Research on Multiple Authentication Fuzzy Logic Relationship

Yuanyuan Wang, Guojian Cheng
Department of Philosopy, Xi'an Peihua University, Xi'an, China
Josefcheng2050@126.com

Keywords: Multiple identity authentications; Fuzzy reasoning; Fuzzy logic relationship

Abstract. Users by different intensity authentication can gain different levels of access in secure operating system. Multiple authentication using Multiple Identity Authentications (MIA) mechanisms and MIA rules authenticate users, through the fuzzy inference, the different users are given different authentication strength, in order to lay the foundation for access control and authorization. In this paper, the implementation of MIA is briefly described, including Single-Mechanism (SM) and Multi-Rule (MR) authentication mode, Multi-Mechanism (MM) and Single-Rule (SR) authentication mode, MM and MR authentication mode. Subsequently, the Fuzzy Logic Relationship (FLR) between requisite authentication mechanism, sufficient authentication mechanism and restraint mechanism, and the FLR between MIA rules are described in detail. The different relations implementation methods and the main problems are analyzed. The methods of calculating under the different relations are given. This paper provides a theoretical foundation for further research on the secure operating system MA, with a theoretical and practical significance.

1 Introduction

Identity authentication is the first barrier to secure operating systems and it is the basis for the effective implementation of a series of security functions such as access control. Secure operating systems use Multiple Identity Authentication (MIA) mechanisms to enhance system security. MIA is also referred to as "robust authentication". For example, passwords and fingerprints are used to authenticate users. MIA further enhances the reliability of identity authentication and provides security for system security.

At the same time, in a secure operating system, users with different levels of authentication should be granted different levels of access. There are many uncertainties in the authentication system. These uncertainties affect the ultimate authentication of the user. This article first briefly introduces the realization method of MIA, and then analyzes and measures the uncertain factors in the authentication system on the basis of FLR, and respectively explains and proves FLR between MIA mechanisms and MIA rules.

2 Multiple Identity Authentication

MIA uses MIA mechanisms and authentication rules to authenticate users. The combination of MIA mechanisms and authentication rules determines different implementations of MIA. Specifically, there are SM-MR authentication mode, MM-SR authentication mode, and MM-MR authentication mode.

2.1 The Principle of Digital Signature.

The SM-MR authentication mode means that each rule uses an authentication mechanism to authenticate users, and users must pass MR before they obtain services. The authentication rules can be expressed as:

$$\text{Rule}(i)\text{: IF } E_i \text{ THEN H } (i=1\sim n)$$

Among them, Ei (i=1~n) indicates that the system uses the authentication mechanism Ei (i=1~n) to authenticate the user; H means the user is trusted.

The PAM (Pluggable Authentication Modules) authentication framework[1][2] currently supported by many security operating systems is actually a SM-MR MIA framework. It realizes the

separation of service programs and authentication mechanisms, and supports the random combination of multiple services and MM to enhance the security of the system. The service program that needs to implement the identity authentication process respectively invokes various authentication mechanisms in the PAM system according to the configuration, and completes the user identity authentication through the joint authentication of MR according to the PAM control marking requirements.

2.2 MM-SR Authentication Mode

The MM-SR authentication mode is that a system uses a variety of authentication mechanisms to synthesize a SR to uniformly authenticate user identities. The authentication rules can be expressed as:

$$\text{Rule: IF} \quad E_1 \ op \ E_2 \ op \ \ldots\ldots \ op \ E_m \quad \text{THEN H}$$

Among them, Ei (i=1~m) indicates that the system uses the authentication mechanism Ei (i=1~m) to authenticate the user; op indicates the prerequisite connection operator, which may be and or or; H indicates that the user is trusted.

In this authentication model, the MM in the rules plays a role in different positions and influences. Through the rational configuration of the interrelationship between mechanisms, the system provides a flexible authentication function.

2.3 MM-MR Authentication Mode

The use of MR can further enhance the flexibility and controllability of the authentication system and enable dynamic MIA capabilities when needed. The authentication rules can be expressed as:

$$\text{Rule(i): IF} \quad E_{i1} \ op \ E_{i2} \ op \ \ldots\ldots \ op \ E_{im} \quad \text{THEN H (i=1~n)}$$

Among them, Ei (i=1~n，j=1~m) indicates that the system uses the authentication mechanism Eij (i=1~n，j=1~m) to authenticate the user; op indicates the premise of the connection operator, it may be AND or OR; H means the user is trusted.

This authentication mode is a combination of the above two authentication modes. By properly configuring the relationship between MIA mechanisms or MIA rules, complex authentication function requirements can be met.

The three authentication modes introduced above can enhance the security and reliability of the system to different degrees through reasonable configuration. In the specific implementation, the relationship between MIA mechanisms and the relationship between MIA rules is the main subject we need to study. By properly configuring different relationships, different authentication requirements can be met.

3 Uncertainty and Measurement in MIA

In a secure operating system, users should be granted different levels of access through different levels of authentication. The user's certification strength and certification conclusion are affected by many uncertainties in the authentication system. The uncertainties in the authentication system mainly include the uncertainty of whether the certification mechanism is credible, the uncertainty of whether the certification rules are credible, and the uncertainty of whether the certification conclusion is credible[3].

The uncertainty of whether the authentication mechanism is credible refers to the subjective degree of trust of the security administrator to the authentication mechanism. The authentication mechanism is not completely trustworthy, and users who use this mechanism for identity authentication cannot be completely trusted. The authentication mechanism may be exploited by hackers. The authentication credentials may be stolen and then deceive the authentication system. Therefore, the authentication mechanism needs to use a certain discount to use.

The uncertainty of whether an authentication rule is trusted refers to whether a user is a legal user. A security administrator can configure different rules to authenticate users. Each rule cannot have 100% trust. At the same time, in the case of MR, whether there are contradictory rules, whether it is necessary to select appropriate rules to apply through a certain contradictory resolution, contradictory resolution strategies also contain the uncertainty of the use of rules.

The uncertainty of the certification conclusion means that under the premise of containing various uncertainty certification mechanisms, the conclusion derived from using uncertain rules will inevitably have uncertainty. The uncertainty of the certification conclusion reflects the final impact of various uncertainties in the certification process. This is a process of dynamic accumulation of various uncertainties. The authentication system must have a way to achieve the most trustworthy certification conclusion in the entire authentication reasoning process by using the calculation model that meets the objective reality.

4 The FLR of MIA Mechanisms

In the MM authentication mode, the conditions between MM can be AND relations, and they can also be OR relations. We use symbols '◇' to represent them uniformly. Write rules as implied forms:

$$R: E_1 \diamond E_2 \diamond \ldots\ldots \diamond E_m \rightarrow H, T(R), \tau$$

Among them, Ei (i=1~m) and H have the same meaning as above; T(R) represents the rule strength, $0<T(R)\leq 1$; τ represents the rule applicable threshold[4], $0<\tau\leq 1$; the authentication strength of the authentication mechanism Ei (i=1~m) is expressed as T(ei), $0<T(ei)\leq 1$.

The relationship and or relationship between the MIA mechanism conditions, expressed as the operation between the credibility correspond to the "cross-type operation" and "parallel operation". In other words, the composite authentication strength is obtained by the "identification operation" or the "parallel operation" of the authentication strength of each authentication mechanism. "Complementary operation" corresponds to the "convergence" relationship, and "parallel operation" corresponds to the "disjunction" relationship. Reference[4][5] give a variety of "algebraic operations" and "parallel operations" that can be used in different situations.

In the certification process, according to the function of the certification mechanism, after a reasonable allocation, each mechanism can play a role with different status and influence. MIA mechanisms mainly include necessary authentication mechanisms, full authentication mechanisms, and constraint mechanisms.

4.1 Implementation of FLR of Necessary Authentication Mechanisms

The necessary authentication mechanism (Requisite) refers to the identity authentication mechanism that the system requires the user to pass, and the mechanism is also a necessary condition for the application of the authentication rule.

The necessary authentication mechanism includes two aspects. One is that the authentication strength of the mechanism must not be less than the rule applicable threshold, otherwise the rule is not available. Second, when the system authenticates a user, the user must satisfy the authentication requirements of the mechanism. That is, the user must be able to provide the corresponding certificate that satisfies the authentication requirements of the mechanism. Otherwise, the system rejects the follow-up authentication of the user and considers the user to be untrustworthy, thus rejecting the login. In the multi-authentication mechanism relationship, a "collection" relationship is used to introduce the necessary authentication mechanism for the authentication rules. For example:

$$R: E_1 \wedge (E_2 \diamond E_3) \rightarrow H, T(R), \tau$$

Where, E_1 is the condition of the necessary authentication mechanism for introducing H. That is, if $T(e1)<\tau$, the rule cannot be used. At the same time, when $T(e1)\geq\tau$, if the user fails to meet the authentication requirement of the mechanism e1, the system will directly refuse the login of the user and assume that the user authentication fails. Conversely, E2 and E3 are not necessarily necessary, as long as the synthetic authentication strength of (E2 ◇ E3) is not less than τ, the rule can be used. Of course, E2 and E3 are other than "collection".

4.2 Full Authentication Mechanism FLR Implementation

The full authentication mechanism (Sufficient) refers to an authentication mechanism with higher reliability. After the user passes the authentication, the system has reason to believe that the user is legal and allows the user to log in to the system, but when the user cannot meet the

authentication of the mechanism when required, the system will enable other mechanisms to authenticate users.

The full authentication mechanism generally has higher authentication strength. In the multi-authentication mechanism relationship, a "extract" relationship is used to introduce a full authentication mechanism for the authentication rules. For example:

$$R: E_1 \vee (E_2 \diamond E_3) \rightarrow H, T(R), \tau$$

Where, E_1 is the full authentication mechanism for H. When the user meets the authentication requirements of the mechanism and passes the authentication of the mechanism, the system considers the user to be authentic, so it will not continue the subsequent authentication and allow users to log in. If the user does not meet the authentication requirements of the mechanism, the system will invoke a subsequent authentication mechanism to authenticate the user.

4.3 Constraint Mechanism FLR Implementation

The constraint mechanism is in fact a special case of the necessary mechanism. It refers to certain constraints of the system on the authenticated user, such as work time constraints, restrictions on login locations, restrictions on the number of authentications, and so on. From the security point of view, in the multi-authentication mechanism relationship, the constraint mechanism and other authentication mechanisms are in a “conjunctive” relationship. That is, the constraint conditions must be satisfied in the authentication inference, only if the constraint conditions are satisfied. The authentication mechanism has meaning to the user's authentication reasoning, otherwise the rule containing the constraint condition cannot be used.

In practical applications, we specify that the credibility of the constraint mechanism belongs to the set {0, 1}, the credibility is 1 to satisfy the constraint condition, and the authentication rule containing the constraint condition can be used; the degree of confidence of 0 indicates that the constraint is not satisfied. Conditions, the corresponding certification rules can not be used.

5 FLR of MIA Rules

The MR authentication mode is written in the form of implication:

$$R_i: E_i \rightarrow H, T(R_i), \tau_i \quad (i=1\sim n)$$

Where Ei (i=1~n) and H have the same meaning as above; $T(R_i)$ represents the rule strength, $0<T(R_i)\leq 1$; τi represents the rule applicable threshold, $0<\tau_i\leq 1$; authentication mechanism Ei (i=1~n), whose certification strength is expressed as $T(e_i)$, $0<T(e_i)\leq 1$.

In fuzzy inference, MR introduce the same "user credible" conclusion, but their user credibility is not the same. According to the system's requirements for authentication, MR can still be configured as an OR relationship. In the case where MR participate in authentication inference, there are two ways to accomplish user authentication.

(1) Reasoning before and after synthesis. According to the authentication configuration requirements, the user first obtains the corresponding user authentication credibility by passing the authentication of each rule, and then uses a certain synthesis algorithm to synthesize the credibility of each user to obtain the final user authentication credibility. This reasoning is called "Type I reasoning."

(2) First synthesis, after reasoning. According to the authentication configuration requirements, MR first synthesize the conditions of the authentication mechanism, convert the MR authentication mode into a MM SR authentication mode, and then the system authenticates the user again to obtain the user authentication credibility. This reasoning is called "Type II reasoning."

5.1 Type I Reasoning - First Reasoning, Then Synthesis

After each user passes the authentication of each rule, the corresponding user authentication credibility $T(H_i)=FR(T(e_i),T(R_i))$ is obtained. Then use some sort of rule synthesis operator RC to obtain the end user confidence $T(H)=RC(T(H_1),T(H_2),\cdots,T(H_n))$. This method of reasoning synthesis is a commonly used algorithm in the field of artificial intelligence. According to the certification configuration requirements, all the rules that participate in the certification are considered to be concurrent, with no distinction between primary and secondary orders. That is to

say, the authentication mechanisms used in the rules are in the same position in the certification, and all the rules have the same impact on the certification. They together determine the ultimate credibility of the user's authentication. Some synthetic operators are given in reference[4][6]. These operators have different characteristics and can be selected according to their needs. It should be noted that if we choose different synthesis operators for the "conjunctive" and "extract" rules, then at the time of synthesis, MR for the "conjunctive" relationship and MR for the "disjunction" relationship should be synthesized separately, then do the final synthesis based on the authentication configuration requirements.

5.2 Type II Reasoning - First Synthesis, Then Inference

This kind of reasoning method is to first synthesize the condition of the authentication mechanism used in each rule according to a conditional composition operator MC to obtain the composite authentication strength $T(e)=MC(T(e_1),T(e_2),\ldots,T(e_n))$, and then obtain the synthesized synthesis rule strength T(R) and the rule application threshold τ, convert the MR authentication mode into a MM SR authentication mode, and then obtain the end-user credibility based on the inference algorithm. (H) = FR(T(e), T(R)). Here, the T(e), T(R) and τ values need to be determined separately according to the different relations of the authentication mechanism conditions. The "conjunction" relationship between certification rules indicates that the certification configuration requires that MIA rules are required in authentication. When a user performs identity authentication, it must pass all the rules to obtain the final authentication credibility.

6 Conclusions

The secure operating system grants different degrees of access to users who have been authenticated with different strengths. MIA uses MIA mechanisms and MIA rules to authenticate users, and different users are given different authentication credibility through fuzzy inference, laying the foundation for access control authorization. This paper elaborates on the FLR between MIA mechanisms and MIA rules in MIA, analyzes the implementation methods of different relationships and the main problems, and gives the calculation methods under different relationships. It provides a theoretical foundation for further research on MIA for secure operating systems, and has strong theoretical and practical significance.

References

[1] Sun Microsystems, Inc. Extending Authentication in the Solaris 9 Operating Environment Using Pluggable Authentication Modules (PAM): Part 1. http://www.sun.com/blueprints/0902/816-7669-10.pdf. 2002

[2] Rich Teer. User Authentication on the Solaris OS Part 2: Introduction to PAM. http://developers.sun.com/solaris/articles/user_auth_solaris2.html. 2007.

[3] Wang Lun-wei, Liao Xiangke, Wang Huaimin. Research on the Credibility of Certification Theory. Computer Research and Development. 2005, 42(3): 501-506.

[4] He Xingui. Theory and technology of fuzzy knowledge processing. Beijing: National Defense Industry Press. 1998.

[5] Dubois D, Prade H. A Class of fuzzy measures based on triangular norms. International Journal of General Systems. 1982，(8)：43-61.

[6] Zhang Wenxiu, Liang Yi, Xu Ping. Uncertain Reasoning Based on Inclusion Degree. Beijing: Tsinghua University Press, 2007.