Research of Safety Hazards of Online Personal Information and Protective Measures

Yanjie Zhou [1], Ma Li [2]
College of Mathematical and Computer Science
Jiangxi Science & Technology Normal University
Nanchang, China
[1]zyanjwm@163.com,[2] liima@sina.com

Min Wen [3]
Department of Civil and Architectural Engineering
Nanchang Institute of Technology
Nanchang, China
[3]sxwenmin@163.com

Abstract—With the popularity of the Internet in the lives, while researchers are enjoying the convenience brought by the Internet, researchers may also find that the personal information are becoming increasingly vulnerable to theft, and then is quickly spread and abused, causing a serious violation to the privacy. This paper researches the problem of online personal information security reflected by the "Prism" to elaborate on the causes and damages of risks to online personal information security, analyze disclosure of online personal information and illustrate protective measures towards online personal information security while combining the two-factor authentication technology.

Keywords- network; personal information;security risks; information disclosure; two-factor authentication technology

I. INTRODUCTION

With the popularity of the Internet in the lives, while researchers are enjoying the convenience brought by the Internet, researchers may also find that the personal information are becoming increasingly vulnerable to theft, and then is quickly spread and abused, causing a serious violation to the privacy. Due to the leakage of the personal information, researchers are almost "naked" on the Internet [1]. In addition, due to the abuse by criminals, researchers have lost the personal security, so in order to protect ourselves, researchers are unwilling to reveal the personal information by any other means, even the form that researchers need to fill out according to the government, causing great interference to the governmental management [2]. The loss of personal information security also causes the loss of personal security, and thus interfering with the govemmental management. This problem of security hazard to personal information online must be solved immediately [3].

II. SECURITY HAZARDS TO ONLINE PERSONAL INFORMATION

A. Causes for Security Hazards to Online Personal Information

1) Openness of the Internet

Openness of the Internet is the "hotbed" for personal information security hazards. There are various types of information on the Internet from the tiny common sense in lives to information about national security, and researchers can carry out a lot of social activities on the Internet because it provides us with enough freedom and convenience. At the same time, it also provides more "chances" for those criminals or profit-oriented organizations as it makes it more convenient for them to collect, gather, trade and spread personal information [4].

2) Virtuality of the Internet

Virtuality of the Internet is the "backing" of personal information security hazards. In the times when the Internet is popular, the boundary of information spreader and receiver in the network world is not very clear because users can be both information receivers and information spreaders. Thus, there are such people who spread topics related to personal privacy by taking advantages of the attribute of the Internet because they will not be found even if spreading others' privacy unscrupulously.

3) Anonymity of the Internet

Anonymity of the Internet is the "secret base" of personal information security hazards. Criminals are fearless because of this anonymity, so they spread others' occupation, identity, telephone number, address and other detailed personal information and speak anything or even make improper comments. All of these result in that the personal information security cannot be guaranteed.

Wherever Times is specified, Times Roman or Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 or Open Type fonts are preferred. Please embed symbol fonts, as well, for math, etc.

B. Common Personal Information Security Hazards on the Internet

In the online environment, personal information security hazards exist in various forms and even let us off guard. Therefore, I hereby summarize these hazards by collecting information through various ways, and these hazards can be mainly divided into the following categories:

1) Illegal Collection of Personal Information

In this regard, the exploration is made in two aspects: (1) collect others' personal information arbitrarily without informing them in advance; (2) collect others' personal information fraudulently.

2) Illegal Use of Personal Information

It refers to that merchants use Netzens' personal information for other purposes without getting their agreement.

3) The Secondary Exploitation and Use of Personal Data

Many merchants will store existing personal information in a database and then analyze them so as to get some private information that has not been revealed.

Then, they will classify them so as to share with other merchants or sell the information. For example, while registering emails for free, the personal information is sold to other merchants, which is why the mailboxes are filled with spams or advertisements [5].

4) Some Online Service Providers Take "Advantage" of their Positions

"Prism" event [6] is a typical case of United States national security agency through network servers, collects your network user logon time, instant messaging, SMS, phone, pictures, chat, use or storage of data with personal information, in order to conduct data mining work, which analyzes the personal contact and action.

5) Cookie Records

Some sites by analyzing the cookie to collect a large number of users ' personally identifiable information, targeted ads to the user, or collected information to sell to other commercial site, organizations or individuals, in order to benefit from.

6) Existence of Hackers

Hackers tend to be hidden in the computer network technology wizards, they work for network attacks is the use of a variety of technical means, and implanted in the user's computer hacking programs, and through this program automatically sends back the desired information one by one, so as to grasp the important personal information of Internet users engaged in illegal operations. In fact, in the final analysis, the hacker is a major cause of safety problems.

C. Influence of Personal Information Security Hazards on Us

In network, security risks make more and more of the personal information transparent, personal account number, mobile phone number, home address, mailbox number, such as messages, usually for no reason was disclosed on the Internet, bring us not only harassing phone calls, SMS spam, advertising messages, and even got us into fraud trap, threatening the lives and safety [7].

III. MEASURES TO PROTECT ONLINE PERSONAL INFORMATION SECURIT

A. Computer Information Security Technology

Network developed in this era, to fully protect personal information enables us to live a normal life and work. Ensure that personal information on the Internet both to play their actual value, but also to ensure that personal information from unauthorized use or dissemination. Therefore, it is necessary to rely on information technology to solve security-related network of personal information security risks. At present, China's computer information security technology is the following, as shown in Fig. 1.

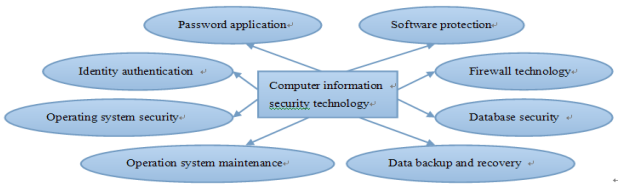

Figure 1. Computer Information Security Technology

Fig. 1 shown these techniques to solve the problem of network information security risks are valid, but in my opinion, the most effective solution to the case of authentication technology, because it is first necessary to enter the security system clearance card, is the basis for all other security mechanisms are running [8]. As shown in Fig. 2: user before entering the security system, first through the authentication system to confirm the identity, then identification by the network monitor and the authorization database to control user access and operation rights of the data sheet. Of course, the database is not intelligent, and it is controlled by the security administrator. Finally, the audit system in accordance with certain security policy, record and review user behavior on various networks, operating systems and applications in various activities related to process information in order to enable the auditors found that the system intrusion or potential system vulnerabilities, which can take appropriate protective measures quickly and accurately. At the same time intrusion detection system for dynamic monitoring system by analyzing safety data, and automatically identify the existence of illegal operating system, such as network attack, abnormal operation, so as to proactively prevent or resist intrusion systems [9].

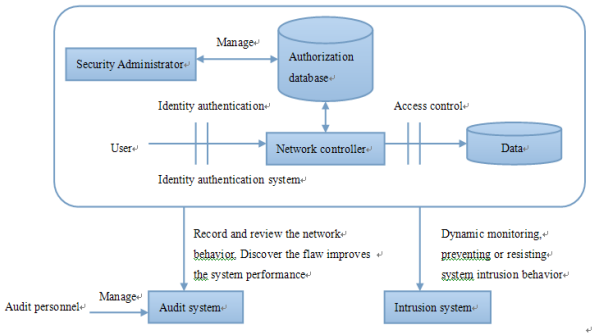

Figure 2. Security Operating Procedures

B. Two-Factor Authentication Technology

In this paper, two-factor authentication is based on the personal digital certificate, dynamic encryption to counter illegal visitors, so as to ensure the security of transactions. And in the realization of a digital certificate (containing identifies a user, such as name, ID number, validity of the public key, and personal information such as, all digitally signed by the issuing CA certificate) authentication mechanism based on the securities of a company to the different needs of users with different two-factor client authentication. As shown in Fig. 3 is a two-factor authentication system chart.

The working mechanism of the system: staff distributed to authorized users single E.T. defenders series of authentication devices, like USBKey or dynamic password tokens. Users when using the certification issued by the device for the first time, the first thing to do is to set a password. Authentication, when users need to set the password used in conjunction with dynamic password tokens display, and dual-factor authentication technologies can be achieved. Time synchronous authentication requirements at the same time, the dynamic password tokens and authentication server must be consistent, so as to guarantee the legal security of the client's securities

transactions. The time synchronization principle in the form of a user pre-set password with dynamic password tokens are randomly generated, as shown in Fig. 4.

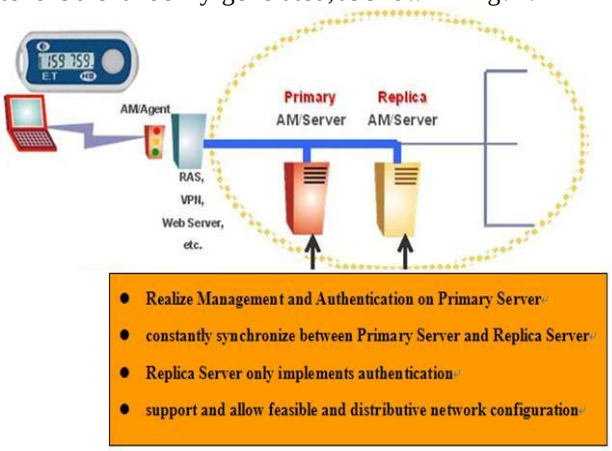

Figure 3. Diagram of Two-factor Authentication System

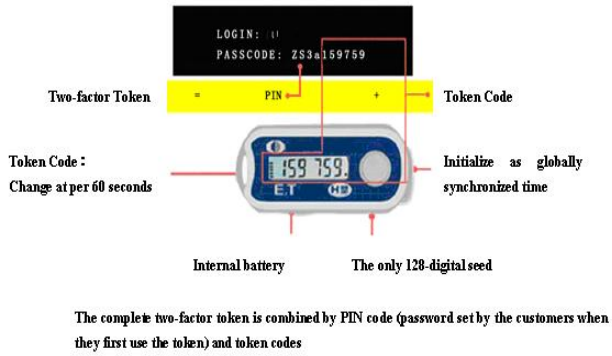

Figure 4. Two-factor Password based on Time

1) Constitution of Two-factor Authentication System

Two-factor authentication system consists of a powerful set of authentication server Authentication Manager, an easy to use authentication token and Authentication/Agent composition of a proxy software. As shown in Fig. 5.

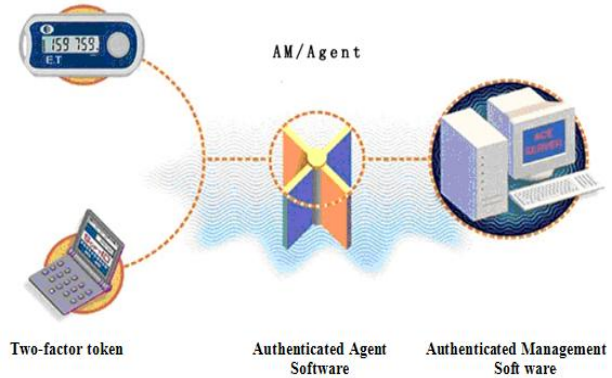

Figure 5. Two-factor Authentication System

2) Authentication Management Software

When the authentication server receives the user's authentication request, the certification management software using a specific algorithm to generate a token code, it uses built-in algorithm and the user authentication token algorithm and the seed value is the same. When customers enter a dynamic password system, proved to be a legitimate user, release, the user can perform any operation that he had the right to. If inconsistency is reminding customers to re-enter password wrong three times in a row, it alerts the user related operations cannot be made today, tomorrow, please come again. The limits of mismatched passwords, network customers ' personal information more secure.

3) Two-factor Authentication Token

In the system of two-factor authentication, two factor authentication token is their product, namely, E.T. guardian series USBKey and dynamic password tokens. USBKey is relatively simple to use, as long as plugged into a computer USB port, then the user can begin to set a password for authentication. Its dynamic password makes brand has h type and d type two species, they inside are has chip and battery and distribution has saving button, has a only of 128 bit seed file, built-in has and time factors related joint of special algorithm, so each 60 seconds will automatically update generated not repeat of password, only different of at is former password displayed for manual operation, then who is can automatically displayed generated of password, using up more convenient. When authentication, pre-set by the user the password combined with the dynamic password tokens display sign with a schema.

4) Agent Software (AM/Agent)

Authentication agent software is similar to a mediator role and plays a role in transmission of information in the user authentication between the authentication and users.

Two-factor client authentication system can be efficient, centralized address the different needs of each customer. From a security point of view, its effectiveness is without a doubt. In order to ensure that the customer's account is more secure, online transactions more secure. Two-factor authentication system digital certificates module and static password authentication module consists of two independent modules, so that the network of customers ' personal information more secure. Customer authentication systems feature a modular design is used in, so it has good flexibility and cross-platform operation is also easy. Because the system has developed a two-factor authentication middleware, the further optimization of the systemmakes it possible for the future.

IV. CONCLUSIONS

The Internet age has brought us great convenience, researchers can chat, shopping, and entertainment on the Internet. The virtual world of the Internet has given us a new identity, but this identity is and the reality of the interdependence. With rapid economic development and the progress of network technology, online personal information security issues come out, and more and more people's attention. Therefore, it is more urgent and important to use a secure networking technology to keep your personal information secure. Two-factor authentication is a feasible and effective solution.

ACKNOWLEDGMENT

This research has been supported by the Education Department of Jiangxi Science & Technology Normal University project JGYB-14-24-32.

REFERENCES

[1] Hur J. Improving security and efficiency in attribute-based data sharing. IEEE Transactions on knowledge and Data Engineering[C], 2013, 25(10):2271-2282

[2] Zhou Z, Huang D. On efficient ciphertext-policy attribute based encryption and broadcast encryption. Proceedings of the 17th ACM Conference on Computer and Communications Security(CCCS'10) [C], Oct4-8, 2010, Chicago, IL, USA. New York, NY,USA:ACM, 2010:753-755

[3] Goyal V, Pandey O, Sahai A, et al. Attribute-based encryption for fine-grained access control of encrypted data. Proceedings of the 13th
Security (CCCS'06) [C], Oct 30-Nov 3, Alexandria, V 人 USA. New York, NY, USA: ACM, 2006: 89-98

[4] Hur J, hoo D, Hwang S O, et al. Removing escrow from ciphertext-policy attribute-based encryption. Computers and Mathematics with Applications[C], 2013, 65(9): 1310-1317

[5] Liang X, Li X, Lu R, et al. An efficient and secure user revocation scheme in mobile social nehvorks. Proceedings of the IEEE Global Communications Conference (GLOBECOM'll) [C], Dec 5-9, 2011

[6] Houston, TX, USA. Piscataway, NJ, USA: IEEE, 2011: Sp Li M, Yu S, Zheng Y. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems[C], 2013, 24(1): 131-143

[7] Hur J, Noh D h. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems[C], 2011, 22(7): 1214-1221

[8] Hur J. Attribute-based secure data sharing with hidden policies in smart grid. IEEE Transactions on Parallel and Distributed Systems[C], 2013, 24(11):2171-2180

[9] Lubicz D, Sirvent T efficient. Advances Attribute-based broadcast encryption in Cryptology: Proceedings of the 1st

[10] scheme made International Conference on Cryptology in Africa (AFRICACRYPT'08) [C], Jun 11-14 2008

[11] Stevens R W. Security of personal information in a new health care system.[J]. JAMA : the journal of the American Medical Association,1994,27119.

[12] Anonymous. CA Survey: Adults Worry about Security of Personal Information Online[J]. Wireless News,2008.