Privacy Protection Method Based on Access Control

Xin Qiao, Lixiaoyang Wang, Bo Qin, Hong Chen, Suyun Zhao
Renmin University of China, Beijing, China
E-mail: qiaoxin@ruc.edu.cn, wlxy@ruc.edu.cn, bo.qin@ruc.edu.cn
chong@ruc.edu.cn, zhaosuyun@ruc.edu.cn
Tel: +86-18110027161, +86-18813123118, +86-010 62512492
+86-010 62511262, +86-010 62514034

Abstract—**In the information era, users are increasingly communicating with each other through mobile devices, and making their personal information more and more involved in the network. As a result, security risks also greatly increase. In such a situation, this paper presents a privacy protection scheme based on access control. By adding permission bits to privacy data for access control and classifying multiple privacy situations, we give the corresponding solutions. This article has improved the existing roles concept and put forward the new concept of identity. It gives fine-grained access to different visitors. The visitors' identities are hierarchically defined and the partial order relation is used to determine the identity level. In order to match the basic principle of "High-level identities cannot modify low-level secrets. Low-level identities cannot read high-level information", the program requires that high-level identities can be transferred into low-level identities and identities must be transferred according to corresponding privacy level. With the flexible permission settings, it can be applied to various privacy protection situations.**

I. Introduction

With the development of the Internet and the widespread use of smartphones, more and more users' private information is stored on the Internet of which the leakage may cause serious security problems[1]. Nowadays, how to protect private information on the Internet from being leaked or maliciously stolen has become a research hotspot, with both theoretical and practical significance.

A. Related work

The issue of privacy protection can be summarized as "who, how, what, where, when (who can do what operation on what information at what locations and what time)", which is access control issues. The relevant technology of privacy protection based on access control over the world include TRBAC[2] , EPAL[3] proposed by IBM, P3P[4]and multi-level security relation database by W3C[5]. They are all proposed for certain specific situations, with some limitations and deficiencies

In an RBAC[6] model, roles represent functions within a given organization. Authorizations are then granted to roles, rather than single users. The authorizations granted to a role are strictly related to the data objects and resources that are needed for exercising the functions associated with the role. Since roles represent organizational functions, a role-based model can directly support an organization's security policy. Authorization administration is also greatly simplified. However, even though RBAC satisfy the basic principles[7] of access control, there are still significant application requirements not addressed by current RBAC models.

B. Our contribution

The new concept of identity is proposed, and the identity and privacy are analyzed. When reading the specific grade data, it must be converted to the corresponding identity, so that different visitors have different access rights. This paper presents a feasibility test of this scheme in different privacy situations. The results show that the access control method has flexible permission settings and can protect users' private data under different circumstances with high applicability.

C. Organization

The remainder of the article e is organized as follows. Section 2 describes the various attributes of privacy and services by giving privacy map and services map, according to which they were graded. Section 3 defines six functions used in the process of obtaining services .What's more, it also formalizes the system structure and finally introduces the access control scheme. Section 4 presents two examples to demonstrate the whole system and ideal effect. Section 5 concludes the article and outlines future research directions.

II. Division of service and privacy level

This article ranks identity and privacy and compares the privileges based on the levels of the two. The level of identity is determined by the services provided by the identity, which means the identity level is equal to the service level.

A. The attributes of privacy

In order to better classify privacy levels, this article analyzes various privacy attributes and design a privacy map as Fig.1.

In this privacy map，the circular frame represents the entity, and the square box represents the relationship between entities. This graph takes network privacy as centered and explained its attributes. It is visible from the graph that network privacy can be classified into different categories according to different standards. These standards includes subject power, the number of privacy ,the number of people involved, its object, its produce mode and the generation time of it. What's more, the subjects of privacy are all natural person.

B. Privacy level

In order to classify privacy levels, this article analyzes various privacy [8]attributes and design a privacy map as Fig.1.

From the map, we can see that personal network privacy is divided into five categories based on subject powers. This article ranks them by the importance:

Level 1: Life safety information, that is, information that may pose a security threat to users after leakage. Including hospital records, medical examination reports, genetic map detection, etc.

Level 2: Property security information and location information. The property security information refers to the private information, the leakage of which may cause the loss of user's property such as the user's credit card, social network account and passwords, etc.

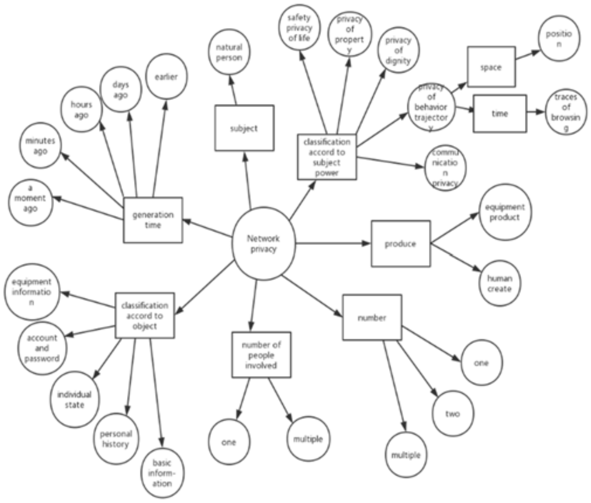


Fig. 1 Privacy map

Level 3: Communication information. Communication information includes telephone records, contacts, WeChat records, etc. Communication information may also include property safety information, giving it higher degree of importance.

Level 4: Identity information. One can be identified based on the identity information. Identity information includes birthplace, workplace, position, etc.

Level 5: Life trace information, which includes browsing records, Google search records, Amazon product browsing records, etc.

C. The attributes of services

The same analysis of service attributes can design the service map as Fig.2.

In reference to four criteria, the service map divide services into many kinds. These criteria include industry, object needs, required permissions and provider. Because the object of services is the same as the subject of privacy, the classification of the two is also a one-to-one matched. Besides, the required permissions of services represent "how to operate privacy".

D. Service level

Corresponding to the privacy level, the system also divides service into five levels and provides services according to respective privacy.

Level 1: Life Safety Services. These services help people stay away from pain, disease and death. The representative service providers include hospitals and clinics. The industries involved in these services include the security industry, the catering industry, the pharmaceutical industry and so on ,which can operate on privacy from level 1 to level 5.

Level 2: Property Security Services and Location Services. The major property security service providers include banks and insurance companies, which involved the financial industry, trade industry, business and so on. Representative service providers for location services are Baidu Map, Amap, etc. These services can operate on privacy from level 2 to level 5

Level 3: Communication services. Communication services store lots of chat records. The leading service providers are China Mobile Communications Corporation(CMCC), China United Network Communications Group Co.,Ltd (China Unicom) , etc, which can operate on privacy from level 3 to level 5.

Level 4: Identity Services. Most of these services are bundled with other services and most service providers ask for confirmation of customer identity before providing services. The services include personal qualifications and files, which can operate on privacy level 4 and level 5.

Level 5: Browse services. The service providers are mainly browsers, which recorded browsing traces and can only operate on the levels 5 of privacy.

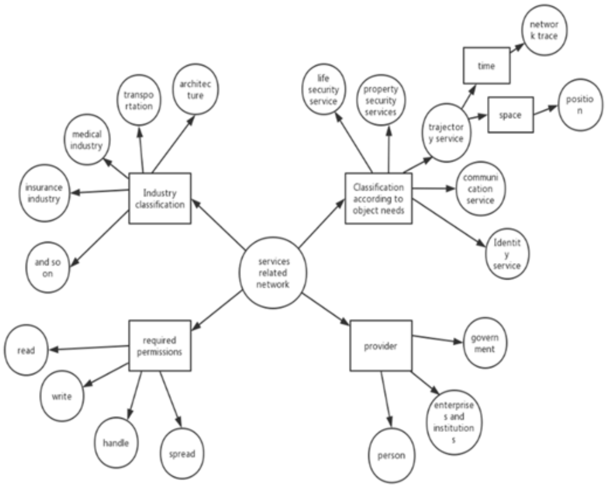


Fig. 2 Service map

III. PROGRAM DESIGN

This section designs a system to ensure privacy would not be leaked. At first part A defines all functions used in this system. Then, part B describes the whole model in which a user wants to operate data. Finally, part C presents the access control scheme in this system based on data level and service level.

A. Preparation

Definition 3.1 Identity login

The user must make clear the currently logged-in identity when logging into the system. The identity login requires three algorithms: Ulogin, Confirm, IdLogin. The algorithm is defined as follows:

1 or 0←Ulogin (userid, hash(password)). Check whether the login is successful based on the username and password hash value.

1 or 0←Confirm(userid,identity,U-ITable). Confirm indicates whether there is a current Identity in U-ITable. The function return value is 1 for existence, otherwise it returns 0.

1 or 0←IdLogin(time, place, identity, U-ITable). IdLogin indicates whether the current identity can be logged in at the current time and place. Inquire U-ITable to see whether the login succeed (return value is 1) or not (return value 0).

Definition 3.2 Identity shift

The partial order relations[9] between different identities are used to determine superiority and inferiority. They are reflexive, anti-symmetric, and transitive, and usually denoted as $\preccurlyeq$. In order to meet the "High-level identities cannot modify low-level secrets. Low-level identities cannot read high-level information"[9]principle, after being logged in, it may need to be transferred to a lower-level identity. For example, student A $\preccurlyeq$teacher B, and teacher B can be transferred to student A[11].

Definition 3.3 data level

Servicelevel←evaluate(service). According to the importance of privacy, the privacy is divided into different levels. See section 2.1 for privacy classification.

Definition 3.4 Service level

Servicelevel←evaluate(service). According to the importance of service provided, the service level are classified. See section 2.2 for the classification. The system recognizes the user's friends as service Level 4.

Definition 3.5 Data permission rules

Data permission rules define the operations that an identity can perform on data, which is a database relation table.

Rule←Require(data level, service level).

Definition 3.6 Data permission inquiry

Data access requires four parameters, data, operation, identity, permission bits, which can be defined as

1 or 0←Require(data, op, id, rule). A return value of 1 confirms that there is permission, otherwise there is no permission.

B. System structure

User: It is abbreviated as U in this system and is the owner and creator of private data[12].

Identity: The main unit of authority control. Users have different identities at different locations and different time. There is a many-to-many relationship between users and roles, but there must be a one-to-many relationship between users and identities, in other word, different users definitely have different identities.

Rules: It limits the operations that an identity can perform on the data.

Privacy Data: It is the user's privacy also the object of access control. All are stored as private files in this system.

C. Data Access Control

Identity creation process:

User Registration: The user submits the username and password hash value, and the manager records the data.

Identity Registration: Administrator posts user identity information into U-ITable and identity inheritance tables.

Data creation process:

User login: The user submits the username and password hash value. The manager runs Ulogin (userid, hash(password)) to confirm whether the login is successful.

Identity login: The Client automatically selects the identity, and submits the time, place, and identity. The server calculates Confirm (userid, identity, U-ITable) & IdLogin (time, place, identity, U-ITable) to confirm whether it can log in with the current identity.

Data writing: Identify the privacy level and the service level of the written data. Based on the two, the permission bits are determined, then the permission bits and the data are combined into a private file, and finally the private file is written into the server.

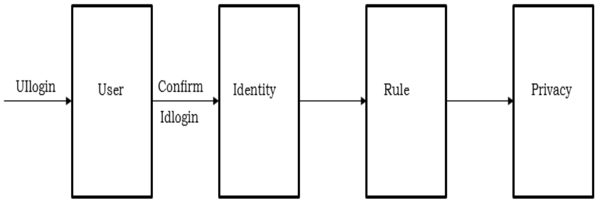


Fig. 3 The frame of privacy security system

Data operation process:

User login: The user submits the user name and password hash value. The manager runs Ulogin(userid, hash(password)) to check whether the login is successful.

Identity login: The Client automatically selects the identity, and submits the time, place, and identity. The server calculates Confirm (userid, identity, U-ITable) & IdLogin (time, place, identity, U-ITable) to confirm whether it can log in with the current identity.

Identity Conversion: The current identity may not have the target data operation permission and may need to be converted to another identity. Based on the current identity ID1 and the converted identity ID2., the server will check the identity relationship table to determine whether there is an ID2⩽ID1, and if it exists, perform the data access operation with ID2.

Data access: The server computes Require (data, op, id, rule), and if the result is 1, it allows the operation[13].

IV. CASE ANALYSIS

A. Hospital

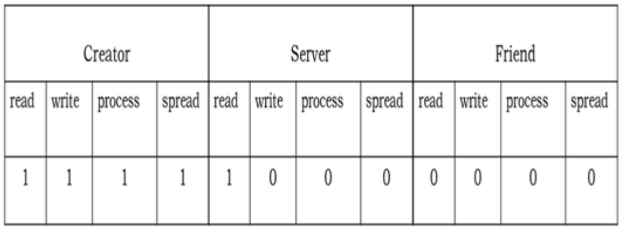
The representative privacy data in hospitals include medical records, patient names, patient ages, etc. Representative users include patients, doctors, and hospital chiefs. The hospital system is created and used as follows:

Registration:

Doctor A and Dean B register users and identities, set their identities as Doctor A and Director B, and recorded as Doctor A⩽Director B in U-ITable. The patient register as the identity P when entering the system. Assuming that the patient needs Doctor A to perform the diagnosis, then add the Doctor A to identities P's service provider group.

Privacy data creation:

This article uses the permissions bit to represent access



Creator				Server				Friend			
read	write	process	spread	read	write	process	spread	read	write	process	spread
1	1	1	1	1	0	0	0	0	0	0	0

Fig. 4 Permission bits of medical record

rights. The service provider requests to read and write private information such as medical records, patient names, and patient ages. The medical records are judged to belong to Level 1 private data, the service belongs to the Level 1 service, and they are at the same level, so the read and write permission bits are set to 1 and the rest are 0. The group of friends belongs to the Level 4 service cannot operate on the Level 1 private data. The permission bits are all set to 0. In general, the creator has full authority, but due to the special nature of medical record, it must be modified by the doctor instead of the user himself .Taking the mention above into account, the following permission bits should be added before privacy data:

After the creator P is written to file header, the system writes the file header, permission bits, and empty privacy data to the file. After writing the file, it will be modified by the doctor.

Data reading:

If Dean B needs to read the medical record, he must request to be converted to ID Doctor A after logging in as Director B. Because Doctor A⩽Director B, the system allows the conversion, this time the Doctor A identity is in the service data group of the private data, the query permission bit is found that the 5th bit is 1, that is, the service provider has the data read permission, so the system allows the Dean B to read the privacy data.

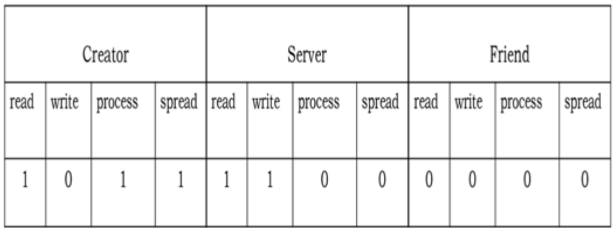
B. Navigation[14]

The representative information in the navigation situation is location information, and the representative identity includes a map software user and a navigation service provider.

Registration:

The navigation service provider and the user respectively perform user registration and identity registration, and set the two identities as Service A and User B, respectively. Then add ServiceA to the userB service provider group.

Privacy data creation:



Creator				Server				Friend			
read	write	process	spread	read	write	process	spread	read	write	process	spread
1	0	1	1	1	1	0	0	0	0	0	0

Fig. 5 Permission bits of position

The location information belongs to the Level 2 private information, and the navigation service belongs to the Level 2 service, thus they are at the same level. Since the navigation service needs to read the location information, only the read permission bit should be set to 1. The Friend group is not qualified at service level. Therefore, the permission bits are all set to 0. Thus, the permission bits are as Fig.5.

After the creator identity is written in the file header, the system adds the file header, permission bits, and empty private data to the file. Then the file is created.

Data reading:

Service provider A requests to read the file, and the manager knows that the creator is User B through the file header. Service A belongs to the User B service provider group, and the corresponding permission bit is 1, so the manager allows this operation.

V. SUMMARY AND PROSPECT

In view of the traditional access-control-based privacy protection method, this paper proposes the concept of identity in an innovative way. The identities and privacy are divided into different levels, the permission bits are set to the privilege, and the more granular permissions are given to visitors. Through case analysis, it is proven to be effective in data protection in different situations. However, with the rapid development of information technology ， higher requirements have been put forward, such as there must be a trusted manager and the additional storage space it takes up, etc., which shows there is still room for improvement.

This paper is supported by the National Key R&D Program of China through project 2017YFB1400700 and 2017YFB0802500, the Natural Science Foundation of China through projects 61772538, 61672083, 61370190, 61532021, 61472429, 91646203 and 61402029, by the National Crypt ography Development Fund through project MMJJ2017010 6.

REFERENCES

[1] Singh A, Liu L, Ahamad M. Privacy analysis and enhancements for data sharing in *nix systems[J]. International Journal of Information & Computer Security, 2010, 2(4):376-410.

[2] Elisa Bertino. TRBAC: A temporal role-based access control model[J] TISSEC August 2001 191-233

[3] Anne H. Anderson.A comparison of two privacy policy languages: EPAL and XACML SWS '06 53-60

[4] Lorrie Faith Cranor. Web Privacy with P3p[M] Sebastopol, CA, USA 2002

[5] James S. Miller. W3C and Digital Libraries[M] Corporation for National Research Initiatives 1996

[6] David F. Ferraiolo. Role-Based Access Control [M] Artech House, Inc. 2007

[7] Mark Stamp. Information Security: Principles and Practice[M] Wiley Publishing 2011

[8] Jaideep Vaidya. Privacy in the context of digital government[J] Proceedings of the 13th Annual International Conference on Digital Government Research 302-303

[9] Darrell Ronald Raymond. Partial-order databases[M] University of-Waterloo 1996

[10] Yi Lin. Bypassing portability pitfalls of high-level low-level programming[J] Proceedings of the sixth ACM workshop on Virtual machines and intermediate languages 23-32

[11] Mark Stamp . Information Security: Principles and Practice[M] Wiley Publishing 2011

[12] Blaze M. A cryptographic file system for UNIX[M]. CiteSeer, 1993

[13] Ravi S. Sandhu, et al., Role-Based Access Control Models,unpublished journal article

[14] Heiko Müller. Proximity sensor: privacy-aware location sharing[J] Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services 564-569