangalore University and M.Tech. in CSE from JNTUH, Hyderabad in 2001 and 2006 respectively. She is currently a Research Scholar of CSE JNTUH, Hyderabad. She is working as Associate Professor, for Aurora’s Technological and Research Institute and has 10yrs of teaching experience in various colleges of Hyderabad and Bangalore. Areas of research interest include Computer Networks and Network Security.