Security Classification-Based Access of Power Information System

Yanshuai ZHAO[1,a], Yang QIAN[1,b], Ruizhong CHEN[1,c], Hongxia MA*[2,d]

[1]Information Center, Guangdong Power Grid Corporation, Guangzhou, 510000, China

[2]SKLOIS, Institute of Information Engineering, CAS, Beijing, 100093, China

[a]email: shuaizi@163.com, [b]email: 1074427744@qq.com, [c]email: crzlhs@163.com,

*Corresponding author: [d]email: mahongxia@iie.ac.cn

Keywords: Key Management; Access Control; Power Information Systems

Abstract. Security and privacy are widely recognized as important requirements for access and management of power information system data. In this paper, we argue that power information system data need to be managed with customizable access control in security classification dimension. We present a role-based and security classification-based access control method that provides more flexibility in security classification dimension to control the access of sensitive data. We have employed a security classification tree method for generating security classification granule values, offering fine granularity of security classification-based access authorization and control.

Introduction

Security and privacy are key issues in a power information system. A sensitive file only can be accessed by authorized users, while other unauthorized users cannot read this file. However, user should not be able to access any sensitive document in a power information system, if he is not a secret-related person. We make use of security classification-based access scheme to control the availability of files in each security class. In this method each user is granted a security classification interval based on his role or attribute, in which he can generate decryption keys by himself. On the contrary, user cannot create any decryption key beyond security classification interval.

Related Works

The Basic idea of this paper is from the time-bound hierarchical key management.

In 2002, Tzeng [1] first proposed a time-bound hierarchical key management scheme that requires each user to store information whose size does not depend on the number of time periods. However, this scheme is costly since that Lucas function operation incurs heavy computational load. Most importantly, Tzeng's scheme has been proved to be insecure against collusive attacks, whereby two or more users assigned to some classes in distinct time period, collude to compute a key to which they are not entitled [2]. Subsequently, Chien [3] put forward an efficient time-bound hierarchical key management scheme based on tamper-resistant devices. However, Santis and Yi [4, 5] showed that malicious users can collusively misuse their devices to gain unauthorized accesses and also proposed countermeasures. Another time-bound hierarchical key assignment scheme was proposed by Huang and Chang [6] and later shown to be insecure against collusive attacks too [7]. Yeh [8] proposed an RSA-based time-bound hierarchical key assignment scheme, which was proved to be insecure against collusive attacks in [9]. Wang and Laih [10] used a modification of the Akl-Taylor scheme to construct a time-bound hierarchical key management scheme. Then, two provable-secure time-bound hierarchical key assignment schemes the one is based on symmetric encryption schemes, whereas, the other makes use of bilinear maps, were posed by Ateniese and Santis [9], who proved their schemes are simultaneously practical and provably-secure. After that new constructions for provably-secure time-bound hierarchical key assignment schemes were

brought forward and tradeoff among storage space and key derivation time were exhibited by Santis [11]. But provably-secure schemes are inefficient when the system has large number of data. Liu and Zhong [12] advanced a practical time-bound hierarchical key scheme without tamper-resistant device, which was claimed to be more secure and need less computational time. However, in their scheme users need to hold a number of keys to decrypt the data on multiple classes. Recently, Bertino [13] proposed another new time-bound scheme using elliptic curve cryptography and claimed that their scheme was efficient and secure against several attacks. Unfortunately, Sun [14] found that Bertino's scheme was not as secure as they claimed and some possible improvements were proposed. Moreover, tamper-resistant device makes Bertino's scheme difficult to implement in EHR systems since it is hard to securely issue tamper-resistant device when users are distributed around the world.

The Structure of Power Information System Data

The structure of power information system data is flexible and dynamic. Figure 1 is an example of role-based hierarchical structure of power information system data. Data can be clustered by the different roles of employees in Figure 1.

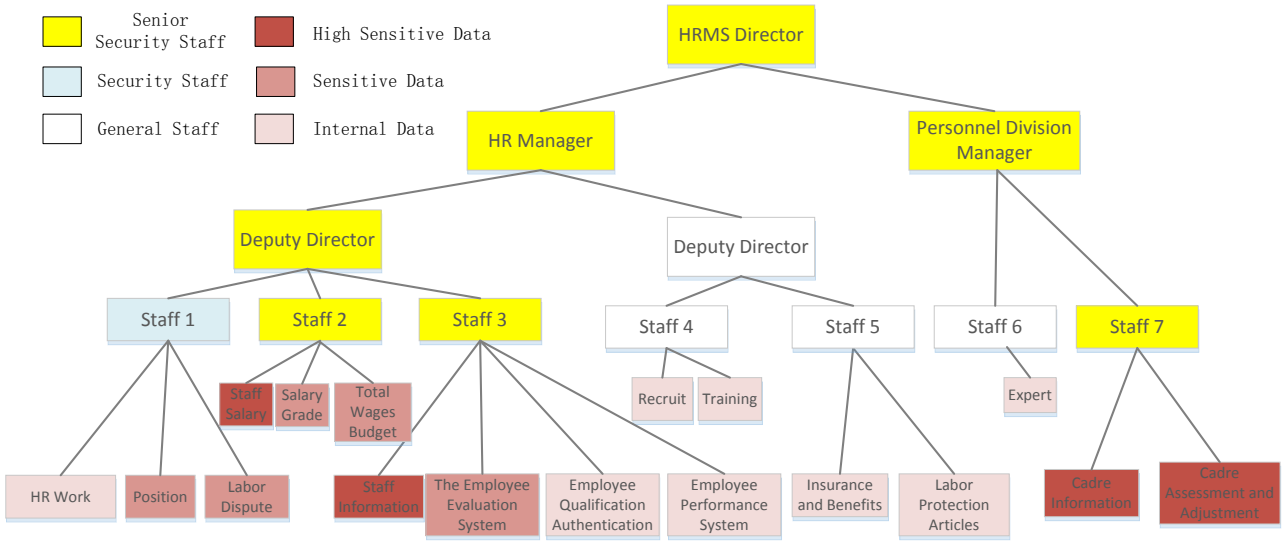

Fig. 1 The Role and Security Classification-Based Hierarchy

Security Classification Tree

In this subsection, we introduce a novel method to compute security classification values. We divide security classification into small granules, which are numbered as 0, 1, 2,…, z, and map these security classification granules into a security classification tree. We call several consecutive security classification granules security classification interval which will be authorized to each user to access a class of data.

Then we give an example to explain how to map security classification granules into a Complete Binary Tree (CBT) (see Figure 2). In Figure 2, the security classification line is divided into four small security classification granules expressed binary numbers 00, 01, …, 11. For simplicity, we use B(s) denotes the binary expression of security classification granule, and $V_{B(s)}$ indicates the value of security classification granule *t*, where the values with star in subscript means internal nodes in the security classification tree. Obviously, the values of smallest security classification granule are labeled by leaf nodes in the CBT. We observe that all security classification interval $[s_b, s_e] \in [0, z]$ can be composed of a number of Full Binary Subtrees (FBS). For example, security classification interval $[s_b, s_e]=[0, 2]=[00, 10]$, which labeled in Figure 4(a), contains two FBSs, one is rooted by node V_{0*}, the other is rooted by node V_{10}, which can be expressed by $[V_{00},V_{10}]=FBS[V_{0*}] \cup FBS[V_{10}]$.

Besides, the value of each node in the CBT can be calculated by the path from the root node which value is H(w), where w is a random integer. So we have following expressions $V_{0*}=H(H(w)||0)$, $V_{1*}=H(H(w)||1)$, …, $V_{11}=H(V_{1*}||1)$, where || denotes string concatenation. Therefore, any leaf node of a FBS can be computed by the value of corresponding root node. For example, V_{00}, V_{01}, V_{10} can be computed from the value V_{0*} respectively, while V_{10} can be directly given. Consequently, security classification granules in interval $[s_b, s_e]=[00, 10]$ can be computed only given value V_{0*} and V_{10}.

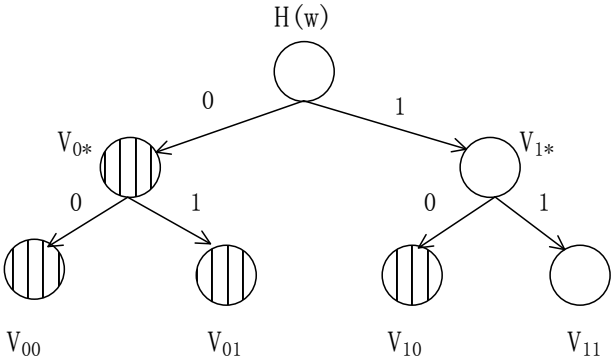

Fig. 2 The Security Classification Tree

Security Classification-Based Access Protocol

The access of power information system data is an interactive process among user, power information system and database. In this paper we focus on the access control of power information system data for user. The security classification-based access control protocol is composed of four sub-protocols: initialization, encryption, user registration and decryption.

1) Initialization

System parameters for access the data are initialized, class keys K_x are generated. Encryptor chooses a keyed HMAC $H_K()$, where K is the system access master key.

2) Encryption

In this phase, the encryptor generates the encryption key $K_{x,s}$ for each class of data at the security classification granule $s \in [0,z]$ and encrypts the data in security class C_x with corresponding key $K_{x,s}$. $K_{x,s}$ is computed as (1):

$$K_{x,s} = H_K(K_x || V_{B(s)}) \quad (1)$$

where $V_{B(s)}$ is computed by the method of security classification tree using the root value $H(w)$.

3) User Registration

When a user D_i wants to access the data, TA first verifies whether the user satisfies the conditions to register in the power information system. If the user passes the verification, according the security classification of the user, TA issues a system identity certificate containing information $Enc_{PK_{Di}}(\{V^u\}, H_K(\cdot))$ to user D_i as the identity proof to access the power information system.

4) Decryption

Suppose a user D_i is received a system identity certificate from TA, user D_i can access data class C_x whose security classification less than or equal to the user's security classification.

When user D_i request to access data of security class C_x, he first retrieves the information from the identity certificate using his private key and computes security classification values $V_{B(s)}$ with $\{V^u\}$. Then User D_i computes $K_{x,s}$ as Equation (1) and decrypts the data with $K_{x,s}$.

Conclusion

We have put forward a security classification-based access model for power information system. Differing from basic RBAC model, this access control model emphasizes more on the flexibility of roles and has the capability to control the access of sensitive data from security classification

dimension. For security classification, we have employed a security classification tree method for generating security classification granule values. The aforementioned description shows that our model can provide more stringent mandatory access control from security classification dimensions and data confidentiality for power information systems. Additionally, the model also can be used in the systems storing a mass of data on the untrusted remote DB or cloud. For such kind of systems, data encrypted stored is necessary. So, how to distribute keys for the legitimate users and how to build an index on the ciphertext are the key issues. Obviously, our key management scheme can be used to solve these issues. Moreover, our scheme gives a solution for the sharing of data across security domains between different settings. It also can be used to guarantee better security and privacy of data sharing.

Acknowledgement

The research was sponsored by the Information Center of Guangdong Power Grid Corporation's project of Study on Data Security in Big Data Environments (No.K-GD2014-1019) and Xinjiang Uygur Autonomous Region science and technology plan (No.201230121), the Strategic Priority Research Program of Chinese Academy of Sciences (No. XDA06040602).

References

[1] W.-G. Tzeng, A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy, IEEE Trans. On Knowl. and Data Eng., 14(1), 182–188, 2002.

[2] X. Yi and Y. Ye, Security of Tzeng's Time-Bound Key Assignment Scheme for Access Control in a Hierarchy, IEEE Trans. on Knowl. and Data Eng., 15(4), 1054 –1055, 2003.

[3] H. Y. Chien, Efficient Time-Bound Hierarchical Key Assignment Scheme, IEEE Trans. on Know. and Data Eng., 16(10), 1301–1034, 2004.

[4] A. De Santis, A. L. Ferrara, and B. Masucci, Enforcing the Security of a Time-Bound Hierarchical Key Assignment Scheme, Inf. Sci., 176(12), 1684–1694, 2006.

[5] X. Yi, Security of Chien's Efficient Time-Bound Hierarchical Key Assignment Scheme, IEEE Trans. on Knowl. and Data Eng., 17(9), 1298–1299, 2005.

[6] H. Huang and C. Chang, A New Cryptographic Key Assignment Scheme with Time-Constraint Access Control in a Hierarchy, Comput. Stand. & Int., 26, 159–166, 2004.

[7] Q. Tang and C. J. Mitchell, Comments on a Cryptographic Key Assignment Scheme, Comput. Standards & Interfaces, 27, 323–326, 2005.

[8] J. Yeh, An RSA-Based Time-Bound Hierarchical Key Assignment Scheme for Electronic Article Subscription, in Proc. of the 2005 ACM CIKM Conf. on Information and Knowledge Management, 285–286, 2005.

[9] G. Ateniese, A. De Santis, A. Lisa Ferrara and B. Masucci, Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, in Proc. of the 13th ACM Conf. on Computer and Communications Security - CCS 2006, 288–297. Full version available as Report 2006/225 at the IACR Cryptology ePrint Archive.

[10] S.-Y. Wang and C.-Laih, Merging: An Efficient Solution for a Time-Bound Hierarchical Key Assignment Scheme, IEEE Trans. on Dependable and Secure Comput., 3(1), 91– 100, 2006.

[11] A. De Santis, A. L. Ferrara, and B. Masucci, New Constructions for Provably-Secure Time-Bound Hierarchical Key Assignment Schemes, in Proc. of the 12th ACM Symposium on Access Control Models and Technologies-SACMAT 2007, 133-138.

[12] J. Liu and S. Zhong, A Practical Time Bound Hierarchical Key Scheme, International Journal of Innovative Computing, Information and Control, 5(10), 3241-3247, 2009.

[13]E. Bertino, N. Shang and S. S. Wagstaff Jr., An Efficient Time-Bound Hierarchical Key Management Scheme for Secure Broadcasting, IEEE Trans. On Dependable and Secure Computing, 5(2), 65-70, 2008.

[14] H.-M. Sun, K.-H. Wang and C.-M. Chen, On the Security of an Efficient Time-Bound Hierarchical Key Management Scheme, IEEE Trans. On Dependable and Secure Computing, 6(2), 159-160, 2009.