Hidden Attribute Certificate-based Encryption Extensions Model

LI Yu[1,2,3], ZHAO Yong[1,2,3], GONG Bei[1] and Xin Si-yuan[4]

[1] *College of Computer Science and Technology, Beijing University of Technology, Beijing, China*

[2] *State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, China*

[3] *Key Laboratory of Information and Network Security, 3rd Research Institute, Ministry of Public Security, Shanghai, China*

[4] *Zhengzhou Information Science and Technology Institute, Zhengzhou, China*
liyue_mail@163.com, zhaoyonge_mail@sina.com, tekkman_blade@126.com, laoxin213@yahoo.com

Abstract

An encryption extensions model based on hidden attribute certificate is proposed in this paper, which can represent any key by using "and", "or" logic and the threshold monotony of the access rules, and in order to resist the collusion attack, multiple users use a combination of their keys to decrypt the ciphertext, it virtually eliminates the possibility of a conspiracy to know the key.

Keywords: *identity-based; attribute-based; hidden attribute; certificate*

1. Introduction

In the cross-domain large Internet network, in order to ensure users' own security, before the communication with others, users must first assume whether the others are potentially malicious objects, only after the full test of the mutual contact and authorization certificates interaction, communication and transactions subjects can establish trusted relationships in distributed environment. The existing hidden certificates has obvious drawbacks in the following: in an open environment such as the Internet when users cooperate with unfamiliar parties (such as permission for access to resources), it often based on the requesting party of some vague set of features, but the identity of the requesting party is not clear. To solve the problems above, this paper proposed an improved ABE program, which can represent any key by using "and", "or" logic and the threshold monotony of the access rules. In order to resist the collusion attack, multiple users use a combination of their keys to decrypt the ciphertext, each attribute certification body has a pseudo-random function PRF for random distribution of keys. In this way, it virtually eliminates the possibility of a conspiracy to know the key.

2. Related Work

IBE System [10]

The IBE-based encryption public key certificate is a non-PKI-structure, while, the private key certificate is issued by the Key Server, which manage the private key. This architecture eliminates the public key certificate for the release, transfer and maintenance caused by the

waste of resources and time. The default is that the private key because all participants were hosted to a master authentication center, it must take various measures to protect against Key Server.

Attribute-based Encryption [16]

Encryption was proposed based on the concept of attribute by A. Sahai and B. Waters. A fuzzy identity used in encryption information is constructed on users' attributes, the user's decryption key contains a series of key components, and each key discreteness is corresponds to an identity of the attribute. A Key with the identity of a user can decrypt the ciphertext encrypted with the public ω', if and only if the collection ω and ω' have some overlap. It allows the recipient's public key and the identity of certain have some differences.

3. Extended Architecture Model

In the ABE hidden certificate extensions model, the certification authority canter is responsible for the distribution of the certificate, the user's certificate contains the user's decryption key. Each user has one and only one certificate. The certificate is made up of a series of certificate components (the certificate is the key component fragments), a certificate for each component corresponds to an attribute of the user, so we can set this attribute certificate as the certificate. During trust negotiation, the sender based on its own confidentiality requirements selects the set of attributes A_c to determine the recipient to encrypt the information, if the set of attributes certificate A_u of recipient and encryption information in the specified set of attributes required have accuracy of the match, the receiver can successfully decrypt and access to information. ABE certificate extensions based on the model the hidden architecture diagram is shown in the following figure.

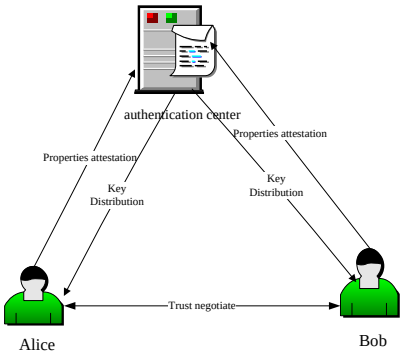

Figure 1. Extended Architecture Model

The figure shows the current proposed expansion of the certificate based on the hidden ABE model is based on a single certification center, at the beginning of trust negotiation, the user A and User B respectively use the global identity with its own GID and apply certificate from the certification center. So different user's set of attributes certificate is generated by different random polynomials, so even if multiple users collude, they can not combine their certificate components. Assuming the user selected set of attributes A (X, Y) as the encryption attribute to the user B and user C sends the encrypted information, and user B has attribute X, the user C has attribute Y. Because B.Y C.Y key the key is different, so the key can not share C.Y and BX key to conspiracy to break the A's information.

4. System Construction

A_u is the attribute set of u, A_c is the user's attribute set which is used to generate ciphertext.

A hidden certificate extended model includes the following:

1. System configure function: Setup, which is run by the authority center, it will generate the public parameter params and the main key master-key;

2. Certificate distribution function: CA_Issue, which is run by the authority center, it will random select polynomials to create the certificate for each user and issue the certificate to each user, each certificate component correspond to a user's attribute; when user acquires the certificate from the authority center, the user can use the only disguise name nym;

3. The encryption function:CT=HCE(R，nym，A_c), which is run by the authority center, it uses A_c as the public key to encrypt the resource R, the receiver of R is nym, CT is the ciphertext, A_c is the access control policy, it is contained in CT;

4. The decryption function: R=HCD (CT，Cred), which is run by the authority center, it decrypt the ciphertext CT, the public key of the certificate cred is A_u, and if and only if $|A_c \cap A_u| \geq d$ is true, it can decrypt the resource R, d is the determined threshold.

It is worth noting that this system does not give the user a certificate issued for each attribute, but the system issues the certificate for each user, a certificate for each component corresponds to an attribute of the user. If the "issuing a certificate for each attribute" method is used, multiple users will be easy to collude with their attributes that they can not decrypt the certificate to decrypt the ciphertext alone, the system will be vulnerable to collusion attack.

5. Trust Negotiation Process of Two Sides

Trust negotiation process based on ABE hidden certificate (User A requests a file R from B) is shown in figure 2.

1. A sends Ta=HEs(request，Prequest) to B;
2. The certificate set of B is CB, if B satisfies Prequest, it can decrypt request=HDs(Ta，CB);
3. B sends the resources Tb=HEs(R，PR) to A;
4. The certificate set of A is CA, if CA satisfies PR, it can decrypt R =HDs(Tb，CA)

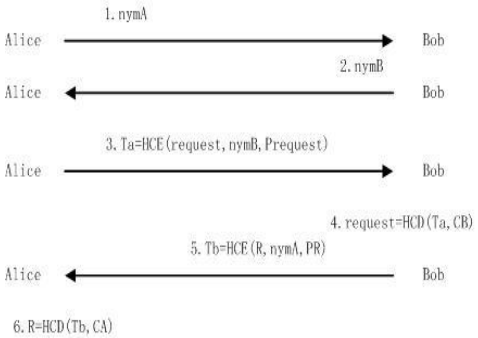

Figure 2. Trust Negotiation Process of Two Sides

6. Trust Negotiation Process of Multi-sides

Trust negotiation process of multi-sides based on ABE hidden certificate (User A requests a file R_k which satisfies the access control policy from all the users) is shown in figure 3.

1.A sends Ta=HEs(request，Prequest) to every user；

2. When the user who receives the request can not satisfies Prequest. It will not decrypt the request, and it can not acquire the access control information, the certificate set of B is CB, and the certificate set of D is CD, if B an D satisfies Prequest, it can decrypt request=HDs(Ta，CB) =HDs(Ta，CD);

3. B sends Tb=HEs(Rb，PRb) to A, D sends the resources Td=HEs(Rd，PR d);

4. The certificate set of A is CA, if A can satisfies PRb, it can decrypt Rb=HDs(Tb，CA), if A satisfies PRd, it can decrypt Rd=HDs(Td，CA)

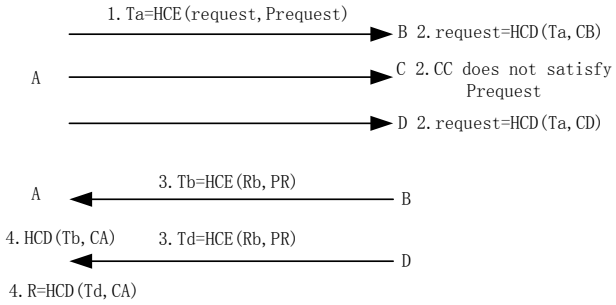

Figure 3. Trust Negotiation Process of Multi-sides

Trust negotiation and trust of both parties in the process of encryption and decryption of the request, encryption and decryption resources use the basic ABE technology.

7. Performance Analysis

Given G_1 is the P order bilinear group, g is a generator of G_1, $e: G_1 \times G_1 \to G_2$ is the bilinear map, the secure parameter k decides the size of the group.

For $i \in Z_p$ and a group of elements S in Z_p , $\Delta_{i,s}$ are the Lagrange parameters:

$$i \in \Delta_{i,s} = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$$

U is the total element, we select the first $|U|$ elements as the total, they are $1,2,3.....|U| \bmod P$, and next we randomly select $t_1, t_2 .....t_{|U|}$ in Z_p , at last we randomly select a parameter y , the public parameters of system are $T_1 = g^{t_1}, ...T_{|U|} = g^{t_{|U|}}, Y = e(g,g)^y$, the main public key is $t_1, t_2 .....t_{|U|}$.

A certificate needs a $d-1$ order polynomial q , this polynomial q can make $q(0) = y$, the certificate is made up of $(D_i)_{i \in A_u}$, for each $i \in Au$, $D_i = g^{\frac{q(i)}{t_i}}$.

When user uses the public key A_c to decrypt $M \in G_2$, the user randomly selects $s \in Z_p$, the ciphertex is $E = (A_c, E' = MY^s, \{E_i = T_i^s\}_{i \in Ac})$

When user decrypts the $M \in G_2$, the user randomly selects a set S which contains d elements selected from $|A_c \cap A_u|$, the decryption is

$$E^{'} / \prod_{i \in S} (e(D_i, E_i))^{\Delta_{i,s(0)}} = Me(g,g)^{sy} / (e(g,g)^{sq(i)})^{\Delta_{i,s(0)}} = M$$

From the formulas above, the extended model based on hidden certificate, Cryptographic operations and attributes of public key encryption has a linear relationship, when the user decrypts the message, the cost relates with the computational cost of d bilinear maps.

The extended model achieves a certificate hidden and resources hidden, in the trust negotiation process this model avoids the multiple certificate exchanges before access to resources, it also reduce network cost while protecting the security of the certificate. In addition, in trust negotiation process, in order to protect sensitive strategy, the sender's information in the encrypted does not need to specify what he uses the public key. IBE-based hidden credentials system, the receiver needs his own certificate to try to decrypt the message, although the implementation of the strategy implements the hidden policy, but it is inefficient. Hidden in the ABE certificate extended model, since each user only has a certificate, it needs only one chance to decrypt the information and it increases the efficiency of the system.

8. Conclusion

In this paper based on IBE / ABE's Web security technology, we proposed an improved ABE scheme which can represent any key by using "and", "or" logic and the threshold monotony of the access rules. In hidden the ABE certificate extended model, since each user only has a certificate, it needs only one chance to decrypt the information. It increases the efficiency of the system.

Acknowledgements

This research is funded by 863 National High Tech Research and Develop Plan Project (2009AA01Z437), 973 National Key Fundamental Research Development Plan Project (2007CB311100), Open Research Project of State Key Laboratory of Information Security in Institute of Software Chinese Academy of Sciences, the program "Core Electronic Devices, High-end General Purpose Chips and Basic Software Products" in China (No. 2010ZX01037-001-001), Funds of Key Lab of Fujian Province University Network Security and Cryptology(2011009) and Doctor Launch Fund in Beijing University of Technology (X00700054R1764).

References

[1] H. Tanaka, "A realization scheme for the identity—based eryptosystem", [C]//Proc of Advances in Cryptology—Crypto'87. [S.1.]: Springer-Verlag, **(1987)**, pp. 341-349.

[2] W. Meier and O. Stafflebach, "The Self-shrinking Generator[C]//Proc of LNCS'94. Berlin, Germany: Springer-Verlag, **(1994)**.

Authors

LI Yu

His major research is in information security.