Encryption Extensions Model based on Hidden Attribute Certificate

LI Yu[1,2,3], ZHAO Yong[1,2,3], GONG Bei[1]

[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
liyue_mail@163.com, zhaoyonge_mail@sina.com, tekkman_blade@126.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 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 cannot decrypt the certificate to decrypt the ciphertext alone, the system will be vulnerable to collusion attack.

3 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 1:

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)

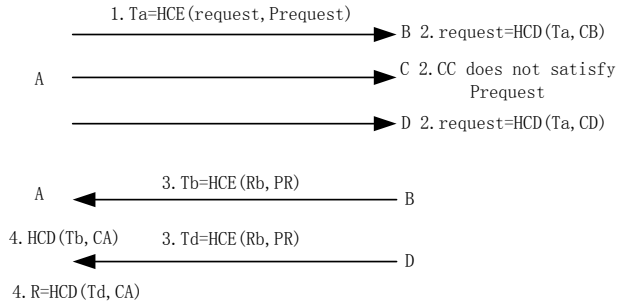

Fig. 1. Trust negotiation process of multi-sides

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.

4 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 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. Liu Hong-yue，Fan Jiu-lun，Ma Jian-feng．Research Advances on Access Control[J]．MINI-MICRO SYSTEM S，2004，25(1)：56-59.
2. Ravi S, Sandhu，Edward J. Coyne，Hal L Feinstein，et a1． Role-based access control models[J]． IEEEComputer, 1996, 29(2):38~47.
3. Barlow T, Hess A, Seamons KE. Trust negotiation in electronic markets. In Proc of 8th Research Symp in Emerging Electronic Markets. Maastricht, 2001. http://isr1.cs.byu.edu/pubs/rseem200l.pdf.