Vector-Based Sensitive Information Protecting Scheme in Automatic Trust Negotiation

Jianyun Lei and Yanhong Li*
School of Computer Science, South-Central University for Nationalities, Wuhan, China
*Corresponding Author, Email: leijianyun@mail.scuec.edu.cn, anddylee@163.com

***Abstract*—The existing sensitive information protecting schemes can not satisfy the actual security requirement of some applications. A vector based sensitive information protect scheme is presented based on the existing schemes. One side in trust negotiation can selectively exposes the sensitive attributes to the other side in trust negotiation process based on personal security policy and the trust evaluation result of the other. The implementation process is given in concrete application instances and the scheme is analyzed.**

***Index Terms*—Access Control; Automatic Trust Negotiation; Sensitive Information Protecting; Trust Evaluation**

I. INTRODUCTION

Resource sharing is very important in large-scale application systems in distributed multi-domain environments [1-3], and access control technique used in these systems is the key to information security issues. In a distributed multi-domain environment, trust management [4] proposed by Blaze is a relatively mature access control technique. The visitor of the resources must provide his certificates to prove the appropriate access rights, and the owner of resources make the appropriate decision whether to allow access or not based on the certificates provided by the visitor. The automatic trust negotiation [5] proposed by Winsborough is also an access control technique in distributed multi-domain environments. Resources visitor and owner establish trust and make access control decisions through repeated exchanging their certificates without the third-party [6-8].

Certificates in trust management system and trust negotiation always contain some sensitive attributes which are necessary to be protected. However, the trust management system does not take this into consideration. It is a deficiency of trust management system. Many scholars have done a lot of research works in how to protect sensitive attributes of certificates in the process of automatic trust negotiation [9-11]. The existing solutions are not able to fully meet the requirements of the users in some applications. The users can't selectively expose some sensitive attributes of certificates according to their own access control policy and the trust assessment to the others [12-14].

Trust negotiation is a method that establishes trust relationship between entities in distributed domain environment. The entities do not know each other before, but they establish trust relationship step by step through exchanging digital certificates again and again [15]. A trust negotiation system is consisted of the entities of negotiation, digital certificates and the police of exposing certificates, etc.

Digital certificate is digitalized tool that contains user identification and attribution, according to the different application background; there are identification certificate and attribution certificate. Digital certificate is signed by the issuer, so it has the unforgeability and verifiability [16, 17].

Access control policy is used to ensure the information not be accessed by the illegal users, so its function is to provide all kinds of the access operation to the data source of the legal user [18]. The access control policy in the trust negotiation resolves how to exchange certificates during the negotiation process, which is just the sequence of the exposing of all kinds of certificates [19, 20].

Compared with the access control system based on identification [21], trust negotiation contains the obvious advantages: (1) Two sides of the negotiation do not have to know the identification and attribution each other before, they establish the trust relationship during the process of exchanging the digital certificates, and this is appropriated in the distributed multi-domain system where the entities do know each other. (2) Two sides of the negotiation can define their own access control policy to provide the access to own sensitive resource. (3) There needn't the trusted third party during the trust negotiation.

In the trust management and trust negotiation systems based on certificates, the relative research on the protection of the sensitive attribution include [22], oblivious signature-based envelope [23], hidden credentials [24] and secret handshakes from pairing-based key agreements [25], etc.

In the secret handshakes from CA-oblivious encryption scheme, based on the scheme of zero-knowledge proof protocol, Bob promise to Alice that he contain a certain attribution, Alice and Bob work according to the protocol, Alice sends Bob an envelop, only when the attribution Bob promised satisfies the assert of Alice, Bob can open the envelop, and Alice knows nothing about any attribution of Bob. The theory of secret handshakes from CA-oblivious encryption and oblivious signature-based envelope are almost the same, the difference between them lies in: oblivious signature-based envelope use the

doi:10.4304/jnw.9.4.927-931

signature of the attribution but not the promise of the attribution.

In the hidden credentials scheme, Alice and Bob exchange some random information, and then Alice uses the random information that provided by Bob and his access control policy to encrypt the information, if Bob has corresponding credential, he can use the random information provided by Alice to decrypt the information. In secret handshakes from pairing-based key agreements scheme, all the users in a group share secret by exchanging information.

All the scheme above can not satisfy the requirement that Alice want to expose part of her sensitive attribution to Bob, and to the certain trust negotiation entity, such as Bob and Charlie, can access the different sensitive attribution in Alice's certificate under the policy that Alice set before. Further more, the schemes above need trusted third party, the safety of the system lies on the trusted third party and the storage also communication cost of the system will increase. A vector based sensitive information protect scheme is presented based on the existing schemes. One side in trust negotiation can selectively exposes the sensitive attributes to the other side in trust negotiation process based on personal security policy and the trust evaluation result of the other, and there needn't any trusted third party.

II. A Simple Protecting Scheme of Sensitive Information

In a digital certificate, properties can be represented by the ordered pair <*attr_name*, *atrr_value*>, where *attr_name* stands for the property name, and *attr_value* stands for the property value. If a property is a piece of sensitive information, the property value should be stored in cipher text. For an example, Alice's certificate contains n attributes, attributes names are N_1, N_2, …, N_n, the corresponding attribute values are V_1, V_2, …, V_n. If there are i ($i \le n$) attributes (subscript are denoted as $j_1, j_2, ..., j_i$) are sensitive information, then the corresponding i properties of the certificate C are stored in cipher text, and the other n-i attributes are stored in plain text. The publisher of certificate C generates the digital signature, and then sends C and decryption key which used to encrypt i sensitive attributes to Alice. The key must be sent through reliable channels, public key system can also be used to ensure the security. When Alice request services or resources from Bob, Alice must submit C to Bob, and selectively expose part or all of the sensitive attributes of C to Bob according to Bob's attributes (or privileges). Alice sends Bob the corresponding decryption keys of the sensitive information which Bob has authority in C through trusted channel. Bob can then get the encrypted property value by using the received decryption key. This scheme of protecting sensitive attributes in certificate has the advantage of being simple and easy to understand, but there are following inadequacies. The simple protecting scheme of sensitive information is shown in Figure 1.

(1) For each sensitive attribute there is no specific trust assessment, Alice identifies which attributes are sensitive in certificate unilaterally. There is no measure of sensitivity, and no algorithm of exposing which sensitive attributes to Bob according to the specific circumstances of Bob.

(2) There is no specific data structure to indicate which sub-keys of the key K should be sent to Bob when Alice sends certificate to Bob. When Bob receives a certificate from Alice, he won't know which sub-key is for the corresponding properties immediately. If Bob use every sub-key of K to tentatively decrypt every sensitive attribute in certificate C one by one, it will greatly increase time and storage overhead of Bob.

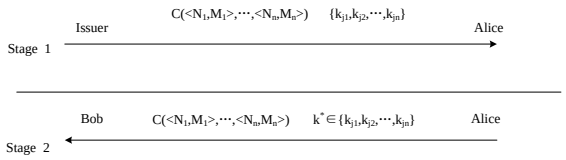

Figure 1. Simple protecting scheme of sensitive information

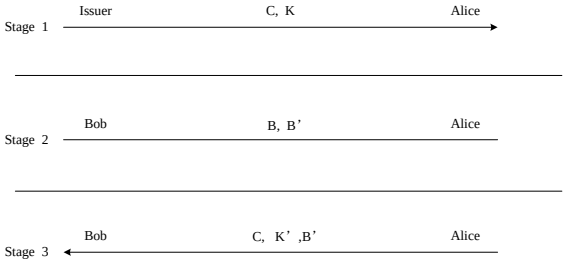

Figure 2. Vector-based sensitive information protect scheme

III. Vector-Based Sensitive Information Protecting Scheme

In order to facilitate formal describing, we use the issuer to represent the certificates publisher; AN and AV to represent attribute name and attribute value, each property has a trust threshold T ($0 \le T \le 100$), issuer defines the trust threshold according to the sensitivity of the attributes. Only when the corresponding value of the property on the other side is greater than the trust threshold, the property will be open to him. Obviously, the threshold value of non-sensitive property is 0. A triad <AN, AV, T> stands for property name, property value and the trust threshold. $E_k(m)$ represents decrypt information m using key k. C represents the certificate.

Based on the previous simple scheme, with the following adjustments, sensitive information protecting scheme based on vector is presented. The whole process of scheme is divided into three stages: The first is the certificate generation phase, the certificate issuer generates certificate and sends it to Alice; The second stage is trust assessment phase, Alice has a trust evaluation process to Bob according to her own attributes, generates a vector B, and then calculates the open vector B' to Bob according to B and trust threshold of each attribute corresponds in certificate C; The third stage is the certificate exchange phase, Alice submit the certificate C to Bob, and expose part or all sensitive properties of certificate C to Bob according to B'. The

protocol of vector-based sensitive information protecting scheme is shown in figure 2.

A. Certificate Generation Stage

Certificate issuer generates a certificate C and sends it to the holder of the certificate Alice. There are two major steps in the phase.

(1) The issuer generates a certificate C based on the T value of the properties. In the certificate C, the values whose T = 0 (Non-sensitive properties) are saved in plain text like <AN,AV>. Suppose there are j sensitive properties, For each sensitive property the property value is stored in cipher text like <AN, E_{Ki}(AV)>, i=1..j, The encryption sub-key Ki Here is randomly chosen.

(2) The certificate C and encryption key K(K contains j sub-keys as Ki, i = 1...j) are sent to Alice, and the key is sent through reliable channels.

B. Trust Evaluation Stage

According to the history of certificates exchanging with Bob and other various factors, Alice can give an assessment of trust to Bob for each attribute in the certificate. Suppose there are N properties in Alice's certificate, and the results of trust assessments to Bob is an N-valued vector containing the trust value, denoted using B, B=<T1,T2,…,TN>, where Ti is the trust value of Alice to Bob on the i^{th} property. Then Alice will compare the trust value of each property in the certificate with B. There will generate a corresponding bit 1 if Ti in B is greater than the trust value of i^{th} property, and that means the property can be disposed to Bob, otherwise there will generate a corresponding bit 0 and that means the property can not be disposed to Bob. A property open vector B' can be obtained according to the chronological order of these bits. B' is formed with these bits, and itself can be a binary number that contains these bits.

The x^{th} bit f(x) in open vector B' can be

$$f(x)=\begin{cases}1, \text{The } x^{th} \text{ property can be disposed}\\ 0, \text{The } x^{th} \text{ property can not be disposed}\end{cases}$$

and B' is shown in figure 3.

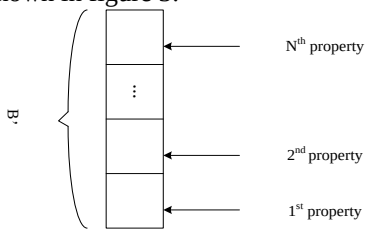

Figure 3. Corresponding relationship between property sensitivity and bits in open vector B'

C. Certificate Exchange Stage

In the certificate exchange stage, Alice sends the certificate C to Bob, and shows Bob about the non-sensitive properties in the certificate and the sensitive properties which are opened to Bob in the following four steps:

(1) Correspondence between the sensitive properties of the certificate C that can be exposed and binary bits B' is established according to the chronological order.

(2) Alice organizes the properties whose trust threshold values are greater than 0 and the corresponding bits in the B' is 1 and those corresponding encryption sub-keys Ki, to form a new group key K'.

(3) Alice sends C, K' and B' to Bob, where K ' must be sent in trusted Channel.

(4) After receiving C, K' and B', Bob decrypts the sensitive properties in C whose corresponding value in B' is 1using the K' as the decryption key.

Subheadings: should be 10 point, italic, left justified, and numbered with letters (A, B, …), followed by a period, two spaces, and the title using an initial capital letter for each word. The paragraph description of the subheading line should be set for 6 points before and 3 points after.

IV. Application Example and Analysis

The implementation of the above sensitive information protecting scheme based on vector is presented using a specific application example.

A. Application Example

The government departments issue each person a certificate about the basic personal information, it contains in this certificate the information such as name, age, gender, education, income, department and address. Supposed those fields like "age", "income", "department" and "address" are sensitive information. The corresponding trust value of the sensitive properties of the certificate are (30, 80, 70, 90). When Alice and Bob are in the trust negotiation, through the trust evaluation to Bob, Bob's trust value according to Alice's certificate for the sensitive attribute are (50, 75, 70, 75). It's easy to get B' = 1010 (binary). Alice Sends B' and the decryption key of "age" and "department" to Bob in the certificate exchanging stage. After Bob receives C, he can only get the values of non-sensitive properties (e.g. name, gender) and can decrypt the value of opened sensitive properties (age, department), and non-opened sensitive attributes (income, address) can not be to obtained due to the lack of access to the corresponding decryption keys.

B. Analysis of the Security Performance of the Scheme

The security of sensitive information protecting scheme based on vector is mainly reflected in two aspects: The one is whether the eavesdropper is able to get Bob's key which is used to decrypt the sensitive properties, the other is whether Bob can get the value of non-opened sensitive properties.

Because the key distribution is sent through the reliable channel which is based on other cryptography and security measures, so the eavesdropper can not obtain the corresponding decryption key. The key distribution is based on the selective vector, thus Bob can not get the keys for non-opened sensitive properties.

C. Other Features of the Scheme

View from the time overhead, there exists the trust assessment and computing process of the vector on the basis of the original trust negotiation. The process takes time overhead is fixed. That is, its time complexity is

O(1). And there exist the process of encrypting the sensitive properties in the certificate generation and certificate exchange stages, since the encryption is symmetric, the time cost compared with the signature and asymmetric encryption algorithm in the certificate exchange process is negligible.

View from the storage overhead, an additional storage overhead of vector B, properties open vector B' and decryption key is required in vector-based sensitive information protecting scheme, besides the holder of the certificate C requires the storage overhead of the certificate itself, but this is the basic requirement for the system implementation and it is acceptable.

View from the communication overhead, in vector based sensitive information protecting scheme, the communication overhead in certificate generation stage is the certificate C and the sensitive properties decryption key, and the communication overhead is the certificate and the decryption key of opened sensitive properties also the properties open vector B' in the stage of exchange certificates.

V. CONCLUSION

Compared with the disclosure tree model proposed by Yu [26], inadvertently attribute certificate scheme and inadvertently signed envelope scheme, those models operate the certificate as a whole, expose all the properties' information in the certificate or do not expose any information at all. But the protecting scheme in sensitive properties which proposed in this article classifies the properties. The properties are divided into sensitive properties and non-sensitive properties, and the sensitive properties are divided into opened sensitive properties and non-opened sensitive properties. The scheme can selectively expose all non-sensitive properties and opened sensitive properties, but non-opened sensitive properties are protected. This can meet the needs of practical applications better, and is also more flexible and convenient.

Liao, who proposed SDSA scheme in 2008[27], Can also selectively expose sensitive properties of some or all, but there exists no assessment of trust with each other, and no corresponding data structure to express and store the value of trust either, so he can only simply define which properties are opened and which are not, and lack of maneuverability. This scheme recovers the bug. The exposure of each sensitive attribute is determined by the trust evaluation and sensitive property vector.

ACKNOWLEDGEMENT

This work was supported by the Natural Science Foundation of Hubei Province, China (No. 2013CFB445).

REFERENCES

[1] D. Brickley and L. Miller, "FOAF vocabulary specification 0. 91. Namespace Document," Online: http: //xmlns. com/foaf/0.1., Nov 2007.

[2] L. Ding, L. Zhou, T. W. Finin, and A. Joshi, "How the semantic web is being used: An analysis of foaf documents," *in HICSS. IEEE Computer Society*, 2005.

[3] B. Carminati and E. Ferrari, "Privacy-aware Access Control in Social Networks: Issues and Solutions," *in Privacy and Anonymity in Information Management Systems, J. Nin and J. Herranz, Eds. Springer, to appear.*

[4] M. Blaze, J. Feigenbaum, J. Lacy. Decentralized Trust Management. In: Proceedings of the 17th Symposium on Security and Privacy. Oakland, California, USA. Los Alamitos*: IEEE CS Press*, 1996, 164-173.

[5] W. H. Winsborough, K. E. Seamons, V. E. Jones. Automated Trust Negotiation. In: Proceedings of DARPA Information Survivability Conference and Exposition. Hilton Head, South Carolina, Los Alamitos: *IEEE press, Volume I*, January 2000, 88-102.

[6] E. Ferrari, A. C. Squicciarini, and E. Bertino, "X-TNL: An XML Language for Trust Negotiations," *4th IEEE Workshop on Policies for Distributed Systems and Networks, Como, Italy*, June 2003.

[7] W. Nejdl, D. Olmedilla, and M. Winslett, "PeerTrust: Automated Trust Negotiation for Peers on the semantic web," *in Workshop on Secure Data Management in a Connected World (SDM'04), Toronto, Canada*, Aug. 2004.

[8] B. Carminati, E. Ferrari, and A. Perego, "Enforcing access control in web-based social networks," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 1, 2009.

[9] F. Bonchi and E. Ferrari, Eds., Privacy-aware Knowledge Discovery: Novel Applications and New Techniques. Chapman and Hall/CRC Press, 2010.

[10] J. Nin, B. Carminati, E. Ferrari, and V. Torra, "Computing Reputation for Collaborative Private Networks," *in COMPSAC '09: Proceedings of the 2009 33rd Annual IEEE International Computer Software and Applications Conference*, 2009, pp. 246–253.

[11] T. Y. K. E. Seamons, M. Winslett, "Protecting privacy during on line trust negotiation," *in 2nd Workshop on Privacy Enhancing Technologies, San Francisco, CA, April 2002.*

[12] N. Li and J. C. Mitchell, "Datalog with constraints: A foundation for trust management languages," *in Proceedings of the Fifth International Symposium on Practical Aspects of Declarative Languages*, Jan. 2003.

[13] K. E. Seamons, M. Winslett, and T. Yu, "Limiting the disclosure of access control policies during automated trust negotiation." *in NDSS*, 2001.

[14] W. H. Winsborough and N. Li, "Safety in automated trust negotiation." *in IEEE Symposium on Security and Privacy*, 2004, pp. 147–160.

[15] E. Bertino, E. Ferrari, and A. C. Squicciarini, "Privacy-Preserving Trust Negotiation." *Proceedings of 4th Privacy Enhancing Technologies Workshop, Toronto, CA, May* 2004.

[16] A. C. Squicciarini, A. Trombetta, and E. Bertino, "Supporting Robust and Secure Interactions in Open Domains through Recovery of Trust Negotiations," *in ICDCS. IEEE Computer Society*, 2007, p. 57.

[17] A. C. Squicciarini, A. Trombetta, E. Bertino, and S. Braghin, "Identitybased long running negotiations," *in Digital Identity Management, E. Bertino and K. Takahashi, Eds. ACM*, 2008, pp. 97–106.

[18] A. C. Squicciarini, F. Paci, E. Bertino, A. Trombetta, and S. Braghin, "Group-based negotiations in p2p systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 99, no. PrePrints, 2010.

[19] S. Braghin, I. Nai Fovino, and A. Trombetta, "Advanced trust negotiations in critical infrastructures," *International Journal of Critical Infrastructures*, vol. 6, no. 3, pp. 225–245, 2010.

[20] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, "Identity Establishment and Capability Based Access Control (IECAC) Scheme for Internet of Things," *In IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC - 2012)*, pp. 184-188. Taipei - Taiwan, September 24-27 2012.
[21] Adjei J. K. and Olesen H., "Keeping Identity Private," *In IEEE Vehicular Technology Magazine*, Volume: 6, Issue: 3, pp: 70-79, September 2011.
[22] C. Castelluccia, S. Jarecki, G. Tsudik. Secret Handshakes from Ca-oblivious Encryption. In Advances in Cryptology – ASIACRPT 2004: 10th International Conference on the Theory and Application of Cryptology and Information Security. Volume 3329 of Lecture Notes in Computer Science, Springer, 2004, 293-307.
[23] N. Li, W. Du, D. Boneh. Oblivious Signature-Based Envelope. In: Proceedings of the 22nd ACM Symposium on Principles of Distributed Computing (PODC 2003). Boston, Massachusetts, USA, New York: ACM Press, July 2003, 182-189.
[24] Holt J, Bradshaw R, Seamons K, et. al. Hidden Credentials. 2nd ACM workshop on Privacy in the Electronic Society. Washington DC: ACM Press, 2003, 1-8.
[25] Balfanz D, Durfee G, Shankar N, et. al. Secret Handshakes from Pairing-Based Key Agreements. *Proceedings of the 2003 IEEE Symposium on Secret and Privacy*. Oakland CA, 2003, 80-196.
[26] T. Yu, M. Winslett, K. E. Seamons. Supporting Structured Credentials and Sensitive Policies through Interoperable Strategies for Automated Trust Negotiation. *ACM Transactions on Information and System Security (TISSEC)*, February 2003, 6(1) pp. 1-42.
[27] Junguo Liao, Fan Hong, Jun Li et. al. Keeping confidentiality of sensitive attributes in credential during trust negotiation. *Chinese Journal of Communications*. 2008, 29(6) pp. 20-25.

Jianyun Lei, born in September, 1972, in Zhejiang province, China, received the B.E degree in computer and application from South-Central University for Nationalities (SCUFN) in 1994, the M.S degree in computer software and theory from Huazhong University of Science and Technology (HUST) in 2004, and the Ph.D. degree in information security from Huazhong University of Science and Technology (HUST) in 2010.

Since 1994, he has been a faculty in South-Central University for Nationalities (SCUFN) which is in Wuhan, China, and he is currently an Associate Professor in the school of computer science. His recent research interests include information security, internet of things (IOT) etc.

Dr Lei is the member of China Computer Federation (CCF).

Yanhong Li was born on 26 April 1973 in Hunan, China. received the B.E. degree in mechanical engineering from Central South University of China(CSU) in 1993, The M.S. degree in computer application from Chongqing University of China (CQU)in 2004, and the Ph. D degree in computer software and theory from Huazhong University of Science and Technology of China (HUST) in 2011.

Since 2012, she has been a faculty in South Central University for Nationalities (SCUFN) which is in Wuhan, China, and she is currently a lecturer in the school of computer science. Her research interests include information security and multimedia network communication technology.