Research of WeChat Public Number's Security of Power Information System

GAO Peng[1, a *], SHI Cong-cong[1, b] and FAN Jie[1, c]

[1]State Grid Smart Grid Research Institute Research, china

[a]gaopeng@sgri.sgcc.com.cn, [b]shicongcong@sgri.sgcc.com.cn, [c]fanjie@sgri.sgcc.com.cn

Keywords: power information system; mobile internet; mobile applications; WeChat public number; security.

Abstract: With the popularization and development of mobile Internet and smart mobile terminals, the WeChat public number which combines traditional services and mobile internet application has become the development require of power information systems, research for the security of WeChat public number of power information system has become an unavoidable problem. The article first introduces the status quo of WeChat public number of power information system, then analyzes the service platform typical logical architecture and data flow of WeChat public number of power information system. Then it analyzes the main security risks of WeChat public number of power information system, and finally the specific security measures for WeChat public number of power information system is proposed.

Introduction

With the popularization and development of mobile Internet and smart mobile terminals, the OTT services which is powerful and low rates rise rapid. Because of wide coverage, promote convenience, low operating costs, making OTT become the important platform which interacts traditional enterprise and Internet, achieves business transformation and upgrading. In this context, the State Grid Corporation combining traditional power service and WeChat and using information technology to help traditional business transformation is an important exploration which achieves business upgrade of internet thinking [1].

WeChat is a free application which provider of instant messaging service for intelligent terminal. WeChat support inter-communications operators, cross-operating system to send free voice, messaging, video, pictures and text through network. WeChat can also use the information of sharing streaming media content and social widget of location-based. WeChat quickly accumulated a large user base, as of October 24, 2013 subscribers has exceeded 600 million, becoming the important user entry of mobile internet. WeChat public platform is a new service platform which provide business services and user management capabilities to individuals, businesses and organizations, through which you can manage millions or even tens of millions of users, and to achieve customer service of self-service, artificial way, a variety of media formats and even e-commerce activities. WeChat public platform includes mobile client and back-end server [2,3,4].

WeChat public platform account includes service number, subscription number and enterprise number. Service number provides greater user capacity and business services for enterprises and users to help companies quickly achieve a new public service platform. Subscription number provides a new way of information dissemination to the media and individuals to build better communication between the reader and management. Enterprise number provides mobile application entrance for businesses or organizations to help enterprise establish connection employees, upstream and downstream suppliers and enterprise applications [5].

Situation of Power System WeChat public number

Using Status Quo of Power System WeChat public number. 2014,power companies require based on 95598 customer service hotline and customer service website, using modern information

technologies and means to build "Six in One" smart interactive services platform which include phone, website, micro-channel, mobile clients, digital television and SMS . By the end of 2014, power company has achieved the provincial WeChat public platform based on the same technology full coverage of the Yangtze River Delta region. Among them, the binding user number of Jiangsu Power WeChat public platform has exceeded million within six months since its launch in August 2013 and amounted to 2.6 million as of the end of March 2015.Fujian Power WeChat public number has been widely recognized since its launch in March 2014. The number of users has been showing a steady growth trend, and exceeded twenty-five thousand in the first month. The promotion of WeChat public number provides wisdom, personalized electricity service for the power users, and provides ready, convenient and unimpeded approach to get power information.

Analysis of typical WeChat public number of power system. The typical logical architecture of WeChat public platform of power system is shown in Figure 1.WeChat side includes WeChat public number and WeChat background server, business side includes application servers and database servers. WeChat side is in the Internet, application servers are in the external information network of the power company, database servers are in the internal information network of the power company. Between the application servers and database servers are internet boundary, external and internal network boundary.

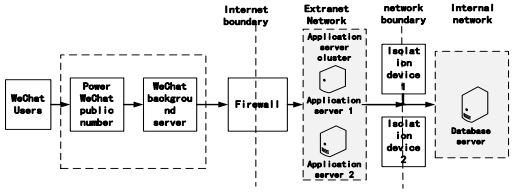

Figure 1 The typical logical architecture of WeChat public platform of power system

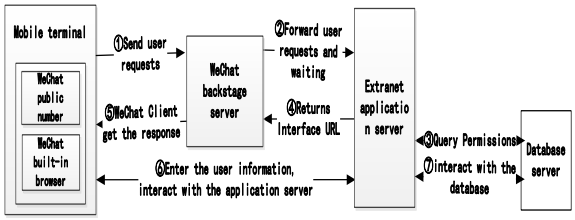

Figure 2 WeChat public platform communication mechanism

WeChat public platform messaging interface provides developers with a new message handling, gained the ability to interact message with the users. For the WeChat public number which receive the message successfully, when users sending messages to the WeChat public number, WeChat public platform backend server using HTTP requests for accessing URLs to push message. Extranet application servers can reply specific configuration information after the response, so as to achieve the purpose of a reply message. Figure 2 describes the communication mechanism of the entire WeChat public platform [6].

Power Information System WeChat public number mainly uses two ways to exchange data between with extranet application server. Mode 1 exchanges data through WeChat backstage server and application server, including basic request, simple information, content directories, etc., as shown in step ①, ②, ④, ⑤; Mode 2 does not exchange data through WeChat backstage server, but through WeChat built-in browser directly to the external network application server, including complex requests, interactive services, content, details, etc., as shown in step ⑥ shown.

Analysis of WeChat public number's security risk of power information system

Combining the analysis of typical architecture and data flow logic of power information system WeChat public number, WeChat public number major has security risks in four aspects, including mobile terminal risk, data risk, application risk, WeChat its own risk.

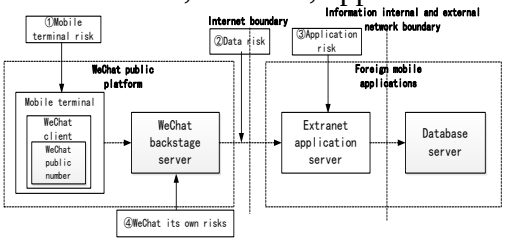

Figure 3 Security risk map of Power Information System WeChat public number

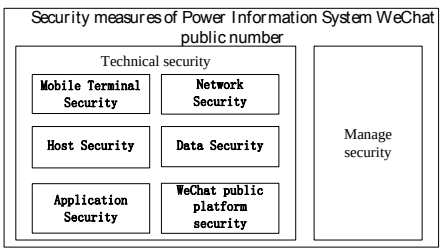

Figure 4 Security Framework of power information system WeChat public number

As shown in Figure 3, Power Information System WeChat public number major has the following security risks:

Mobile Terminal Risk.1) *Mobile terminal is infected*: which can lead to the mobile terminal itself be controlled by malicious users, disclosure of users' sensitive information. 2) *Mobile terminals or WeChat account loss:* which can lead to malicious users to gain unauthorized access and modify others sensitive information through WeChat account. 3) *User phishing:* which cause malicious users illegally obtain others sensitive information, and malicious tamper with business data.

Data Risk.1) *Data eavesdropping:* When the data is in the transmission process, if not take appropriate security precautions can lead to a malicious user to illegal steal user sensitive information and business data. 2) *Data tampering:* When the data is in the transmission or storage process, if not take appropriate security precautions can lead to a malicious user to steal sensitive information, modify business data.

Application Risk.1) *Unauthorized login*: which can lead to a malicious user to obtain other users permissions to steal and tamper with users sensitive information. 2) *Unauthorized access*: that has not been allowed to access the external network application server legal resources, can lead to malicious users to steal and tamper with other users information. 3) *The risk of common Web applications:* which including SQL injection, cross-site attacks, denial of service attacks that can lead to paralysis of the external mobile applications, disclosure of users' sensitive information and business data tampering.

WeChat Its Own Risks.1) *WeChat backstage server is attacked:* illegal user can control the WeChat backstage server forward the user request, return the user malicious response, may lead to user sensitive information was stolen, WeChat backstage server paralysis, business data has been tampered with. 2) *WeChat Vulnerability:* if the WeChat application vulnerabilities is not repaired in time, can be exploited to attack WeChat clients, WeChat backstage server, extranet network application server that can lead to user sensitive information was stolen, WeChat backstage server paralysis, business data has been tampered with.

Security measures of Power Information System WeChat public number

According to the using status of power information system WeChat public number, together with the security risk analysis of WeChat public number, this paper consider the security of power information system WeChat public number from technical security and manage security. As shown in Figure 4.

Technical security. 1) *Mobile Terminal Security*. a) When the mobile terminal access to company applications through the WeChat public number client, it should access using read online, prohibit the use of attachment downloads, avoid local retention file. b) Extranet network mobile applications should be able to remotely destroy data of mobile terminals, prevent sensitive data leaks when the mobile terminal device is lost. c) Prohibit the mobile terminal side to store any sensitive information, including corporate business secret data, business data, account information and user privacy. 2) *Network Security*. Network security should be designed from Structural safety, access control, security audit, border integrity checking, intrusion prevention, malware prevention, network equipment protection, which should follow the requirements of "Baseline for classified protection of information system" [7], " The security program of National Grid company informational "SG186" project"[8]. 3) *Host Security*. Host security should be designed from authentication, access control, security audit, remaining information protection, intrusion prevention, malware protection, resource control, etc., should follow the requirements of "Baseline for classified protection of information system" [7], " The security program of National Grid company informational "SG186" project"[8]. 4) *Data Security*. a) The data between WeChat backstage server and the external network application server should use HTTPS for secure transmission, while important data (such as user names, passwords, business data) should be secondary encrypted transmission. b) The simple business such as request service catalog and the message list that based on public numbers can interact through WeChat backstage server, other business operations involving sensitive information, user privacy should adopt B / S mode (browsers,

URL address) interact directly with the external application system application server, avoid forwarding through WeChat backstage server side. c) All the business data should be stored in the internal network data server, other areas (such as mobile terminals, WeChat public platform server, the external network) prohibit storage of any business data. d) Sensitive information (business data, account information, user privacy, etc.) should be encrypted storage. e) The mobile terminal should avoid storing sensitive information, including business data, account information, user privacy. 5) *Application Security*. a) The user's password security policy should be designed in accordance with companies unified security company, including password length, complexity and life cycle. It should provide a unique user identification and authentication information complexity checking functions. b) User account should support binding with phone number. First logon user should be forced to modify the initial password, along with login abnormal alarm and account lockout. We should strengthen the external application background development, maintenance personnel accounts and permissions management, timely write-off, clean up privileged account. c) Important operation (such as the initial login, password changes, online payment, etc.) should use a mobile phone for secondary verification. d) We shall manage user account privilege in accordance with the principle of least privilege, avoid unauthorized access. e) The each data exchange for WeChat public platform and extranet application server, you should use signature to authenticate each other to ensure the requests from trusted sources, at the same time you should hide the request URL address by setting the validity and redirection, prevent phishing attacks. f) Sensitive information should be stored in the internal network data server, and other areas (such as mobile terminals, third-party public platform and external network) prohibit storage. Important data should be stored encrypted. g) We should follow the "Application Security for information systems Part 2: Security design" [9]," Application Security for information systems Part 3: Security coding" [10] to security develop. Strengthen the design of development and security codes to prevent SQL injection, cross-site scripting attacks and other common Web application security risks, reduce and control security vulnerabilities and security risks of public mobile application systems. 6) *WeChat public platform security*. a) We should select the "secure (encrypted) model" for development, to ensure messages encrypted transmission [11,12]. b) Encryption algorithm key should be set to the maximum string length which WeChat public platform provides, and should include upper and lower case letters and numbers, and modify periodically. c) Digital signature key (Token) should be set to the maximum string length which WeChat public platform provides, and should include upper and lower case letters and numbers, and modify periodically. d) We should shield the upper right sharing button of WeChat. e) We shall periodically reset the interface credentials of WeChat public platform management side, to prevent users call interface maliciously. f) Company internal applications or large customer applications should use "Enterprise WeChat account" for enterprise-level management.

Manage security. 1) Strengthen approval and record management of WeChat public number. New WeChat public number should be approved by the Power Corporation information and communication management and business, and record in the relevant departments. 2) We should do a really good early demonstration about develop routes and security risks of WeChat public number, and in strict accordance with " The security program of National Grid company informational "SG186" project" to deploy security protection." 3) The released and interactive data which WeChat public number involved should strictly follow the relevant requirements of power companies' dense scope and commercial secret content [13,14], prohibit critical data stream through the WeChat public platform backend server. 4) WeChat public number should strictly abide by information systems management regulations of the State Grid Company [15]. Do good lifecycle security control of needs analysis, security design, development, testing, system on-line, operation and maintenance. 5) We should strengthen information security management system and personnel security management. We should require the development and maintenance personnel to participate in information security training organized by the company.

Summary

With strengthening smart grid work of the power industry, in the help of WeChat, through WeChat public platform and WeChat public numbers, the power company greatly improves the communication and interaction with power users, but also brings the appropriate security risk. Combined with typical logical structure of WeChat public number of the power information system, this article analysis the WeChat public number security risk of the power information system. At the same time, combining with the actual characteristics of the power industry information system, this article propose the security measures of the power information system WeChat public number from technical security and management security, which has some significance and role for the electricity industry to further develop WeChat public number construction and public security.

References

[1] Zhao Jing, "Development of WeChat public platform"[J], Practical Journalism,2013,08, pp.8-10.

[2] Liu Yu-ting, "Application of WeChat public platform for mobile learning"[J], Software Guide, 2013,10:91-93.

[3] Baidu Encyclopedia, "WeChat public platform", 2015.http://baike.baidu.com/link?url=irLBrhn62TpIU-vOO9Vadf66ejkOWSdYmt0KNbD8F1x1gz-rWIUFih_DjzIPUBcHP2-BljeblqqmoQfXqnO38q.

[4] Li Yang, "Role positioning and function Adjustment of WeChat public platform"[J], Social Science Journal, 2014,02:57-61.

[5] Zhang Deshen, "Develop of WeChat public platform- Function Development of subscription number"[J], Electronic Technology & Software Engineering , 2013,19:65-68.

[6] Xie Yuanchao, "Design and Implementation of the WeChat Public Account Information Service Platform"[D], Sun Yat-sen uniwersity , 2014.

[7] State Grid Company, "Baseline for classified protection of information system" （GB/T 22239-2008）[S], Beijing: Security Information Security Protection Evaluation Center of ministry of Public, 2008.

[8] State Grid Company, "The security program of National Grid company informational "SG186" project"[R], Beijing: State Grid Company, 2009.

[9] State Grid Company, "Application Security for information systems Part 2: Security design"[S], Beijing: State Grid Company, 2013.

[10] State Grid Company, "Application Security for information systems Part 3: Security coding"[S], Beijing: State Grid Company, 2013.

[11] Zhong Zhiyong, "Application development actual combat of WeChat public platform"[M], Beijing:China machine press , 2013.

[12] WeChat, "Developer documentation of WeChat public platform", http://mp.weixin.qq.com/wiki/13/80a1a25adbc46faf2716774c423b3151.html,2015.

[13] State Grid Company, "Provisions of the State Grid Company's security classification range"[R], Beijing: State Grid Company, 2013.

[14] State Grid Company, "Several provisions of the State Grid Company's trade secrets"[R], Beijing: State Grid Company, 2013.

[15] State Grid Company, "Management Measures of the State Grid Company's network and information system security"[R], Beijing: State Grid Company, 2013.