Classifying the Security Level of User Authentication for Secure Computing

Jong-Whoi Shin

Korea Information Security Agency, Seoul, Korea

Summary
In order to provide more suitable user authentication services for secure computing environments, we classify the level of the user authentication into three security levels. As the security level of user authentication is classified, not only the legacy schemes can be used properly, but also the improved schemes will be introduced for more efficient secure services. In addition to this work, we also propose the improved user authentication schemes using either public key certificate or self-certified public key. At last, these schemes will be reasonable to provide the secure services for secure computing environments.

Key words:
Authentication, security levels, public key certificate, self-certified public key

1. Introduction

As Internet grows, where lots of transactions occur, computing environments is exposed to many threats such as hacking, virus, illegal access, etc. To protect from these threats, it requires much more reliable security services than now. In general, computing environments consist of two elements, user and device. The authentication is the most considerable security property in exchanging information securely between these elements. The center of computing environments is user. User authentication is composed of holder authentication and device authentication. In this paper, we classify the user authentication into three security levels using holder authentication and device authentication.

As the security level of user authentication is classified, not only the legacy schemes can be used properly, but also the improved schemes will be introduced more efficient security services. We also propose the improved user authentication schemes using either the public key certificate or self-certified public key.

The remainder of this paper is as follows. Section 2 describes the classification of user authentication according to the security level. At section 3, we propose the improved user authentication schemes and section 4 is the conclusion of this paper.

Manuscript received October 5, 2007.
Manuscript revised October 27, 2007.

2. Classifying the Security Levels for User Authentication

User authentication can be composed of holder authentication and device authentication as follows.

- **Holder Authentication:** when device authenticates user.
- **Device Authentication:** when device authenticates other device.

In this section, we classify the user authentication into three security levels in terms of holder and device authentication. The purpose of the classification of user authentication is to provide the criterion of authentication and to help risk assessment of authentication system. Table 1 shows level of user authentication.

Table 1 : Level of User Authentication

Level	Description
Level 1	Holder or device authentication is only occurred.
Level 2	Holder authentication and device authentication are simultaneously occurred but the device cannot check if the holder authentication was carried out.
Level 3	Holder authentication and device authentication are simultaneously used and the device can check if the holder authentication was carried out.

At level 1, the case of only holder authentication, for example, when accessing local host computers or simple electronic storages, user can use ID/Password, fingerprint mouse or keyboard. As related schemes, there is Auto-ID [1] that reads and analyzes outer information such as barcode and biometric information. Its task is capturing an external signal from specific object that should be identified, and analyzing it. Biocrypt Portable^{TM} [2] is a module to process biometric information. Fig. 1 shows the use of holder authentication at level 1. The case of only device authentication, for example, when mobile device is used to access remote server or when electronic key is used to open electronic door, certification token or cryptographic module can be used.

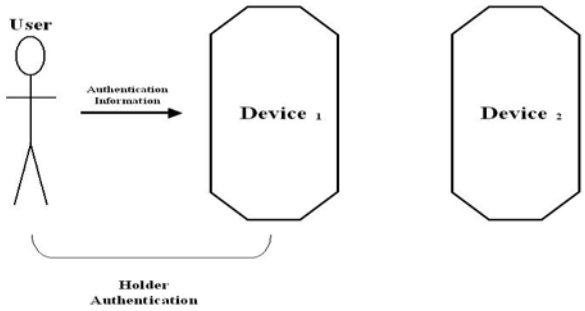

Fig. 1 Level 1- The case of only holder authentication

As related schemes, there is Active Badge [3], a very simple device like a conventional name badge. It can send identification information using infrared transmitter. The signal generated from the badge is transmitted to a sensor through an optical path like a TV remote controller. iButton [4] is the small device armed with cryptographic operation module. Fig. 2 shows the use of device authentication at level 1.

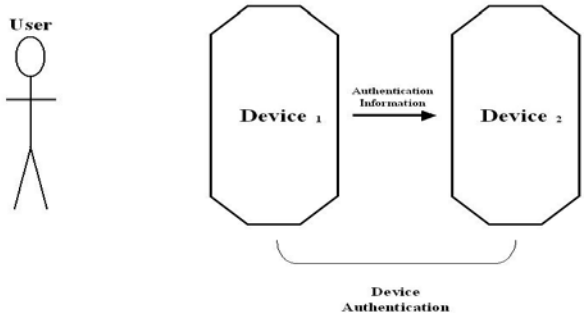

Fig. 2 Level 1-The case of only device authentication

At level 2, as shown in Fig. 3, $Device_1$ authenticates user, and $Device_2$ authenticates $Device_1$ but $Device_2$ does not know that $Device_1$ authenticates user. As related schemes, there is Wearable Key with fingerprint reader that is a part of TouchNet [5]. When it sends the encrypted information to the keyhole, holder is authenticated by identifying key owner using the fingerprint information and device is authenticated by identifying key using the encrypted information transmitted to the keyhole.

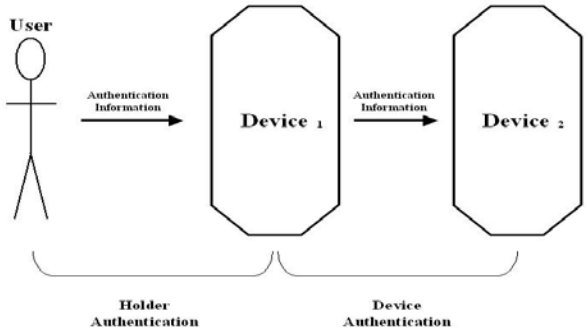

Fig. 3 Level 2-$Device_2$ does not know that holder authentication was carried out

At level 3, as shown in Fig. 4, $Device_2$ authenticates both of $Device_1$ and User. Most of related researches have been fulfilled at level 1 and level 2, but they have security weaknesses compared to level 3.

In recently computing environments, user will have many small devices, so the probability of losing the devices will increase. Especially, in financial area, abnormal use of the lost devices will be a critical problem. Therefore, to implement secure user authentication system, level 3 will be the most desirable. Next section, we propose the improved user authentication schemes to level 3.

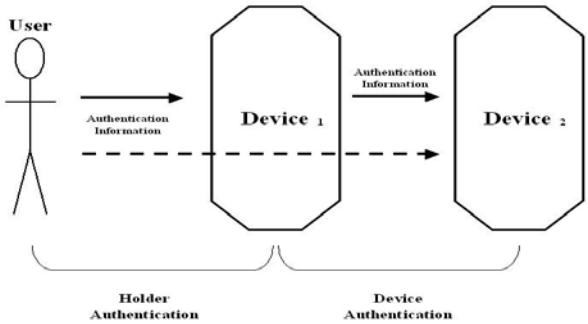

Fig. 4 Level 3-$Device_2$ knows that holder authentication was carried out

3. Our Proposal

We propose the public-key user authentication schemes to level 3. The schemes are the most well-known approach to protect the active attacks [6]. Our proposed schemes are taken account of two types.

3.1 The Scheme using the value of Subject field in Public-key Certificate

In this scheme, we use the value of subject field in public-key certificate. As the value of subject field, we generate the double-hashed value that hashes secret random number R with PIN(Personal Identification Number) such as social security number, user ID and etc. The value is generated by equation (1):

$$H(H(\mathrm{PIN}||R))=H^2(\mathrm{PIN}||R) \quad (1)$$

The PIN generally has a tendency to be easily estimated such as name, phone number, date of birth and address. Since most of the PIN length is short and using only alphanumeric characters, the PIN could be easily obtained by guessing attack. A random number R is 512 bits long and the secret value only known to the user. It is concatenated with a PIN and can be served to increase the complexity. The sequential use of nested hash structure can protect PIN from disclosure. If the user doesn't want to disclose PIN and random number R for ensuring anonymity, the user only sends the intermediate value

Table 2 : Notations in Public-Key Certificate Schme

User	the owner of ubiquitous device
Device1	the ubiquitous device of authenticating User
Device2	the ubiquitous device of authenticating Device1
CA	Certificate Authority
x	user's private key, it is stored in Device1
q	prime number, public value
p	prime number, public value (p-1 is divisible by q)
g	$1 \leq g \leq p-1$, having multiplicative order q, public value
y	user's public key, it is stored in Device1
R	random number, H(x), Device1 can generate it using x
H(•)	hash function

H(PIN||R). We use H^2(PIN||R) as the value of subject field, and use the Schnorr identification protocol [7] for device authentication. Fig. 5 shows the procedure of this scheme. $Device_2$ authenticates both $Device_1$ and User. In the procedure, previously, certificate was generated and saved by Certificate Authority (CA). We summarize the notations used in this section as shown Table 2.

• **Key and The Subject Field value Generation**

1. User selects x, and generates $y = g^{-x} \pmod p$.
2. User generates PIN and R.
3. User generates the value of subject field
   $Subject\ Field\ Value = H(H(PIN||R)) = H^2(PIN||R)$
   and sends it with y to CA through the secure channel such as secure offline or SSL/TLS.
4. CA generates the certificates of y including $H^2(PIN||R)$ in the subject field.
5. CA issues the certificate.

• **$Device_2$ authenticates User**

1. User sends ID and PIN to $Device_1$ through the secure channel such as secure keystroke directly.
2. $Device_1$ generates R
3. $Device_1$ sends [PIN and R] or [H(PIN||R)] to $Device_2$ through the secure channel such as SSL/TLS.
4. $Device_2$ extracts certificate from CA.
5. $Device_2$ extracts the value of subject field from certificate.
6. $Device_2$ generates $H^2(PIN||R)$ by using PIN and R.
7. $Device_2$ compares $H^2(PIN||R)$ with the value of subject field and verifies.
8. $Device_2$ authenticates user.

• **$Device_2$ authenticates $Device_1$ (Using Schnorr authentication)**

1. $Device_1$ sends m to $Device_2$.
   $m = g^r \bmod p,\ 1 \leq r \leq q\text{-}1$
2. $Device_2$ sends e to $Device_1$.
   $1 \leq e \leq 2^t \leq q\ (t \geq 40)$
3. $Device_1$ sends n to $Device_2$.
   $n = xe + r \bmod q$
4. $Device_2$ computes z. $z = g^n y^e \bmod p$
5. $Device_2$ compares z with m and verifies.
6. $Device_2$ authenticates $Device_1$.

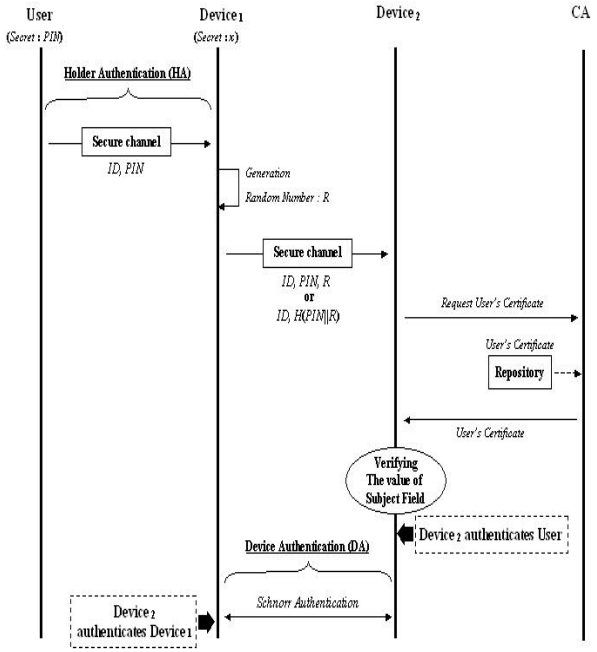

Fig. 5 The procedure of user authentication using public key certificate

In this approach, the PIN and random number R are transmitted to the only reliable device, and they are used for verifying the value of subject field. It enables the user authentication to be more secure and accurate.

3.2 The Scheme using Self-certified Public key

In this scheme, we use self-certified public key [8][9]. It is generated by CA using user's public key and $H^2(PIN||R)$. For example, in small computing environments, if CA is not available, this scheme will provide the advantage. Fig. 6 shows the procedure of this scheme. In the procedure, previously, self-certified public key w is generated and saved in a repository such as $Device_1$'s local storage. We generate the self-certified public key. The value is generated as shown in equation (2):

$$w = (y \oplus H^2(PIN||R))^{ID^{-1}} \pmod n \qquad (2)$$

• **Key Generation**

1. User selects x, and generates $y = g^{-x} \pmod n$.
2. User generates PIN and R.
3. User generates the hashed personal information
   $H(H(PIN||R)) = H^2(PIN||R)$
   and sends it with y to CA through the secure channel such as secure offline and SSL/TLS.
4. CA generates the self-certified public key
   $w = (y \oplus H^2(PIN||R))^{ID^{-1}} \pmod n$
5. CA sends it to $Device_1$ through the secure channel such as secure offline and SSL/TLS.
6. $Device_1$ saves w and y in a repository such as local storage.

Table 3. Notations in Self-Certified Public Key Schme

X	user's private key, it is stored in Device1
Q	prime number
P	prime number
G	public value
Y	user's public key
N	n = p•q, n is public value (Only CA knows p and q)
W	user's self-certified public key
ID	ID is user's identification information (Only CA knows ID-1mod Ø(n))
R	random number, H(x), Device1 can generate it using x
H(•)	hash function

We summarize the notations used in this section as shown Table 3.

• **Device$_2$ authenticates User and Device$_1$**

1. User sends ID and PIN to Device$_1$ through the secure channel such as secure keystroke directly.
2. Device$_1$ generates R.
3. Device$_1$ extracts w from a repository such as Device$_1$'s local storage.
4. Device$_1$ sends [ID, PIN, R, and w] or [ID, H(PIN||R), and w] to Device$_2$ through the secure channel such as SSL/TLS.
5. Device$_2$ generates $y = (w^{ID} (\mathrm{mod}\ n)) \oplus H^2(PIN||R)$.
6. Device$_1$ sends m to Device$_2$. $m = g^r \bmod n$, r is random number
7. Device$_2$ sends e to Device$_1$. e is random number
8. Device$_1$ sends n to Device$_2$. $n = xe + r$
9. Device$_2$ computes z. $z = g^n y^e \bmod n$
10. Device$_2$ compares z with m and authenticates both of Device$_1$ and User.

4. Conclusion

In this paper, we classified the level of the user authentication into three security levels. For more secure user authentication, we proposed the improved user authentication schemes using the public key certificate and self-certified public key in level 3. These schemes will support strong authentication system for secure computing environments. Our approach made two contributions. First, we showed the useful criterion of user authentication for secure computing environments by classifying security levels for user authentication. Second, we showed the improved user authentication schemes using the value of subject field in public-key certificate and self-certified public key in level 3.

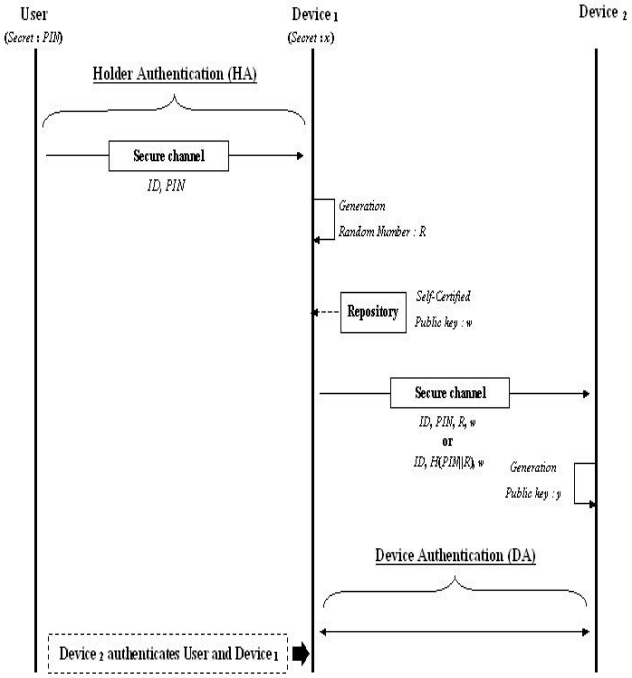

Fig. 6 : The procedure of user authentication using the self-certified public key

References

[1] AIM Homepage – Auto-ID Manufactures, http://www.aimglobal.org, online: 12-Jun-2002.
[2] Bioscrypt : http://www.bioscrypt.com.
[3] Roy Want, Andy Hopper, Veronica Falcao and Jonathan Gibbons. "The Active Badge Location System", ACM Transactions on Information Systems, 10(1): 91-102, Jan 1992.
[4] iButton : http://www.iButton.com.
[5] Nobuyuki Matsushita et. al., "Wearable Key: Device for Personalizing nearby Environment", 4th International Symposium on Wearable Computers, 2000.
[6] Jean-Pierre Hubaux, Levente Buttyan, Srdan Capkun, "The Quest for Security in Mobile Ad Hoc Networks", ACM Symposium on Mobile Ad Hoc Networking and Computing, 2001.
[7] C.P. Schnorr, "Efficient identification and signatures for smart cards", Advances in Cryptology, Proc. of CRYPTO'89, LNCS 435, Springer-Verlag, pp. 239-252.
[8] Seungjoo Kim et. al., "On Saeednia's Key-Exchange Protocols", Proc. of KICS(Korea Institute of Communication Sciences) Conference, Vol. 17/No. 2, Korea, (1998), pp. 1001-1004.
[9] Seungjoo Kim et. al., "Verifiable Self-Certified Public Keys", Proc. of WCC'99, INRIA Workshop on Coding and Cryptograph, 1999, pp. 139-148.

Jong-Whoi Shin received M.S. and Ph.D degrees in Computer Science and Technology from Korea University, South Korea, in 2001 and 2007, respectively. He is working for the Korea Information Security Agency as a principal researcher. His research interests include security for mobile ad hoc wireless networks, ubiquitous sensor networks, security APIs and intrusion tolerant systems.