Design of Space OS Authentication System Based on Finger Vein Recognition

Wang Jianhui[1, a, *], Liu Jingang[1, 2]

[1]Information Engineering College, Capital Normal University, Beijing, China

[2]Institute of Computing Technology, Chinese Academy of Science, Beijing, China

[a]wangjianhui@live.com

Abstract: Aiming at the problems of low efficiency, easily forgotten and stolen authentication of traditional operating system password authentication scheme, based on the finger vein recognition technology, by utilizing the features of non-contact, liveliness, high adaptability and high security, modifying the original code of open source project SDDM and using PAM authentication mechanism, a secure and reliable identity authentication system is designed on Space OS platform. The experimental result shows that the Space OS authentication system using finger vein recognition technology as authentication mode can run on Space OS for a long time and without fault, whose finger vein recognition has high pass rate and low false accept rate, and has good stability and higher security.

1. Introduction

The traditional operating system login is mainly done through a combination of user name and password authentication. There is a problem of being stolen and forgotten, which cannot guarantee the accuracy and security of identity authentication [1]. Biometric technologies can verify their identities through some physiological characteristics of human beings, with better safety and convenience. As a result, more and more identities are now starting to use more secure biometric technologies. At present, biometric technologies mainly include fingerprint recognition, iris recognition, face recognition, palm vein recognition and finger vein recognition [2]. Among them, the finger vein recognition technology as a rising star in recent years has been rapid development. Due to the uniqueness of the finger vein, forgery difficulty and biopotency, its safety has obvious advantages over the traditional authentication methods and other biometric technologies [3]. However, no solution based on finger vein recognition technology at present is used in the authentication of the operating system when logging in.

Space OS is a new operating system based on the Linux kernel with a number of independent intellectual property rights, with features such as security, reliability, cross-platform and support for interoperability. Its login, logout, session establishment, and shutdown are mainly achieved through SDDM (Simple Desktop Display Manager). SDDM is an open source display manager that can easily extend its original capabilities by modifying the source code.

In this paper, authentication system is based on SDDM by modifying and adding a large amount of codes. Its finger vein recognition is supported through the PAM (Pluggable Authentication Modules) authentication framework, by which the identity of the user is authenticated when they login Space OS. Unlike other biometric technologies, such as fingerprint, finger vein is not easily damaged, the recognition rate is high, and is not easily affected by environmental factors, which greatly improves the stability and security of identity authentication system [4]. In addition, the PAM mechanism is a very mature security authentication mechanism that provides secure and reliable authentication services for a wide range of applications [5]. The Space OS authentication system designed in this paper is applied to the identity authentication of the Space OS login, which can effectively solve security problems such as password leakage and hacker attacks.

2. Plan design

Space OS authentication system mainly includes login user interface, SDDM, PAM service and finger vein recognition module. The login user interface is designed by QML in the custom SDDM theme. The authentication framework at the bottom of the system uses PAM, combined with finger vein recognition and achieve the login user interface and background service communication through Qt signals and slots. Specific structure is shown in Figure 1.
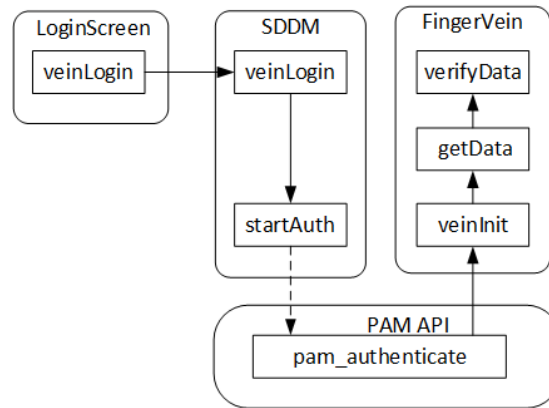

Figure 1 Architecture diagram of finger vein authentication system

2.1. SDDM module

SDDM connects other modules of the Space OS authentication system together as a hub. Its development is based on Qt, a cross-platform application development framework. The core communication mechanism of Qt is signals and slots mechanism. This communication mechanism simplifies programming, avoids the use of a large number of pointers, and improves the efficiency of programming [6]. There are many slots in SDDM, which are bound to the corresponding signals on the display interface. Through the way of signals and slots communication, the background service can monitor mouse clicks and keyboard key events of the user login interface. A finger vein login event is triggered when the user selects finger vein login, which send a signal about finger vein login. The corresponding slots in background service captures this signal, then initiates finger vein authentication. SDDM made a further encapsulation of the PAM API and will call the pam_ authenticate () function in the PAM authentication service to begin finger vein authentication.

2.2. Login user interface design

The user interface of the Space OS authentication system is designed by QML, starting before Space OS logins, and used as a login user interface to the operating system. QML is a descriptive scripting language with high readability and is also one of the core components of Qt Quick [7]. If the QML properties of the objects made with C++ are set up in Qt Quick, they can be used directly in a QML environment [8]. As SDDM supports the theme of QML design language, the interface designed by QML can interact with background services in the Space OS authentication system.

The main interface layout is written in the main file Main.qml in SDDM theme folder. Buttons can be customized by the ActionButton component. The text and iconSource properties define its style and the onClicked property defines the click event of the vein login. In QML, a Connections object can create a connection to a QML signal. Through the target property of Connections developers can specify the object for receiving the signal. In this way, developers can specify the SDDM object in Main.qml to receive a signal sent by Connectionns. Finally, add the sddm.conf file into etc directory in Space   OS to configure the SDDM theme and set the current value of Theme label to spaceVein in sddm.conf.

2.3. The mechanism of PAM authentication

The Space OS authentication system uses PAM, an authentication mechanism proposed by Sun

Microsystems, as the authentication system at the bottom layer of the system.

Through this mechanism, application and authentication protocols are separated from each other. Then developers can invoke their own authentication protocols with this mechanism. As shown in Figure 2, PAM authentication framework is divided into three levels. The PAM applications are at the top, corresponding to SDDM in the Space OS authentication system, the PAM API that connects the application and service modules configuration file is at the middle, according to different configuration files to load different service modules, and the PAM service module is at the bottom. PAM is easy to use, it shields a number of specific details of authentication, through which the upper application can use a variety of authentication mechanisms. The PAM service module consists of four modules: account, auth, password, and session [9].

Among them, the authentication service is used to authenticate the user's identity information. PAM provides a series of functions for application calls. The pam_start() function reads the configuration file, loads and assembles the plug-in according to the rules described in the configuration file, and initializes the PAM library. Each application starts with pam_start() function and ends with pam_end() function. The pam_authenticate() function is used to call the authentication module and the pam_setcred() function is used to modify the user certificate. In the Space OS authentication system, the authentication of user identities is achieved through the invoking of the finger vein recognition API by the PAM authentication service.
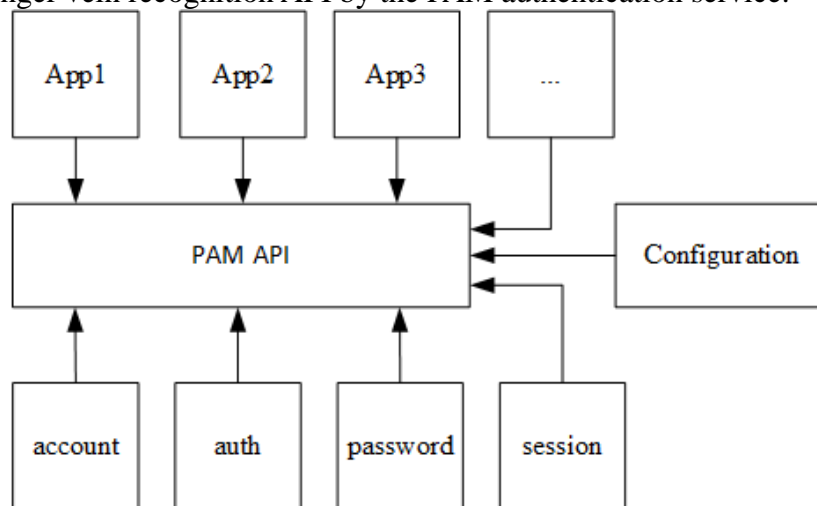

Figure 2 Authentication framework diagram of PAM

The PAM service module used by the Space OS authentication system needs to be configured in the sddm.pam file located in etc directory of the operating system as follows:

auth   include   system-login

Configure the authentication module path in sddm-autologin.pam file as follows:

auth   required   pam_env.so
auth   required   fingervein.so

2.4. Finger vein recognition

The processing of finger vein information by the Space OS authentication system is mainly done by the finger vein device. Finger vein information processing is composed of finger vein image collection, image processing (including image enhancement, segmentation and feature extraction) and identify matching, as shown in Figure 3. When a certain wavelength of near infrared light shines on the user's finger, it can capture the user's finger vein image information [10]. In recent years, the research on finger vein has been increasing day by day. The related algorithm researches mainly focus on image processing and recognition matching [11].
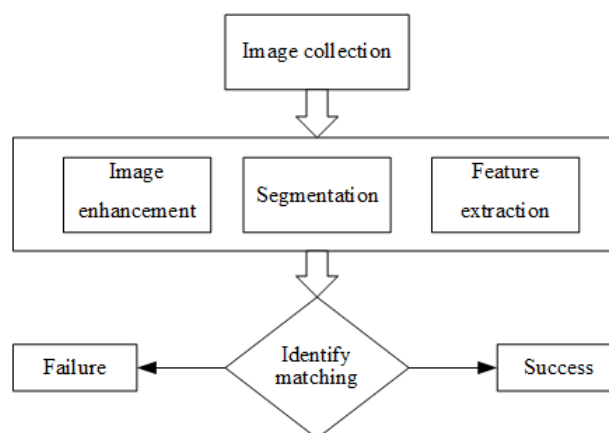
Figure 3 Schematic diagram of finger vein recognition

Finger vein recognition functions are encapsulated in the fingervein.so library located in the system library directory, which can be used by the Space OS authentication system to configure the PAM service. When calling the finger vein recognition API, the Space OS authentication system establishes a communication with the finger vein instrument and starts a series of operations. First, the finger vein instrument is initialized; after the initialization is completed, the finger vein information is collected and further processed; finally, matching of the finger vein information is started to complete the authentication.

2.5. The process of Space OS authentication system login

After the Space OS kernel is loaded, the daemon for the SDDM service and PAM service is also initialized. Then, the Space OS login user interface is started. After the user selects finger vein login, if it is the first time, finger vein information of the user needs to be input to the finger vein library of the instrument for future identity matching. In order to improve the accuracy of recognition, the times the user need to repeatedly input finger vein information should be no less than three. If the user has input the finger vein information, finger vein login will start. After the finger vein information is collected, the finger vein instrument stores the finger vein information that has been generated and processed into the finger vein database. These data are used for the authentication of the identity authentication system. If the information of the finger vein to be authenticated matches with the previous record, start a new session and login the Space operating system. Otherwise, it fails to match, the authentication system will return to the finger vein login interface, and need to collect finger vein information to login again.

3. Experiment analysis

The experiment tests the stability, security and authentication time of the Space OS authentication system and verifies the robustness of each module. At the same time, all the authentication system is detected whether there is a breakdown during running, and whether there is a problem that affects the normal operation of the Space operating system.

Hardware environment: i5-5200U CPU, 4G RAM, 24G SSD.

System environment: Space OS 2.17, Linux kernel version 4.8.17.

Running time: 30 days.

Experiment data: Twenty individuals were chosen as experimental subjects and five finger veins were collected for each individual. It captures each finger vein five times, and finally obtains five hundred finger vein images information. Then, the Space OS authentication system is tested several times with the same recognition algorithm.

In the experimental each module of the system was in good condition and the operation of multiple authentication can be completed normally without any other failure during running. After counted the pass rate and false accept rate of authentication in experiment and computed the authentication time which took the average of multiple tests, the result is shown in Table 1.

Table 1 Experiment result

Passing rate (%)	False accept rate (%)	Authentication Time(s)
97.2	0	2

The experimental result shows that successful authentication of Space OS authentication system is basically impossible to complete in the case of different finger vein information and its security is verified. The stability, security and authentication time of the authentication system basically meet the practical requirements.

4. Conclusion

The Space OS authentication system designed in this paper, based on SDDM, integrates the finger vein recognition technology through the PAM authentication framework，which joins the Space operating system to authenticate the identity information of the logged-in user to make it safer and more effective, effectively protects the privacy of users, and reduces the risk of theft of important data by others. The experimental result shows that the Space OS authentication system is both stable and secure, and the application scenario is very broad on account of the finger vein recognition technology.

References

[1] Wu Xiao. Design and implement of identity authentication system based windows security architecture[D]. Beijing University of Posts and Telecommunications,2014.

[2] Chen Hong. The research and implementation of social security system based on finger vein recognition technology[D]. Beijing University of Technology,2012.

[3] Liang Aihua, Fu Kang. Design of near-infrared finger-vein image acquisition system,2014,33(01):113-115+119.

[4] Guangdong Liu, Xiaohui Qiu. Finger vein recognition using 2DGabor combined with OECA[A]. Wuhan Zhicheng Times Cultural Development Co., Ltd.Proceedings of 2nd International Conference on Computer Engineering,Information Science & Application Technology(ICCIA 2017)[C].Wuhan Zhicheng Times Cultural Development Co., Ltd:,2017:7.

[5] Fan meng. Design and implementation of a security enhancement shceme for Linux login authentication[D]. Beijing Jiaotong University,2014.

[6] Ji Sanyou, Zhang Weijian. Interface design of embedded monitoring control system for portal crane based on Qt/Embedded [J]. Construction Machinery and Equipment,2014,45(02):1-7+122.

[7] Ray Rischpater. Application development with Qt Creator [M]. PACKT,2013.

[8] Zhao Rentao, Tian Xiaoxiao, Cao huifang. Design of Qt serial port server base on in Linux OS [J]. Shanxi Electronic Technology,2016,(04):63-65.

[9] Ma Yuting, Liu Zhaoyuan. Research and design of a two-way authentication based on PAM[J]. Journal of Xi'an University of Arts & Science(Nat Sci Ed),2014,17(02):43-47.

[10] Yihua Shi, Jinfeng Yang.Image Restoration and enhancement for finger-vein recognition[A]. IEEE Beijing Section.Proceedings of 2012 IEEE 11th International Conference on Signal Processing(ICSP 2012)[C].IEEE Beijing Section:,2012:4.

[11] Yu Yun. Research on finger vein recognition algorithm and its cipher application [D]. Hangzhou Dianzi University,2017.