An E-Mail Signature Protocol for Anti-Spam Work-in-Progress

Kai-Jie Chang
Department of Computer Science and Information Engineering
National Chung Cheng University
168 University Rd., Min-Hsiung
Chia-Yi 621, Taiwan, R.O.C.
886-4-24517250-3790, incl. country code
ckch94@cs.ccu.edu.tw

Chin-Chen Chang
Department of Information Engineering and Computer Science
Feng Chia University
100 Wenhwa Rd., Seatwen,
Taichung 40724, Taiwan, R.O.C
886-4-24517250-3790, incl. country code
ccc@cs.ccu.edu.tw

ABSTRACT
Communication via E-mail is one of the most convenient ways to replace the traditional mailing system. However, spam appears and has become a serious problem. Most computation is on the spam e-mails, which becomes heavy burden of a mail server. In this paper, we proposed an e-mail authentication protocol to solve the problems of spam and phishing attacks by verifying if the e-mails come from the reliable source.

Keywords
E-mail, authentication, signature, spam, phish

1. INTRODUCTION
With the popularity of using electronic-mail (e-mail), more and more spams appear in different networks, including the Internet and mobile networks. In 2004, the e-mail security vendor MX Logic found that 60 to 93 percent e-mails were spams[2,3]. This means that 60 to 93 percent of the resource of an e-mail system is wasted, and sometimes it is even higher. This spam problem also leads to some attacks on e-mail systems. One famous attack is called the phishing attack [1, 4, and 5]. In this attack, phishers (attacker) forge a bank or a credit card company website. Then, they send the link of the forged website to e-mail users. Users do not know the fact and enter the account number, password as well as confidential information. An attacker can use that sensitive information to conduct other attacks.

The most popular approach to identify and reject a spam is adopting an e-mail filter. An e-mail filter examines an e-mail by checking the e-mail title or content to see whether there has some specific keywords. However, these anti-spam approaches require mass user experiments of spam to analyze the e-mail. And there is high possibility of mistaken alarm which regards a regular e-mail as spam. Moreover, the efficiency of spam filter is low mentioning the digit signature and public key cryptosystem.

An attacker may be classified into spam because of using the same e-mail address. Thus, the attacker has to change the sender's e-mail address often to avoid the detection of an anti-spam system. Therefore, sender address becomes a key point to classify a spam. An e-mail comes from a reliable source become a very important issue. Thus, we proposed a method to improve the SMTP and achieve the e-mail authentication.

The rest of this paper is organized as follows. We review some preliminaries in Section 2. Our proposed protocol is described in Section 3. Then, the security analysis and performance are discussed in Section 4. Finally, the conclusions are given in Section 5.

2. PRELIMINARIES
Domain Name System (DNS)

The DNS stores associates many types of information with domain names. The most important job is to translate the domain name to IP address.

Mail User Agent (MUA)

An E-mail client is also called MUA. The main functionality of MUA is to help the user send and read e-mails. The most famous examples are Outlook and Thunderbird.

Mail Delivery Agent (MDA)

The MDA is a software which is used to receive e-mails from the Internet and then distribute those e-mails to the mailbox according to the recipient's will.

Mail Transfer Agent (MTA)

The main function of MTA is to transfer received e-mails to another MTA. If the MTA receives an e-mail, it will query the Mail eXchanger (MX) and transfer the mail to the destination MTA.

3. PROPOSED METHOD
In our protocol, the sender generates the authentication message accompanied with the e-mail. And the recipient mail server queries the sender's mail server. Then, it sends the authenticated message back to sender's mail server for verification. The notations are listed in Table 1.

Notation	Description
H()	A secure one way hash function
T	A timestamp
PW	Sender's password
SID	Sender's e-mail address
RID	Receiver's e-mail address
MTitle	E-mail subject title

3.1 REGISTRATION PHASE

In this phase, every user registers his/her e-mail address and password in the mail server. The user sends the identity and the password to the mail server via a secure channel. The mail server will create an e-mail account in the mail server and keep the hashed password in the password table. Generally, this phase has already ended in the mail server. The mail system did not change anything in this phase.

3.2 E-MAIL AUTHENTICATION PHASE

In this phase, the sender generates an e-mail authentication message to the receiver's mail server. Then, the mail server will check whether the e-mail comes from a reliable source. The detailed protocol is described as follows.

Step1. The e-mail sender generates the authentication message $H(SID|RID|H(PW) | MTitle | T|H(Mail\ Content))$ accompanied with the e-mail to the receiver's MDA.

Step 2. Receiver's MDA queries the sender MTA's IP address.

Step 3. The DNS checks if the sender MTA exists or not, and returns the result to the receiver MDA.

Step 4. If there is no such MTA, MDA deletes this e-mail; otherwise, the MDA sends the *SID,RID,MTitle,T and H(Mail Content)* back to the MTA.

Step 5. The MTA generates the authentication message and sends it back to MDA. MDA classifies this e-mail according to the returned messages correctness.

Step 6. The receiver gets the authenticated e-mail

4. DISCUSSIONS

In this phase, every user registers his/her e-mail address and password in the mail server. The user sends the identity and the password to the mail server via a secure channel. The mail server will create an e-mail account in the mail server and keep the hashed password in the password table. Generally, this phase has already ended in the mail server. The mail system did not change anything in this phase.

4.1 SPAM

Assume that an attacker wants to send a spam to the users, trying not to let anyone else know the sender's address to avoid being listed in the black list. However, each mail must contain an authentication message $H(SID|RID|H(PW) | MTitle | T|Mail\ Content)$. The mail server checks the sender's domain and verifies whether the mail server is correct. Then, the message will be sent back to this mail server for authentication. Hence, the attacker cannot pass the verification.

4.2 PHISHING ATTACK

Because only the sender himself can sign the authentication message with the e-mail, the attacker cannot impersonate the illegal user to send the e-mail. And the authentication message cannot be reused since the authentication message contains the e-mail title and a timestamp. Therefore, phishing attack cannot succeed in our protocol.

4.3 FORGERY ATTACK

An attacker may generate an authentication message to impersonate a legal user or forgery an e-mail. However, the e-mail contains the sender's mail address. The system will check the DNS to find out the sender's e-mail. If the sender's domain is not true, this e-mail will be deleted. Otherwise, the MDA will send the authentication message back to the mail server to check the validity of this authentication message. Because the authentication message contains the *SID* and the hashed password *H(PW)*, the mail server will check if the user is valid or not. Thus, we can make sure that it is impossible for the attacker to forge an authentication message. This forgery attack is not practical in our protocol.

4.4 REPLAY ATTACK

Assume that an attacker wants to resend the e-mail or send it to another receiver with the same title. Since the authentication message includes the timestamp T and receiver's mail address *RID*, the replay message cannot pass the verification of sender's mail server. And therefore, it is impossible for the attacker to send the mail to other users the same authentication message. Even though the attacker can pass the verification successfully and send it to the same receiver, it is meaningless to receive the same e-mail. And because the authentication message also contains the mail content, the attacker also cannot change the content and pass the verification.

5. CONCLUSIONS

Spam becomes a serious problem of communication on the Internet. However, many spam mail filters can solve the problem efficiently. In this paper, we proposed an efficient e-mail authentication protocol to make sure that each e-mail comes from a reliable source, which can let the mail server block the spam and phishing attacker easily. Therefore, the mail server can provide a secure communication environment for Internet users, not only protect e-mails but also against possible attacks.

6. REFERENCES

[1] Goth, G., "Phishing attacks rising, but dollar losses down," *IEEE Security & Privacy Magazine* , Vol. 3, Issue. 1, pp. 8, 2005.

[2] Hoanca. B, "How good are our weapons in the spam wars?," *IEEE Technology and Society Magazine* , Vol. 25, Issue 1, pp. 22-30, 2006.

[3] Ivey. K.C., "Spam: the plague of junk E-mail," *IEEE Computer Applications in Power* , Vol. 11, Issue 2, pp. 15-16, 1998.

[4] Lawton, G, "E-mail authentication is here, but has it arrived yet?," *Computer* , Vol. 38, Issue. 11, pp. 17-19, 2005.

[5] Ross P.E., "Microsoft to spammers: go phish [e-mail security] ," *IEEE Spectrum* , Vol. 43, Issue 1, pp. 48-49, 2006.