I.J. Wireless and Microwave Technologies, **2011, 6, 38-45**
Published Online December 2011 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijwmt.2011.06.06

Available online at http://www.mecs-press.net/ijwmt

Design and Implementation of Anti-phishing Authentication System

Wang Binjun[a], Wei Yang[b], Yang Yanyan[c], Han Jia[d]

Department of information security, Chinese people's public security university, Beijing, P.R.China

Abstract

For phishing problems and its essential characteristics, the authentication protocol of anti-phishing based on two-direction, two-factor, and interaction is proposed, and its safeties are investigated. For PKI security infrastructure and B/S technology model under Internet, an interactive authentication mechanism based on special custom image and client program is designed and implemented. The method is universal to authenticate any server on Internet. It is a new solution of anti-phishing.

Index Terms: Phishing; Authentication; Two-Direction; Two-factor and Iinteraction Authentication; PKI

1. Introduction

With the rapid development of Internet, various electronic frauds come in great numbers. Among them, phishing is the most deceptive and influential [1]. As the situation of phishing becomes more and more serious, Anti-Phishing Working Group (APWG) is established in the world. In the end of 2006, "*Report on Phishing*" was published by the United States and Canadian government. According to the report of APWG, global "phishing" attack in the first half year of 2008 was about 47324 [1]. The data of CNCER/CC showed that there were two phishing attacks aiming at the banks of Chinese country separately in 2002 and 2003, the number of such cases in the report of 2004 was 223, 456 cases in 2005, 563 in 2006, and 645 phishing incident reports were received by CNCERT in the first half year of 2008. "Phishing" has already become a common hazard around the world, and the situation is deteriorating.

Phishing (Phishing is the compound of "Phone" and "Fishing") derives from utilizing the vulnerability of the telephone system to embezzle user's account and toll fraud. With the rapid development of Internet, hackers use the principles of phone phishing to form "phishing" on Internet. Different experts and scholars have different definitions of phishing. Phishing in this article is defined as follows: It is a kind of Internet fraud that phishers imitate some important websites, then use social engineering and various techniques [2] to lure the victims to the fake website in order to cheat the accounts, password and other sensitive information of the users.

* Corresponding author.
E-mail address: [a]b.j.wang123@263.net; [b]cpp_vo@yahoo.cn; [c]wixinini@163.com; [d]h7505@soho.com

According to the research on phishing and the understanding of its essence [2], the writer considered the essence of phishing as a spoofing technique that phishers lure the victims to the fake website using a variety of techniques, and then get the sensitive information of the users through the realistic fake website. A lot of experts and scholars have already proposed some prevention methods and techniques against phishing [3, 4, 5]. Through systematic research and analysis on phishing, the writer believes that the fundamental reason of phishing is the lack of server authentication. The server would be authenticated firstly in the login process in order to make sure the server is true, after that users provide the sensitive information and do the follow-up interactive work. If doing like this, then no matter what smart tricks the phishers will use to lure, no matter how realistic the phishing website will be, there is not phishing. Therefore, the key of solving phishing is providing the authentication of the server.

There is another issue must be considered: if authentication is set up for each server on Internet, it will greatly increase the burden of users, and will seriously affect the users to use the Internet. According to the characteristics of the B/S structure and the environment of PKI, a new method of one customized client program for every server on Internet to authenticate is designed. This method can enhance the security of Internet, especially for preventing phishing. It is a scientific and practical new thinking to share with readers.

2. Conventional Authentication and Its Security Analysis

Authentication is one of the fundamentals and the threshold of the information security [6]. Only the truth of the identity could be guaranteed correct implement, the access control, security audit and other follow-up series of security measures could be guarantee. Just as previous section description, the key way of resisting phishing is the server authentication.

Usually, authentication can be divided into the following three types:

- User knows, such as password.
- User has, such as ID, IC card, USB Key, etc.
- User own, such as fingerprint, iris, face, voice pattern, handwriting, DNA, etc.

The first method is simple, easy to implement, but easy to guess, poor security. For example, in the first Gulf War, 34 computers of American military computer system were captured by five Dutch hankers used the words such as “nuclear”, ”weapons”, ”missile”, ”desert storm”, ”desert shield”, etc, and hacker got large amount of confidential information on military action against Iraq [7]. The passwords were captured by using dictionary attack, birthday attack and other attacks. The second method is complex to implement, and the security is better, but may be faked. IC card, USB Key and such “hardware” devices can store the password long enough, which have amount of key space to enhance security. The certification process can be done automatically by the related equipment, not requiring the users to input, avoiding the difficulty of remembering the long password for users and reducing the potential safety hazard of peeping when input. However, this method also has some risks, for example, IC card, USB Key and others may be lost or copied, etc. The third method has the best security, but implementation costs are also highest. It needs expensive hardware device and related software to support, only be used for the system with high level of information security. It should be noted that, with the progress of science and technology, this method can also be forged, such as man-made fingerprints and iris, and so on.

Thus, although many types of authentication are invented and created in the engineering practice, there are defects in one way or another. So further study and improvement of authentication need be researched. In the authentication, one important problem required careful consideration is that when one person under authentication certifies the truth of himself, he tries not to let out his own identification information, otherwise the third parties or verifier may intercept the person’s authentication information, this may cause a security risk. Therefore, zero-knowledge proof as the following condition should be satisfied under authentication:

- Verifier can not be cheated by shower under authenticated. If the shower knows how to prove, he should make the verifier to be almost believed that he can prove; if the shower doesn’t know how to prove, he should make the verifier to believe that the probability he knows how to prove is zero.

- Verifier dose not know the process of proof, so that he can not leak the proof process to a third party.
- Verifier can not receive any information of proof from shower under authenticated, so that authentication process can not leak any information to the verifier.

Usually, it is called the minimum leak proof when the first two conditions are satisfied, and it is called the zero-knowledge proofs when all of the three conditions are satisfied.

In recent years, security verified code turned up in the field of authentication technology, which was a authentication mechanism that the identity of the client was verified in the interaction process between client and server. Brute-force attack of computer program or replay attack is prevented when the security verified code is used.

3. Authentication Mechanism and Its Security Analysis of Two-Direction, Two-Factor, Interaction

According to the above two sections, we know that phishing can be eliminated fundamentally with authentication of server, and the authentication method can be any of the above authentication mechanisms. In this thinking, client software should be designed for each server in the C/S mode. In the B/S mode, since the client software is downloaded dynamically from the server, the server maybe fake. So it is difficult to ensure the process of the user login is the process to implement the two-direction authentication. Therefore, client software should be installed for each server. So, specific client software is needed for each authentication of server. But it may be serious burden for users to use Internet because there are many servers on the Internet.

This article assumes that under the Internet environment, fairly complete PKI security infrastructure has been established [8, 10]. It is designed a new authentication mechanism of two-direction, two-factor, and interaction for verifying the truth of server (short for ATTI), which can effectively prevent the threat of phishing. The so-called two-direction means that when the user login the server, not only identities of user would be authenticated by the server, meanwhile the identities of servers would be authenticated by users. The two-factor referred to the mechanism use two way of above authentication, that is not just the authentication message of the user know needed (for example: password), at the same time, It also need the authentication message of the user has (for example: USB Key etc). The purpose is that once the password of user has been conjectured, phishers could not simply take advantage of the sensitive information been cheated from users because he doesn't have the other factor. USB Key is used as the second factor of authentication in this paper. Interaction means that only the client confirms the related information returned by server in the two-direction authentication, further action only can be done in the authentication process.

For describing conveniently, there are some agreements as follows: A represents as the user. B represents as the server. It is supposed that there is the PKI network security infrastructure in the system environment (CA center), which is called C. $(M)_K$ indicates the ciphertext using the key K to encrypt M. x+ and x- represent respectively as the public key and the private key of x.

3.1. Registration Phase

When the user A registers in the CA center, a specific image I is generated customarily for the user by CA server, the private key of user , $(I)_{c+}$ and a specific authentication program are kept in USB key, and then user receives the USB key.

User A submits his name, password and other information to server B.

Server B registers in the CA center, CA product the public and private key for B. Only B receives its private key.

3.2. Login Phase

Login procedure is as follows:

1. A->B: when user A intends to login the website of server B, the specific login program in the USB Key should be started, generates random number RA, and the program sends $(((I)_{c+}, RA)_{a-}, A)_{b+}$ to server B.
2. B->C: when $(((I)_{c+}, RA)_{a-}, A)_{b+}$ is received by server B, $(I)_{c+}$ can be got by using b- and a+ respectively to decrypt. If A is an illegal user, stops the login process. Otherwise, generates the random number RB, and sends $((I)_{c+}, A, B, RA, RB)_{c+}$ to C.
3. C->B: when CA center receives $((I)_{c+}, A, B, RA, RB)_{c+}$, the specific image I is got by using c- to decrypt twice, then delivers $((I', RA, RB)_{a+}, RB)_{b+}$ to server B. I' is the image which is added watermark with current time.
4. B->A: when server B receives $((I', RA, RB)_{a+}, RB)_{b+}$, $(I', RA, RB)_{a+}$ and RB are got by using b- to decrypt. After server B verifies RB, delivers $(I', RA, RB)_{a+}$ to client A.
5. A->B: when A receives $(I', RA, RB)_{a+}$, I', RA and RB are got by using a- to decrypt. After A verifies RA, image I' will be displayed in the user login interface as background. If the user sees the specific image I', it indicates that the identity of server has verified. Then A inputs PWD, and sends $(PWD, A, RB)_{b+}$ to server B.
6. When B received $(PWD, A, RB)_{b+}$, PWD, A and RB are got by using b- to decrypt. After verifies RB, authenticates A according to the PWD and A.

In the above process, any failed will indicate that the two-direction, two-factor, interaction authentication failed, and the process of authentication would end. The workflow shows in Fig. 1, and the topological structure shows in Fig. 2.

This process indicates that only after the login interface with customized image is seen by user, then the sensitive information can be input and send to server B. The authentication process can be seen by users. Because the specific image is customized, phishers can not imitate. The login authentication process ensures that when users see the customized image they believe they are interacting with the true server. User A only needs register in CA center once, can visit and authenticate all the servers of the Internet , and needs not apply for different USB keys for different servers. This method is universal.

3.3. Analysis of Security

The security of above-mentioned anti-phishing authentication mechanism based on two-direction, two-factor and interaction will be analyzed as follows:

- If the user is lured to a phishing website, this server should be authenticated by client in this mechanism, so the above procedure can not be completed because the phisher doesn't have the b- of real server, that is to say the password of user and other sensitive information can not be obtained by the phisher.
- If the name, password and other sensitive information of the user are acquired by cheating, stealing, and so on, but the phisher doesn't have the user's USB key , which is the other factor of the two-factor authentication, so the phisher can not complete the above procedure neither, no further advantage will be got form using the sensitive information of the users.

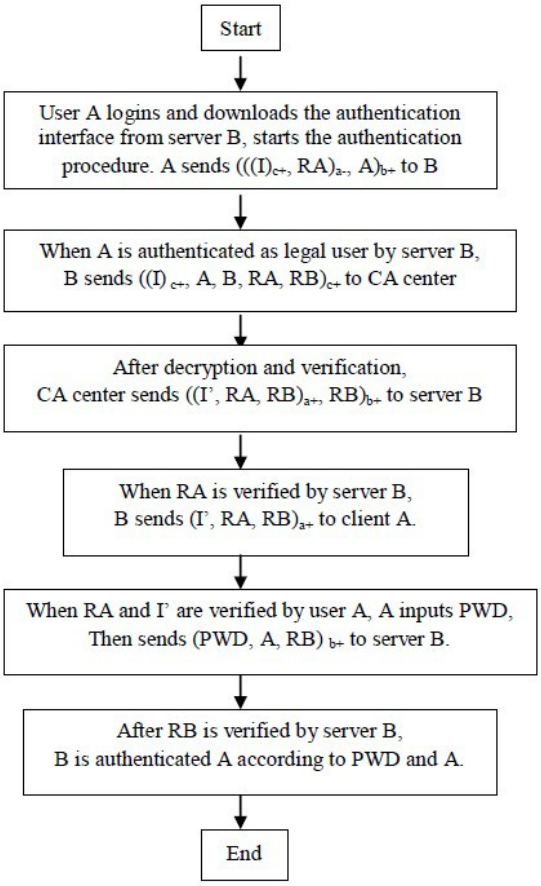


Fig 1. Authentication procedure of the ATTI login

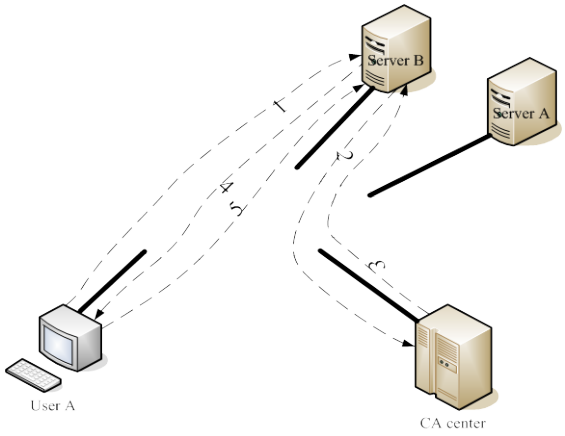


Fig 2. Topological structure of the ATTI login

- if $(((I)_{c+}, RA)_{a-}, A)_{b+}$, $((I)_{c+}, A, B, RA, RB)_{c+}$, $((I', RA, RB)_{a+}, RB)_{b+}$ or $(I', RA, RB)_{a+}$ is captured by phisher, because the customized image of user's I and I' are encrypted by either c+ or a+, but only user A and CA center own a- or c-, so image I can't be captured by phisher.
- Replay attack can't be implemented because of using the random RA and RB for the designing [8].
- If Trojan is injected in the computer of users, the customized image I' might be captured, but for the watermark with current time designed in this mechanism, malicious use of the customized image I' captured by phisher can be effectively prevented. The essence of this design is another way of preventing replay attack.

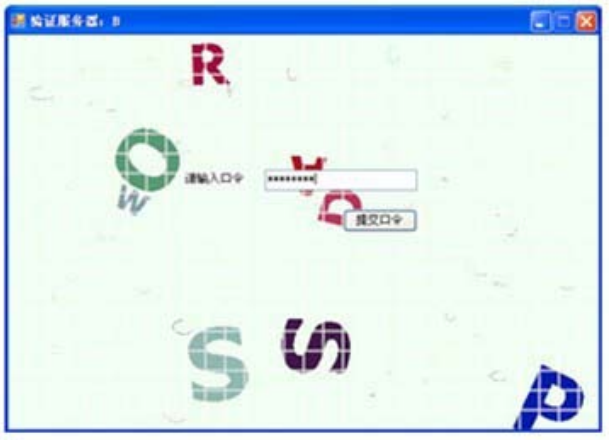
Therefore, the authentication mechanism of the two-direction, two-factor and interaction presented in this paper can effective prevented from phishing, Man-in-the-Middle and other attack. Even though phisher can effectively attack the private key or get the password, they can't get the second authentication factor, USB key, in this mechanism. So, the security of authentication can be effectively guaranteed.

4. The Key Technology of the B/S Authentication System

Because most of the application systems on Internet are B/S model, two key technologies must be implemented in order to complement the above authentication procedure.

The first key technology is the generation of the specific image. The letters of "PASSWORD" in four dimensions: location, size, color, and font, will be randomly generated in a specific image area for users. Because the image of each user is different, a user can judge on the basis of relative position (referred to grid lines ,text boxes, and buttons, etc) that 'P', 'A', 'S', 'S', 'W', 'O', 'R', and 'D' are in the interface of the image, it is called customized. For example, a user login screen shows in Fig. 3(a). In addition, in order to prevent the customized image of user from filching (for example Trojan malicious code screenshots, etc), customized image need some overlapping of image and the current date and time, with which the users can verify conveniently. Just as Fig. 3(b) shows.

The second key technology is the client authentication program, which must be started when the authentication procedure begin. The specific authentication program of user in the USB key should be started to download the login interface of server when the user login the true server in order to complete related encrypt and decrypt, and shows the final customized image to users.



(a) original customized user interface

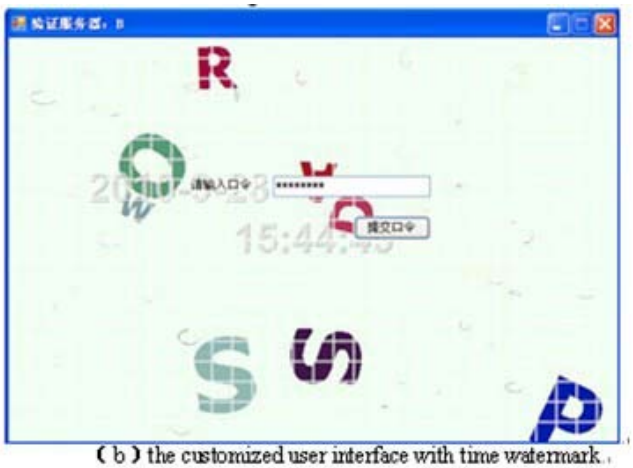


Fig 3. The customized login interface

5. Conclusion

By the research on the classification of phishing [2], it is concluded that phishing's essence is a security threats by setting up a phishing website, where users are lured to with social engineering and other various kinds of techniques, then the sensitive information of users are filched. The fundamental method to respond phishing is authenticating the server. Only the server is authenticated, the phishing can be eliminated fundamentally. This article put forward an anti-phishing authentication mechanism, gives the fundamental way to solve phishing theoretically. The two-direction, two-factor, and interaction authentication m echanism based on PKI network security infrastructure is designed in this article, skillfully making use of CA center information security infrastructure. There is only one USB key (including the private of asymmetric cryptography, specific authentication program of client and customized image of users $(I)_{c+}$) in the entire network, but not different USB key for each user to verify each server in the network environment. The implementation technique is simple, scientific, and effective. It has extensive application value, provides a feasible technique for widespread authentication for server in the Internet environment currently, which is a technical proposal to prevent the threat of phishing efficiently. The main problem of this proposal is that CA center authentication server is needed by each user when login the server on the Internet, it makes CA center become a bottleneck of the system. Further research is needed.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of The Anti-Phishing Working Group. Phishing Activity Trends Report Q2/2008 [OL], http://www.antiphishing.org/resources.html.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
[2] J.Gong Rong, Wang Binjun. "Research on Classification of Phishing Based On Systems Engineering". Journal of Chinese People's Public Security University, 2009.4: 91–94.巩荣，王斌君.基于系统工程的网络钓鱼分类研究[J].中国人民公安大学学报，2009.4: 91–94
[3] J.Kong Weiguang. "Technical Analysis of Phishing Attack and Precautionary Measure" Journal of Wuhan University of Science, 2006.3: 63–65M. Young, The Technical Writer's Handbook. Mill Valley, CA:

University Science, 1989. 孔维广.Phishing 攻击的技术分析与防范措施[J].武汉科技学院学报，2006.3: 63–65
[4] C.Zhang Jian, Wang Jishu, Liang Hong. “The Current Situation and Countermeasure of Phishing and Pharming”.The Twentieth National Computer Security Academic Exchanges Conference Collection, 5–8. 张建，王吉树，梁宏.网络钓鱼与域欺骗的现状与对策[C].第二十次全国计算机安全学术交流会议论文集，5–8.
[5] Chen Juan, Guo Chuanxiong “Detection Online and Prevention of Phishing Attack.” Journal of PLA University of Science and Technology (Natural Science Edition). 陈涓，郭传雄.网络钓鱼攻击的在线检测及防治.解放军理工大学学报(自然科学版) [J]，2007.8: 134-135.
[6] M.Wang Binjun, Jing Qianyuan, Ji Zhengrui. Information Security System. Beijing: Higher Education Press, 2008. 王斌君，景乾元，吉增瑞.信息安全体系［M］.北京：高等教育出版社，2008
[7] M. Xiao cases. Information security and information warfare.Beijing: Tsinghua University Press, 2004. （美）晓宗.信息安全信息战［M］.北京：清华大学出版社，2004
[8] M.Qing Sihan. Security Protocol Beijing: Tsinghua University Press, 2005. 卿斯汉.安全协议［M］.北京：清华大学出版社，2005
[9] C.Wang Binjun, Wei Yang, Gong Rong. “ Design and Implementation of Anti-phishing with Two-direction Authentication System in the B/S Model”.The Proceedings of the Twenty-fifth Computer Security Committee. 王斌君，韦杨，巩荣.B/S 环境下反网络钓鱼双向身份鉴别系统的设计与实现[C].第二十五届计算机安全专业委员会论文集
[10] J.Guo Zhengrong, Zhou Cheng. “Implementation of Electronic Signature System Based on PKI” Computer Science, 2006.9: 83–88. 郭正荣，周城.基于 PKI 的电子签章系统的实现[J].计算机科学，2006.9: 83–88.