Security Studies and Implementation on Power Mobile Application in the Internet plus Environment

Zaojian Dai [1, a], Zhipeng Shao [2,b] and Mu Chen[3,c]

[1] Research Institute of Information Technology & Communication

State Grid Smart Grid Research Institute Nanjing, China

[2] Research Institute of Information Technology & Communication

State Grid Smart Grid Research Institute Nanjing, China

[3] Research Institute of Information Technology & Communication

State Grid Smart Grid Research Institute Nanjing, China

[a]daizaojian@sgri.sgcc.com.cn, [b]shaozhipeng@sgri.sgcc.com.cn, [c]chenmu@sgri.sgcc.com.cn

Keywords: Secure access System; encryption card; public key infrastructure; two-factor authentication

Abstract. Analyze the security risks of traditional power mobile operating system, design and implement a more secure access system and analyze the overall structure and function of the secure access system in detail in the Internet plus environment. The system can process two-way certificate authentication, secure transmission of data, security access control, network isolation and secure data filtering, real-time monitoring and management, and solve the security problem of mobile power operation applications effectively.

Introduction

In the recent years, personal cellphones have been widely used in the electricity production, marketing, supplies, emergency command system and other electric internal systems. Compared to the traditional paper-fill mode operation，this way improved the operational efficiency, quality, regulatory and other aspects greatly. But some security risks still exist, such as authentication, secure data transmission, terminal monitoring management and so on. We have not had the perfect solution yet. In this paper, these security issues are analyzed in detail, and security access systems overall functional architecture and access procedures designed to overcome the above-mentioned safety risks.

Security Analysis of Traditional Power Mobile Operating System

The main power of a conventional mobile operating system architecture cellphones [1] access system can be summarized by mobile workers holding cellphones, via GPRS / CDMA wireless network by dialing the line access point, and terminal authentication based on user name and password. The main security risks are as follows:

Low Authentication strength. The phone number bound in the specific APN network via GPRS gateway supporting node access can not solve the problem of counterfeited number, and the intensity of username and password authentication is low.

Network isolation strength is weak. Two-way security isolation and data filter are not adopted between power information network and the Internet. The routers, firewalls of Network border can not fully ensure the security of core internal network.

Centralized monitoring and access control for terminals are difficult. Each mobile operating subsystems are independent, the information can not be reused. It is difficult to monitor and manage and easy to cause secure problems.

Security audit of terminal behavior is difficult. It is hard to carry out a real-time monitoring and fine-grained security audit in the terminal access behavior such as uploading, downloading, and so on.

Design of the Security Access System

To solve above problems, some key technologies are taken to design the architecture of the security access system.

Logical Design. As shown in Figure 1, the logical structure of the entire system can be divided into secure terminal layer, the channel layer security, security access system layer, four logic levels of the business services layer. Secure terminal layer comprises end encryption hardware, security client software and mobile applications. APN [2] based security channel layer bottom line and other professionals to build a wireless network, and the establishment of secondary encryption data secure transmission tunnel thereon. Security access system layer is the core of the whole system, relying on the power of public key infrastructure (PKI) [3] digital certificates Book system, two-way digital certificate authentication key features access, authorization and access control, security isolation filtering, real-time monitoring and management, and control of each module messaging and synergy through the message bus, at the same time on the lower level between the security access system cascade messaging. Business Services layer includes mobile application pre-service systems, service systems and other back-office applications, by extracting the former foreign minimize provide mobile service operations in order to further achieve shield unauthorized and illegal access.

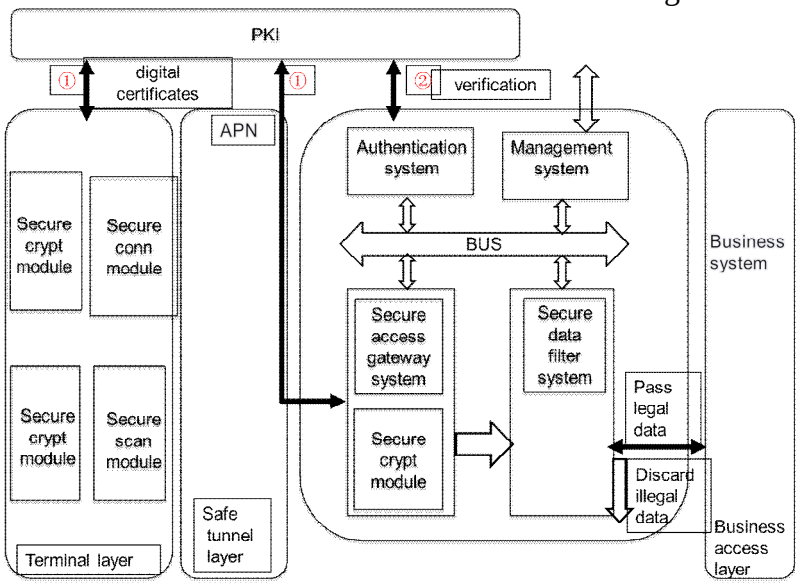

Fig. 1 Logical structure design of system

Key Technologies.

Technology for Combined Authentication and Security Access. In order to achieve strong authentication for cellphones, digital certificate authentication system are taken with a terminal, scanning feature identification and security status in one of the combination authentication mechanism. Meanwhile, in order to enhance security, and prevent a multi-purpose card, hacker attacks, a random collection of terminal hardware and certificate information, host software and hardware characteristics are adopted and the platform generates a unique identification code access through a hashing algorithm, each time the access will be on the terminal access identification verification.

Development of Security Client Software. Secure access software development cellphones, the focus should be considered IOS, Android and other mobile operating system compatibility and adapt the original move jobs client / server (C/ S) mode two-way communication process. In the design, a transparent proxy and forwarding tunnel reuse technology are mainly used in order to ensure seamless integration with existing mobile operating software. Through transparent proxy technology, the

connection remains transparent monitor packets, tunneling, encryption package forwarding, data decryption, and delivered to the designated business systems and other steps for client packets transparently forwards, shielding the difference client application and back-office services, so that mobile applications, seamless business background are as shown in Figure 2.

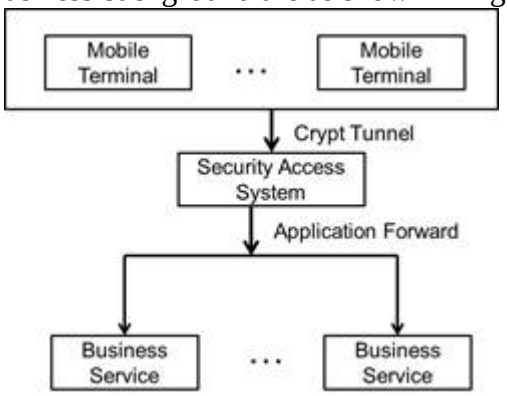

Fig. 2 Design of reuse encrypted tunnel

Safety Data filtering technology. Traditional network security isolation gates and other technologies through a central processor (CPU) processing unit network isolation, TCP layer protocol stripped bare data exchange, but the processing performance, to achieve the technical difficulty and so difficult to achieve security filtering application protocol, or only support simple uniform resource locator (URL) filtering. The move operation agreement for power limited, controllable characteristics, in the traditional insulation product architecture design optimization, the inner and outer network processing units were designed switching layer, scheduling layer, a plug-in layer, as shown in FIG. Exchange layers are implementing a custom protocol data encapsulation, interface, and application data check, depending on the application layer protocol interface plug-in format, data format definition, illegal data filtering. Scheduling level for application plug-transfer tasks, access control strategy of dispatching management, task priority can be dynamically adjusted based on business importance, and can be white, black list management. At the same time, it can be combined with specific business actually balance between safety, transport efficiency, selective filtration.

Typical projects Applications

Currently, the system has been in the domestic part of the network of provincial, municipal company conducted a pilot application, it can be widely used in electric power production safety, materials, marketing, emergency command, emergency repair work and other mobile applications, and effectively protect the power production , security and stability in managing business operations.

The first layer of protection: wireless APN and other green channel, routers and firewalls. By wireless operators to offer APN and other green channel, the boundary Device Access Control List (ACL) [4] control, packet filtering policy settings, prevent illegal packets, and Internet public channel isolation.

Layer 2 protection: security access systems. Relying on the power PKI / CA system terminal and digital certificate authentication, access control and fine-grained access control, and establishing two-way encrypted data secure transmission tunnel, while internal and external network security isolation protection and data security filtering to ensure the safety of the application interface and data. At the same time, providing for terminal security access policies, real-time monitoring real-time status and operational behavior, security and auditing functions. Security access system hardware embedded security operating system with mandatory MAC (MA) and other security mechanisms to ensure safety from the underlying operating system.

Layer 3 Protection: mobile application front-end system. To improve the security of the system, using the mobile application front-end system to access external network terminal business of logic

extraction, only minimize mobile operation service interfaces, such as queries, upload, download interface, to prevent unauthorized access to the terminal.

The mobile terminal includes a cellphone terminal support system layer encryption hardware, a wireless communication function. Security access system layer is the core of the system, the main transmission secure authentication and confidentiality, security isolation filtering, centralized monitoring audit function, with the following three layers of protection logic.

Conclusion

Electricity here in cellphone mobile job security access systems for the power of traditional job security cellphone mobile access system design possible, by using a variety of security technologies such as two-way digital certificate authentication and data encryption, transparent forwarding, security, data filtering , unified messaging bus, etc. For a new system architecture design, the platform greatly enhances the security and protection of power moving job applications. The system will be subsequent filtration efficiency and data accuracy, use a higher level of security encryption algorithm, a cellphone security protection, support a variety of embedded mobile terminal access and other aspects of further in-depth research.

References

[1] Dj.M. Maric, P.F. Meier and S.K. Estreicher: Mater. Sci. Forum Vol. 83-87 (1992), p. 119

[2] Zhang D. Web content adaptation for mobile handheld devices. Communications of the ACM，2007，50(2):75 -79

[3] Naik K. A survey of software based energy saving methodologies for handheld wireless communication devices. Department of ECE, University of Waterloo : Technical Report No.2010 -13,2010

[4] Das T, Mohan P, Padmanabhan V N et al. PRISM; Platform for remote sensing using smart phones//Proceedings of the 8th International Conference on Mobile Systems, Applications, and Services(Mobi Sys'10). San Francisco, USA, 2010:63-76