Wuhan University
Journal of Natural Sciences

2018, Vol.23 No.1, 079-083

Article ID 1007-1202(2018)01-0079-05
DOI https://doi.org/10.1007/s11859-018-1297-y

A New Anti-Spam Model Based on E-mail Address Concealment Technique

☐ **ZHANG Yuqiang[1,2], HE Jingsha[3], XU Jing[4]**

1. Beijing Institute of Aerospace Control Devices, Beijing 100039, China;

2. College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China;

3. School of Software Engineering, Beijing University of Technology, Beijing 100124, China;

4. Department of Automation, Tsinghua University, Beijing 100084, China

Abstract: To deal with the junk e-mail problem caused by the e-mail address leakage for a majority of Internet users, this paper presents a new privacy protection model in which the e-mail address of the user is treated as a piece of privacy information concealed. Through an interaction pattern that involves three parties and uses an e-mail address code in the place of an e-mail address, the proposed model can prevent the e-mail address from being leaked, thus effectively resolving the junk e-mail problem. We compare the proposed anti-spam method with the filtering technology based on machine learning. The result shows that 100% spams can be filtered out in our scheme, indicating the effectiveness of the proposed anti-spam method.

Key words: spam; e-mail address; protection model; e-mail address code

CLC number: TP 393

Received date: 2016-07-15

Foundation item: Supported by National Natural Science Foundation of China (U1736116, 61272500, 60373075), and the National High-Tech R&D Program (863 Program) (2015AA017204)

Biography: ZHANG Yuqiang, male, Engineer, Ph.D., research direction: network security. E-mail: yuqzhang@emails.bjut.edu.cn

0 Introduction

E-mails have brought us more and more convenience. However, at the same time, we also receive numerous unwanted messages from outsiders. Most of these messages are useless to us, and these destructive e-mails even contain viruses or malicious codes [1].

When users visit a website for the first time, they are often asked to register by the website by providing some personal information in order to get more services conveniently. During the registration, user's e-mail address is a very important piece of information [2]. Users may receive an e-mail subsequently to activate the new account. And when users want to perform a transaction with the website, the e-mail address will be used to receive service information from the website. In such interactions between users and website, e-mail addresses become essential in the process of interactions. The current interactive pattern is that users provide their commonly used e-mail addresses to the website and the websites send customized service information to the e-mail addresses that they have provided [3, 4].

E-mail addresses are used not only for visiting websites, but also for communicating with other users. However, there are some unsafe factors in the network that make the real e-mail addresses very easily obtained by malicious parties. Once a commonly used e-mail address is revealed, junk mail may flood the e-mail [5].

Users can hardly change this situation. Neither do they have any way to make their e-mail address information a piece of secret information. Possible ways of dealing with this problem include adopting anti-spam

technologies by the service providers on behalf of the users and switching to new e-mail addresses frequently by the users. But these two methods may cause some inconvenience or have some technical deficiency and, consequently, can hardly solve the problem from user's point of view.

The first type of method that has been adopted by service providers is the mainstream method of anti-spam in which filtering is the major technique [6]. Filtering techniques can be distinguished based on the role, such as MAT filtering, MDA filtering and MIJA filtering, and based on the method, such as key character-based filtering technique, white-list filtering technique, black-list filtering technique, reverse DNS query technique, rule-based filtering technique, content-based filtering technique and other mail filtering techniques. In recent years, with a wide application of machine learning methods, many technologies based on it were applied in anti-spam, such as text mining, classifier and so on. For example, Basavaraju *et al*[7] proposed a spam detection method to classify the spam using the text clustering techniques based on vector space model. Roul *et al*[8] proposed an approach to identify the spam pages by combining content and link-based techniques.

To some extent, these techniques can effectively inhibit spam [9], but spammers constantly update their anti-filtering skill to deceive filters. In addition, these techniques are used to control the spam at the destination and are thus unable to stop spam from the source. The user can adopt another method, that is, not to use the disclosed e-mail address again. Instead, the user will apply for a new one. This method seems simple and feasible. But when the user re-visits the same website or starts a new network interaction, the same problem will happen again and the new e-mail address has the same chance of being stolen by malicious parties [10]. In addition, although the process of applying for a new e-mail address is easy, all of the user's classmates, friends, commercial partners and other interactive websites whom the user has communicated with through the old mail address can no longer keep in contact with the user. The user has to update the newly applied e-mail address with these friends and partners to re-establish the new address book for normal daily communication. This effort is cumbersome and time-consuming, and may cause the loss of contacting with some important communication parties [11].

In order to fundamentally solve the problem in the proliferation of spam, in this paper, we propose a new method of privacy protection in which user's e-mail address is considered as a piece of privacy information that should be protected. In this method, we use an e-mail address code to replace user's real e-mail address and propose some technical measures to ensure that e-mails can be transmitted through this e-mail address code transparently to the user. The users can flexibly control the e-mail address code and independently stop junk mail. Using this new model, users can easily find out the spammers, thus effectively stop the spam from reaching the users and also allow the users to report the spammers promptly.

The rest of this paper is organized as follows. In Section 1, we describe our proposed privacy protection model in details including the architecture. In Section 2, we use an example to illustrate how our privacy protection model works. Finally, we conclude this paper in Section 3.

1 Proposed Model

In this section, we briefly introduce the working pattern of our model and describe the core method in the new model. We then present the architecture and workflow of the new privacy protection model.

1.1 Working Pattern

Compared with traditional ways of communicating with e-mail addresses, our method does not provide commonly used e-mail addresses for the interactive websites directly. Instead, we propose to use a special and flexible e-mail address code to replace the commonly used e-mail address. Through this e-mail address code, the website that interacts with the user can still send service information to the user's commonly used e-mail box. This method can not only protect the user's e-mail address but also complete the whole process of interactive services as usual.

E-mail address code is a user-centered design with the characteristic of being temporary, flexible in management, among others. This code is generated by the user and then used as the e-mail, i.e., the user now replaces the real e-mail address for sending and receiving e-mail within a valid period of time set freely by the user. Once the e-mail address code expires, the user's commonly used e-mail address can be used again. Or the user can set up another e-mail address code to be used for the next time period. The working pattern of the proposed model is shown in Fig. 1.

1.2 Interactive Entities

This model involves three main interaction entities: subject A, objects B, and the e-mail server C.

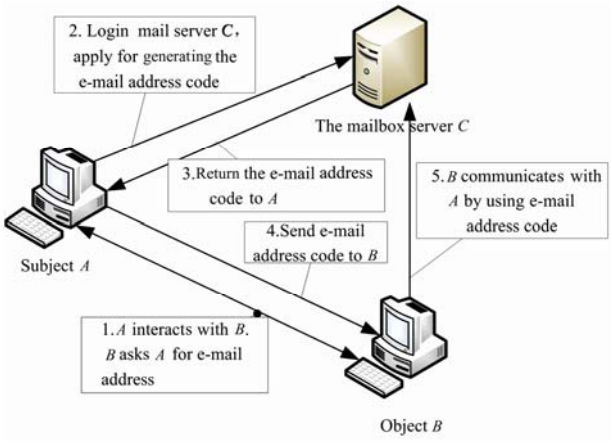

Fig. 1 Working pattern of the model

Subject *A*: The owner of the privacy information which initiates the interactive process (the user).

Object *B*: The user's interaction partner who requires users to provide the e-mail address in order to continue with the interactive services.

E-mail server *C*: *A* server that provides e-mail services for the user and is considered as the provider of the e-mail address privacy information.

The user shares the e-mail address as privacy information with the server. But the interaction partner is an irrelevant third party of the e-mail address information. As long as the interactive process can be completed smoothly, it is not necessary for the user to provide the real e-mail address for the interaction partner.

1.3 Main Architecture

This main architecture of the model contains four elements: generation, storage, management and verification modules as in Fig. 2. The generation module takes the user supplied e-mail address information to generate the e-mail address code. The storage module stores the e-mail address code and other relevant information in the system. The user can manage the e-mail address code through the management module such as modifying the period of validity, opening or closing the e-mail address code, and revoking the e-mail address code, etc. The verification module is used to verify the information from the interactive party in order to receive or reject the message.

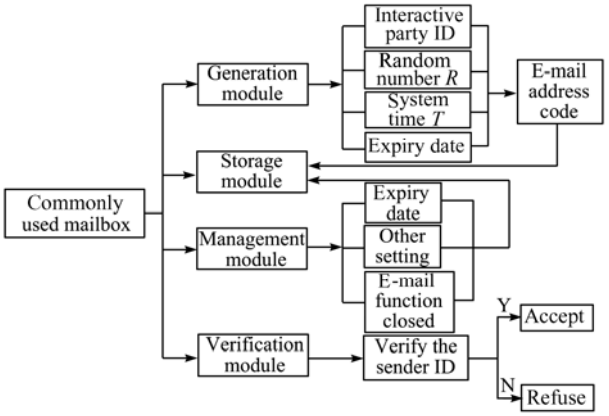

Fig. 2 Main architecture of the model

Generation module (producer): This module is used by the user to apply for an e-mail address code. It generates the e-mail address code based on information such as ID number of the interactive party, random number *R*, current system time *T* and expiration date. The expiration date depends on the interaction situation with the interactive party.

Storage module (storage): This module stores all the information of the e-mail address code after the e-mail address code and the related information is produced. The module would bind the e-mail address code with the user commonly used e-mail to enable information transmission using the new e-mail address code.

Management module (manager): This module can be used by the user to manage the e-mail address code information. Through this module, user may modify the e-mail address code information parameters based on different interaction situations. Especially, when the user receives some junk mail, he/she may adjust the parameters and the interactive patterns associated with the e-mail address code.

Verification module (verifier): This module is used to verify the ID information of the e-mail sender who sends the e-mail through the e-mail address code to the user. If the sender's ID information is the same as the ID information stored at the interactive party during the generation of the e-mail address code, the e-mail will be accepted. Otherwise, it will be rejected.

1.4 Workflow of the Model

Based on the anti-spam privacy protection methods, implementation of the model takes the following steps. The entire framework of this method includes the user's commonly used e-mail, the e-mail server and other people or website that interacts with the user. If *A* is the user's commonly used e-mail, *B* is another user or a website that interacts with the user, and *C* is the mail server, the method includes the following 6 steps.

1) When *A* browses website *B* to get some services, A needs to fill out the registration information and supplies the commonly used e-mail address in order to complete the interaction smoothly.

In our new privacy protection model, subject *A* will do the following to finish the registration.

2) *A* logins into the mail server *C* and applies for an e-mail address code. Based on the e-mail address of *B*, the random number, and the current time of the system, a message digest can be generated by using algorithm SHA-1. Digital signature can be generated by using algorithm RSA, and *C* generates the e-mail address code. This code binds the commonly used e-mail of *A* with the mail server *C*. To manage the e-mail address code of *A* based on the situation during the process of interaction with *B*, all the information related to the e-mail address code will be stored in *A*'s commonly used e-mail.

3) *A* obtains the e-mail address code generated by *C* and sets the initially information for the e-mail address code: the expiration date of the e-mail address code, the temporary name for *B*, the key words of the interactive service and other security parameters.

4) *A* uses the e-mail address code to replace the commonly used e-mail address when it provides registration information for *B*. This e-mail address code is used only for the interaction between *A* and *B*.

5) *B* uses the e-mail address code in all interactions with *A*. At *B*, all received messages from *A* now show the e-mail address code but not the real e-mail address of *A*. Of course, the e-mail address code of *A* is transparent for *B* during the process of interaction.

6) In the process of each interaction, because the e-mail address code contains the ID information of *B*, *C* can verify the ID information of the message sender who sends the message through the e-mail address code. If the ID information is the same as the ID information of interactive party which is stored during the generation of the e-mail address code, the message will be received. Otherwise, the message will be rejected.

2 Experiment

Based on the proposed anti-spam and privacy protection model, we have developed a prototype system. Comparison experiments have been conducted on the system to evaluate the effectiveness and the performance of the proposed model.

In our experiments, the e-mail address of user *A* is AAA@126.com, the e-mail address of website *B* is BBB@126.com and the spam website is *C*. The comparison of the three schemes is shown in the following: scheme 1 uses our anti-spam privacy protection model, scheme 2 uses the related detection technology to filter the spam, and scheme 3 does not use any anti-spam method.

1) Scheme 1

User *A* communicates with website *B* via the unique e-mail address code B754fc@126.com. Website *B* does not have the true e-mail address of user *A* (as shown in Fig. 3). Therefore, even though website *C* obtains the unique e-mail address code (B754fc@126.com) from website *B*, the spam e-mails sent from *C* to *A* can be easily identified by our systems and will not be forwarded to the true e-mail address of user *A* (AAA@126.com).

Fig. 3 Program interface of anti-spam privacy protection model

2) Scheme 2

This scheme adopts the newest method that using monitoring and filtering techniques in anti-spam. In this scheme, after an e-mail contacts with website *B* via AAA@126.com, website *C* may get the true e-mail address of *A*. Then website *C* will send spam e-mail to *A*. And in the process of sending the spam e-mail to the mailbox *A*, the scheme uses the approach of combining content and link-based techniques to detect and filter the spam e-mails [8]. Therefore, a portion of spams are blocked from being sent to the user's mailbox *A*.

3) Scheme 3

This scheme does not use the proposed model. After an e-mail contacts with website *B* via AAA@126.com, website *C* may get the true e-mail address of *A* and send spam e-mail to *A*.

Figure 4 shows the result of 1 000 runs of the experiment. In each test, 100 spam messages were sent to user's mailbox *A* by using scheme 1, 2, 3, respectively, and the received numbers of spam are recorded.

From Fig.4, we can see that in scheme 1, all spams can be filtered out, and the number of junk mail received is 0. In scheme 2 which uses the filtering technology based on machine learning in Ref. [8], 26 spam messages are received, indicating that the spam-filtering rate is

about 74%. Scheme 3 does not take anti-spam methods, so the user's mailbox *A* received all test junk mails. The result demonstrates the effectiveness of the proposed anti-spam method.

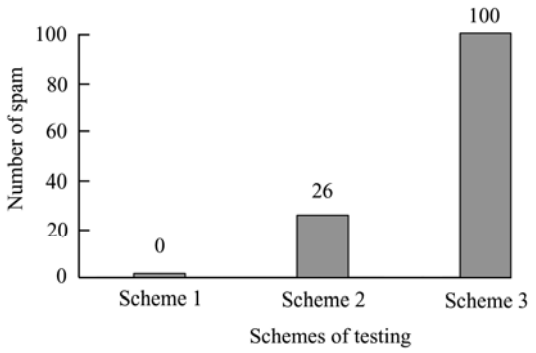

Fig. 4 Comparison of three schemes for avoiding the spam e-mail

3 Conclusion

We propose a new model for preventing e-mail spam in this paper. The merits of our proposed model are as follows:

1) The real address information of e-mail used commonly will not be disclosed to any other interactive parties. Users do not need to update their e-mail frequently to deal with the problem of e-mail address leakage. The protection on user's commonly used e-mail addresses can ensure normal communication between users and good friends.

2) Users can easily determine which messages are spam by depending on their own preferences and can set parameters of e-mail address code flexibly depending on specific interactive situations.

3) Users can clearly know the source of the e-mail problems such as spam and thus can take appropriate measures.

4) Management of the e-mail address code is flexible. Users may reduce or extend its date of expiry or open, close and cancel its receiving and sending mail function. These operations really depend on the need of the users.

In our future research, the privacy protection model that we proposed in this paper will be further refined and the performance and functionality of the application of this model will also be analyzed in greater depth.

References

[1] Ku C H, Leroy G. A decision support system: Automated crime report analysis and classification for e-government [J]. *Government Information Quarterly*, 2014, **31**(4): 534-544.

[2] Lai G H, Chen C M, Laih C S, *et al*. A collaborative anti-spam system [J]. *Expert Systems with Applications*, 2009, **36**(3): 6645-6653.

[3] Liu Y, Cen R, Zhang M, *et al*. Identifying web spam with user behavior analysis [C] // *Proceedings of the* 4*th International Workshop on Adversarial Information Retrieval on the Web*. New York: ACM Press, 2008: 9-16.

[4] Burghardt T, Buchmann E, Müller J, *et al*. *Understanding User Preferences and Awareness*: *Privacy Mechanisms in Location-Based Services* [M]. Heidelberg: Springer-Verlag, 2009.

[5] Xu F, Chow K P, He J, *et al*. Privacy reference monitor — A computer model for law compliant privacy protection [C] // *Parallel and Distributed Systems* (*ICPADS*), 2009 15*th International Conference*. Washington D C: IEEE, 2009: 572-577.

[6] Marsono M N, El-Kharashi M W, Gebali F. A spam rejection scheme during SMTP sessions based on layer-3 e-mail classification [J]. *Journal of Network and Computer Applications*, 2009, **32**(1): 236-257.

[7] Basavaraju M, Prabhakar D R. A novel method of spam mail detection using text based clustering approach[J]. *International Journal of Computer Applications*, 2010, **5**(4): 15-25.

[8] Roul R K, Asthana S R, Shah M, *et al*. Detecting spam web pages using content and link-based techniques[J]. *Sadhana*, 2016, **41**(2): 193-202.

[9] Junejo K N, Karim A. PSSF: A novel statistical approach for personalized service-side spam filtering [C] // *Proceedings of the IEEE/WIC/ACM International Conference on Web Intelligence*. Piscataway: IEEE, 2007: 228-234.

[10] Ali A B M, Xiang Y. Spam classification using adaptive boosting algorithm [C] // 6*th IEEE/ACIS International Conference on Computer and Information Science* (*ICIS* 2007). Piscataway: IEEE, 2007: 972-976.

[11] Li K, Zhong Z, Ramaswamy L. Privacy-aware collaborative spam filtering [J]. *IEEE Transactions on Parallel and Distributed Systems*. Piscataway: IEEE, 2009, **20**(5): 725- 739.

□