In Mobile Internet Era, How To Open "Smart Identity Authentication"

Ying Wu
Shanghai University of Political Science and Law,
Shanghai, China
wuying@shupl.edu.cn

***Abstract*—In mobile Internet era, the identity of people will become more and more important in the Internet. Identity authentication has become the foundation of the whole mobile Internet. This paper introduces the current development trend of mobile Internet and the importance of identity authentication, and aiming at the challenges of identity authentication in mobile Internet, various intelligent authentication solutions and core technologies are proposed.**

Keywords—mobile Internet; multifactor authentication; digital signature; device fingerprint; face recognition

I. INTRODUCTION

The wave of mobile Internet has swept our current life and work. More and more confidential or private information is transmitted and stored through the network, regardless of the state, the company or the individual. The rapid development of mobile Internet, personal information value gradually highlights, such as news, games, social, financial and so on are customized, everyone has a corresponding account password system on different platforms, in order to adapt to this change, the change is the essence of Internet Security technology. Specifically, the traditional network security is to deal with the attack and defense, namely the shift in the confrontation with the hackers, but business security is often neglected and problems in dealing with personal attacks will appear weak, which bring tremendous space for the development of a new information security technology.

As a protector of personal assets, identity authentication is the cornerstone of mobile Internet security. Certification is an integral part of the mobile Internet business. Personal business registration, landing, bank transfer, query balances and other transactions, electricity providers, online shopping and other activities, in the final analysis to verify who you are.

Last year, CCTV news broadcast "5 minutes online buy thousands of bank card information almost all right" in the documentary, Xu broke open several QQ group, in less than 5 minutes, and the reporter sent a 33 page document. This document records more than 1000 bank card information, each message has the card master's name, bank card number, ID number, bank reserved cell phone number and bank password. Reporters in the document randomly selected seventy different provinces of the information to verify, of which 65 bank card passwords are all correct.

It also contributed to a dramatic rise in cybercrime for the purpose of gaining such information. Human centric scene is becoming more and more, and many businesses are moving to a human centered business model. Human identity authentication becomes very important.

In the mobile Internet era, security is more important than the development of the development, need to establish on the basis of security, mobile internet security is directly related to the interests of hundreds of millions of Internet users, network security must effectively maintain the mobile Internet, and the identity authentication is a very important part in the application of mobile Internet security. As one of the first and even the most important defensive lines of network security, authentication technology has a very important position.

In order to solve the Internet trust crisis caused by authentication defects and ensure that information is accessed only by "right people", it is necessary to raise the level of identity authentication and adopt more advanced techniques and methods.

II. THE CHALLENGE OF IDENTITY AUTHENTICATION IN MOBILE INTERNET ERA

A. Personal information leakage risks increase

The mobile Internet era, while bringing us convenience, is also increasingly threatening the security of personal privacy. We have been shrouded in cloud of information leakage. The big event information disclosure have occurred in almost every month, the enterprise is not only the core of trade secrets leaked, causing users to cause a crisis of confidence, the loss of a large number of users, after being exposed, but also attracted public vocal opposition, led to serious damage to the brand. Such as the social security system was traced to vulnerabilities in 2015, social security has become the disclosure of personal information "disaster area"; the second Health Insurance Company was hacked 80 million user data affected; Russian dating website leaked 20 million user data. Internal control, information safety of Xingcheng Life Insurance exposed vulnerabilities in 2016; the new security vulnerabilities shuilao vulnerabilities hazard more than ten thousand websites in our country; the sale of 200 thousand children's information is packaged, accurate information to the family number...... having caused extensive concern.

Mobile Internet era, everyone is a contributor to the data, in the personal contribution of information at the same time, information leakage and other security issues have become more severe. There are statistics, personal information was leaked Internet coverage is very extensive, including users of personal identity information was leaked before the 78.2%, including the Internet education, name, home address, ID number and work units; 63.4% of the users of personal information being leaked online activities, including phone records, records, online shopping website browsing traces, IP address, software traces and location. In the adverse effects of personal information leakage, 82.3% of Internet users personally feel the impact of personal information leakage on daily life.

Personal information disclosure risks continue to increase, personal use of mobile Internet services to bring concern, affecting the development of mobile internet.

B. *Enterprises face significant challenges in identifying real identities*

Mobile Internet applications in many traditional industries, including finance, education, tourism, real estate, transportation, agriculture, manufacturing and so on, relates to the social and economic aspects, each traditional industry has its own characteristics in the business process, combined with the Internet, will encounter the problem of identifying the true identity of the customer. For example, "Internet plus finance", the industry chain including the funds, financing, payment, internet currency and financial information services and other aspects, in such a large financial services chain, Internet financial transactions cannot be met, not face to face identification of the true identity of the user name, ID number or upload plus documents a scanned copy of himself as Zhang San is three, most enterprises through online verification to the Ministry of public security background check the identity card is true, but Zhang San is still unknown whether the operator.

C. *The security risks of the explosive growth of mobile APP application*

Surging high-tech era, the popularity of intelligent terminals, not only to promote the development of mobile Internet, but also brings explosive growth of mobile APP applications. According to Gartner forecast: in 2017, more than 50% of employees in the world use mobile office. In the mass of APP applications, enterprise APP as a new marketing means gradually displayed in front of us, and the concept of enterprise self-built APP applications have also been brought up. Mobile APP applications push enterprise and government work to a new mode, improve work efficiency and save funds.

Mobile APP applications have brought convenience to enterprises and governments, but also created a series of security risks. Openness and anonymity of the characteristics of Internet makes these security issues become increasingly prominent, how to ensure the authenticity of the identity of the Internet, how to carry out the identification and recognition of the Internet in various roles, how to protect the objectivity, integrity and non-repudiation is the need to study, and the identity authentication as the first gate of network security, can ensure the enterprise and personal information is only legitimate users access, can be said that the identity authentication technology is the foundation of information security. The identity authentication system in the application system occupies a very important position in the mobile APP applications.

III. Smart Identity Solutions and Core Technologies

The traditional authentication methods are characterized by static, passive, easy diffusion and poor experience. This static verification will not change as a result of hacker attacks. Only after the security attack occurred, the account stolen, leaked information will find the problem. Once the problem arises, the range will be great and it will be difficult to solve. More and more complicated, frequently changing passwords, and the inconvenience of U shield also make people feel annoyed.

Traditional solutions that rely on media authentication have been unable to better adapt to mobile office trends and fail to balance security and ease of use. Then, how to change the traditional way of authentication and seek a dynamic, intelligent, safe and convenient way to prove that "I am me"?

At this stage, the method of authentication for public mobile applications is more appropriate, using an active, dynamic and intelligent way.

A. *Authentication solutions*

1) *Multi factor authentication*

Multi factor authentication solution aims to use the mobile devices that users hold at any time to achieve security and convenient identity authentication. Multi factor authentication products integrated use of equipment, fingerprint space-time code and a number of safety technology, at the same time using PKI digital signature technology system, a variety of authentication methods the State Encryption Standard to realize security scan code, important information to confirm, biometrics, based on end users only need to hold the mobile device (such as mobile phone) to complete the authentication and electronic signature.

Specifically, multi factor authentication products is established through the relationship between the terminal and the mobile device users with mobile devices and various business systems (such as banking system) the relationship between the final realization of identity authentication between business systems and end users. Multi factor authentication products by digital signature and face recognition technology, establishes the corresponding relationship and trust relationships between users and mobile terminal equipment; and through the device fingerprint, space-time code technology in business systems (the banking system as an example) between the mobile device and to establish the relation between trust and relationship. When the terminal user, service system at the same time with the mobile device to establish a unique correspondence between, actually realized the correspondence and trust relationship between business systems and end users, business systems can rely on mobile devices to accurately identify the end user's personal identity, thus completing the business transaction.

2) Mobile multidimensional joint authentication

Mobile multidimensional joint certification is based on the mobile Internet to all products and trade to protect mobile products and solutions, it is mainly used for financial sectors such as banking, brokerage, third-party payment scenarios, certified by the unique device, terminal security, identification and authentication protocol technology, realize know, holdings and all mobile multidimensional joint certification. The main function of this scheme is to ensure that every transaction in the Internet is done by the customer.

3) Intelligent behavior certification

Intelligent behavior authentication is based on the massive data analysis technology, processing, data mining and machine learning using flow cytometer, constructing a unique intelligent real-time identity anti-fraud model with safety equipment as the core, no sense of user identity authentication "". Through this automated intelligent behavior certification, the most important feature of intelligent behavior authentication is to bring the user's perception experience is very good.

4) One station mobile identity authentication management

The use of one-stop mobile identity management is very extensive, it can be said that as long as there are places where the network can be used. The most important purpose of this product is to eliminate passwords, and also to ensure the safe and convenient use of customers. It is understood that a one-stop mobile identity management (IDaaS) is designed to solve the enterprise users' numerous accounts, authentication cumbersome, permissions distribution complex, and other issues, to provide users with safe, convenient and manageable IDaaS services.

B. Core technology of identity authentication

1) Digital signature technology

Digital signature technology carries on the authentication to the user, namely through the private key signature and the public key examination sign completes the authentication process. Mobile phone users can set a password gesture on mobile devices, using the private key encryption algorithm in generating user exclusive to which the user private key protected by encryption, and then stored in the mobile device, the user public key is uploaded to the server and storage, and establish a secure binding relationship with the user account. When the user carries on the gesture password verification, uses the user private key to sign the data information, and sends to the server, verifies the signature by the public key corresponding to the server.

The technology implementation process safety is reflected in the following three points: first, the mobile terminal does not store users public key private key and plaintext, so as to protect the private key to the safety of users; second, the user private key stored in the mobile device, ensure that the private key is never transmitted on the network, to avoid the theft and hijacking; third. The private key and public key corresponding to only, the private key to correctly sign, signature verification process, i.e., only when the user input the correct password to sign, through authentication, access to resources in the service business system to complete the transaction or operation.

2) Face recognition technology

Face recognition is one of the authentication methods for the end user to log in to each service system and perform business operations on the mobile device. Through continuous facial movement (rotation, head up, bow, blink) detection and analysis, live detection. The face recognition engine has the advantages of superior performance, stability and reliability, and the detection rate of the face detection algorithm (the number of face samples that are correctly detected is higher than the total number of samples).

3) Space-time code technology

Time and space code technology is a secure and credible quasi hardware level dynamic multidimensional code technology. Through the dynamic algorithm, P2P (Center) check and other advanced technology, multiple safety factors into the time factor, space factor, behavior factor, logic, hardware fingerprint encryption, the effective protection of short range anti photographed and anti-security credentials, screenshots and anti-hijacking; while also protecting the remote security credentials, anti-virus and anti-spyware. Ensure document security and transaction security. Space time code technology is equivalent to building secure channels between devices in an open mobile Internet environment.

4) Equipment fingerprint technology

The fingerprint technology is network equipment from leading international library technology based on hundreds of hardware attributes and behavioral attributes quickly identify and capture devices, for each network device ID only device to generate anti fake, virtual space, as the "identity card", the formation of an open platform contact account system. The device is the carrier of the end user and the establishment of each business system, and the accuracy of the device fingerprint ensures the uniqueness of the user equipment. The unique fingerprint generation equipment, through different browsers still can only locate the equipment; in addition, also has the enforceability, equipment to fingerprint has been tampered with, it is difficult to counterfeit criminals.

IV. Conclusion

For the future development of mobile identity authentication, human centered mobile Internet has become the second generation of Internet development. Human identity will become more and more important in the Internet, and authentication has become the basis of the entire mobile internet. In recent years, domestic and foreign well-known security conference, mobile Internet authentication enterprises have become the highlight of innovation of enterprise, it also shows that the mobile Internet era identity is worth us to spend more energy and time to explore, because this will be the future of mobile Internet is an important entrance.

References

[1] Xiangdong Zhang. Analysis of high security identity authentication technology for mobile Internet. Beijing: telecommunication technology, 2012, 1 (4): 36-39

[2] Shuanglan Cao. Research on cloud service authentication. Wuhan: Journal of Higher Correspondence Education. 2012, 25 (6): 52+83-84 In Chinese

[3] Huiyi Liu . Research on identity authentication technology in mobile Internet. Shandong: Shandong University, 2014

[4] Minqian Wu. Research on cloud computing platform of digital certificate. Nanjing: Journal of Nanjing Radio and TV University. 2016 (4): 82-84 In Chinese

[5] Jiuqiang Cui, Qi Xu. Research on authentication technology of mobile Internet. Beijing: Information Security and Technology. 2015, 6 (7) In Chinese

[6] lilin Ma. Cloud computing environment, the mobile terminal authentication scheme based on two dimensional code. Beijing: Microelectronics and Computer. 2016, 33 (1): 140-143 In Chinese

[7] Quan Zhu. PKI CA identity authentication technology. Beijing: Information Security and Technology. 2016, 7 (9-10): 37-39 In Chinese

[8] Anbin Liu. Mobile Internet era, your data security?. Hainan: Super Science. 2017 (3) In Chinese