Pseudonym-based Anonymous PKI with Short Group Signature

Sokjoon Lee, Byung-Ho Chung
Information Security Research Division, ETRI
{junny, cbh}@etri.re.kr

Abstract*-Nowadays, Internet becomes an essential element in our life. We can make use of numerous on-line services through Internet such as information search, on-line shopping, e-mail service, etc. But, while getting the benefits of Internet service and e-commerce, invasion of our privacy frequently occurs because on-line service providers tend to request excessive or unnecessary personal information. So, there have been some researches on anonymous authentication, which means that user can authenticate herself, not revealing her identity or personal information. But, most of the researches are not somewhat applicable to current authentication infrastructure. In this paper, we propose a pseudonym-based anonymous PKI with short group signature. Using our proposed scheme, we can provide anonymity with conditional traceability to current PKI.*

Keywords: anonymous authentication, PKI, pseudonym, group signature

1. Introduction

Nowadays, Internet becomes an essential element in our life. We can search or share information, send e-mail, purchase some products, and make use of other numerous on-line services through Internet. But, while getting the benefits of Internet service, invasion of our privacy frequently occurs because on-line service providers tend to request excessive or unnecessary personal information such as social identification number, cell phone number, birthday, hobby, etc. Moreover, due to their carelessness, there have been many incidents of personal information leakage.

There are some ideas to solve these privacy issues. In one idea among them, the private information is securely located in the trusted third party (TTP) and partial information that on-line service providers necessarily need is provided to them. But, this idea has a limitation that user's privacy relies on the TTP totally. What on-line service providers really need to know is not the user's private information but her privilege to get the service.

There have been many researches on anonymous authentication, which means that user can authenticate herself, not revealing her identity or personal information. These researches are based on pseudonym systems[4,6,7] or anonymous signature schemes such as group signature[1,5], ring signature[10] and traceable signature[11]. Most of them focus on anonymous authentication in the theoretical sense and are not somewhat applicable to real world. For example, it is difficult to apply these studies to current authentication infrastructures such as PKI.

In this paper, we propose a pseudonym-based anonymous PKI with short group signature. Using our proposed scheme, we can provide anonymity with conditional traceability to current PKI.

2. Background

Anonymous authentication is the technology that a user can be authenticated and/or authorized while a certain level of anonymity is still satisfied. It can be accomplished using pseudonym or anonymous signature. Pseudonym systems allow users to interact with multiple organizations anonymously. Generally, the pseudonyms cannot be linked, and attacker or third party cannot tell if transactions of one user are from same user.

The first pseudonym system was introduced by Chaum[4] for a user to prove her identity anonymously with multiple organizations. There have been many researches[6,7] that make enhancements to the first one. But, pseudonym systems are not used in widespread today. Some of them use very complex zero-knowledge interactive protocol and this aspect makes it difficult to construct practical solutions.

2.1. Group Signature

Anonymous signature[1,5,10,11] is another technology to provide anonymous authentication. Group signature is first introduced by Chaum and van Heyst[5]. Any member of the group can sign messages, and verifier can know only correctness of the signature. The verifier can not know any information of the signer.

Group manager is the most important entity in

group signature scheme. Group manager can trace the signature, or reveal identity of the signer. There are variable group signature schemes, but most of them have the following procedures.

- ***Key Generation (or Setup)***: the generation process of group public key and group secret key from some security parameters
- ***Join***: a protocol between the group manager and a user, by which the user can become a group manager. Group member gets her group member secret key in this protocol.
- ***Sign***: an algorithm by which any group member can compute group signature for given message using her secret key
- ***Verify***: an algorithm by which the validity of any group signature is verified, given group public key. In this algorithm, verifier cannot know signer's identity.
- ***Open***: an algorithm by which group manager open signer's identity, given a signed message.

Group signatures must the basic requirements as follows.

- ***Unforgeability***: only group members can sign messages on behalf of their group.
- ***Anonymity (or Signer Ambiguity)***: Given a signed message, no one except group manager can identify the actual signer.
- ***Unlinkability***: Given two or more signed messages, no one can determine if the signatures are generated by same signer.
- ***Exculpability***: no member of the group (including even group manager) can produce the signatures on behalf of other members.
- ***Traceability***: the group manager can open user's identity from a signature.

2.2. Short Group Signature

Group Signature is studied for protecting signer's privacy. There are some applications that require the properties of group signatures. They need not only user's privacy but also short length of the signature.

With these requirements, Boneh et al[1] proposed short group signature. In this scheme, for the generation of group signature, the authors used zero-knowledge protocol for SDH (Strong Diffie-Hellman) problem. For open procedure by group manager, signer's pseudonym is hided by linear encryption based on decisional linear assumption.

There are four entities for short group signature.

- ***Group Manager***: entity who can open signer's identity and revoke the signer. This entity opens the group public key $gpk = (g_1, g_2, h, v, h, w)$. The private key of the group manager is $gmsk = (\xi_1, \xi_2)$.
- ***Private Key Issuer***: entity who issues user's private key pair. The issuer has its private key γ.
- ***User***: entity who joins the group to be a member of the group. She can sign messages anonymously with her private key pair $gsk[i] = (A_i, x_i)$, issued by private key issuer.
- ***Verifier***: entity who verifies the signature and checks if the singer is a member of the group.

The short group signature also has five procedures, described in section 2.1. (see [1] for detailed description and proof)

- ***Key Generation***: group manager generates key pairs and opens the group public key. The group manager and private key issuer select keys such that $u^{\xi_1} = v^{\xi_2} = h$, $\gamma \in_R \mathbf{Z}_p^*$, $w = g_2^{\gamma}$.
- ***Join***: private key issuer or user randomly selects $x_i \in_R \mathbf{Z}_p^*$ and the issuer gives $gsk[i] = (A_i, x_i)$ to the user, while $A_i = g_1^{1/(\gamma + x_i)} \in \mathbf{G}_1$ was computed by the issuer.
- ***Sign***: user can sign the message M as $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$, where T_1, T_2, T_3 are linear encryptions for blinding A_i, $s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2}$ are the values for zero-knowledge proof of (A_i, x_i), and c is the hash value of M and other values for simulating random oracle.
- ***Verify***: given the message M and signature $\tilde{\sigma} = (\tilde{T}_1, \tilde{T}_2, \tilde{T}_3, \tilde{c}, \tilde{s}_\alpha, \tilde{s}_\beta, \tilde{s}_x, \tilde{s}_{\delta_1}, \tilde{s}_{\delta_2})$, the verifier computes $\tilde{R}_1$, $\tilde{R}_2$, $\tilde{R}_3$, $\tilde{R}_4$, $\tilde{R}_5$ such as $\tilde{R}_1 \leftarrow u^{\tilde{s}_\alpha} \cdot \tilde{T}_1^{-\tilde{c}}$, $\tilde{R}_2 \leftarrow v^{\tilde{s}_\beta} \cdot \tilde{T}_2^{-\tilde{c}}$, $\tilde{R}_3 \leftarrow e(\tilde{T}_3, g_2)^{\tilde{s}_x} \cdot e(h, w)^{-\tilde{s}_\alpha - \tilde{s}_\beta} \cdot e(h, g_2)^{-\tilde{s}_{\delta_1} - \tilde{s}_{\delta_2}} \cdot (e(\tilde{T}_3, w) / e(g_1, g_2))^{\tilde{c}}$, $\tilde{R}_4 \leftarrow \tilde{T}_1^{\tilde{s}_x} \cdot u^{-\tilde{s}_{\delta_1}}$, $\tilde{R}_5 \leftarrow \tilde{T}_2^{\tilde{s}_x} \cdot v^{-\tilde{s}_{\delta_2}}$. The verifier checks if $\tilde{c}$ is equal to $H(M, \tilde{T}_1, \tilde{T}_2, \tilde{T}_3, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5)$. He accepts if this check succeeds.
- ***Open***: the group manager opens the signer's A_i as $A_i = T_3 / (T_1^{\xi_1} \cdot T_2^{\xi_2})$.

According to the paper, the total signature length of this scheme is 1533 bits or 192 bytes, while the security is approximately the same as a standard 1024 bit RSA signature.

2.3. PKI with Anonymity

X.509[9] public key and attribute certificates are used widely to authenticate users in Internet. X.509 public key certificates bind the public key to the only subject who knows the associated secret key. The certificates contain the identity of the subject. It means that the certificates do not provide anonymity.

X.509 attribute certificates contain user's attributes such as group membership, role, age, etc, which can be basic information for the authorization by service provider. Although attribute certificates are linked with public key certificates, but both certificates can be managed independently. (see [9] for detailed description)

There are two approaches to provide anonymity to X.509 based PKI. First approach[2] is to extend the semantic of X.509 certificates to use anonymous signature schemes. The authors proposed the X.509 certificate infrastructure where the public key is not bound to a single entity but to a concept. The concept would be a single entity in traditional environment, and also would be all group members in group signature. This approach is not applicable where there are group members who have different attributes and service authorization must be achieved according to the attributes.

Second approach[3,8] is to use pseudonym on behalf of the real identity of users. The point is how pseudonym certificates of users are issued anonymously. Generally, this approach cannot provide unlinkability because the transactions of a specific user will be linked with the pseudonym in the certificate.

3. Requirements in the Real World

3.1. (Local) Linkability and Traceability

There are many researches on anonymous authentication for providing user's privacy. But, Most of them deal with the problem in the theoretical sense and are not somewhat applicable to real world.

On the other hand, requirements in the real world are different from those of group signature or pseudonym systems. Most types of anonymous authentication provide unlinkability, but service providers often request 'local linkability'. Local linkability means that a service provider can link multiple signatures of same user while other service provider cannot. They need it for statistics and service strategy about user's class. Of course, it sacrifices user's privacy but absence of even local linkability will make service providers depressed.

Some types of anonymous authentication scheme such as ring signature[10] satisfy untraceability. But it is not desirable due to legal reason or emergency status. In fact, there are many illegal cases such as character defamation in Internet. Untraceable anonymity may incite some people to attempt such crimes. So, we need conditional traceability in the anonymous authentication.

3.2. Service Authorization

Group Signature is a good candidate for anonymous authentication in the real world. But, this scheme cannot provide any information for service authorization. Sometimes, Internet services need user's attribute such as age, job, etc. Examples can be an adult service or head-hunting service.

PKI attribute certificates can be a solution if anonymity is provided. PKI is used widely to authenticate users in Internet, but it is difficult to apply these studies to current authentication infrastructures such as PKI.

4. Proposed Scheme

We can summarize that real world requires anonymous PKI scheme with local linkability and conditional traceability. In this section, we propose pseudonym-based anonymous PKI with short group signature.

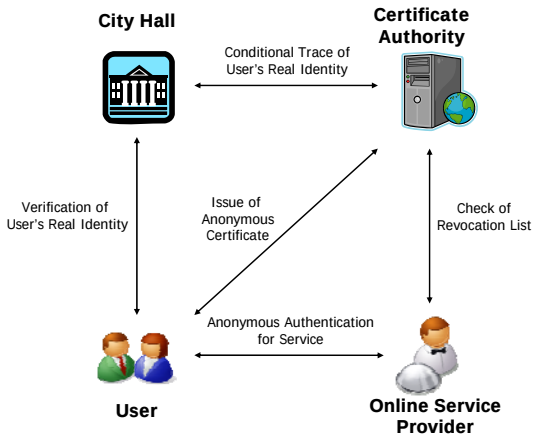
In 2.3, we mentioned two approaches of anonymous PKI. Pseudonym-based PKI cannot provide unlinkability, but we choose this approach because there are requirements of (local) linkability and traceability in the real world. To solve the problem how certificates are issued anonymously, we will use short group signature.

4.1. Architecture of our anonymous PKI

In the conventional PKI, CA issues user's public key certificate with her real identity. But, in anonymous PKI, if CA does so, it can always link the anonymous certificate to real identity, and it will have full traceability. This is very dangerous because it could act like a big brother.

So, we need to divide CA into two parts. One role is to verify user's real identity, and the other is to issue user's pseudonym certificate. There are four entities in our scheme like Figure 1.

Figure 1. Architecture of our anonymous PKI



- ***City Hall (CH)***: the entity who knows and can verify user's real identity. CH issues user's private key of group signature and gives user to one-time credential for issuing pseudonym certificate.
- ***Certificate Authority (CA)***: the entity who issues pseudonym PKI certificate of user. Using CH's credential, CA issues attribute certificate as well as public key certificate.
- ***User***: the entity who gets Internet services from online service providers anonymously using pseudonym certificate.
- ***Online Service Provider (OSP)***: the entity who authenticates user anonymously and authorizes suitable services with reference to attribute certificate.

We assume that CH and CA are independent authority and they will not collude with each other except for a special condition such as the consent of the judicature.

4.2. Issuing Protocol

User proceeds with the following steps to obtain a pseudonym-based certificate.

1) User ↔ City Hall (CH)

User verifies her real identity and attributes by offline visit or conventional PKI. CH acts as private key issuer and group manager in short group signature and issues private key (A_i, x_i). CH issues one-time credential which has a serial number, user's attributes, and signature signed by CH. CH must maintain user's identity and private key in its database.

2) User ↔ Certificate Authority (CA)

User generates and sends a message and its group signature. The message consists of pseudonym certificate issuing request and the one-time credential from CH. The issuing request has message header, time stamp and the user's signature.

The signature should be made with conventional PKI and encrypted using CH's public key in order that user cannot deny the issue event and CA does not know user's real identity. CA sends the issuing request and one-time credential to CH to make sure that this issuing request is valid. CH will verify the signature and inform the result.

After informed, CA acts as a verifier in short group signature. CA checks validity of the signature and the credential. If valid, CA issues pseudonym public key certificate and corresponding attribute certificate for the user. CA must maintain user's initial message, its group signature, and pseudonym. In this step, CH cannot know the user's pseudonym.

4.3. Open of User Identity

The rests of scenarios are similar with conventional PKI except for opening user's identity. When it is necessary to open user's identity, OSP would report the pseudonym of anonymous user to CA. Then CA finds out the user's signature and sends it to CH for request of opening the user. CH can compute A_i from the signature. Using the database, CH will come to know the real identity of the user.

5. Conclusion

In this paper, we propose pseudonym-based PKI using short group signature. In our method, for user's privacy and anonymity, pseudonym certificate is applied. To guarantee user's privacy, she utilize group signature when her certificate is issued by CA.

We are trying to find out the method where each group member gets her own anonymous certificate such that nobody can guess its owner. Also, we are researching how to provide the local linkability in the group signature. With the future works, we can make more practical anonymous authentication scheme. They can lead more privacy-enhancing Internet service.

References

[1] D. Boneh, X. Boyen, H. Shacham, "Short group signatures," CRYPTO '04, volume 3152 of LNCS, pp. 41-55, 2004.

[2] V. Benjumea, S. G. Choi, J. Lopez and M.

Yung, “Anonymity 2.0 – X.509 extensions supporting privacy-friendly authentication,” CANS ’07, pp. 265-281.

[3] V. Benjumea, J. Lopez, J. A. Montenegro, and J. M. Troya, “A First Approach to Provide Anonymity in Attribute Certificates,” PKC 2004, volume 2947 of LNCS, pp. 402-415.

[4] D. Chaum, “Security without identification transaction systems to make Big Brother obsolete,” Communications of the ACM, Vol. 28, No. 10, 1985.

[5] D. Chaum and E. van Heyst, “Group signatures,” EUROCRYPT 1991, volume 547 of LNSC, pp. 257-265.

[6] A. Lysyanskaya, R. L. Rivest, A. Sahai, and Stefan Wolf, “Pseudonym systems,” SAC ’99, pp. 184-199.

[7] J. Camenisch and A. Lysyanskaya, “An efficient system for non-transferable anonymous credentials with optional anonymity revocation,” EUROCRYPT 2001, volume 2045 of LNCS, pp. 93-118.

[8] T. Kwon, J. H. Cheon, Y. Kim, and J. Lee, “Privacy Protection in PKIs: A Separation-of-Authority Approach,” WISA 2006, volume 4298 of LNCS, pp.297-311.

[9] X.509, “Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks,” ITU-T Recommendation X.509, March 2000. Also available at ISO/IEC 9594-8, 2001.

[10] R. Rivest, A. Shamir, Y. Tauman, “How to leak a secret,” ASIACRYPT 2001, volume 2248 of LNCS, pp. 552–565, 2001

[11] A. Kiayias, Y. Tsiounis, M. Yung, “Traceable signatures,” EUROCRYPT 2004. volume 3027 of LNCS, pp. 571–589, 2004