Analysis of security risk control of mobile application under BYOD scenario using in energy enterprises

Zhang Wenjie¹, Li Wei¹, Li Zheng¹, Liu Yubo¹, Zhang Zhiru*¹

¹ State Grid Liaoning Electric Power Co. LTD Information & Telecommunication Branch Company, Shenyang Liaoning 110000, China
*Corresponding author’s e-mail: sg_eiconf@126.com

Abstract. In recent years, with the popularity of bring your own device (BYOD), energy employees have tended to use personal mobile devices to access company resources. The use of the same device to access both corporate and personal data introduces new security threats, such as the disclosure of confidential corporate data. Existing BYOD solutions lack multi-entity management, role-based access control (RBAC) support. Therefore cannot address the critical issue of external enterprise collaboration when the same device needs to access the resources of multiple companies. Based on this, security risk control of mobile applications in BYOD scenario is carried out in this paper. A face in vivo detection algorithm based on FLGS is proposed to improve the reliability of face recognition on current BYOD mobile devices.

1. Introduction

Bring your own device BYOD essentially means that employees can carry personal mobile devices to access the office network and carry out mobile work. The mobile devices referred to here can be smart phones, pads, laptops and other smart devices. Through these smart devices, employees can receive and receive corporate emails, access corporate resources and process corporate business at any time and any place, so as to realize mobile office. BYOD represents a phenomenon, which is personalized, mobile and intelligent. People's life and work are connected together by a variety of intelligent terminals. BYOD also represents an emerging trend that is breaking through the confines of the office, blurring the line between life and work, and enabling employees to have a better work experience.

In recent years, with the popularity of BYOD energy employees have tended to use personal mobile devices to access company resources. The use of the same device to access both corporate and personal data introduces new security threats, such as the disclosure of confidential corporate data. Existing BYOD solutions lack multi-entity management, role-based access control (RBAC) support. Therefore cannot address the critical issue of external enterprise collaboration when the same device needs to access the resources of multiple companies. Based on this, security risk control of mobile applications in BYOD scenario is carried out in this paper. A face in vivo detection algorithm based on FLGS is proposed to improve the reliability of face recognition on current BYOD mobile devices.

2. Design of AppShield security model

As mentioned above, BYOD has become a commercially acceptable mobile office solution, but due to the lack of appropriate security mechanisms to support BYOD. Specifically, you cannot flexibly and dynamically grant access to enterprise data to a selected set of applications. Although the mobile operating system currently has the feature of multi-user login, it is essentially based on user management
control and lacks the support of multi-entity management and RBAC. In order to meet the application requirements of energy enterprises for BYOD and solve the security problem of mobile terminals of enterprise sensitive data in BYOD scenario, this paper adopts the method of application repackaging to realize a complete version of the prototype system, called AppShield.

The security model for AppShield is shown in figure 1. In this system, enterprise data can be shared between enterprise applications, but is isolated from individual applications. Enterprise applications can be divided into any number of logical sets. The agent-based data access mechanism of this system allows the parallel access of data in each group to support the management of multiple entities and role-based access control. To provide special protection against highly confidential data, access control policies can be defined at file level granularity in a collection of enterprise applications.

In this system’s security model, personal applications share data through Android’s existing security mechanisms, such as external common SD card storage. Instagram, for example, can access photos managed by Dropbox, a personal app. Enterprise applications share internal company data through the security mechanism provided by AppShield, which is stored in the private space of AppShield and managed uniformly and dynamically by AppShield, and provides fine-grained authority management.

In addition, the system is based on the proxy data access mechanism. In an energy enterprise application, any operation on enterprise data through the file system goes through our customized underlying system call. The injected bytecode can be used to collect the context of the operation at the time of the system call, such as the application name, signature, and so on-some property data, which is then sent to the context policy execution point (PDP). AppShield maintains almost a file system in its own internal storage. If data sharing is allowed, AppShield generates a data index and provides file descriptors for enterprise applications to manipulate files. For reasons of security, performance, and synchronization, the system tries to avoid duplication of data, through which enterprise applications indirectly manipulate enterprise data. Because the file system is stored in the private storage space of AppShield, the data cannot be accessed by other informal enterprise applications, and the PDP can be used to verify whether the application that requests to manipulate the data is a formal enterprise application. If so, it further validates its permissions through the security policy set. The data storage in this system is mainly for file system. When the enterprise application to the data stored in external memory (SD card) on B, AppShield to redirect enterprise application file operations to AppShield own internal space, in order to monitor the application of file system access and operation level data access mechanism based on agent, need hook documents related to the underlying system API, such as open(), creat(), etc. The principle of agent-based access mechanism is shown in figure 2.
3. Face detection algorithm based on FLGS

The security of enterprise sensitive data mobile terminal in BYOD scenario is introduced above, and a security model based on AppShield is designed. Under the above framework, this chapter further designs the biometric authentication technology that supports BYOD mobile devices. A face in vivo detection algorithm based on (face local graph structure) FLGS is proposed to improve the reliability of face recognition on current BYOD mobile devices.

Local graph structure (LGS) was proposed by Eimad et al in 2011. This method is to form a strong correlation between a given pixel I (x, y) and its surrounding pixels. A control diagram with six pixels is usually sufficient to represent the relationships between the elements. A large number of applications show that LGS has a good effect in the face of Mordicaro gray change. FLGS also adopts the six-pixel method to form an interrelated pixel set around the target pixel I (x, y). First, we move the left image of the target pixel I (x, y) counterclockwise to find the sample pattern. If the gray value of the adjacent pixel is greater than or equal to the gray value of the target pixel 0, then the edge connecting the two pixels is assigned a binary value of 1, otherwise the value is assigned to 0. We performed a similar operation on the face recognition system of the BYOD application, with the difference that we first performed a horizontal movement and then a clockwise movement to complete the above operation, as shown in figure 3.

![FLGS feature generation diagram](image)

In order to generate the FLGS feature of pixel \((x_d, y_d)\), we assign a binomial weight \(2^p\) to each signal \(s\), and these binomial weights are summarized as:

\[
\text{Feature} = 2^p \cdot s
\]
4. Experimental results and analysis

In order to test the face in vivo detection effect of FLGS, we used real and photo-based face photo database for analysis. The pixels of the experimental images were 203×203, and the images were collected at intervals of two weeks, with different environments and lighting conditions. In figure 6, three groups of photos are extracted from the test database, among which the left is the photos taken by real people, and the right is the photos based on photos.

Figure 5. Flow chart of FLGS face recognition detection algorithm.

Figure 7 shows the set of drawings based on the characteristics of FLGS histogram, which left a real face generated histogram, right column display is based on the photos remake face FLGS histogram, can clearly see that based on the photos remake pattern has the characteristics of less in the histogram,
and relatively concentrated, most of the characteristics of the component is 0, so in the diagram shows a piece at the bottom of the dark. This is because after the picture is printed, it is concentrated on a few feature Spaces, which are not as average as the original picture. We use this feature to do live detection on the face picture.

Figure 6. Flow chart of FLGS face recognition detection algorithm.

5. Conclusion
This paper studies the security risk control of mobile application in BYOD scenario. In order to improve the reliability of face recognition of existing BYOD mobile devices, a live face detection algorithm based on FLGS is proposed. The main results are summarized as following:

(1) Starting from the BYOD application security model, this paper proposes an AppShield system deployment model and explains the deployment mode of the whole system. Finally, the security policy of energy enterprise BYOD application accessing enterprise sensitive data is designed.

(2) This paper presents a face detection algorithm based on in vivo detection, which has an important impact on face recognition. The experiment proves that the algorithm has a stable detection rate, can effectively detect non-living face, and prevent electronic fraud in energy enterprise BYOD application.
References

[1] Miller, Keith W, Voas, Jeffrey, Hurlburt, George F. BYOD: Security and Privacy Considerations[J]. It Professional, 14(5):53-55, 2012.

[2] Gaff, Brian M. BYOD? OMG![J]. Computer, 48(2):10-11, 2015.

[3] Liu, Xuan-zhe, Xu, Mengwei, Teng, Teng, etal. MUIT: A Domain-Specific Language and its Middleware for Adaptive Mobile Web-based User Interfaces in WS-BPEL[J]. IEEE Transactions on Services Computing:253-262, 2016.

[4] Rios-Aguilar, Sergio, Llorëns-Montes, Francisco-Javier. A mobile business information system for the control of local and remote workforce through reactive and behavior-based monitoring[J]. Expert Systems with Applications, 42(7):3462-3469, 2015.

[5] Ismail, Khairun Ashikin, Singh, Manmeet Mahinderjit, Musta?a, Norlia, etal. Security Strategies for Hindering Watering Hole Cyber Crime Attack[J]. Procedia Computer Science, 124:656-663, 2017.

[6] Lei Li, Paulo Lobato Correia, Abdenour Hadid. Face recognition under spoofing attacks: countermeasures and research directions[J]. Iet Biometrics, 7(1):3-14, 2018.

[7] Jiwen Lu, Venice Erin Liong, Jie Zhou. Simultaneous Local Binary Feature Learning and Encoding for Homogeneous and Heterogeneous Face Recognition[J]. IEEE Transactions on Pattern Analysis & Machine Intelligence, 40(8):1979-1993, 2018.