Security Risk Analysis of Mobile Application in Power System

Guo Jing[1,a,*], Jiang Haitao[1,b] , Zhou Chao[1,c], Guo Yajuan[1,d], Huang Wei[1,e]

[1]Jiangsu electric power company research institute, Power Grid Technology Center, Power Road, Nanjing, China

[a] guojing5126@163.com , [b] jianghaitaoxin@163.com , [c] userrr@qq.com, [d] 124765606@qq.com, [e] kakasio@163.com

*Guo Jing

Keywords: security risk, reverse engineering, power system

Abstract: With the rapid development of mobile phone and the growing popularity of mobile Internet, mobile applications has been widely promoted in the field of power system, its business scope covers production, marketing, finance and other aspects, greatly changing the service mode. But at the same time, mobile applications have also brought more serious security risks. This paper focuses on current security risks of mobile applications in power system. Firstly, the security situation and application situation of mobile service in power system is expounded. And then through analyzing the deployment characteristics and application status, meanwhile combining with possible attack approaches, revealed the security risks in client, data transmission, management background. Finally, the mobile application security recommendations are given, which provides technical guidance for mobile application security and reinforcement.

1. Introduction

With the rapid development of new technologies such as Cloud computing, large data, Internet of things and mobile technology, mobile applications have gradually penetrated into the power System. Mobile applications is so convenient and personalized that greatly enhance the user experience, changing the service model of power system greatly[1]. However, it is also due to its characteristics such as openness, flexibility,and the terminal easy to lose which bringing more security risks to the power system. At present, the security technology research for mobile applications is still in the initial stage. Because of industry characteristics, security, privacy, stability are requires highly in power system, but it still lack a comprehensive security risk assessment. Based on the development of mobile applications in power system, this paper analyzes the security risks of mobile applications, and puts forward simple and effective safety suggestions which ensured the applications operated safely and stably.

2. Development of Electric Power Application

2.1. Security Situation

At present, for power mobile applications, the damage caused by the attack is divided into three areas, one is the disclosure of personal information of electricity users, the second is the leakage of information within the power company, the third is malicious and malicious spread. In recent years, WooYun and other secure sites have released two high-risk sensitive information disclosure vulnerabilities (WooYun-2015-94789 and WooYun-2015-111621), the vulnerabilities were fixed quickly and the version was updated , did not cause serious consequences and adverse social impact. 2016, “Dian E Bao”, “pocket power” have been suspected of a large number of customer information outflow, resulting in a greater social impact. Mobile application security situation is grim, security vulnerabilities and security risks are a serious threat to the interests of each power users and security of enterprise data . Therefore, to ensure the safety of power mobile applications has become an urgent problem to be solved.

2.2. Application Situation

Mobile application started late but rapid developed in power system. Recent years, it integrates with production, marketing, financial payment, scheduling, office and other areas, and has been accepted by enterprises and users. The main types of power system mobile applications are that can be installed independently and services developed on the micro-messaging platform. However, it is a little different with the mobile application on the market. Power mobile applications not only serve the majority of power users, but also support internal production and services. It can be divided into dedicated devices mobile applications and non-dedicated device mobile applications.

Dedicated devices mobile applications: installed on a customized mobile device, usually with a special chip or encryption device, using dedicated network access. It is mainly for field operations or inspection, the scope of its application is within the company, only employees with operational authority can use them. Service scope of this kind of application is limited, and the device is not easy to obtain. So it is much confidential, can guarantee the secure of production data.

Non-dedicated device mobile applications: installed on a regular mobile device. This type of application can be divided into two categories according to the use of the crowd: One is the mobile application used by internal employees, which use the internet as a network channel, we call it “internal applications”. They are typically used for move offices and services, with strict user identity authentication mechanisms. The other mobile applications is for the majority of power system users and the community, which also use the internet as a network channel, we call it “external applications”. Its services does not involve the company's secrets or sensitive information, only include sevices such as e-mall, electricity information inquiries, electricity payment and others. Non-dedicated device applications exposed to the internet, facing much more threats, this paper will focus on the security of these applications.

In order to response security problems caused by the rapid development of mobile use and take full protection of user privacy and internal electricity production data, currently completed applications are usually only provide display function, and other key operations are set less. The main purpose of applying restrictions to user operations is to reduce the operational risk in the client terminal and to prevent the illegal user from triggering a system crash or sensitive information leakage. With the increasing of attack methods and attacks number, the application must fundamentally regulate the security mechanism to enhance their own robustness.

3. Security Risk Analysis

3.1. Architectural Analysis

Electricity belongs to the national infrastructure, and its information is sensitive. So its information security protection system has always adopted with a safe partition, network-specific, horizontal isolation, vertical certification is the basic principles. Established Intranet, the security isolation and logical isolation between the partition, both provides a solid foundation for the information protection. Mobile applications in power system are also strictly in accordance with the principles of construction and protection, the following figure is structure block diagram for the general mobile application :

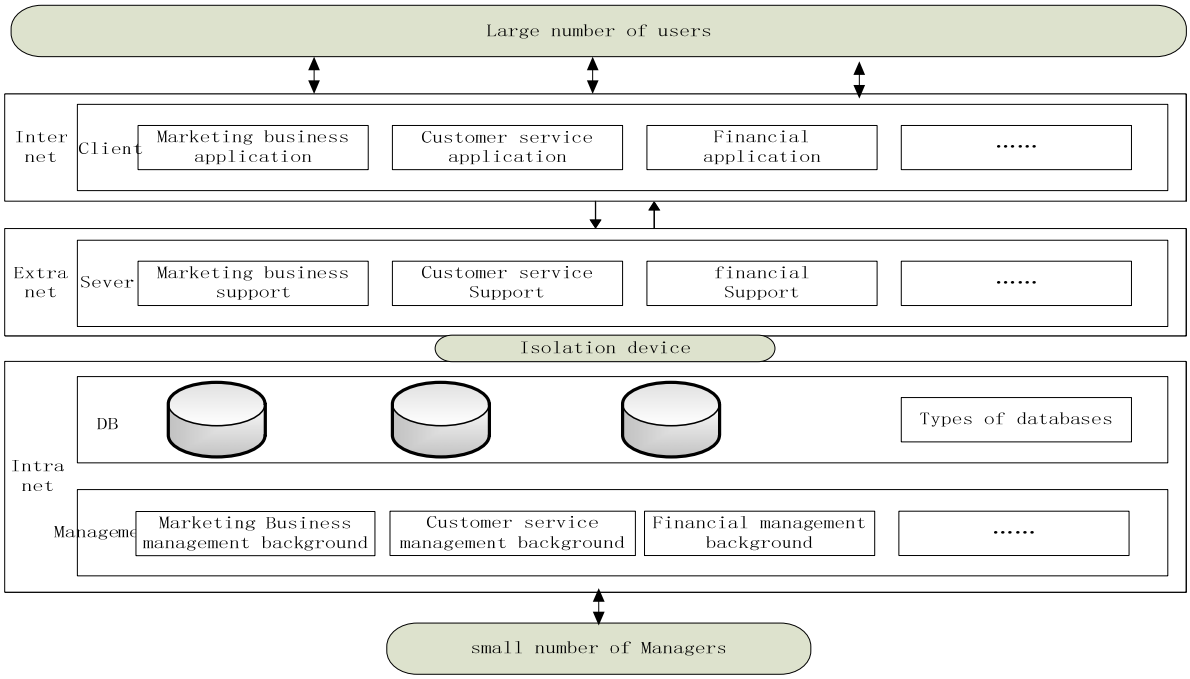

Figure 1 Architecture diagram of mobile application in power system.

According to the figure above, we can see that the deployment of power mobile applications still follow the principle of partitioning and secure access. Client and service are in different partitions, and use the firewall and other equipment to achieve logical isolation. Background management and database and extra-net(relative to the intranet) services are qualified by isolation devices to achieve physical isolation. The specific components of each partition are as follows:

Client: deployed on the Internet, install specific applications. The client is a bridge between the user and the service, it will send a variety of requests to the server. Users can review and operate functions such as marketing, customer service, power transactions and other business modules through the client application,

Server: deployed in the extra-net which is used to separate the intranet and the Internet, providing background service interface. The server receives various requests from the client and processes the feedback, and can interact with the database, and the interactive process has been protected by some security measures.

Database: deployed in the intranet, storage various types of application-related data.

Management: deployed in the intranet, for information dissemination and statistics.Provide the relevant background management and services, it can be used by authorized system operation and maintenance person.

3.2. Secure Risk Analysis

Either a module or partitions with risk are likely to trigger security events. In the internet, attack path is freely available. Intranet has a hidden feature, not easy to attack, but security incidents that occurred in the past prove that "physical separation" defense can be cross-network intrusion, information can be stolen. Taking security risks in internet as a springboard, using bypass, remote control and other means likely to penetrate into the intranet.

Both the attacker's main goal is to get the customer or internal information, or release harmful information, the basic attack is as follows: first, using client vulnerabilities to collect background server information, and then through the site weak password, righteousness, etc., to "black station" or directly attack the database which contains sensitive information, and then implant the backdoor procedures and other acts, access to the background server control right. This kind of attack can obtain more resources, once the background server been hacked, the database of personal information will be leaked, the company's trade secrets and even the core secrets will be stolen.

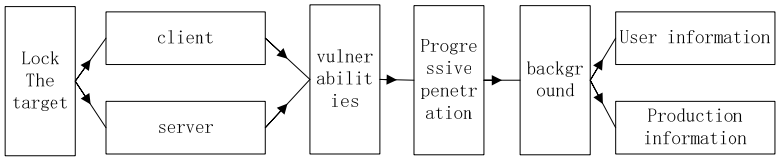

Figure 2 Attack path.

The path of attack is connected by risks each of the elements involved is essential. Following, analyses security risks module-by-module.

3.2.1. Clients Risk

- Physical threats: client terminals, including smart phones, tablet devices and other intelligent devices. The device is flexible and portable, easy to be stolen illegally. After the device is lost, if the application data and login information is not destroyed in time, may cause the user to disclose personal information or even economic loss.
- The operating system threats: At present, Android and iOS operating system occupied the mainstream market. To protect the user's data, applications and equipment security, both systems set a relatively comprehensive security mechanism. Android set up the sandbox mechanism, the signature mechanism, the authority mechanism, the access control mechanism, the process communication mechanism, the memory management mechanism and so on, iOS establishes the authority separation, the code signature mechanism, the sandbox mechanism, DEP, ASLP and so on. But inevitably, the system still exists potential risks, in recent years has burst out of arbitrary code execution, remote rights, signature vulnerabilities, file injection and other high-risk vulnerabilities. By using system vulnerabilities, attacker can step by step to obtain the highest authority of the mobile phone, access to the client file and malicious read and write, and even listen to access to SMS and data traffic and so on. The current intensified root and jailbreak, is to achieve this goal directly. Root or jailbreak equipment, perfect bypass the security mechanism, although the equipment manufacturers to take a series of equipment locking and other measures, but with little success, and many users because of their own needs will take the initiative to select the root device.
- Virus Trojans and malicious code: virus Trojans and malicious code has been plagued by the user, the attacker take open source technology solutions as weapons which brought by the accumulation of technology. The virus, SMS attacks, gateway attacks caused user losses. In 2016, Android platform, the device infection rate of 10%. "Malicious charges", "hooliganism",

"privacy theft", "SMS hijacking" and "trickery" virus or less the number of samples occupied most of the client.

- Application threats: mobile application is a bridge to connect users and servant. Take it as the entrance, by carrying out and analyzing vulnerabilities, it can be gradually penetrated into the management background.

(1) Traditional web threats: mobile applications usually use development architecture of C/S or C/S and B/S combination, the APP development of technology and web development technology gradually mixed together. Therefore, the common web application-related vulnerabilities are likely to exist in APP. Owsap top 10 details the 10 major security vulnerabilities faced by web development, including SQL injection, cross-site scripting, CSRF, and so on. These vulnerabilities may result in the theft of confidential information, the disruption of network services and remote control. But because most of the APP is not directly embedded in the web page model, but use API interface to return data, resulting in scanner crawler can not get a lot of links, so the vulnerability of this type are in low utilization.

(2) Reverse engineering[4]: In addition, reverse engineering for mobile applications is common. reverse engineering analyzed the core binary code and business logic to obtain the application of source code, library files, algorithms and other assets. Commonly used analysis methods include packet analysis, protocol analysis, code injection, component attacks, etc., can cause denial of service, running crash, data monitoring, source code leakage and other consequences. Commonly used tools are: IDA Pro, Hopper, apktool and other binary verification tools, so that attackers can insight into the internal work principle of the application, used to find other vulnerabilities, and further expose the back-end server, encryption constant, password and intellectual property information. The following are possible breakthroughs that may cause this risk:

- Problems of security mechanism[2][3]

Unsafe data storage: mainly refers to the client storage sensitive information improper. Such as: storage of user information or enterprise production data in clear text; private information storage in SD card and other external storage which are easy to access; after uninstalled the application, the private information is not destroyed.

Unsafe authentication: mainly refers to the user identity is not valid. Such as: the use of a single identity authentication; the use of weak password authentication, resulting in user password can be guessed; not set up anti-security crack mechanism.

Too many authorizations: mainly refers to the authority of the application is in a high level, the attacker can use high-level authority to carry out righteousness.

No source code protection: mainly refers to the application package can be decompiled, easy to obtain or analyze the source code.

- Third-party reference improper

the application often involves third-party services, such as payment, map positioning, etc., it can be a security risk. Such as access to third-party applications, then the original page is replaced or covered.

- Business design unreasonable

For example, in the internal application scenario, the two-dimensional code is used to store the employee's internal information as the authentication information. The employee can acquire some resources or production information by scanning the two-dimensional code. Two-dimensional code technology to encode the way to store information, which itself does not have any encryption features, in this case through the camera to obtain or reconstruct the two-dimensional code may cause information disclosure and unauthorized access.

3.2.2. Transmission Risk

App network transmission security refers to process that data transmit from the client to the server. Transmission security is essentially a matter of trust. Attackers through a variety of means disguised as a trusted object, to do data theft or tampering, is the so-called middleman attack. Man-in-the-middle attack is commonly used means of attack, is also recognized as the most devastating attack. There are many ways to do middleman attack, through the use of certificate forgery, digital signature forgery, etc., using ARP spoofing, DNS spoofing, proxy deception and other means to be sent to the target host data stream redirect to the middleman host, in order to read or modified Interactive information, and the two original computers mistakenly believe that they are communicating with each other, so this attack is not easy to detect[5][6]. In addition, the mobile communication data transmission using wireless network access server, the client can also carry out Wi-Fi fishing or base station camouflage, etc.to monitor and analyze user information.

The risk is mainly due to two, data tampering, data leakage. Such as operating log, server information, etc .; analysis of communication process which has not yet encrypted or protect the information, to get more background information. And then log on the background and use of struts loopholes, access to system permissions. Take this as a springboard, it is possible to invade the internal network database and management background; replace the malicious code with the upgrade package link to the user, thus controlling the mobile device; intercept the user key login information, operation information, to achieve identity fraud.

3.2.3. Management Background Risk

Application management background is usually the use of web technology development, to provide convenient and efficient management of the page, by the system administrator personal use, to assume more management functions. Able to carry out information dissemination, data additions and deletions and other key operations. In the event of an attack, can cause a wide range of user impact, is the ultimate goal of the attacker.

- Traditional web threats: Discussed in Section 3.2.1.
- Internal risk: Power system relies on the protection of physical isolation, intranet users have unreasonable behaviors when they use manage system. System weak password and user misuse and other phenomena occur, account password stored in the personal computer and administrator account share with number of user. These behavior may result in the use of a weak password to log in to the system to change the application configuration information which will make services cannot be accessed; publish malicious announcements, resulting in adverse social impact. However, contrary to the uncontrollable behavior of the public network users, the behavior of the internal user can be regulated[7].
- Environmental risk: environmental security, including the network layer, the host layer, application layer, data layer security. Mainly network equipment, operating systems, databases, middle-ware, application servers and other types of equipment and systems security configuration problems; host infected with viruses, Trojans and malicious code problems. These issues will become exploited vulnerabilities, such as the use of system vulnerabilities remote access or administrative authority to control the entire system[8].

4. Security Advice

In summary, the power system is faced with both internal and external risks, once the risk being used may cause large scope of social impact.

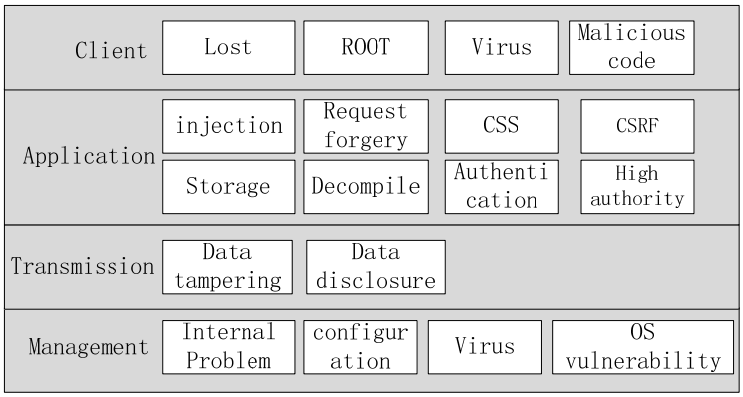

Figure 3 Risk of mobile application in power system.

To ensure mobile applications in power system operate safely and stably, the following suggestions are given:

- Using security protocols to transmit data, using encryption technology on key information. Using the https protocol when translate the log in data, privacy data, etc. To ensure that the encryption algorithm is valid and the key is long enough.
- Computer network anti-virus technology. Timely deployment of anti-virus software in the production environment, regular investigation.
- Improve the system security mechanisms, including identity authentication, access control, data integrity confirmation, source code protection mechanism, establish a proper data recovery system.
- Carry out code security testing. source code security testing should be carry out before mobile application on-line. To verify the effectiveness of the remaining information protection measures to ensure that the important application data storage space is released or re-assigned to other users before the complete removal.
- Regulate the operation of internal user behavior to prevent administrators leak confidential. Construction system audit function, real-time monitoring the abnormal operations.

References

[1] Xu Zhen, Liu Ren, Yu Aimin, Wang Dans, N. (2012) Mobile Application Security Technology for Smart Grid. Automation of Electric Power System, 16, 82-86.

[2] DWIVEDI H, CLARK C, THIEL D, M. (2010) Mobile application security. New York, NY, USA:McGraw Hill, 2010.

[3] BUGIEL S, EKBERG J E. C.(2010) Implementing an application-specific credential platform using late-launchied mobile trusted module. Chicago, IL, USA: 21-30

[4] Nikolay Elenkov, M.(2015) Android Security Internals, USA

[5] Payne J. J.(2013) Secure Mobile Application Development. It Professional, 15(3):6-9.

[6] Pekkala R, Saaskilahti J, Wiren K J. P.(2011)Network and node for providing a secure transmission of mobile application part messages: US, US 8037297 B2

[7] Msgna M G, Ferradi H, Akram R N, et al. M.(2016)Secure Application Execution in Mobile Devices// The New Codebreakers. Springer Berlin Heidelberg,

[8] Prabhu K. P.(2011)SECURE APPLICATION CONTROL IN MOBILE TERMINAL USING BIOMETRIC SENSOR: US, WO/144988.