http://dx.doi.org/10.5392/IJoC.2012.8.3.079

Attribute based User Authentication for Contents Distribution Environments

Hyejoung Yoo*
Department of Information Security
Sejong Cyber University, Seoul, Korea

ABSTRACT

In digital contents distribution environments, a user authentication is an important security primitive to allow only authenticated user to use right services by checking the validity of membership. For example, in Internet Protocol Television (IPTV) environments, it is required to provide an access control according to the policy of content provider. Remote user authentication and key agreement scheme is used to validate the contents accessibility of a user. We propose a novel user authentication scheme using smart cards providing a secure access to multimedia contents service. Each user is authenticated using a subset of attributes which are issued in the registration phase without revealing individual's identity. Our scheme provides the anonymous authentication and the various permissions according to the combination of attributes which are assigned to each user. In spite of more functionality, the result of performance analysis shows that the computation and communication cost is very low. Using this scheme, the security of contents distribution environments in the client-server model can be significantly improved.

Keywords: *User Authentication, Multimedia Security, IPTV Broadcasting, Contents Distribution, User Anonymity, Smart Cards.*

1. INTRODUCTION

To provide multimedia contents to only legal users, the contents provider should encrypt the contents and give an encryption key used in encrypting content to valid users. To do this, an authenticated key exchange is an important primitive on the Internet. In other words, secure communication channel is essential for multimedia contents distribution environments.

An IPTV system enables a broadcaster to provide multimedia contents to a legal user using the architecture and networking methods of the Internet Protocol Suite over a packer-switched network infrastructure. In 2004, Jiang et al.[9] firstly proposed an authenticated key exchange scheme between a set-top-box and a smart card of user by using a Conditional Access System (CAS). In their scheme, a symmetric encryption scheme, which identical cryptographic keys are used for both decryption and encryption, is used. Hence, if the authentication between the smart card of a legal user and a set-top-box is succeeded, a set-top-box can obtain a decryption key and a user can obtain the contents with decrypting the transferred data from a set-top-box i.e. only a legal user having his/her identity, password, and smart card issued in a registration phase can access contents in previous works.

In an International Telecommunication Union Telecommunication Standardization Sector Focus Group on IPTV meeting was held in Geneva 2006, the requirement of user authentication technologies by using digital certificate, token, smart card, fingerprint, and other multi-factor authentication was opened[10].

In an insecure communication channel, an authenticated key agreement is an important primitive for a secure communication system[11]. As the concern of privacy of user is increased, anonymous authentication procedures have been increasing to provide anonymity of the user. Anonymous user authentication enables a legitimate user to access a remote server without actually revealing the identity of the user in the client-server model. In particular, due to the temper-resistance and convenience issues involved in managing a password file, various anonymous user authentication schemes using smart cards have been proposed in the client-server model[2]-[4],[6]. However, these schemes do not provide a diversity of authentication. That is, the server can check only that the login message is generated by the honest user, who registers his/her identity and password to the authentication server and receives his/her smart card from the server without revealing his/her identity and password. Recently, Frikken et al.[7] and Pirretti et al.[8] proposed attribute based systems.

Frikken et al. proposed an Attribute Based Access Control (ABAC) with user privacy. The goals of ABAC are both (1) to authenticate not the identity of user but attributes in the user's credentials, such as group membership, employment, or credit status, in a privacy-preserving manner and (2) to protect the sensitive credentials and policies. That is, user can pass the authentication only if he/she satisfies the policy and the outsiders do not learn anything about his/her credentials. Moreover, in their scheme, even though honest user learns neither the server's policy structure nor which credentials

* *Corresponding author, Email: hjyoo@sjcu.ac.kr*
Manuscript received May. 29, 2012; revised Jun 25, 2012; accepted Jul 10, 2012

caused the user to obtain access. The merits of this ABAC system are to provide both user anonymity and more diversity of authentication. That is, the target of authentication is not an entity but an attribute, such as authority, position status, or post.

Pirreti et al. proposed attribute based system using Attribute Based Encryption (ABE) primitives. ABE[5], a generalization of Identity-Based Encryption (IBE), allows for a private key of attribute to decrypt to a ciphertext encrypted with an attribute. The construction of policy system using attributes can meet the needs of diversity of authentication and user anonymity. To prove the legitimacy of user in the client-server model, the validity of attributes assigned to each user should be confirmed by the server.

In this paper, we introduce a new reference model for attribute based authentication scheme for contents distribution environments in which permissions are associated with attributes. This diversifies the management of authentication suitable to each user. The basic concept of this scheme originated not with fixed all or nothing proof of legitimacy but with the segmented one. Also, because a user should store securely his/her secret key, it is natural that the secret key corresponding to attributes is stored on smart cards having the temper-resistance property. Moreover, our work provides the diversity of authentication and lowers the costs of communication and computation. We define an attribute-based user authentication scheme for contents distribution environments using smart cards.

Our scheme consists of three phases: registration, login, and authentication phase. In registration phase, the user U_i registers his/her identity and password (ID_i, pw_i) to the authentication server S. U_i securely receives his/her smart card from S containing the authentication information generated by S. In login and authentication phase, U_i sends his/her login messages, generated by U_i to authenticate his/her attributes using his/her smart card and (ID_i, pw_i), to S. Then S tests the validity of U_i's login messages and unknown user's attributes with his/her secret key x_S and responds the reply message. Through the authentication, S can check the validity of (ID_i, pw_i) of U_i possessing his/her smart card in the past schemes considering only the entity authentication using smart cards, S can check only the validity of authentication message without the knowledge of (ID_i, pw_i) in the anonymous user authentication schemes using smart cards. In our scheme, S checks only the validity of attributes without knowledge of (ID_i, pw_i) and U_i can pass the login and authentication phase with authenticating his/her attributes from S. Also, U_i generates the login message with the secret values corresponding to attributes are stored on smart cards having the temper-resistance property and S can obtain the information of not (ID_i, pw_i) but attributes from the login message.

This paper describes a practical framework of authentication scheme to multimedia contents distribution environments and analyzes the security and performance of our scheme. This results show that the proposed scheme is secure and efficient in the client-server model.

2. NOTIONS

We provide the notations in the proposed model. Table 1 summarizes the notations throughout this paper.

Table 1. Notations

Notations	Meaning
p	an l-bit prime number
G	a group of order p
$h(\cdot)$	a one-way function from {0,1}* to {0,1}[1]
$\mathcal{H}(\cdot)$	a full-domain hash function from {0,1}* into G
$\oplus$	an Exclusive-OR operation
$\|$	a string concatenation operator
U_i	a legitimate user
S	a remote authentication server
ID_i, pw_i	an identifier of U_i, a password of U_i
$x_S \in G$	a master secret key of S
ΔT	a valid time interval for transmission delay
$\rightarrow, \dashrightarrow$	an unauthenticated channel, a secure channel

3. ATTRIBUTE BASED USER AUTHENTICATION USING SMART CARDS

We propose an attribute based user authentication scheme using smart cards and prove the security of our scheme.

3.1 Proposed Scheme

As illustrated in the following figures, our scheme consists of three phase: registration, login, and authentication phase. Suppose that a_i $(i = 1, 2, \cdots, n)$ is an attribute chosen by the server and let $S_A = \{a_1, a_2, \cdots, a_n\}$. The server S randomly generates a secret key $x_S \in G$, where G is a group of the order p. In registration phase, the server identifies user U_i and then issues a smart card to each identified user. Unless the user loses his/her card or forgets the password, the registration phase is executed only once for each user. To login the system, the user inserts the smart card into a card reader and then inputs his/her password. The smart card computes the authentication message and sends it to the server. When the server receives the authentication message, it determines whether the authentication is successful or not.

Registration Phase: A user U_i registers his/her ID ID_i and password pw_i to the authentication server S. S identifies user U_i and chooses a set $A_i = \{a_{i,1}, a_{i,2}, \cdots, a_{i,t} | a_{i,j} \in S_A\}$ of t attributes for U_i and securely saves the authentication information in the U_i's smart card as follows:

(1) U_i chooses his/her ID ID_i and password pw_i and sends (ID_i, pw_i) to S securely.
(2) On receiving the values (ID_i, pw_i), S chooses a set $A_i = \{a_{i,1}, a_{i,2}, \cdots, a_{i,t} | a_{i,j} \in S_A\}$ of t attributes for U_i and computes $V = h(x_S) \oplus h(pw_i)$, $I = h(x_S) \oplus h(ID_i \oplus pw_i)$, and $y_{i,j} = h(a_{i,j} \oplus x_S) \oplus h(x_S)$ $(j = 1,2, \cdots, t)$ and let $Y_i = [y_{i,1}, y_{i,2}, \cdots, y_{i,t}]$.
(3) A smart card containing $(V, I, Y_i, h(\cdot), h_1(\cdot), A_i, p)$ is

issued by S to U_i securely.

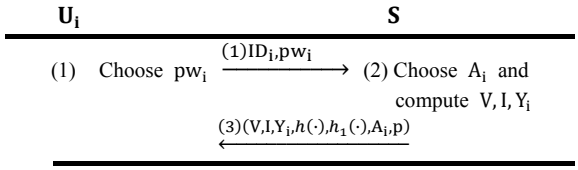

Fig.1. Registration Phase

Login Phase: A user U_i inserts his/her smart card and inputs password pw_i and k values of attributes a_{i,j_e} $(1 \le e \le k)$ in an input device. U_i's smart card then computes the following authentication information and sends login message $(\{a_{i,j_1}, a_{i,j_2}, \cdots, a_{i,j_k}\}, T, C_1, C_2, C_3)$ to the authentication server S.

(1) Compute and check if $V \oplus h(pw_i) \oplus h(ID_i \oplus pw_i) \stackrel{?}{=} I$. If it holds, the smart card goes to Step (2). Otherwise, the smart card aborts.
(2) Compute $X_{j_e} = y_{i,j_e} \oplus V \oplus h(pw_i)$ $(1 \le e \le k)$ and $X = \prod_{e=1}^{k} X_{j_e}$.
(3) Choose random values $r, r' \in \mathbb{Z}_p^*$ and compute $C_1 = (X \| X^{r'} \| T)^r$, $C_2 = h_1(x_S) \oplus r$ and $C_3 = X^{r'}$, where h_1 is a one-way function from $\mathbb{Z}_p^*$ to $\{0,1\}^l$ and T is the current timestamp of the smart card.

Authentication Phase: Upon receiving the login message from U_i's smart card, the authentication server S performs the following operations at time T', where ΔT is a valid time interval for transmission delay.

(4) If $|T - T'| \ge \Delta T$, S rejects the login request.
(5) Check if the form of a_{i,j_e} $(1 \le e \le k)$ is correct. If it is valid, S executes Step (7). Otherwise, S rejects this request.
(6) Compute $r'' = C_2 \oplus h(x_S)$ and $Z = \prod_{e=1}^{k} h(a_{i,j_e} \oplus x_S)$.
(7) Check if $(Z \| C_3 \| T)^{r''} \stackrel{?}{=} C_1$. If the condition is hold, S accepts the login request and goes the next step. Otherwise, the login request is rejected.
(8) To authenticate with U_i, S chooses $s \in \mathbb{Z}_p^*$, and computes $C_4 = (Z \| C_5)^{r''+1}$ and $C_5 = X^s$, and then returns C_4 and C_5 to the U_i's smart card.
(9) Upon receiving C_4 and C_5, the smart card checks if $(W \| C_5)^{r+1} \stackrel{?}{=} C_4$, where $W = V \oplus h(pw_i)$.

If it holds, U_i's smart card believes that the responding party is S and mutual authentication between U_i and S is completed. Also, U_i and S can get the session key $K = X^{rs}$.

3.2 Security

We now turn to proving security of our system. The proposed scheme can withstand replay, impersonation, and off-line password guessing attack. Moreover, it is forward-secure and provides user anonymity as below. Here, it is assumed that attacker A has full control over the network but cannot corrupt the user smart card.

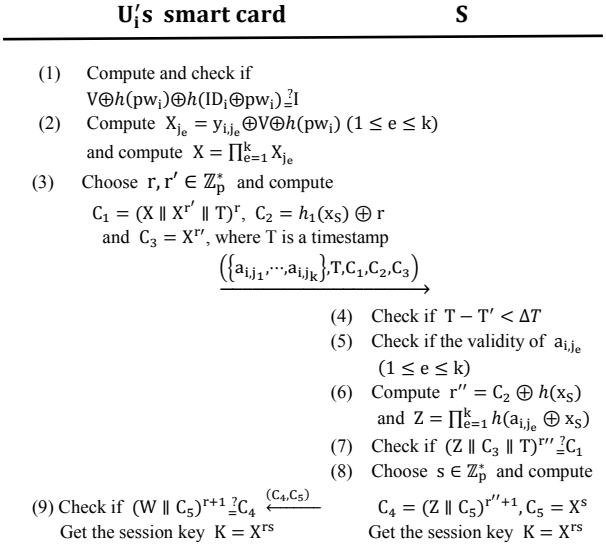

Fig.2. Login and Authentication Phase

assumed that attacker A has full control over the network but cannot corrupt the user smart card. This attacker is a Probabilistic Polynomial Turing(PPT) machine.

1. ***Replay Attack***: Suppose that an attacker $A_{\mathcal{R}}$ replays an intercepted valid login message and S receives the login message at time T*. Because it fails in the Step (5) of the authentication phase as the time interval $|T - T*| \ge \Delta T$, exceeds the expected transmission delay ΔT. Hence, the replay attack cannot succeed.

2. ***User Impersonation Attack***: To forge a valid login request $(\{a_{i,j_1}, a_{i,j_2}, \cdots, a_{i,j_k}\}, T, C_1, C_2, C_3)$, the attacker A_U has to know the value $h(x_S)$ or the chosen values $r, r' \in \mathbb{Z}_p^*$ used in generating C_1, C_2, and C_3. As a smart card is temper-resistant and x_S is the server's secret key, it is unlikely that A_U gets $h(x_S)$ from the user's smart card and r from C_2. Therefore, A_U cannot forge a valid login request.

3. ***Server Impersonation Attack***: To forge a valid reply message C_4 and C_5, the attacker A_S has to know the random value r and $h(x_S)$ from the login request $(\{a_{i,j_1}, a_{i,j_2}, \cdots, a_{i,j_k}\}, T, C_1, C_2, C_3)$, where x_S is the server's secret key. However, it is computationally infeasible for the adversary to get x_S or $r, r' \in \mathbb{Z}_p^*$ from C_1, C_2 and C_3 based on the difficulty of solving DH problem. Therefore, the adversary cannot forge a valid reply message.

4. ***Forward-Secrecy***: The forward secrecy means that even if the server's master secret key x_S is disclosed for some reason, it will not reveal the session key of any earlier session. Suppose that the secret key x_S is compromised. Then the intruder can get the values X, $X^{r'}$, and X^s from the login and reply message. However, based on the difficulty of solving DH problem[1], it is computationally infeasible for the intruder to derive the exchanged session key $K = X^{r's}$ from the given $(X, X^{r'}, X^s)$. Consequently, the proposed scheme is forward-secure.

5. ***Off-line Password Guessing Attacks***: As a smart card is temper-resistant and the login message does not contain the user password, the proposed scheme does not leak any redundancy information which may be used as a verifier to ensure whether a guessed password is correct or not. Hence, the proposed scheme is secure against off-line dictionary attacks.

6. ***User Anonymity***: Suppose that the malicious adversary A wants to know the identity of the login message and/or the linkability of the login message. In our scheme, the knowledge of the password is proven in Step (1) of the login phase and the login request does not contain the user identity and password information. Therefore, even both the malicious server with the verifier table and the outside attackers cannot obtain user identity information from the login request.

7. ***Collision Resistant Authentication of Attributes***: Suppose that the malicious adversary A_C wants to generate the new login message about the new attributes using the given login message generated by the honest user. In our scheme, the knowledge of the signature of attributes generated by the server is proven in Step (1) of the login phase and the login request contains the blinded signature of attributes assigned to the honest user. However, the outside attacker cannot get the server's signature of attributes assigned to the honest user. Moreover, attacker cannot generate the new login message about the new set of attributes.

3.3 Performace Analysis

Due to the resource constraints of smart card, the authentication scheme must consider the efficiency evaluation. We compare the performance of our scheme with that of the previous schemes in terms of computation costs and the results are shown in Table 2. It turns out that both Das-Saxena-Gulati[3] scheme and Yoon-Yoo[6] scheme are more efficient than our scheme. However, only our scheme and Chien-Chen[4] scheme among the schemes achieve authenticated key exchange. Also, our scheme is more efficient than Chien-Chen's scheme. Moreover, we first propose an attribute based user authentication scheme using smart cards which are provided the diversity of authentication.

Table 2. Comparison between our scheme and the others

	Functionality					Efficiency	
	MA	KE	PW	UA	ABA	CCL	CCA
ours	***Yes***	***Yes***	***Yes***	***Yes***	***Yes***	***2H+1E***	***2H+2E***
[3]	No	No	Yes	No	No	5H	3H
[4]	Yes	Yes	Yes	Yes	No	1E+1H+1S	3H+2E+2S
[6]	Yes	No	Yes	Yes	No	5H+1E	4H+3E

*MA: Mutual Authentication * KE: Key Exchange
* PW: Freely Changed Password *UA: User Anonymity
*ABA: Attribute based Authentication * CCL: Computation Cost in Login Phase
*CCA: Computation Cost in Authentication Phase *E: Exponential Operation
*H: Hashing Function *S: Symmetric Encryption or Decryption

4. CONCLUSION

We have been proposed an attribute based user authentication scheme using smart cards in multimedia contents distribution environments. The proposed scheme guaranteed mutual authentication and secure key exchange while enjoying all of the advantages of the previous anonymous authentication schemes. It is possible to restrict an access ability of user to contents according to various attributes. This scheme is not only more efficient than other schemes providing the same functionalities but also achieves user anonymity and diversity of authentication.

REFERENCES

[1] W. Diffie and M.E. Hellman, "New Directions in Cryptography," *IEEE Transaction on Information Theory*, vol.6(11), 1976, pp. 644-654.

[2] M.S. Hwang and L.H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transaction on Consumer Electronics*, vol.46(1), 2000, pp. 28-30.

[3] M.L. Das, A. Saxena, and V.P. Gulate, "A dynamic ID-based remote user authentication scheme," *IEEE Transaction on Information Theory*, vol.6(11), 2004, pp. 629-631.

[4] H.Y. Chien and C.H. Chen, "A Remote Authentication Scheme Preserving User Anonymity," *Proceeding of 19th International Conference on Advanced Information Networking and Applications*, 2005.

[5] A. Sahai and B. Waters, "Fuzzy identity based encryption," *Proceeding of Eurocrypt'05*, 2005.

[6] E.J. Yoon and Y. Yoo, "Improving the Dynamic ID-Based Remote Mutual Authentication Scheme," *Proceeding of OTM Workshop 2006*, LNCS 4277, 2006, pp. 499-507.

[7] K. Frikken, M. Atallah, and J. Li, "Attribute-Based Access Control with Hidden Policies and Hidden Credentials," *IEEE Transaction on Computers,* vol.55(10),2006, pp. 1259-1270.

[8] M. Pirretti, P. Traynor, and B. Waters, "Attribute-Based Systems," *Proceeding of CCS 2006*, 2006.

[9] T. Jiang, Y. Hou, and S. Zheng, "Secure Communication between set-top-box and smart card in DTV broadcasting," *IEEE Transactions on Consumer Electronics,* vol.50(3), 2004, pp. 882-886.

[10] *http://www.itu.int/ITU-T/IPTV/*

[11] R.S. Pippal, S. Tapaswi, and L. Li, "Secure Key Exchange Scheme for IPTV Broadcasting," *Informatica,* vol.36(1), 2012, pp. 47-52.

Hyejoung Yoo
She received the B.S., M.S., and Ph.D in Mathematics from Korea university, Seoul, Korea in 1997, 1999, 2002 respectively. Since 2004, she has been with the Sejong Cyber University, Seoul, Korea. Her main research interests include user authentication and contents security.