Hybrid-Style Personal Key Management in Ubiquitous Computing

Byoungcheon Lee
Dept. of Information Security, Joongbu University,
101 Daehak-Ro, Chubu-Myeon, Geumsan-Gun, Chungnam, 312-702, Korea
sultan@joongbu.ac.kr

Keywords: Personal Key Management, Hybrid-style, ID-based Cryptography, Certificate-based Cryptography, Bilinear Pairing, Ubiquitous Computing.

Abstract: In ubiquitous computing environment it is common that a user owns and uses multiple computing devices, but managing cryptographic keys in those devices is a complicated matter. If certificate-based cryptography (PKI) is used such that each device has independent certificate, then user has to be involved in multiple certificate issuing processes with certification authorities (CA) and has to keep multiple private keys securely. If a single user certificate is copied and shared in multiple user devices, then a single exposure of private key among multiple devices will destroy the secrecy of every devices. Each device has to have import and export function of private key, which will be a major security weakness that attackers will focus on.
In this paper we propose a user-controlled personal key management scheme using hybrid approach, in which certificate is used to authenticate a user and self-generated ID keys are used to authenticate user's computing devices. In this scheme user operates a personal key management server (PKMS) which has the role of personal key generation center (KGC). It is equipped with user's certified private key as a master key and is used to issue ID private keys to user's computing devices. Users normally use multiple computing devices equipped with different ID keys and enjoy secure communication with others using ID-based cryptography. We show that the proposed hybrid-style personal key management scheme is efficient in many aspects and reduces user's key management load drastically.

1 INTRODUCTION

In ubiquitous computing environment it is common that a user owns and uses multiple computers such as office computer, home computer, notebook, and multiple mobile devices such as smart phone, tablet computer, car computer, wearable computer, etc. Users expect that their devices, even mobile devices, should provide full support of secure communication function with other users and their devices. If a device is lack of secure communication function, it will be used only in limited, non-critical applications.

Since user wants to use their devices for secure communication with other users, each user device has to be equipped with secure communication function. To be used in open networks, using public key cryptography is essential and the public key should be a certified one. Certificate-based cryptography (PKI) is a traditional solution to provide certified key to user. A certification authority (CA) issues a certificate to a user, which is CA's signed document on user's public key and user certification information. A recipient of the certificate accepts the authenticity of user's public key by verifying CA's signature. Private key corresponding to the certificate is generated by the user in user's device and it should be managed securely in user's device.

If certificate-based cryptography is applied to multiple user device scenario, we can consider two possible ways of using certificates in multiple user devices.

1. If each device uses independent certificate, then user has to be involved in multiple certificate issuing processes with CAs and has to manage multiple private keys securely in those devices. For security reason user may have to backup the private keys. If user had lost a device, the corresponding certificate has to be revoked, which should be also managed by the user.
2. If a single certificate is copied and shared in multiple devices of the same user, devices have to have import and export function of private keys, and it will be a major security weakness that attackers will focus on. Moreover, a single exposure of private key among multiple devices will destroy the

secrecy of every devices. If a certificate is issued to a secure hardware device such as smartcard, then exporting the private key from the device is impossible.

For these reasons we think that traditional certificate-based cryptography is not a good solution for multiple user device scenario.

Since device ownership is a personal matter, it is very natural that key management for user devices is controlled by user. For example, if a user bought a new computer or a smart phone, the access password to the system will be set by the user. If a cryptographic key is required to be set into the device for secure communication, it is better to be established by the user in such a way that it is acceptable by others.

In this paper we show that ID-based cryptography can be used together with certificate-based cryptography to provide more efficient user-controlled personal key management rather than all certificate-based implementation. We got the idea of the proposed hybrid-style personal key management scheme from the following observations.

1. We need to separate user authentication and device authentication. It is essential for users to be authenticated in public with a certificate issued by CA, but device authentication is a personal matter and is not very stable, which need to be controlled by the user without depending on other trusted authority.
2. One of the main obstacle of using ID-based cryptography is the key escrow problem that KGC should be fully trusted, but it is hard to be accepted in the real world. But, if it is a matter of personal key management for user devices such that the same user generates ID keys for all these devices and also uses them, trust issue is not a problem anymore and ID-based cryptography can be a good solution.
3. Cryptography based on bilinear pairing can be used to implement both certificate-based and ID-based cryptosystems and they can be made interoperable easily.

Based on these observations we propose a hybrid-style personal key management scheme which is a good combination of certificate-based and ID-based cryptosystems. In this scheme user is authenticated in public by a certificate issued by CA. User operates a personal key management server (PKMS) which has the role of personal key generation center (KGC). It is equipped with user's certified private key as a master key and is used to issue ID private keys to user's computing devices. User is explicitly authenticated with a certificate and user devices are authenticated with self-generated ID keys. If user bought a new device, then he can generate a new ID key using PKMS and install it into the device. Since PKMS and computing devices are in the possession of the same user, all these processes can be executed in highly trusted local communications.

We present that user devices equipped with ID keys provide full secure communication function such as encryption, digital signature, digital envelop, etc, and it is acceptable by others. We also show that this approach is much more efficient than the typical approach of all certificate-based key management.

The rest of the paper is organized as follows. Proposed hybrid-style personal key management system is presented in Section 2 and analyzed in Section 3, respectively. We finally conclude in Section 4.

2 HYBRID-STYLE PERSONAL KEY MANAGEMENT SCHEME

The proposed hybrid-style personal key management scheme has two sub-protocols, certificate issuing protocol and device registration protocol. It can be implemented by using any digital signature scheme, but it can be implemented more efficiently using the pairing-based cryptography.

2.1 Background

Let G_1 be an additive group of prime order q and G_2 be a multiplicative group of order q. Let P denote a generator of G_1. A bilinear pairing is a map $e : G_1 \times G_1 \to G_2$ with the following properties (Boneh & Franklin, 2001; Lee, Boyd, Dawson, Kim, Yang & Yoo, 2004):

1. Bilinearity: $e(aQ_1, bQ_2) = e(Q_1, Q_2)^{ab}$, where $Q_1, Q_2 \in G_1$ and $a, b \in Z_q^*$.
2. Non-degeneracy: $e(P,P) \neq 1$. If P is a generator of G_1, then $e(P,P)$ is a generator of G_2.
3. Computability: There exists an efficient algorithm to compute $e(P,Q)$ for all $P,Q \in G_1$.

We also use the following three hash functions used in ID-based cryptography (Lee, Boyd, Dawson, Kim, Yang & Yoo, 2004).

- $H_1 : \{0,1\}^* \to G_1$ (extract point from arbitrary string, which is used in key generation).
- $H_2 : G_2 \to \{0,1\}^l$, where l is the length of a plaintext message (hash to the message space, which is used in encryption scheme).
- $H_3 : \{0,1\}^* \to Z_q^*$ (hash to the finite field, which is used in signature scheme).

2.2 System Configuration

Before we go into the details, we need to explain some terms used in this paper.

- Certified Key Pair: Assume that user A generates a long-term key pair (s_A, P_A) where $P_A = s_A P$ and then gets a certificate $Cert_A = Sig_{CA}(CI_A, P_A)$ from CA, where CI_A is a certification information of A. Then s_A is a certified private key and P_A is a certified public key.
- ID: In ID-based Cryptography any string can be used as an ID public key. User A is identified with a string A and user's device M is identified with a string M. To identify a device with its ownership we denote it using a dot notation. For example, $A.M = A||M$ denotes a device M which is owned by user A.
- Personal Key Management Server (PKMS): It is owned by a user and is used to issue ID private keys to user's computing devices.
- ID Key Pair: Any string including user ID, device name can be used as an ID public key. PKMS generates the corresponding ID private key and installs it into the device.
- ID Signature: Signature generated by using ID private key, which can be verified using the corresponding ID public key.
- ID Encryption: Encryption using ID public key, which can be decrypted using the corresponding ID private key.

There are 2 entities, CA and user, and user has 2 kinds of user systems, PKMS and user devices.

- Certification authority (CA) issues certificate to users through a certificate issuing protocol following the X.509 and PKIX standards (PKI).
- User has a PKMS and multiple computing devices.
  - PKMS has the role of managing all cryptographic key materials of user. Using PKMS user generates long-term key pair and get a certificate from CA through certificate issuing protocol. Using PKMS user generates ID keys and installs them into user devices through a local device registration process.
  - User's computing devices are equipped with ID keys generated by PKMS under the control of the user. User devices are used by the user for various secure communication purposes.

2.3 Proposed Scheme

Short signature scheme (Boneh, Lynn & Shacham, 2002) is the first signature scheme that is used to issue ID private key in (Boneh & Franklin, 2001) and it can also be used to issue certificate. In the literature there are lots of cryptographic schemes that use BLS-style ID key, thus once BLS-type ID key is set up, it can be used in lots of cryptographic schemes. Here we describe the BLS signature based implementation of the proposed hybrid-style personal key management scheme.

Protocol 1: Certificate Issuing (CA $\rightarrow$ PKMS).

Assume that CA has a master key pair (s_0, P_0) where $P_0 = s_0 P$. User A operates PKMS to generate long-term key pair (s_A, P_A) where $P_A = s_A P$. User identifies himself to CA and requests certificate issuing. CA verifies user's identification according to its business process and issues certificate as $Cert_A = s_0 H_1(CI_A, P_A)$ where CI_A is a certification information of A. User verifies the certificate by

$$e(Cert_A, P) = e(H_1(CI_A, P_A), P_0).$$

Now user has a certificate $Cert_A$ and PKMS is equipped with $Cert_A, (s_A, P_A)$.

Protocol 2: Device Registration (PKMS $\rightarrow$ User device).

If user gets a new device M_i, user operates PKMS to generate ID key. PKMS generates ID public key $Q_{A.M_i} = H_1(A, M_i)$ and computes $D_{A.M_i} = s_A Q_{A.M_i}$ using the certified private key s_A. Here $A.M_i$ denotes that device M_i is owned by the user A. PKMS installs $D_{A.M_i}$ into the device M_i through local communication and deletes it from PKMS. Now device M_i is equipped with $(D_{A.M_i}, Q_{A.M_i})$ and identified as $A.M_i$ by others.

2.4 Secure Communications Using ID Keys

Here we show that the self-generated ID key installed into a user device can be used for secure communication with others in public though it is self-generated by the user. Any cryptographic scheme that uses BLS-type ID key can be used, but as a typical application we show some examples of encryption and signature schemes.

Assume that user A with device $A.M_i$ and user B with device $B.M_j$ try to communicate each other securely. Let A and B have the following key materials.

- User A has a certified key pair (s_A, P_A) with certificate $Cert_A$ and a device $A.M_i$ which is equipped with ID public key $Q_{A.M_i} = H_1(A, M_i)$ and ID private key $D_{A.M_i} = s_A Q_{A.M_i}$.

- User B has a certified key pair (s_B, P_B) with certificate $Cert_B$ and a device $B.M_j$ which is equipped with ID public key $Q_{B.M_j} = H_1(B, M_j)$ and ID private key $D_{B.M_j} = s_B Q_{B.M_j}$.

To start secure communication they need to verify opponent's identity by verifying the certificate. Then they can enjoy secure communication using ID keys installed into the devices.

Encryption (Boneh and Franklin's IBE Scheme). A can send a message M in ciphertext to B using Boneh and Franklin's IBE scheme as follows.

- Encryption: A picks a random $r \in_R Z_q^*$, and computes $g_B = e(Q_{B.M_j}, P_B)$, $U = rP$, $V = M \oplus H_2(g_B^r)$. A sends $C = (U, V)$ to B.
- Decryption: B can decrypt $C = (U, V)$ by

$$V \oplus H_2(e(D_{B.M_j}, U)) \rightarrow M.$$

Note that both $Q_{B.M_j}$ and P_B are used in encryption and $D_{B.M_j}$ is used in decryption.

Digital Signature (Cha & Cheon's Scheme). A can send a signed message M to B using Cha & Cheon's signature scheme as follows.

- Signing: A picks a random $k \in_R Z_q^*$, and computes $U = kQ_{A.M_i}$, $V = (k + H_3(M, U))D_{A.M_i}$. A sends $Sig = (U, V)$ to B.
- Verification: B can verify the signature $Sig = (U, V)$ by

$$e(P, V) \stackrel{?}{=} e(P_A, U)e(P_A, H_3(M, U)Q_{A.M_i}).$$

Note that $D_{A.M_i}$ is used in signing and both $Q_{A.M_i}$ and P_A are used in verification.

Key Agreement (Chen & Kudla's Scheme). (Chen, & Kudla, 2002) proposed a key agreement scheme with separate KGCs, which is the same situation in this paper. A and B randomly choose ephemeral private keys $a, b \in_R Z_q^*$ and compute the corresponding ephemeral public keys, $T_A = aP$ and $T_B = bP$. They exchange the ephemeral public keys and then compute the agreed key as follows.

$A \rightarrow B : T_A$
$A \leftarrow B : T_B$
$A : K_{AB} = e(D_{A.M_i}, T_B) \cdot e(Q_{B.M_j}, aP_B)$
$B : K_{BA} = e(D_{B.M_j}, T_A) \cdot e(Q_{A.M_i}, bP_A)$

We can show that A_{AB} and K_{BA} are same.

In the original ID-based cryptosystems where ID private key is generated by KGC, encryption and signature verification processes require KGC's public key. But, in the above secure communication examples, we have noted that both certified public key of the user and ID public key of the device are used together in encryption and signature verification. Thus, to enjoy secure communication a user device has to get an authentic copy of the certified public key of the opponent. Therefore, the proposed scheme provides more concrete and explicit conviction of the authenticity of opponent in secure communication.

The use of ID private key installed in the device has to be protected with proper level of access control, possibly using human memorable password, such that any other person who occasionally got the device cannot use the ID private key without passing the access control of the device. ID private key can be installed in secure hardware device such that it cannot be exported from the device in any way.

3 ANALYSIS AND DISCUSSION

3.1 Features of the Proposed PKMS Scheme

In this section we summarize the key features of the proposed key management system.

Explicit Authentication of Signer. In traditional ID-based cryptosystems only user's ID and the public key of KGC are used in signature verification, thus it provides only implicit authentication. On the other hand, in the proposed key management system user's device ID and user's certified public key are used together in signature verification. It can be interpreted that verification of an ID signature is equivalent to verifying both the validity of signature on the message and the validity of ID key of the device in a single logical step. Thus a valid ID signature provides explicit authentication of the signer and its validity will be accepted by others.

Full Non-repudiation. An ID private key installed in a device includes user's short signature on ID information using the certified private key. Verification of ID signature requires certified public key of the signer. Though ID key was personally generated by the user, an ID signature provides full non-repudiation evidence that it can be used for any general purpose secure transaction.

Easiness of User Key Management. Although it looks like that user has many keys in many devices, actually user has a single certified key and many device keys derived from it. Since ID private key is generated by PKMS and installed into the device through a local registration process and it will never be exported from the device, user cannot take any extra care of it. Therefore, user can focus all his effort to take good care of the single certified private key.

User doesn't need to backup the ID keys, since he can regenerate them anytime. If user loses the device, ID key is gone, but he can generate the same ID key again. Others who illegally gets the device cannot use the ID private key, if they cannot pass the access control. If user bought a new device, he can register it with a proper name and install ID private key into the device by himself. If user does not need to distinguish device name, he can use the same device name in multiple devices.

In the point of managing others' key, user doesn't need to manage opponent's device key, but only needs to manage the certificate of opponent. Though we are considering multiple user device scenario, the number of keys that user has to manage is not much different from the single device situation.

Validity Period of ID Keys. In traditional ID-based cryptosystems it is hard to set validity period to ID key. To achieve this, ID key was sometimes set including explicit validity period in ID information. But in the proposed scheme ID private key was derived from the certified key of the user and is always used together with it that its validity is highly coupled to the validity of the certified public key. If user has renewed certificate and got a new certified key pair, the ID private keys also have to be renewed using the new certified private key. Thus the device ID keys have the inherent validity period which is equal to that of the certificate.

Same ID Public Key in Certificate Renewal. Certificate has to be renewed periodically using a new key pair and in this case ID keys also have to be renewed. But note that ID public key, for example, $A.M_i$ can remain the same though ID private key has to be changed. Since ID is a kind of persistent information advertised to others, this property is a big advantage of the proposed key management system compared with the traditional certificate-based system. This property is very useful specially for login management where login ID to service should be persistent for long time.

Easy Adaptation/transition. In the proposed key management scheme certificate issuing for user (by CA) and personal key management for user devices (by user) are independent. Existing PKI systems, mainly based on RSA signature, can be used for the proposed scheme without big change with the only condition that user's long-term key should be pairing-based. All ID-based functions such as device key management and secure communication will be implemented in user-side systems. Thus, it is expected that the transition from current PKI-based systems to the proposed hybrid-style key management system can be easy and smooth.

Offline PKMS. PKMS needs to be connected to the Internet only during the certificate issuing stage. Once it acquired the certificate, it can be maintained in offline state or local communication state in personal area network (PAN). Since PKMS is used only for device registration, it can be switched off if device registration is finished. Thus PKMS can be maintained safely against various online attacks.

3.2 Comparison with Chen *et al.*'s Scheme

If we compare our proposal with the PKI-IBE hybrid scheme of Chen *et al.* (Chen, Harrison, Moss, Soldera & Smart, 2002), both schemes use similar hybrid approach of certificate-based and ID-based cryptography, but application scenario is different. Chen *et al.*'s scheme applied the hybrid approach to user authentication in public sector while our proposal is an application to personal key management for multiple user devices in ubiquitous computing environment.

Chen *et al.*'s scheme is not practical in the sense that it requires user's full trust to the KGC. In our proposal PKMS and devices are owned by the same user and personal key management is a highly trusted environment that we don't need to worry about the key escrow problem of the ID-based cryptography. For real world deployment Chen *et al.*'s scheme requires a severe change to the existing PKI mechanism, replacing end CA to KGC, but our proposal does not require big change in PKI.

3.3 Efficiency Analysis

User is using multiple devices with different ID keys, but he only needs to take good care of the certified private key, thus the proposed scheme provides great efficiency in key management. In the proposed system the certified private key is used only for generating ID private keys for user devices, normally not used for everyday secure communications between users, which results that the number of key usage is reduced a lot and key is less exposed to attack. If certificate becomes a stable one and revocation occurs less frequently, then the cost of operating CRL mechanism will be reduced a lot. In this case certificate can be issued with longer validity period.

Finally, we need to compare the efficiency of the proposed hybrid-style personal key management scheme with the more typical approach of using certificates instead of ID keys. In this case user has to take care of the following drawbacks of certificate-based systems.

1. If a user received other's self-generated certificate for user device, then its validity has to be verified before usage, while there is no need of verification in the case of ID public key.
2. To prevent the lost of device private key, user may have to back up the device private keys.
3. If some device or key is lost, the certificate should be revoked and a new certificate should be issued. Thus user's PKMS may have to operate a personal CRL system. Operating a personal CRL system is a big burden in the whole key management system.

Identifying a user device with ID key is more intuitive and easy to use than the traditional certificate-based approach.

3.4 Security Analysis

In the proposed hybrid-style personal key management scheme any standard digital signature scheme can be used for certificate issuing and any ID based key issuing scheme can be used for ID private key generation. In the BLS-based implementation BLS signature scheme is used both for CA to issue certificate to user and for PKMS to generate ID private keys for user devices. Thus any successful forgery of certificate or ID private key will be reduced to the successful forgery of the BLS signature scheme.

4 CONCLUSION

In this paper we considered the ubiquitous computing environment that a user owns and uses multiple computing devices and discussed the difficulty of cryptographic key management. We proposed a hybrid-style personal key management scheme which is a combined use of certificate-based cryptography for user authentication in public domain and ID-based cryptography for personal key management of user devices in private domain. In this proposal user operates a PKMS which is equipped with user's certified key and is used to generate and install ID keys to user devices. We showed that key management is much more efficient in the proposed system than traditional all certificate-based approach and the resulting ID-based cryptosystem provides full non-repudiation function. This kind of hybrid-style key management can be applied to wide range of real world situations where user needs to have multiple certified keys, but wants to reduce the key management load.

Until now ID-based cryptography had been investigated a lot in research community, but rarely applied to the real world. We think this is a very practical proposal of applying ID-based cryptography for personal key management and daily secure communication applications. We expect that it can possibly change the landscape of real world cryptography such that users normally use ID-based cryptography for key management and daily secure communications.

Secure and user-friendly implementation of the proposed key management system, PKMS and user devices, will be a challenging task, which is our continued research focus.

REFERENCES

Boneh, D. & Franklin, M. (2001). Identity-based encryption from the Weil pairing. *Advances in Cryptology – Crypto'2001*, LNCS 2139, pp. 213–229. Springer-Verlag.

Boneh, D., Lynn, B. & Shacham, H. (2002). Short signatures from the Weil pairing. *Advances in Cryptology – Asiacrypt'2001*, LNCS 2248, pp. 514–532, Springer-Verlag.

Cha, J. & Cheon, J. (2003). An Identity-Based Signature from Gap Diffie-Hellman Groups. *Practice and Theory in Public Key Cryptography – PKC'2003*, LNCS 2567, pp. 18–30, Springer-Verlag.

Chen, L., Harrison, K., Moss, A., Soldera, D. & Smart, N.P. (2002). Certification of Public Keys within an Identity Based System. *ISC 2002*, LNCS 2433, pages 322–333, Springer-Verlag.

Chen, L. & Kudla, C. (2002). Identity based key agreement protocols from pairings. *Proceedings of the 16th IEEE Computer Security Foundations Workshop*, pages 219–233, IEEE Computer Society Press.

Lee, B., Boyd, C., Dawson, E., Kim, K., Yang, J. & Yoo, S. (2004). Secure Key Issuing in ID-Based Cryptography. *ACSW Frontiers 2004 - Second Australasian Information Security Workshop 2004*. Volume 26 of Australian Computer Science Communications, pages 66–74. Australian Computer Society.

Public-Key Infrastructure (X.509) (pkix), http://datatracker.ietf.org/wg/pkix/charter/