Applied Mathematics & Information Sciences
An International Journal

A Robust User Authentication Protocol with Anonymity, Deniability, Key Agreement and Efficiency

Chien-Lung Hsu[*] *and Yu-Hao Chuang*

Department of Information Management, Chang Gung University, Tao-Yuan, 333, Taiwan

Received: 11 Feb. 2011; Revised 8 Jun. 2012; Accepted 12 Oct. 2012
Published online: 1 Jan. 2013

Abstract: An authentication protocol allows on-line service providers to validate the identity or legitimacy of a logging user. Once passing the verification, an authorized user can obtain useful and valuable resource or services from the service provider through Internet conveniently. However, most the current authentication protocols cannot protect user's privacy perfectly. To improve this deficiency, we proposed a robust and efficient authentication protocol attempting to preserve user's privacy entirely and also provide the following properties: i) user anonymity, ii) deniability, iii) key agreement, and iv) efficiency. Moreover, our proposed protocol is non-interactive, which is achieved by reducing the number of message exchanges between users and service provider upon performing the authentication activity. Hence, our proposed protocol is more suitable for current wireless mobile network environments due to only need message exchange once avoiding the channel error rate. Moreover, analysis showed that our proposed protocol can withstand various known kinds of attacks.

Keywords: Authentication, anonymity, deniability, non-interactive, wireless.

1. Introduction

With the distributed nature of computer networks, hosts and user terminals connected into the same network can share information and services with each other. On-line service providers can provide services or resources to multiple users via Internet. Generally, such a service provider will control the security privilege to access the services or resources by using a user identification protocol. A user identification protocol allows the server to assure the identity of the user is as declared and then provides suitable access privilege to him, thereby preventing impersonation. Many studies have focused on this field of user identification [4, 10, 13, 18]. Technically, a user identification protocol requires logging-on to a server with authorized identity, which might be suffered from the following potential threats: (1) obtrusive and untrue requests for information, (2) annoyance by potential information stealers, and (3) traceability of the original information introducers (for instance, when employees are speaking out against the management). It would cause a security drawback that an adversary might obtain sensitive personal information (e.g. user's preferences, shopping patterns, etc.) by analyzing the logging information, the services, or the communications. Therefore, it is desirable that the source of information (for example, user's true identity) is hidden but authorized simultaneously for protecting user's privacy. In general, user authentication protocols without revealing user's identity can be divided into two categories.

(i) ***User authentication protocols with anonymous channel*** [7-8, 17, 19-20]: Such a kind of protocols allows users to login anonymously and to perform user authentication activities with the server. Hence, only the server may know user's identity, others cannot. By this way, the user's sensitive identification is not revealed to outsiders (such as eavesdroppers, malicious adversary, etc.). At present, many papers have been proposed based on the studies of authentication protocols with anonymous channel [17, 19-20]. Such an authentication protocol can allow the users to be authenticated to the server without revealing their identities via Internet. Unfortunately, in such protocols, the server still knows who is communicating with him, and hence it might be insecure against identity disclosure if the server is non-trustworthy or unfriendly.

(ii) ***Anonymous authentication protocols*** [1-3, 7, 9-10, 16, 21]: In such a protocol, it allows all users to prove

[*] Corresponding author: e-mail: clhsu@mail.cgu.edu.tw

their legitimacy to the intended server (or the authenticator) without revealing their identifications via Internet. The requirement is that a member must identify himself to authenticate his membership in one group by using an identity group key. Hence, each member can use his individual group key to perform authentication activities anonymously. In 1991, Chaum and Van Heyst [3] first introduced this new concept of group signature scheme. In such group signature schemes, the trusted group manager predetermines member groups and distributes specially keys to all members of each group. All members can use these keys to anonymously sign messages on behalf of their group without revealing their identities. Thereafter, many related cryptographic protocols to achieve such a security requirement are proposed, such as group authentication protocols, anonymous group identification protocols, group signature schemes, ring signature schemes, and etc [1-3, 7, 9-10, 16, 21]. It is noted that several anonymous authentication protocols allow a user to identify himself as a member of a legal group in a secure and anonymous way [1, 9-10, 16]. However, in such protocols, if the group shrank to one member in the group, the member's identity will be discloser in his next authentication activity. Hence, the anonymity property of these protocols will be compromised and not secure as they claimed. In 2001, Rivest $etal$. proposed a ring signature scheme [14] to allow a member of a group to anonymously sign a message on behalf of this group without revealing his identity. It does not need to prearrange the member groups and no need for procedures setting, changing or distributing specialized key to all members.

From above discussions, it can be seen that an anonymous authentication protocol is to enable a user to identify himself as a member of a legal group in a secure and anonymous way. However, such kinds of user's privacy protection are passive and the logging user cannot assure that his identity does not leak out. When the server is dishonorable and has the ability to detect the logging user's identity by using the following tricks, the user privacy is insecure.

1. **Tracing logging user's actions:** The server can trace the logging user's actions to other on-line service providers. If any logging action is non-anonymity, the user's true identity will be detected.
2. **Acts of swindling:** Considering a scenario that if there are few memberships in a group, the server can seek out the member's identity who is logging-on to the server by colluding with other members.

Once the server detects the logging user's true identity, he can prove it to any third party arbitrarily. That is not an active way to preserve user's privacy.

In this paper, we provide high-grade privacy protections for users and re-analyze the security requirements of an anonymous authentication protocol. In general, the following security requirements are the most essential of an anonymous authentication protocol to authenticate the validity of a logging user in a secure and anonymous way.

AUTHENTICATION: Only the member of a legal group G can be authenticated.

ANONYMITY: If a user is authenticated, he only reveals that he is a member in the group G. However, he reveals nothing if he is not authenticated.

UNLINKABILITY: An individual cannot show separate authentication transactions that have been made.

Note that all above definitions of anonymity are as broad as possible, since the security requirement only needs a member of G can be authenticated. A server may choose to compromise the security by authenticating a logging user who is not a member in the group G. Also, a logging user may choose to forfeit his anonymity by disclosing the identity. For these reasons, we have to assume that the server acts in a way to maintain the security and that a logging user acts to preserve his own anonymity.

The above requirements do not consider that the membership in the group G is likely to increase or to decrease. In addition, members are liable to lose or reveal their keys and not to keep them secret. To address these concerns, the following requirement should be included in an anonymous authentication protocol.

KEY REPLACEMENT: Each member in the group G can replace his authentication key with a new one.

KEY AGREEMENT: Each member in the group G can agree on a key with the server without revealing to eavesdroppers.

DYNAMIC GROUP MEMBERSHIP: Need a trusted third party to add or remove members of G and to confer only with the authenticator to do so.

In order to make membership dynamic in the group G, a trustworthy third party is needed to add or remove members. However, if the third party is non-trustworthy, he can manipulate the set G as he pleases to destroy anonymity. For example, if the third party shrinks G so that only one member in the group G, the member's identity will be discloser during him next authentication activity. To overcome this drawback, Rivest et al. introduced a new concept without the need of third parties to manage the size of a group G that is so called ring signature scheme [14].

All above security requirements of anonymous authentication protocols are passive to protect user' s privacy, that is, once the server resorts to every conceivable means to detect the logging user's identity, the logging user's true identity still may be revealed and further proved to any third party. For addressing this concern, a secure anonymous authentication protocol should also include the following properties to preserve user's privacy actively.

DENIABILITY: The member's identity and authentication activities cannot be proved to any third party by the server. Even if it is proved, the third party cannot be convinced. Hence, the user identity cannot be disclosed to any third party except the intended server.

Based on above discussions, this paper proposes a robust user authentication protocol with the requirement of anonymity, deniability, key agreement, and efficiency. Organization of this paper is sketched as follows. In Section 2, we discuss the security requirements of the proposed

protocol and introduce our proposed protocol. Its security analysis and comparisons of the security properties are given in Section 3. Finally, we give the conclusions.

2. The Proposed Protocol

First of all, we begin to set a legal group G and each member in G has individual public key and the corresponding private key. The proposed protocol allows the intended server to authenticate the legitimacy of a logging member and simultaneously achieve the following security requirements.

AUTHENTICATION: Only the member of G can be authenticated by an intended server.

ANONYMITY: A member can be authenticated to the intended server without revealing sensitive information such as member's true identity.

DENIABILITY: All logging members' identities and authentication activities cannot be proved by the intended server.

KEY AGREEMENT: Each member of G can agree on a key with the intended server without revealing to the eavesdroppers.

KEY REPLACEMENT: Each member of G can replace his authentication key with a new one.

DYNAMIC GROUP MEMBERSHIP: Each member is capable of adding or removing memberships of G without the need of a trusted third party to do so.

EFFICIENCY: Only one message exchange between the user and the intended server for performing authentication activities.

The proposed anonymous authentication protocol consists of three phases: the system initialization, the key generation, and the anonymous deniable authentication. In the system initialization phase, it requires a trusted authority (TA) to determine all system public parameters. In the key generation phase, all public and private keys will be generated. In the anonymous deniable authentication phase, the intended server (or the authenticator) can validate the logging user's legitimacy without revealing logging user's identity. Descriptions of these phases are given below.

System initialization phase

The trusted authority (TA) determines the following system parameters:

(p, q): Two large primes, where q is the divisor of $p-1$;

g: A generator with order q over the multiplicative group Z_p^*;

$H(\cdot)$: A collision-free hash function such as SHA-1 [12] and MD5 [15].

Key generation phase

Every user U_i randomly chooses his private key $X_i \in Z_p^*$ and computes the corresponding public key $Y_i = g^{X_i} \bmod p$. Each user publishes his public key Y_i, while keeps the corresponding private key X_i secret. It is noted that all public keys should be certified by a certification authority (CA) for verifying their authenticity.

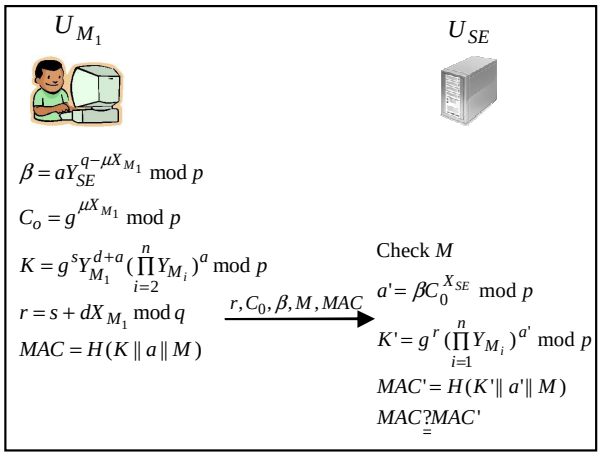

Figure 1 The proposed anonymous authentication protocol.

Anonymous deniable authentication phase

Without loss of generality, let U_{M_1} be a member of the group G and U_{SE} be the intended server. The member U_{M_1} can perform the following steps to deniably prove the legitimacy to the server U_{SE} without disclosing his identity (as depicted in Figure 1):

Step 1. U_{M_1} determines $n-1$ public keys (Y_{M_2}, Y_{M_3}, ..., Y_{M_n}) corresponding to other discretionary members (U_{M_2}, U_{M_3}, ..., U_{M_n}) of G without their agreement. Let M be the authentication message comprising the timestamp T.

Step 2. U_{M_1} randomly chooses $a, \mu, s, d \in Z_p^*$ and computes

$$\beta = aY_{SE}^{q-\mu X_{M_1}} \bmod p, \quad (1)$$

$$C_0 = g^{\mu X_{M_1}} \bmod p, \quad (2)$$

$$K = g^s Y_{M_1}^{d+a} (\prod_{i=2}^{n} Y_{M_i})^a \bmod p, \quad (3)$$

$$r = s + dX_{M_1} \bmod q, \quad (4)$$

$$MAC = H(K \parallel a \parallel M). \quad (5)$$

Then, U_{M_1} sends (r, C_0, β, M, MAC) to U_{SE}.

Step 3. After receiving (r, C_0, β, M, MAC) from U_{M_1}, the server U_{SE} first verifies the validity of M. If it is valid,U_{SE} continues to compute

$$a' = \beta C_0^{X_{SE}} \bmod p, \quad (6)$$

$$K' = g^r (\prod_{i=1}^{n} Y_{M_i})^{a'} \bmod p, \quad (7)$$

$$MAC' = H(K' \parallel a' \parallel M). \quad (8)$$

Finally, U_{SE} verifies if $MAC = MAC'$. If it holds, U_{SE} is convinced of the authentication message (r, C_0, β, M, MAC). Otherwise, U_{SE} rejects it.

Note that if the proposed protocol wants to provide the anonymous channel, the message M can be encrypted with the server U_{SE}'s public key.

3. Security Analysis and Discussions of the Proposed Protocol

We analyze the security of the proposed protocol to show it can achieve the requirements of the anonymous deniable authentication. In the following, we discuss the security considerations for *key agreement*, *authentication*, *user anonymity*, and *deniability*.

Theorem 1. (Considerations for key agreement) The proposed protocol can allow a member and the server to agree on a key.
Proof:

From Eqs. (1), (2), and (5), we can have

$$\begin{aligned} a' &= \beta C_0^{X_{SE}} \\ &= a Y_{SE}^{q-\mu X_{M_1}} (g^{\mu X_{M_1}})^{X_{SE}} \\ &= a \pmod p. \end{aligned} \tag{9}$$

From above equation, it can be seen that a is derived from the private key X_{SE} or X_{M_1}. We can raise both sides of the equation Eq. (4), $r = s + dX_{M_1} \bmod q$, to the exponent with the base g to have

$$g^r = g^s Y_{M_1}^d \bmod p. \tag{10}$$

From above equation and Eq. (2), Eq. (3) can be rewritten as

$$\begin{aligned} K' &= g^s Y_{M_1}^{d+a} (\prod_{i=2}^{n} Y_{M_i})^a \\ &= g^s Y_{M_1}^{d} (\prod_{i=1}^{n} Y_{M_i})^a \\ &= g^r (\prod_{i=1}^{n} Y_{M_i})^a \pmod p. \end{aligned} \tag{11}$$

which implies Eq. (3). It can be seem that the member and the server can compute $K = K'$ individually to agree on a session key.

Q.E.D.

Theorem 2. (Considerations for authentication) The proposed protocol can convince the server of the legitimacy of an individual membership identity.
Proof:

According to **Theorem 1**, it has shown that only the membership and the server can compute a by individual private key X_{M_1} or X_{SE} based on Diffie-Hellman key exchange protocol [5] and to agree on a session key $K = K'$ individually. Then if $MAC = MAC'$, the server can be convinced the legitimacy of the logging user because of the (r, C_0, β, M, MAC) is only generated by one of the members (U_{M_1}, U_{M_2}, ..., U_{M_n}) from a legal group G. Consider a scenario where the adversary attempts to derive the session key K from the intercepted message (r, C_0, β, M, MAC) exchanged between the member and the server. The adversary can consider the following possible methods to plot such an attack.

Case 1:

From Eqs. (3), an adversary can derive K if s, d, and a can first be obtained. However, from Eqs (1), (2), and (4), the adversary will face the DLP assumption to derive s, d, and a respectively.

Case 2:

Under the OWHF assumption, the adversary cannot derive the session key K from the intercepted $MAC = (K \parallel a \parallel M)$.

Q.E.D.

Theorem 3. (Considerations for user anonymity) The server cannot disclose and ensure the identity of an individual with the knowledge of the message (r, C_0, β, M, MAC).
Proof:

According to **Theorem 1**, the message (r, C_0, β, M, MAC) can convince the server that one of the members (U_{M_1}, U_{M_2}, ..., U_{M_n}) of G uses his private key to generate. With the knowledge of (r, C_0, β, M, MAC), the adversary might disclose the member's identity from Eq. (8). From Eq. (8), the adversary must derive the secret parameter d in advance. However, the adversary will face the intractability of solving the DLP and reversing the OHF to derive d from Eq. (5). Hence, the proposed protocol can achieve the user anonymity requirement.

Q.E.D.

Theorem 4. (Considerations for deniability) The server cannot prove the legitimacy of an individual identity to the third party.
Proof:

Consider the scenario that the server attempts to reveal (a', K', r, C_0, β, M, MAC) to convince the third party of the authentication activities. From Eqs. (6), (7), and (8), the third party cannot be convinced of (a', K', r, C_0, β, M, MAC), since the server is able to universally forge it. In addition, the third party with knowing (a', K') can subsequently masquerade as the member to cheat the server below. The third party can let $\overline{a} = \Delta a'$ and $\overline{K} = \Delta K'$ for a random integer Δ. Then, he can use the message (r, C_0, β, M, MAC) to forge a new authentication message ($\overline{r}$, $\overline{C_0}$, $\overline{\beta}$, $\overline{MAC}$), where

$$\begin{aligned} &\overline{\beta} = \Delta\beta = \Delta a Y_{SE}^{\Delta q - \Delta\mu X_{M_1}} \pmod p, \\ &\overline{C_0} = \Delta C_0 = g^{\Delta\mu X_{M_1}} \pmod p, \\ &\overline{K} = \Delta K = g^{\Delta s} Y_{M_1}^{\Delta d + \Delta a} (\prod_{i=2}^{n} Y_{M_i})^{\Delta a} \pmod p, \\ &\overline{r} = \Delta r = \Delta s + \Delta d X_{M_1} \pmod q, \\ &\overline{MAC} = H(\overline{K} \parallel \overline{a} \parallel \overline{M}). \end{aligned}$$

The server will be forced to avoid leaking (a', K'). Therefore, the proposed protocol can achieve the deniability requirement.

Q.E.D.

We compare some security properties of our proposed scheme (HC for short) with various protocols including user identification (UI), anonymous authentication (AA) and deniable authentication (DA) ones in Table 1. In order to facilitate observation and comparison, we divide the current user authentication protocols into three groups: user identification protocols, anonymous authentication protocols, and deniable authentication protocols. From Table 1, it can be seen that both user identification protocols and deniable authentication protocols cannot achieve user anonymity. That is, such kinds of protocols are not able to withstand the identity disclosure attack upon performing user authentication activities. Moreover, only deniable authentication protocols and our proposed protocol have the ability to withstand the malevolent server's attempt to convince the third party of the logging user's identity or authentication activities. In addition, the proposed protocol can insert a timestamp into authorized message to preserve reply attack, but others are implicit.

Table 1 Security properties of the proposed protocols versus previously protocols

	UI [a]	AA [b]	DA [c]	HC
Security (authentication)	O	O	O	O
User anonymity	X	O	X	O
Deniability	X	X	O	O
Key agreement	O	O	O	O
Single registration	O	O	O	O
Prevention of a replay attack	(Implicit)	(Implicit)	(Implicit)	O

[a] Note that user identification protocols we listed only allow achieving user identification without including other extra functions.

[b] Note that anonymous authentication protocols we listed only allow achieving user authentication with anonymity without including other extra functions.

[c] Note that deniable authentication protocols we listed only allow achieving user authentication with deniability without including other extra functions.

4. Conclusion

Information technologies and networks are developed rapidly in recent years and consequently the network security is getting important to log into a network. In general, each user can perform the authentication activities with an authentication centre of a service provider to prove his legitimacy. Basically, the service provider can control the security privilege to access the services or resources by using a user authentication protocol. Once the logging user passes the examination, he can obtain useful and valuable resource or services from the service provider via Internet directly. However, interception of exchange information may endanger the confidentiality of sensitive information of a logging user when he performs authentication activities. To improve this deficiency, we have proposed a robust and efficient authentication protocol in this paper. In our proposed protocol, it can be achieved the following security requirements: i) user anonymity, ii) deniability, iii) key agreement, and iv) efficiency. In addition, for adapting the current mobile wireless communication network environments, the proposed protocol is non-interactive. That is, it only needs one transmission to avoid high channel error rate in mobile wireless networks. Hence, our proposed protocol is suitable for all kinds of communication network environments.

Acknowledgement

We would like to thank anonymous referees for their valuable suggestions. We thank Healthy Aging Research Center (HARC) of Chang Gung University for excellent technical assistance. This work was supported in part by the Chang Gung University Grant UARPD3B0061 and in part by National Science Council under the grant NSC 100-2628-H-182-001-MY3.

References

[1] D. Boneh and M. Franklin, Anonymous authentication with subset queries, *The 6th ACM Conference on Computer and Communications Security (ACM-CCS'99)*, 1999, 113-119.

[2] S. Chang, D.S. Wong, Y. Mu and Z. Zhang, Certificateless threshold ring signature, *Information Sciences*, 2009, 179(20): 3685-3696.

[3] D. Chaum and E. Van-Heyst, Group signature, *Advances in Cryptology-Eurocrypt'91*, Lecture Notes in Computer Science, 1991, 547: 257-265.

[4] Y.C. Chen and L.Y. Yeh, An efficient nonce-based authentication scheme with key agreement, *Applied Mathematics and Computation*, 2005, 169(2): 982-994.

[5] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, 1976, IT-22(6): 644-654.

[6] J.Y. Hwang, A note on an identity-based ring signature scheme with signer verifiability, *Theoretical Computer Science*, 2011, 412(8-10): 796-804.

[7] M.S. Hwang, C.C. Lee and W.P. Yang, An improvement of mobile users authentication in the integration environments, *International Journal of Electronics and Communications*, 2002, 56(5): 293-297.

[8] W.S. Juang, C.L. Lei and C.Y. Chang, Anonymous channel and authentication in wireless communications, *Computer Communications*, 1999, 22(15-16): 1502-1511.
[9] J. Kim, S. Choi, K. Kim and C. Boyd, Anonymous authentication protocol for dynamic groups with power-limited devices, *The 2003 Symposium on Cryptography and Information Security*, 2003.
[10] C.H. Lee, X. Deng and H. Zhu, Design and security analysis of anonymous group identification protocols, *The 5th International Workshop on Practice and Theory in Public Key Cryptosystems (PKC'02)*, 2002, 188-198.
[11] I.C. Lin, M.S. Hwang and L.F. Li, A new remote user authentication scheme for multi-server architecture, *Future Generation Computer Systems*, 2003, 19(1): 13-22.
[12] National Institute of Standards and Technology, FIPS 180-1: Secure Hash Standard, 1995
[13] H. Rhee, J. Kwon and D. Lee, A remote user authentication scheme without using smart cards, *Computer Standard and Interfaces*, 2009, 31: 6-13.
[14] R. Rivest, A. Shamir and Y. Tauman, How to leak a secret, *Advances in Cryptology-Asiacrypt'01*, 2001.
[15] R. Rivest, The MD5 message digest algorithm, *RFC 1321*, 1992.
[16] S. Schechter, T. Parnell and A. Hartemink, Anonymous authentication of membership in dynamic groups, *Financial Cryptography*, Anguilla, February 1999.
[17] T.S. Wu and C.L. Hsu, Efficient user identification scheme with key distribution preserving anonymity for distributed computer networks, *Computers and Security*, 2004, 23(2): 120-125.
[18] T.Y. Wu and Y.M. Tseng, An efficient user authentication and key exchange protocol for mobile client-server environment, *Computer Networks*, 2010, 54(9): 1520-1530.
[19] C.C. Yang, Y.L. Tang, R.C. Wang and H.W. Yang, A secure and efficient authentication protocol for anonymous channel in wireless communications, *Applied Mathematics and Computation*, 2005, 169(2): 1431-1439.
[20] Y. Yang, S. Wang, F. Bao, J. Wang and R. Deng, New efficient user identification and key distribution scheme providing enhanced security, *Computers and Security*, 2004, 23(8): 697-704.
[21] F. Zhou, J. Zhang and J. Xu, Research on anonymous signatures and group signatures, *Computer Communications*, 2008, 31(17): 4199-4205.

Chien-Lung Hsu received a B.S. degree in business administration, an M.S. degree in information management, and a Ph.D. degree in information management from the National Taiwan University of Science and Technology, Taiwan in 1995, 1997, and 2002, respectively. He was an Assistant Professor and an Associate Professor in the Department of Information Management, Chang Gung University (CGU), Taiwan from 2004 to 2007 and from 2007 to 2011, respectively. Currently, he is a Professor in the Department of Information Management, Chang Gung University since 2011. He is also the leader of the Ubiquitous Security and Applications Lab, the director of Chinese Cryptology Information Security Association (CCISA, Taiwan), the chair of Education Promotion Committee of CCISA, the member of Academia-Industry Cooperation Committee of CCISA, the chair of Program of RFID Applications in Logistics Supply Chain Management of CGU, the chair of Program of Information Security with Medical Applications of CGU, the director of Division of Instructional Support of Computer Center of CGU, the researcher of Healthy Aging Research Center (HARC) of CGU, the researcher of Elder Industry Development and Research Center (EIDRC) of CGU, and the senior researcher of Taiwan Information Security Center (TWISC). His current research includes cryptography, information security, wireless sensor network, mobile commerce, digital forensics, vehicular system security, healthcare system and user acceptance, smart home system, and etc.

Yu-Hao Chuang received a Bachelor's degree from Chinese Culture University in 2004, a Master's degree in information management from Chang Gung University in 2006, and a Ph.D. degree in information management from National Central University in 2012, respectively. His current research topics include information security, information systems, social technology, innovation, strategic information systems, and mobile commerce.