Advances in Engineering Research (AER), volume 82
2016 International Conference on Engineering and Advanced Technology (ICEAT-16)

Information security technology based on mobile communication technology

Yan Yi [1] and QingJiang Zhao [2]

[1] Personnel division Kunming University, Kunming, 650214

[2] Assets and laboratory administrationy, Kunming University, Kunming, 650214

KEYWORD: Mobile communication technology; Protecting; risk

ABSTRACT

This article mainly expounded the general development situation of security technology of mobile communication system, analyzed the unsafe factors in mobile communication network, discussed the information security technology of mobile communication technology in four aspects of encryption technology, authorization technology, digital integrity technology, authentication technology, and on this basis proposed the information security measures of mobile communication. Hope that the elaboration of this article could provide some references to relevant areas.

1 INTRODUCTION

In the mobile communication system, assuming that there is no perfect security protection measures, users' information and service networks will be leaked or tampered, invaders could use the drawbacks of the network protocol or the system to deny service, track location and carry out other operations, at the same time intercept users' information in the air interface, which could cause that the users cannot communicate normally, and bring a loss for the communication enterprises. Therefore, the use of information security technology in mobile communication system, can effectively protect the security of user information and network system, and therefore has been widely used in the communications business.

2 SECURITY TECHNOLOGY OF MOBILE COMMUNICATION

2.1 Encryption technology

There are two kinds of simple security technologies of mobile communication, the first is encryption technology, and the second is the key management. Coordination of data encryption is mainly to use some special calculation methods to process the original plaintext information or data, transfer the original plaintext information or data into some unreadable codes, we usually call the codes "ciphertext". These ciphertexts could show only after inputting the corresponding keys and the main purpose is to protect the users' information and data. In mobile communication system, each user has a user number (PIN), each user number is corresponding to a user password (PIN code), the PIN code is formed by 4 to 8 digits, only entering the user number and the corresponding user password, communication facilities will query and read the data of SIM card, but we should know the times of inputting password will be restricted to protect the information security of users, password could only be input three times, after inputting incorrect password three times, the SIM card will be locked automatically, the user needs to go to the related communication department to unlock for using it again.

The so-called encryption refers to the password settings setting for protecting users' information and data, after setting the encryption system, it could effectively prevent that the users' information is stolen and eavesdropped. Encryption is mainly the key management in the process of under authorization, the keys are in two main device, the first is the SIM card; the second is AUC. The key is mainly by means of random digitals transmitted network system, mobile systems and networks receive these random digitals at the same time, and use the keys appear under authorization process, because when choosing random numbers, it has the encryption function, the safety of the operation can be ensured. Typically, the key of data encryption the user accesses also need to be protected to ensure the security of users' information and privacy.

***2.2* Authorization technology**

The authorization mainly refers to the device for avoiding the unauthorized, illegal personnel to intrude into the mobile system, and its working principle is to use authentication technology to identity invaders' authentication in the process of mobile system accessing the register VLR.

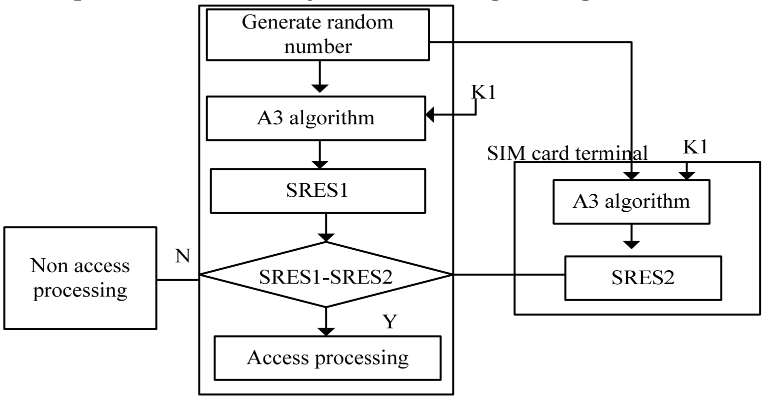

Figure 1 Flow chart of authorization

In authorization, it needs to realize in the communication network and SIM card. When a mobile communication user logs on mobile network or communicates, he needs to be authenticated, and the mobile network interrupt system will randomly show a string of numbers, which is 128 bits. In the SIM card, it needs to use the A3 calculation to process the random string of numbers and the key in SIM card, then gets the authorization code SRES2, compares authorization code SRES2 with the authorization code SRES1 received by authorization center, if the comparison results are same, it indicates that the user is a valid user, and receives the processing requirements; on the contrary, if the results are not the same, it indicates that the user is illegal, and will not receive the processing requirements. Using authorization technology could ensure that the legitimate rights and interests of mobile communication users are not infringed, also effectively prevent the invasion of illegal users. The flow chart of authorization is shown in figure 1:

***2.3* Digital integrity technology**

The working principle of the digital integrity technology mainly refers that when sender transmits the data, it needs to add redundant encoding section to the data transmitted, and takes this encoding section as a verification code, under normal circumstances, the verification code attaches after the message. In data transmission, it needs to send the master data and verification code together to the receiver, after the receiver receives data, according to the corresponding decoding method, the verification code sent by sender is validated, if the same, information is received. Because the verification code evolves based on the data transmitted, therefore, by inverse operation, the accuracy of the verification code could be accurately determined.

In view of the steady development of digital integrity technology, based on the digital integrity technology, the derived tampering technology has developed rapidly. The illegal user only needs to fake the verification code, uses the verification code to change the data, and the digital integrity technology cannot accurately identify. Because there is a certain correlation between the verification code and the transmitted data, we can spread the verification codes to every verification space, so that it can effectively reduce the intrusion risk of illegal users.

2.4 Authentication technology

In communication system, it usually uses the way of access – response to identity a user's authentication. This article mainly summaries the authentication method of shared key. The principle of this technology mainly refers that, the first user inform the randomly accessed data A to the second user, after the second user receives the data, using the corresponding calculation method to encrypt, at this time, it will generate a new random data B, the second user will transfer the encryption result and random data B together to the first user, after the first user receives them, they should be decrypted, decryption results and the data A are compared, if the results are consistent, then key a is used to encrypt data B, and encrypted result 2 is sent to the second user. On the contrary, if the contrast results are inconsistent, it indicates that the first user and the second user do not pass the authentication.

3 INFORMATION SECURITY MEASURES OF MOBILE COMMUNICATION

3.1 Digital signature

The digital signature is the service system which could securely connect the user and the mobile communication system and has the function for protecting information security of users' communication, for example: when the mobile communication user accesses the mobile system, network system could use the digital signature to ensure the efficient use of communication resources.

3.2 Authentication protocol

In order to ensure the information security of mobile communication, it is necessary to establish the authentication and key processing system, mobile network can use authentication protocol to supervise anonymous services, avoid that communication system is intruded by criminals, and illegal intruders cannot track the mobile system, steal the user's personal information, so as to ensure the information safety of user. In order to ensure that the user information could not be stolen by others and prevent the phenomenon of misusing number, mobile communication operators can provide user authentication to ensure the legitimate rights and interests of mobile communications users. In addition, in order to meet the requirements of the 3G/4G network users, it also needs to ensure the two-way authentication, and construct the mutual constraints. In the conditions of mutual authentication, it ensures the information security of 3G/4G mobile communication.

3.3 Data encryption

In order to avoid that mobile communication information is stolen and leaked, the data encryption process should be carried out. In the process of data encryption, RSA algorithm and PKI algorithm need to be fully used, and taken as the core of encryption. For example: using CPU chip to achieve the application of RSA algorithm, and to ensure the security of mobile communication information. Using PKI algorithm could effectively reduce the impact from the risky factors to mobile communication information, on the basis of guaranteeing the security of mobile communication information to meet the needs of mobile communication users.

4 CONCLUDING REMARKS

Using information security technology in the mobile communication system could not only ensure the safe operation of mobile communication information, but also could enhance the level of information transmission, and prevent the information delay, stolen, so as to provide a good communication environment for mobile communication users. Using encryption technology, authorization technology, digital integrity technology, authentication technology and other advanced technologies, could ensure the information security of mobile communication, so as to promote the stable and healthy development of mobile communication in our country.

5 REFERENCES

1. Qiu Honghua, Liu Xiaoli. A comparative study on the patent information of 4G mobile communication technology between China and the United States[J]. Journal of Intelligence, 2013,08:81-86.

2. A Maji. Research on information security technology based on mobile communication technology [J]. Information Security and Technology, 2013,11:57-58.
3. Hu Guohua, Yuan Shujie, Tan Min. 4G mobile communication technology and security defects analysis [J]. Communications Technology, 2008,07:155-157.
4. Zhuang Dekui. Research on information security technology of mobile communication [J] Management & Technology of SME (late month journal), 2015,03:192-193.
5. Zhang Lizhe, Qiu Xin, Zhang Fusheng. Study on intelligent transportation information service system based on mobile communication technology [J]. Mobile communications, 2015,18:82-86.
6. Shang Shuai. Key technologies and security threats review of the fourth generation of mobile communication system (4G) [J]. Security science and technology, 2011,03:50-53.
7. Yu Zhe, Sun Wenyu. Research on information security technology based on mobile communication technology [J]. Heilongjiang Science and Technology, 2014,07:161.
8. Farah Kandah, Yashaswi Singh, and Weiyi Zhang, "Mitigating Eavesdropping Attack Using Secure Key Management Scheme in Wireless Mesh Networks," Journal of Communications, vol. 7, no.8, pp.596-605, 2012. Doi: 10.4304/jcm.7.8.596-605