

# A countermeasure to email sender address spoofing

Toshiyuki Tanaka, Akihiro Sakai, Yoshiaki Hori, Kouichi Sakurai

Department of Information Science and Electrical Engineering,  
Kyushu University,  
744 Motooka, Nishi-ku, Fukuoka 819-0395, Japan,  
yuki@itslab.csce.kyushu-u.ac.jp,  
sakai@itslab.csce.kyushu-u.ac.jp, {hori, sakurai}@csce.kyushu-u.ac.jp

**Abstract.** Anyone can easily transmit an email that misrepresents the source address because the sender can freely decide information such as “From:” and “To:” fields in an email header part by using SMTP. Therefore, some email servers use the sender domain authentication technology. It cannot prevent source address spoofing of emails. However, it is used to prevent spam mails and the phishing. In this paper, we performed experiment of sender address spoofing by the free mail and TELNET, and evaluated SPF by using Gmail as a recipient server. Moreover, we paid attention to IP (Internet Protocol) address described in “Received:” of the header fields. We compared the sender domain name obtained by using Auto Whois with a domain name below @ in the mail address written in “Received:” and “From:”. We suggested that authentication succeed if they all agreed, and notify recipient if they not agree.

**Key words:** free mail, sender spoofing, IP address

## 1 Introduction

Recently, email is indispensable for life. Because the Web-based free mail offered by Yahoo! and Google, etc. can be acquired free of charge, and can be exchanged with other users anywhere in the world if you have an environment that can access to the Internet, it is being used by a lot of people. However, “sniffing”, “manipulation”, and “spoofing” by the third party become problems as email becomes an important infrastructure.

Recently, free mail by “spoofing” is used for the phishing to aim at these account takeovers on the portal site such as Yahoo! because various services are consolidated in one ID and password and being provided.

Therefore, the sender domain authentication technology is used to detect whether sender’s mail address is not pretend other domains. This is divided two. One is an electronic signature-based “DomainKeys” and other is the Internet Protocol (IP) address-based “SPF”. DomainKeys is used in Yahoo! and Gmail.

In our research, we used Gmail as a free mail because users of Gmail have been increasing in recent years. Also, we used Gmail as a recipient server and showed

that it is possible to pretend a sender mail address. Moreover, we verified whether receiving side can distinguish whether received mail address is pretending other mail address when we used the IP address-based authentication technology for Gmail.

## 2 Free mail

The free mail service is service that the mail account can be acquired free of charge if we input a necessary item (mail address and password, etc.) even if we do not join the Internet access service. Such a mail account is called a free mail.

A lot of companies that are offering the portal site are providing this service. Many of mail accounts of such mail use the Web mail. Because many of mail accounts of such mail use the Web mail, we can exchange email from anywhere if we have an environment that access to the Internet. However, anonymity and the danger of crime and mischief, etc. rise because we can easily acquire mail account even if the personal identification is not done.

The security of the free mail of the major company that provides the free mail service can put trust of some degree. But we need to take heed of its use because the fishing site exists to acquire ID and the password of the free mail illegally. Also, the following three risks exist in the free mail.

- **sniffing**

When we send the message with email, we send it with the sender address attached on the head of the message as address. By way of many computers, this message reaches the recipient.

To look at the message in email by the operator of the computer that passes on the way of this.

- **manipulation**

To change the content of the sniffed email and send a different message.

- **sender spoofing**

To send an email that pretended sender address by writing another mail address in sender address.

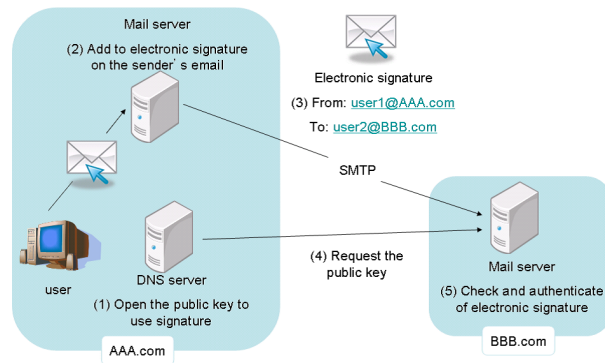
The free mail is used for the phishing in recent years and the damage has been increasing. The portal sites which provide the free mail are prevents spoofing by using the electronic signature-based and IP address-based authentication technology.

## 3 Related Work

### 3.1 DomainKeys

DomainKeys[1] is the electronic signature-based sender domain authentication technology, and it is used by the Yahoo! mail and the Gmail, etc. Because the

electronic signature is added to the header of email when mail is sent from the server corresponding to DomainKeys, we can judge on the receiving side whether email is sent from which server. Therefore, it is used to prevent the spam mail and the phishing that pretended sender address. Process of DomainKeys is shown in Fig.1.



**Fig. 1.** Process of DomainKeys

1. In AAA.com, The public key used to sign is opened with the DNS (Domain Name System) server in advance.
2. The mail server of AAA.com gives the electronic signature based on the text and the header of the sent mail.
3. Email is sent to BBB.com by SMTP.
4. The mail server of BBB.com refers to DNS server of domain part AAA.com of "From:" for the public key.
5. The electronic signature is checked by the public key acquired from AAA.com, and the authentication succeeds if the electronic signature corresponded.

### 3.2 SPF (Sender Policy Framework)

SPF[2] is the IP address-based sender domain authentication technology. It can detect whether sender's mail address is not pretend other domains. This is set on to the basis of assumption that the spoofing of IP address is difficult, and can complete the authentication only by acquiring information described on DNS server. Process of SPF is shown in Fig. 2.

1. The SMTP communication is begun from the mail server of AAA.com to the mail server of BBB.com.
2. The mail server of BBB.com refers to the SPF record for the DNS server of AAA.com based on the domain part of the mail address described in "From:".

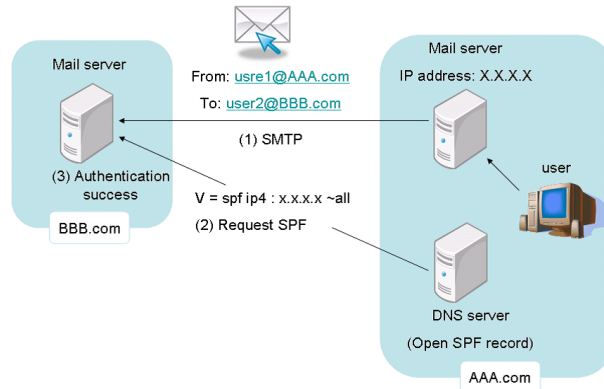


Fig. 2. Process of SPF

3. The authentication succeeds if the mail server of the sending side is included in the list of IP address shown on the SPF record of AAA.com.

## 4 Email sender address spoofing

### 4.1 Email sender address spoofing by the free mail

The following free mail have the function that change mail address in “From” field into another mail address.

- Gmail
- Yahoo! mail
- Windows Live Hotmail (Hotmail)
- @nifty WEBMAIL

In Gmail, we can send email by using another address instead of the Gmail address and easily manage two or more accounts from the Gmail interface by using “Addressor” originally set ourselves. The mail address and the password of the added account are needed to add the new address. If we use this function, it is possible to show like sending mail from the mail address except for the Gmail. Then, we investigate how it is displayed in the “From” field or another fields on the receiving side when we send email by actually using this function. We use “yuki@itslab.csce.kyushu-u.ac.jp” as sender email address. For example, the following Figure 3 ~ Figure 7 is information on the “From” field displayed on the receiving side.



Fig. 3. Gmail Yahoo! mail

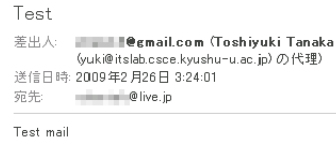


Fig. 4. Gmail Hotmail

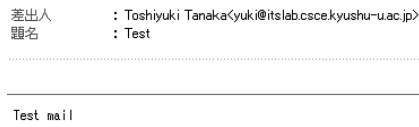


Fig. 5. Gmail @nifty WEBMAIL



Fig. 6. Yahoo! mail Gmail



Fig. 7. Hotmail Yahoo! mail

As a result, information on the “From” field displayed on the receiving side is shown in Table 1.

	<b>Gmail</b>	<b>Yahoo! mail</b>	<b>Hotmail</b>	<b>@nifty WEBMAIL</b>
<b>Gmail</b>	-	1	2	Nothing is displayed
<b>Yahoo! mail</b>	signed-by yahoo.co.jp	-	2	Nothing is displayed
<b>Hotmail</b>	mailed-by live.jp	Nothing is displayed	-	Nothing is displayed
<b>@nifty WEBMAIL</b>	signed-by nifmail.jp	1	2	-

**Table 1.** Information displayed on receiving side by each vender

1. This mail guarantee the sender domain by DomainKeys authentication
2. (supply yuki@itslab.csce.kyushu-u.ac.jp)

#### 4.2 Email sender address spoofing by TELNET

In our research, we consider email sender address spoofing. Here, we use Gmail as receiving side.

The protocol named SMTP (Simple Mail Transfer Protocol) is used for the transmission of mail. It is a protocol used to send email. SMTP client accesses to SMTP server and sends SMTP command. We examine doing actually when email is sent by using the command prompt.

1. HELO  
(Establishment of access, 250 (Requested mail action okay, completed) is returned)
2. MAIL  
(Specification of sender, 250 (Requested mail action okay, completed) is returned)
3. RCPT  
(Specification of recipient, 250(Requested mail action okay, completed) is returned)
4. DATA  
(Sending of text, 354 (Start mail input; The end of input sends the line only of ".") is returned)
5. QUIT  
(Processing termination, 221 (Service closing transmission channel) is returned)

In email sending ahead, we add the “From” column and the “To” column to the header. Then, the place that transmits sender mail address to SMTP server becomes two (the character string given following “MAIL FROM” that is SMTP command and the character string following the “From” field that exists in the header of email). Also, the place that transmits recipient mail address to SMTP server becomes two (the character string given following “RCPT TO” that is SMTP command and the character string following the “To” field that exists in the header of email). Here, recipient mail address is correct (exist) because we consider email sender address spoofing. Here, Gmail receives as Fig. 8 even if sender mail address is rewritten another mail address and it is transmitted.



Fig. 8. Receiving of email sender address spoofing

In receiving side of email, it is possible to impersonate by rewriting mail address written in the “From” field because the part where general user refers to sender’s mail address is only here. If this is used, spoofing is possible because these settings are freely actually decided in the sending side.

It is possible because sender’s mail address check in SMTP server look at whether domain name only exist, and it do not completely examine whether the account name of ahead of “@” exist or user who sent email is really an owner of the account.

### 4.3 Evaluation of SPF

Next, we explain how SPF is evaluated when email is actually received as an example of Gmail. There is an area where various information that was called a header fields was described in email besides the text.

First, when email is sent from the mail server that does not specify the SPF record at all, the following two lines are found in the header field.

```
Received-SPF: neutral (google.com: xxx.x.xx.xx is neither
permitted nor denied by best guess record for domain of
uso@uso.uso) client-ip=xxx.x.xx.xx;
Authentication-Results: mx.google.com;
spf=neutral (google.com: xxx.x.xx.xx is neither permitted nor
```

```
denied by best guess record for domain of ****@****.com)
smtp.mail=****@****.com
```

The part of “\*\*\*\*@\*\*\*\*.com” is sender’s mail address and as the result of the evaluation of SPF it is “neutral”. “?all” is defined in the end of the record like “v=spf1 ?all” for instance, and when it does not match to other conditions and it is match to “?all”, the SPF record of the sender domain becomes “neutral”. SPF should not immediately refuse the receiving of email even if the result is “neutral”.

On the other hand, when email is sent from the mail server that the SPF record is appropriately set, evaluation of SPF becomes the following two lines, and the result of it is “pass”.

```
Received-SPF: pass (google.com: domain of
****@yahoo.co.jp designates xxx.xx.xxx.xx as permitted sender)
client-ip=xxx.xx.xxx.xx;
```

```
Authentication-Results: mx.google.com; spf=pass (google.com:
domain of ****@yahoo.co.jp
designates xxx.xx.xxx.xx as permitted sender)
smtp.mail=****@yahoo.co.jp; domainkeys=pass (test mode)
header.From=****@yahoo.co.jp
```

This is the case that IP address in the sending side matches to the SPF record and succeeds in the authentication. Email is processed according to the evaluation of the sender domain because it is valid.

## 5 Proposal

Much information is described in the header field, and the header field is described in shape of “field name: field value”.

- **Return-Path**  
Mail address transmitted by SMTP communication as sender
- **Received**  
Mail transfer agent (IP address) where by way of by the time this mail reaches and date passed
- **Message-ID**  
Peculiar number added by each mail
- **In-Reply-To**  
List of value of Message-ID such as reply sender mail

- **From**  
Writer’s address
- **Sender**  
Sender’s mail address. When the same writer and sender, that is, “From” is a single address and same as Sender, this should not be used
- **To**  
Recipient mail address
- **Reply-To**  
Mail address for which sender hopes a reply
- **Subject**  
Short sentence that shows topic
- **manipulation**  
Date that sender transmitted
- **MIME-Version**  
Version of MIME
- **X-Priority**  
Importance that sender specified
- **X-Mailer**  
Type of email client
- **X-IP**  
Sender’s global IP address
- **X-FROM-DOMAIN**  
Sender’s domain

When MTA (Mail Transfer Agent) forwards email, the content of the work is recorded in “Received:.”. “Received” is added whenever the server’s passing. “Received:” with the header field most below passed first is a server near the sender and “Received:” with the header field most up passed at the end is a server near the recipient. In addition, information of “Received: from X by Y” means “Mail was sent from the server of X to the server of Y”. For example, it means the transmission from the server Web4007.mail.ogk.yahoo.co.jp to the server Mx.google.com when recorded as follows.

```
Received: by xx.xxx.xx.x with SMTP id ...  
Received: by xx.xxx.x.x with SMTP ...
```

•  
•  
•

```
Received: from web4007.mail.ogk.yahoo.co.jp
(web4007.mail.ogk.yahoo.co.jp [xxx.xx.xxx.xx])
by mx.google.com with SMTP id ...
```

Here, the server name written in “MAIL FROM” is displayed in X. But this is possible to misrepresent. However, because SMTP server automatically acquires other party’s IP address as data while communicating SMTP, the IP address written its next cannot be misrepresented. Sender host’s information can be obtained by watching here.

Then, we propose the check technique of the “Received:” field shown in Fig.9. There is a research[3] to distinguish the spam mail as a technique for evaluating the message of email by checking the “Received:” field on such a user side.

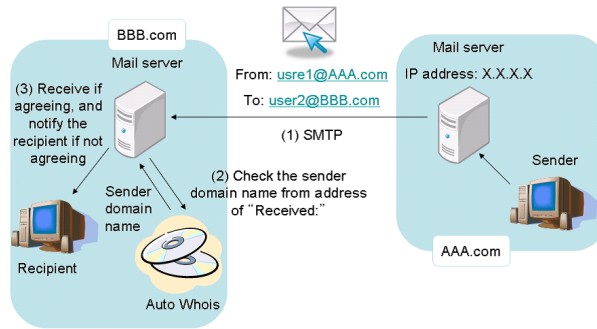


Fig. 9. Sender domain authentication that uses Auto Whois

1. SMTP begins from the mail server of AAA.com to the mail server of BBB.com
2. The mail server of BBB.com obtains a sender domain name by using Auto Whois from IP address described “Received” of the most below header field
3. A sender domain name obtained by using Auto Whois, domain name below @ in the mail address written in “Received:”, and “From:” is compared. The authentication succeeds if they all agree, and recipient is notified if they don’t agree.

Auto Whois is a program that acquires DNS information and Whois information from the domain name and IP address and displays it. The management origin of a sender server is understood by using and examining Auto Whois.

## 6 Conclusion

In this research, we used TELNET to explain simply the procedure of email sender address spoofing, but if the setting of the email software such as OE is changed and own mail address is rewritten in other one, “spoofing” mail that pretended the sender can be transmitted. This is because there are no functions that certify the other party who transmitted correctly in SMTP. Therefore, the spoofing is prevented by using the sender domain authentication technology such as DomainKeys or SPF. Gmail used by the experiment did the authentication that used SPF in addition to DomainKeys. However, this information can’t be watched as long as the receiving side does not watch the header field for me. Moreover, when only the account part is pretended in the same domain, SPF can not detect. Therefore, recipient is not necessarily able to distinguish whether received mail address is misrepresented.

As future assignments, we examine how authentication technology is used in free mails other than Gmail, compare and evaluate them.

## References

- [1] M. Delany, “Domain-based email authentication using public-keys advertised in the DNS (DomainKeys),” RFC4870, IETF, May 2007. <http://tools.ietf.org/html/rfc4870>
- [2] Mark Lentczner and Meng Weng Wong, “Sender Policy Framework (SPF) a Convention to Describe Hosts Authorized to Send SMTP Traffic,” May 2004. <http://tools.ietf.org/html/draft-mengwong-spf-01>
- [3] Yukiko Sawaya, Yutaka Miyake, “An Examination of Spam Mail Filtering with k-NN Analysis Based on Mail Header Information”, The 2008 Symposium on Cryptography and Information Security (SCIS 2008), 3C2-1, 6pages, January 2008.