A Novel Weight Adaptive Multi Factor Authorization Technology

Ruiqi Zeng[2,3(✉)], Leyu Lin[2,3], and Yue Zhao[1,2,3]

[1] Science and Technology on Communication Security Laboratory, Chengdu 610041, China
[2] No. 30 Research Institute of China Electronics Technology Group Corporation, Chengdu 610041, China
zengruiqi@sina.com
[3] Electronics Technology Cyber Security Co. Ltd., Chengdu 610041, China

Abstract. Facing the increasingly complex computer network system, the importance of network security has become increasingly prominent. Authentication and authorization are important components of computer network security protection. Authentication is the process of verifying the user's identity, and authorization is the process of verifying the user's right to access. In terms of authorization, although there has been a lot of research on related aspects, from the perspective of authority determining factor, it mainly focuses on single-factor authority. For authority control in complex scenarios, single-factor often has great limitations, because it cannot carry out precise control. This paper takes multi-factor authorization as the research object, studies the role of multi-factor in the authorization process, and designs a simple multi-factor authorization algorithm. On this basis, the factor weight adaptive technology is studied, and two adaptive weight algorithms are designed to meet more precise authority control in complex scenarios. Through construction and testing of the actual prototype system, the utility and advantages of multi-factor and weight adaptation in authorization are verified, which expands ideas for subsequent in-depth study of authorization technology in complex scenarios.

Keywords: Authorization · Authority control · Multi-factor · Weight adaptive

1 Introduction

Internet is open to the whole world, and any unit or individual can conveniently transmit and obtain various information on the Internet. The open, shared, and international characteristics of the Internet pose a challenge to computer network security. There are many factors that constitute insecurity to computer information, including human factors, natural factors and accidental factors. Computer network security is to protect hardware, software, and data resources in computer network system from being damaged, modified, or leaked due to accidental reasons or malicious attacks, so that network system can operate continuously and reliably, and network service is normal and orderly [1].

W. Fu and L. Yun (Eds.): ADHIP 2022, LNICST 469, pp. 446–457, 2023.
https://doi.org/10.1007/978-3-031-28867-8_33

In computer security system, identity verification and authorization protection are an important part. Authentication is used to verify user's credentials, such as user name, user ID, etc., to determine user's identity. Common authentication is usually done through username and password, sometimes combined with authentication factors. There may be several authentication factors: single-factor authentication, which is the simplest method of authentication, and usually relies on simple passwords to grant users access to specific systems (such as websites or networks); two-factor authentication, which is a two-step verification process that requires not only a user name and password, but also some sort of user characteristics to ensure a higher level of security; multi-factor authentication, which is the most advanced authentication method, uses two or more security conditions in independent authentication categories to grant users access to the system [2].

Another aspect of system protection is authorization. Authorization is the process of determining whether an authenticated user can access a specific resource. Authorization occurs after system successfully authenticates user's identity, and finally grants user some access to resources (such as information, files, databases, funds, locations, and almost any content). Authorization determines user's ability to access system and extent to which it can reach.

In the process of authorizing a user, it can be determined by a single factor or by using multiple factors. The single-factor authorization system uses only one condition as the authorization basis, such as role authorization. Multi-factor authorization is the process of using two or more conditions to control user access. Thus, access security is effectively improved by combining multiple attribute conditions, such as user characteristics, environmental factors and resource attributes [3].

In multi-factor authorization, in order to better express relationship between each factor and improve accuracy of the final authorization result, it is necessary to assign weight to each factor and establish a multi-factor authorization algorithm. Generally, the weight of the system is pre-configured and will not change arbitrarily, but for complex scenes, a fixed weight value often cannot reflect changes in environment and cannot achieve a very accurate authorization effect. At this time, a multi-factor authorization method with adaptive weights can be considered [4]. Self-adaptive means that in the process of processing and analysis, the processing method, processing sequence, processing parameters, boundary conditions or constraint conditions are automatically adjusted according to characteristics of the processed data, so as to adapt to statistical distribution characteristics and structural characteristics of the processed data, and achieve the best treatment effect. Weight adaptation means that the weight automatically adjusts and adapts to changes in environment to achieve the best weight value.

At present, there are not many related researches on weight adaptive multi-factor authorization control. In order to explore weight adaptive and multi-factor authorization algorithms, this paper first studies the role of multi-factor in authorization, and gives some multi-factor authorization algorithms to verify the advantages of multi-factor authorization in complex scenarios. On the basis of this research, weight adaptation is discussed, some weight adaptation algorithms are proposed, and the design scenarios are verified. Finally, the verification results are summarized, and the follow-up research is prospected.

2 Multi-factor Authorization

In network security, user identification and authorization are very important parts, among which authorization is to grant permissions to user after identification. There are many ways of authorization, such as ABAC [5], RBAC, DAC, MAC, etc. Some authorization systems are based on a single factor. This type of system is often used in simple scenarios. For some complex scenarios, it cannot achieve good results. At this time, a multi-factor authorization method is required. Multi-factors can take multiple factors into consideration, realize multi-dimensional and multi-level authorization, and achieve more precise authority control.

2.1 Multi-factor Combination

Single factor analysis refers to the analysis of a certain variable at a certain moment, such as time factor, spatial factor, and personnel characteristics. Through the analysis of a certain variable, a certain conclusion can be drawn, or a certain operation can be carried out.

Multi-factor analysis is a series of statistical analysis methods that study the relationship between multiple factors and the individuals with these factors. Multi-factor analysis is used to explain the direction and extent of the overall change caused by each factor change when the total change of a phenomenon is affected by three or more factors. Through multi-factor analysis, it is possible to observe the target in multiple dimensions, obtain target characteristics, gain a deep understanding of the system from different angles, and find related relationships, so as to obtain more comprehensive and in-depth results and support subsequent operations more accurately.

In a single-factor authorization system, authorization is often performed based on a certain factor, such as granting a certain authority based on a certain identity. For general simple scenarios, single-factor authorization can meet the target requirements, but in some complex scenarios, the actual conditions are often more complicated, and single-factor conditions cannot meet the needs well. In this case, it is necessary to combine multiple factors to analyze at the same time, so as to make a more comprehensive and accurate judgment, and carry out more precise authority control. At the same time, multiple factors can achieve different combinations, thereby enabling multi-level authorization from different angles and dimensions to meet richer needs.

In the design of our authorization scheme, we adopted a multi-factor analysis method and used multiple factors as the basis for judgment to construct a complex authorization control scenario. When building our prototype system, a scenario with three factors acting simultaneously was simulated, and the accuracy value of each factor was used as a measure to achieve more precise authority determination.

2.2 Multi-factor Weighting Algorithm

When a multi-factor strategy is adopted, multiple factors jointly affect the decision-making, and the analysis result is calculated by the multi-factor weighting algorithm.

We use weighted average method, which is to set a weight for each factor and find their weighted average [6]. The calculation formula is shown in formula 1.

$$score = \sum_{k=1}^{k=n} (V_k * W_k) \tag{1}$$

In the above formula, the measured value of each factor is multiplied by its own weight, and their sum is the final result. In addition to the weighted average method, other algorithms can also be used, or you can customize the algorithm according to the actual situation.

In our prototype system, we simulated four factors, as shown in Fig. 1. The four factors are: facial recognition, gender, coat color, and identification accuracy weighted average. Among them, the weighted average of factor accuracy is a comprehensive value of the previous three factor accuracy, which is obtained by the above weighted average algorithm.

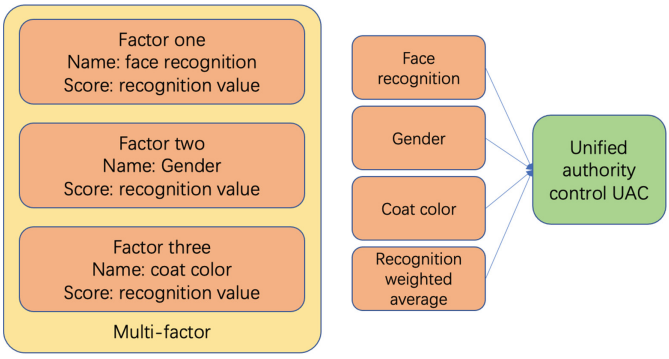

Fig. 1. Authority factors.

2.3 Multi-factor Authorization Prototype System Experimental Results

In order to verify the effect of multi-factor authorization, we designed a prototype system to simulate the role of multiple factors in the authorization determination process.

In our design, we deployed three identification factors, namely: name, gender, and coat color. The system structure diagram is shown in Fig. 2. Three cameras are used to shoot separately, corresponding to the three factors of name, gender, and coat color. Each camera has a monitoring program which records captured image and sends the pictures to the multi-factor authorization program. The multi-factor authorization program contains a multi-factor authorization algorithm to calculate the final recognition value. The final recognition value here is the weighted average of the recognition degrees mentioned above. The multi-factor authorization program also includes weight configuration, and the weight of each factor can be manually set to meet customized requirements. After that, the system will sort out all user attributes, including: name, gender, coat color, and final recognition value, and send these attributes to the unified authority control UAC

system connected to the multi-factor authorization program for authority determination. For users who pass the authorization judgment, the program will call the door lock application of the Internet of Things to open the door lock.

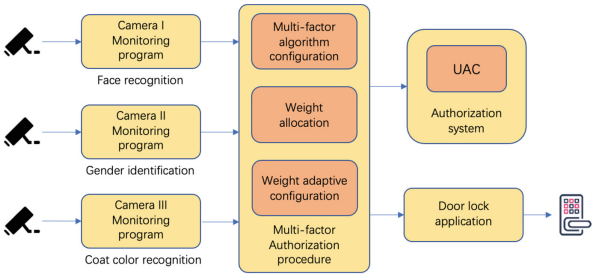

Fig. 2. Weight-adaptive multi-factor authorization prototype system architecture.

The experimental environment is shown in Fig. 3, including cameras, camera program, multi-factor authorization program, UAC authority control program, door lock application, and Internet of things devices.

Fig. 3. Experimental environment.

The overall system configuration interface is shown in Fig. 4. Including weight setting, weight algorithm, and weight adaptive algorithm. The weight adaptive algorithm will be discussed in next section.

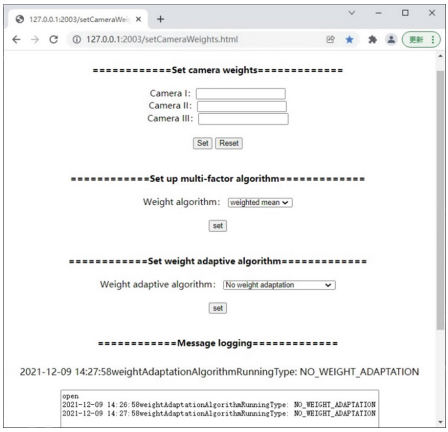

Fig. 4. System configuration user interface.

The factor weight can be manually set to meet specific needs. The configuration result is shown in Fig. 5.

Fig. 5. Weight configuration successful.

The effect of multi-factor authentication is shown in Fig. 6. It can be seen that the determination strategy is defined, multiple user characteristics are obtained through different cameras, and the final score value is calculated, after that all the characteristic value and final score value are passed to authority control system to authorize user to unlock the door. The system message records the entire multi-factor authority process.

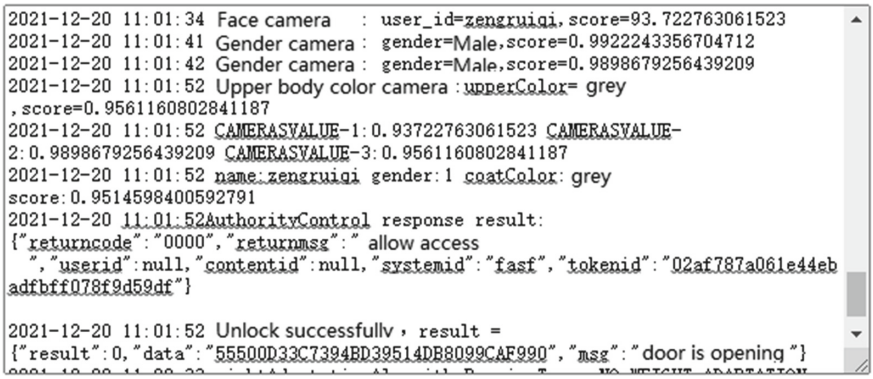

Fig. 6. System running process display.

2.4 Multi-factor Authorization Advantages

In our multi-factor authority determination design, we combine multiple factors for authority control, which can be applied to complex control scenarios. Factors can be adjusted according to the actual situation to monitor in different dimensions, and control more precisely. At the same time, the multi-factor weighting algorithm can also be adjusted to meet the various needs of different scenarios.

3 Weight Adaptation

Self-adaptation means that in the process of processing and analysis, the processing method, processing sequence, processing parameters, boundary conditions or constraint conditions are automatically adjusted according to characteristics of the processed data, so as to adapt to statistical distribution characteristics and structural characteristics of the processed data, and achieve the best treatment effect. Applying adaptive technology to multi-factor authority control can continuously achieve the best control effect as the environment changes.

3.1 Weight Adaptation

In multi-factor algorithm, each factor has a weight, which is used to determine factor proportion, and illustrate its importance. In some simple scenes, the weight is fixed, but in many complex scenes, fixed weight does not reflect real situation, because environment is constantly changing, and the actual proportion and importance of each factor are also constantly changing. At this time, the weight needs to be changed accordingly, automatically adapting to changes in the environment, that is, the weight is adaptive [7].

3.2 Adaptive Algorithm

There are many kinds of adaptive algorithms, the more common ones in industrial applications are LMS, RLS algorithms, etc. [8].

For our multi-factor authorization process, our multi-factor weights have customized some algorithms according to our own scenarios, including fixed weight, time period adaptation and average value adaptation.

Fixed weight means that the weight value of each factor is a fixed value, and it will not change as the environment changes.

The time period-based adaptive algorithm takes time periods as a reference and sets different weight values in different time periods. In the factor setting, three factors (name, gender, and coat color) are set. The weight of each factor is set separately according to the time period. The weight values of name, gender, and coat color in first time period are set as: 0.6, 0.2, 0.2, and the weight values in second time period are set to: 0.2, 0.6, 0.2, and the weight values in third time period are set to 0.2, 0.2, and 0.6 respectively. This simulates the weight change of different time periods (Fig. 7).

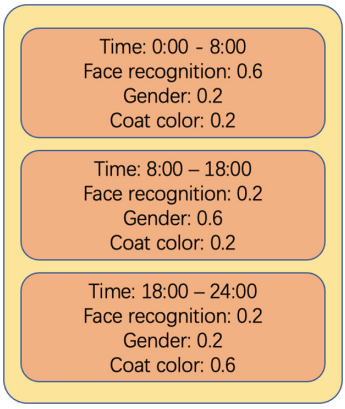

Fig. 7. Time period weight adaptation.

The average value adaptive algorithm is based on the average value of recognition accuracy of each camera. The specific algorithm process is, first record the recognition accuracy of the last 20 photos taken by a single camera (a certain factor), and then calculate their average accuracy value, the calculation formula is shown in formula 2. After that, the accuracy averages of all factors are compared and sorted, and finally a set of weights is defined and these weights are assigned to the ranked factors.

$$averageScore = (\sum_{k=1}^{k=n} V_k)/n \tag{2}$$

Figure 8 is the algorithm flowchart. In our setting, we also define three factors: name, gender, and coat color, and define three weights: 0.45, 0.35, 0.2. Three weight values are assigned to each of the three factors respectively based on the order of the average value of each factor recognition degree. In this way, the weight value of each factor will be adjusted in real time according to recent recognition accuracy status. Here we simulate a scenario, in which the factor with higher recognition accuracy will be assigned a high weight value, and the factor with lower recognition accuracy will be assigned a low weight value.

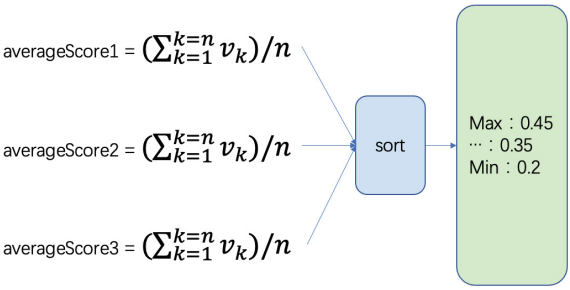

Fig. 8. Average value adaptive algorithm steps.

A variety of weight adaptive algorithms can be configured to use the optimal algorithm at the right time.

3.3 Experimental Results of Adaptive Algorithm

After prototype system is configured, system runs as shown in Fig. 9.

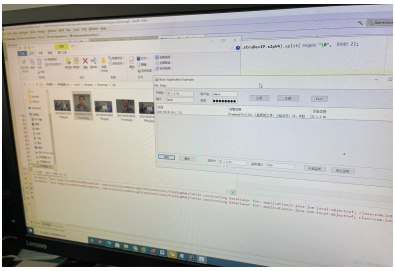

Fig. 9. System operation diagram.

After our prototype system is deployed, no adaptive algorithm is selected in initial stage, so it displays “NO_WEIGHT_ADAPTATION” as shown in Fig. 10. At this time, there is no weight adaptation, and each factor weight is initial value. In our experiment, the default weights of three factors name, gender, and coat color are set to: 0.33, 0.33, 0.33.

Fig. 10. No weight adaptation.

Set system weight adaptation algorithm to "time period weight adaptive", the output window will show "TIME_PERIOD_WEIGHT_ADAPTATION", and we can see that weight values of the three factors (name, gender, and coat color) are set to: 0.2, 0.6, 0.2, match time period 8:00–18:00 (Fig. 11).

Fig. 11. Time period weight adaptation.

Set system weight adaptation algorithm to "Average weight adaptive", the output window will show "AVERAGE_VALUE_WEIGHT_ADAPTATION". In initial stage, the average recognition value of the three factors (name, gender, and coat color) are set to 0.8, 0.6, and 0.4 by default, so the weight values of the three factors default to: 0.45, 0.35, 0.2. The default weights can be seen in the output window (Fig. 12).

The average value weight adaptation algorithm will count average value of the recognition degree of each factor for the last 20 values to reflect the latest environmental changes. In the subsequent system operation, the weight value changed in real time will be used for calculation, and the result will be used in authority judgment.

Fig. 12. Average value weight adaptation.

3.4 Weight Adaptation Advantages

Through our multi-factor weight adaptive algorithm, the weight can be automatically adjusted with time and environment changes in real-time and will achieve best matching-degree for factor weight. At the same time, the adaptive algorithm can also be configured to meet different needs in different scenarios.

4 Conclusion

This paper studies multi-factor authorization technology with adaptive weights. The paper first explains that with the development of computer network system, authentication and authorization play an important role in computer network security. Then it explains the drawbacks of single-factor authorization and conducts related research on multi-factor authorization, and designs a simple multi-factor authorization algorithm. On this basis, the factor weight adaptive technology is studied, and two adaptive weight algorithms are designed to meet more precise authority control in complex scenarios. Through construction and testing of the actual prototype system, the utility and advantages of multi-factor and weight adaptation in authorization are verified, which expands ideas for in-depth research of authorization technology in complex scenarios.

This research innovatively adds multi-factor authorization algorithms, carries out multi-factor correlation analysis, and can realize multi-level and more accurate authority control, which is impossible in general authorization system. At the same time, the proposed factor weight adaptive algorithm can adapt factor weight to environmental changes, so that the subject analysis is more in-depth, and the authorization process can adapt to more complex application scenarios which general authorization systems cannot be applied to.

In the follow-up research, we will continue to in-depth study of weight adaptation and authorization algorithms in complex scenarios, and introduce some more complex analysis systems, such as big data platforms and artificial intelligence, to further increase the accuracy of authority control.

Acknowledgements. Foundation Item: Supported by Sichuan Science and Technology Program (No. 2021YFG0164).

References

1. Nameless. Cybersecurity Law of the People's Republic of China. Communique of the Standing Committee of the National People's Congress of the people's Republic of China, 2020(3):9
2. Jing, K., Zhang, X., Xu, X.: An overview of multimode biometric recognition technology. In: The 6th International Conference (2018)
3. Ayfaa, B., Apa, C.: LMAAS-IoT: lightweight multi-factor authentication and authorization scheme for real-time data access in IoT cloud-based environment. J. Network Comput. Appl. (2021)
4. Melki, R., Noura, H.N., Chehab, A.: Lightweight multi-factor mutual authentication protocol for IoT devices. Int. J. Inf. Secur. 19(6) (2020)
5. Shen, H.B., Hong, F.: Research on attribute-based authorization and access control. J. Comput. Appl. **87**, 39–45 (2007)
6. Dong, H.L., Park, D.: An efficient algorithm for fuzzy weighted average. Fuzzy Sets Syst. **87**(1), 39–45 (1997)
7. Sun, M., Dou, H., Yan, J.: Efficient Transfer Learning via Joint Adaptation of Network Architecture and Weight. Springer, Cham (2020)
8. Narayan, S.S., Peterson, A.M., Narasimha, M.J.: Transform domain LMS algorithm. IEEE Trans. Acoust. Speech Signal Process. **31**(3), 609–615 (1983)