DOI: 10.23977/cpcs.2023.070112
ISSN 2371-8889 Vol. 7 Num. 1

Digital Tiger Symbol Authorization Method Based on PKI System

Yanhang Chai[1], Wen Li[1,*], Wentao Zhang[2], Wei Bai[1]

[1]Army Engineering University of PLA, Nanjing, Jiangsu, 210007, China
[2]School of Software, Liaoning Technical University, Fuxin, Liaoning, 123032, China
[*]Corresponding author

Keywords: PKI, digital tiger symbol, fine-grained authorization, digital certificate, cryptography

Abstract: Under modern high-tech conditions, the importance of personnel authorization security is increasingly prominent. A set of safe authorization method can ensure that human resources are properly distributed to each unit, thus providing reliable guarantee for the successful completion of tasks. However, current personnel authorization are still paper-based or verbal, prone to errors or inconsistencies, and difficult to verify. In this paper, a method of digital Tiger Mark authorization based on PKI system is proposed, using modern cryptography technology to provide support for the security and reliability of personnel authorization. This method realizes fine authorization, and the authorization can be verified. The method uses digital certificates to assign people's identities to their respective roles, and uses encryption algorithms to enforce access control policies and prevent unauthorized access. The feasibility of this method is verified by us in a simulated cross-domain task environment.

1. Introduction

Personnel authorization has always been one of the core concerns for leaders. In ancient times, military power was granted through tiger symbols. There are many details on the tiger symbol, so it has the anti-counterfeiting function, but also has great limitations: the tiger symbol is usually awarded by the ruler to the marshal, but the specific content of the authorization cannot be reflected from the tiger symbol. In general, the tiger symbol is more of a symbolic meaning. Under high-tech conditions, personnel authorization is also a key process in modern mission operations, as it governs the allocation of resources and operational tasks across multiple domains such as land, sea, air, cyberspace and outer space. The process involves several steps, including verifying identities and credentials of personnel, authorizing them according to the mission plan, allowing them to use resources within the scope of their authorization, and allowing them to verify the validity of the superior authorization through the Digital Tiger Symbol system. However, current personnel authorization practices are often paper-based or vobal, and prone to human error, duplication, and inconsistency. In addition, cyber threats have increased the need for secure and reliable personnel authorization mechanisms that can adapt to changing environments and threats.

2. Key Technology of Authorization Method

In order to deal with these challenges, this paper proposes a Digital Tiger Symbol authorization method based on PKI system, which uses principles of PKI public key system and cryptography to establish trust among participants in a multi-domain environment by using digital certificates, and provides a secure and scalable framework for fine-grained authorization. Specifically, the method mainly comprises the following key technologies:

Granular Role-based authorization: A solution for identity authentication and rights management. According to factors such as task planning, user roles, job responsibilities, resource requirements and the like, the authorization content can be subdivided into dimensions such as time, region, object, command mode, authorization type, etc., rapid authorization can be realized based on roles. At the same time, each dimension can be adjusted according to the actual situation of the task to realize refined management of authorization.

Identity Authentication Management: uses CA certificate chain-based technology for online authentication and authorization, issues and revokes digital certificates to personnel, verifies the identity and level of the holder, and maintains a centralized directory of all certificates. It is used to realize various functions such as command authorization, authorization validity verification, etc., so as to ensure that certificate management plays its due role in various occasions.

Encryption Protocol Layer: to ensure the secure transmission of authorization commands, and can provide functions such as encryption, decryption, signature and verification. Due to the relatively small data volume of commands, but high requirements for keys, we mainly use RSA asymmetric encryption algorithm to generate public-private key pairs to encrypt, decrypt and sign command authorization [1]. It shall maintain the functions such as private key/public key management, security script detection, alarm handling of abnormal events to ensure that data will not be attacked and leaked, so as to realize the functions such as identity authentication, access control, data encryption, login protection, etc., to ensure confidentiality, integrity and authenticity of messages exchanged between participants.

User Interface: Use visual operation mode to bring users a simpler and more comfortable solution. The system user interface module relies on highly optimized interaction design and interface aesthetics to complete fast human-computer interaction, so that users can easily complete various tasks such as registration and issuing commands.

2.1. Granular Role-based Authorization

Fine-grained authorization supports user-defined roles. Permission control is realized by granting resource permissions and operation permissions to roles and then assigning roles to users. It supports one-to-many, many-to-one, many-to-many authorization models. Users can perform fine-grained resource authorization according to business requirements to ensure that corresponding personnel only have corresponding resource permissions.

The specific process of role-based fine-grained authorization is shown in Figure 1:

1) The authorization establishes personnel authorization decision-making system and norms;

2) The authorization collects and organizes intelligence and data from various sources;

3) The authorization analyzes and judges the information, and formulates various battle plans;

4) The authorization decomposes battle plans into different task units and establishes corresponding task sets;

5) According to the urgency of tasks, mutual relevance, feasibility, and other factors, the authorization completes the task authorization and issues instructions;

6) The authorization continuously monitors and evaluates the implementation effects, and adjustment command and decision-making according to the situation.

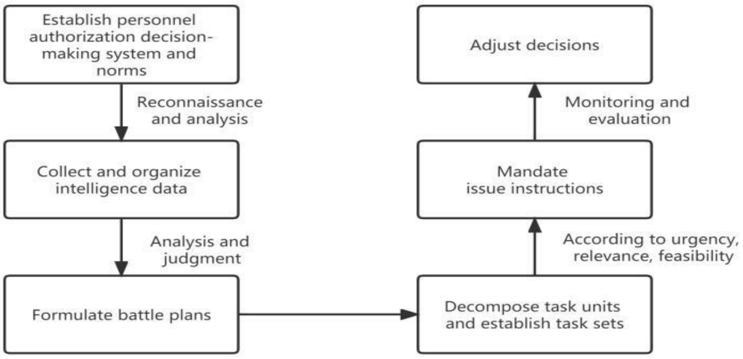
Establish personnel authorization decision-making system and norms
Reconnaissance and analysis
Collect and organize intelligence data
Analysis and judgment
Formulate battle plans
Decompose task units and establish task sets
According to urgency, relevance, feasibility
Mandate issue instructions
Monitoring and evaluation
Adjust decisions

Figure 1: Basic Flow of Fine-grained Authorization

2.2. Identity Authentication Management

After analyzing and comparing the common identity authentication technologies at home and abroad, Hesong [2]. proposed the applicability of the authentication protocol based on shared secret key. Wu Bo [3]. proposed five common identity authentication technologies, among which the authentication based on digital certificates has been widely accepted, which adopts the public key cryptosystem, and the private key of CA and user will not be transmitted on the network, even if the attacker intercepts the certificate of the user, the attacker cannot obtain the user's private key, nor can the information sent to the user by the server be interpreted.

Identity authentication management is usually made up of the following components.

1) Information Collection: Luo Yun [4]. Proposes in various ways in the design of the identity authentication system to collect the relevant identity information and the identity-related security code, fingerprints and other trust evidences, and store them in the authentication system database.

2) Authentication: the method uses the data such as identification materials for identity verification, to verify the validity of the applicant's identity information, and perform data encryption processing with program holding algorithms such as random key generation, and countersignature with digital certificate.

3) Digital Certification Data Preparation: the method archives and organizes the verified identity information, converts it into a digital form so as to be searched and identified during verification, and establishes a user personal information database;

4) Identity Registration: By encrypting and confirming the verified information, the method generates authentication information, and the corresponding encryption key is recorded in the authentication data stream for subsequent use.

5) Identity Authentication: based on CA system, unified authentication system, mobile security authentication system and other basic templates, the method realizes unified identity authentication service, unified user identity management service, unified user authority authorization service, unified user login portal service and so on, and greatly enhancing the security. In authorization, a request will be sent to the authentication center, and the authentication center will perform identity authentication according to the user identity information and the public key stored in the database. After successful, a digital signature is generated as the authentication result. The basic process is shown in Figure 2:

1) The user enters the user name and password;

2) The system verifies the correctness and integrity of the information input by the user, and performs identity verification according to preset conditions (such as privilege level, etc.);

3) If the identity verification is successful, the user can continue to use and has the corresponding

authority and operation capability;

4) If the identity verification fails, the user will not be able to use or only have limited permission;

5) Digital certificate management will record and monitor all user operations in real time to ensure the security and reliability of all kinds of orders and command information.

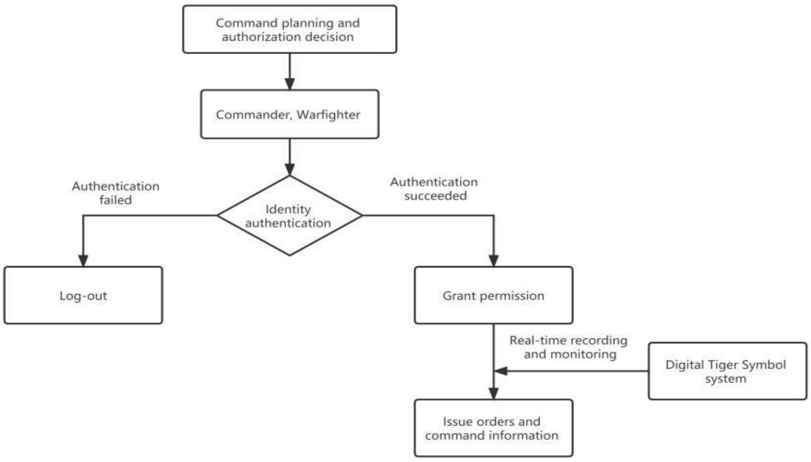
Command planning and authorization decision
Commander, Warfighter
Authentication failed
Identity authentication
Authentication succeeded
Log-out
Grant permission
Real-time recording and monitoring
Digital Tiger Symbol system
Issue orders and command information

Figure 2: Flow Chart of identity Authentication

2.3. Encryption Protocol

Encryption protocol is mainly used to guarantee the secure transmission of authorization commands. Compared with symmetric cryptosystem, asymmetric cryptosystem has higher confidentiality and asymmetric cryptographic algorithm can be used to encrypt information. Li Shimin [5]. Put forward in the exploration of hospital electronic archives security management system based on PKI technology that in the process of data encryption and transmission, the data information can be obtained by hash calculation method, and then the data can be encrypted by RSA so as to form the digital signature of the data. The efficiency and integrity of data transmission can be further ensured. Effective data encryption transmission in the entire application of PKI technology can improve the effectiveness of PKI technology to a great extent. By encrypting the information by PKI technology, the security of the information system can be improved, and the risk of information leakage and hacker attack can be reduced.

The design shall follow the principles of safety and reliability, flexibility, Scalability, ease of use, etc.

The basic process is shown in Figure 3:

1) The protocol establishes a safety management system and defines the management responsibilities and duties at all levels;

2) The protocol adopts advanced technical means to carry out strict operation maintenance and monitoring to ensure the stable operation of the system;

3) The protocol regularly conducts vulnerability scanning, checks the operation status and log of the system, and timely discovers and solves the potential safety hazards of the system;

4) The protocol strictly controls the external network and set up multiple security protection mechanisms to prevent malicious intrusion;

5) The protocol formulates comprehensive password security management regulations, conduct identity verification for all users and assign different levels of operation permission;

6) The protocol strengthens the capacity of data backup and recovery, and establish emergency plans for various risks;

7) The protocol regularly conducts safety assessment, collects and organizes information on safety incidents, summarizes lessons learned and makes improvements.

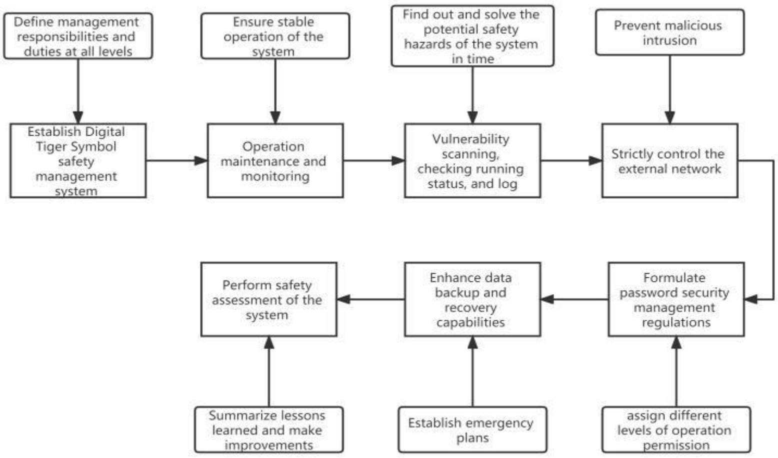
Define management responsibilities and duties at all levels
Ensure stable operation of the system
Find out and solve the potential safety hazards of the system in time
Prevent malicious intrusion
Establish Digital Tiger Symbol safety management system
Operation maintenance and monitoring
Vulnerability scanning, checking running status, and log
Strictly control the external network
Perform safety assessment of the system
Enhance data backup and recovery capabilities
Formulate password security management regulations
Summarize lessons learned and make improvements
Establish emergency plans
assign different levels of operation permission

Figure 3: Basic Flow of Encryption Protocol

2.4. User Interface

User interface is a window that directly interacts with the user, which is related to the efficiency and user experience of the system. Therefore, when designing and developing the user interface of the Digital Tiger Symbol, we should consider the user habit, operation experience, interface aesthetics, information prompts and other factors, so as to improve the efficiency and convenience of users when using the Digital Tiger Symbol system as much as possible.

The user interface typically includes the following functions:

1) User Registration and Login: the user logs in the Digital Tiger Symbol system through a registered account or an existing account to operate according to the relevant operation interface and process logic.

2) Digital Tiger Symbol Management Operation: different operation interfaces are displayed according to user rights, including issuing, withdrawing, command issuing, command execution and other operation functions.

3) Account Information Management: Users can view their own account information, modify passwords, log records and other personal information.

4) Data Statistical Report: User interface visualizes various data inside the system in charts to help the operating personnel better understand the operation of the system.

The visual operation mode of the Digital Tiger Symbol’s user interface brings a simpler and more comfortable solution for the user. The technology and function it uses rely on highly optimized interaction design and interface aesthetics to complete rapid human-computer interaction, so that users can easily complete various tasks, thus realizing data controllability.

The basic process of the user interface is shown in Figure 4:

1) The system administrator sets the user privilege level of the Digital Tiger Symbol according to the actual requirements;

2) A user logs in the Digital Tiger Symbol system and inputs the user name and password;

3) According to the user's identity and privilege level, the Digital Tiger Symbol system will display different user interfaces, including various function buttons, data charts, interactive maps, etc.

4) The user selects the corresponding function buttons according to the needs, and uses various functions of the system to conduct command and data analysis;

5) The module monitors and reflects the global situation and the operation of each task unit in real-time through various visualization modes, and supports multiple data query and filtering rules;

6) Users can freely adjust the content and layout of the user interface to meet personalized requirements and operating habits.

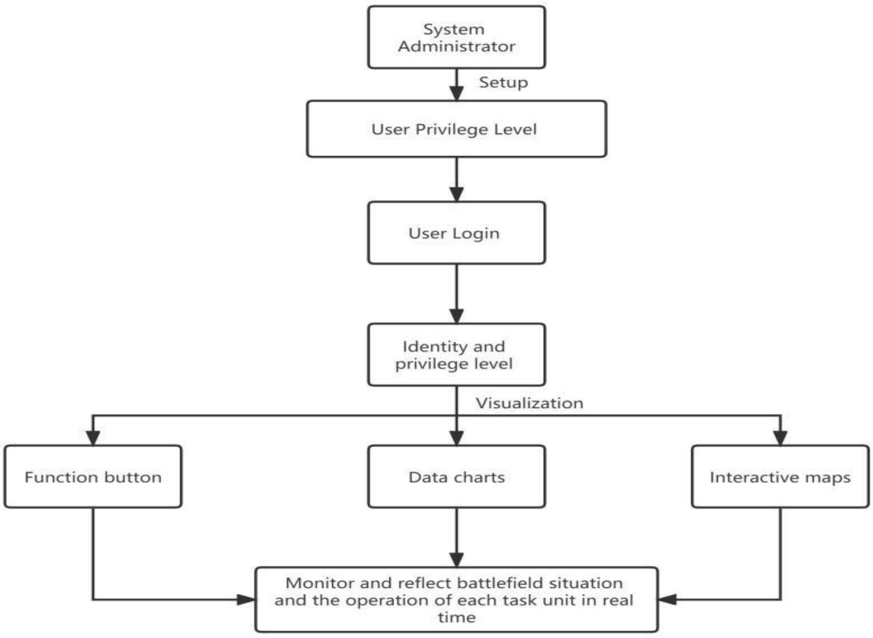
System Administrator
Setup
User Privilege Level
User Login
Identity and privilege level
Visualization
Function button
Data charts
Interactive maps
Monitor and reflect battlefield situation and the operation of each task unit in real time

Figure 4: Basic Flow of User Interface

3. Summary and Prospect

In this paper, we propose a method of digital Tiger Symbol authorization method based on PKI system, which uses digital certificate, access control policy, cryptography and role-based authorization to enhance the security, accountability and efficiency of processes. This approach can be easily integrated with existing military systems and infrastructure, and can adapt to changing environments and threats. Further research can explore the use of emerging technologies such as block chain and artificial intelligence to achieve decentralization and more intelligent and multi-effect.

References

[1] Dong Z. G., (2021) Research on the Implementation of Network Communication Security Based on PKI. Electronic Technology & Software Engineering, (20): 241-242.

[2] He S., (2013) Design and Implementation of Multi-domain Unified Authentication and Authorization System Based on PKI. Beijing: Beijing University of Posts and Telecommunications: 2-3.

[3] Wu B., (2008) Research and Implementation of Unified Authentication and Authorization System Based on PKI. Hubei: Wuhan University of Technology, 13-16.

[4] Luo Y., (2021) A Brief Discussion on the Design and Implementation of Unified Identity Authentication Technology Based on PKI. Yunnan Science and Technology Management, (10): 62-64.

[5] Li S. M., (2022) Research on Hospital Electronic Archives Security Management System Based on PKI Technology. Information Technology, (09): 16-18.