Cryptography Methods for Preventing Phishing Attack

Imam Habibi

Informatics Engineering Department
Bandung Institute of Technology
Ganesha 10 Street Bandung 40132

E-mail : if12042@students.if.itb.ac.id, imam_beckham@yahoo.com

Abstraction

In the electronic business activity, the aspect of e-commerce security has become an important consideration because some attacks, such as phishing, happen frequently. The techniques which are applicable to ensure the security of Internet connection, especially to prevent phishing attack will be explained at this paper. Those techniques are strong website authentication, mail server authentication, and mail authentication via digital signature. Moreover, the advantage and disadvantage for each technique will be analyzed.

Keywords*: authentication, phishing, digital signature.*

1. Introduction

Information technology is growing rapidly nowadays. Its role becomes more and more important. A lot of people have enjoyed it through electronic transaction (e-commerce). The usage of world wide connection such as Internet, goods and services are widely promoted in global scale. The consumer can also get access to buy the products with credit card.

On the other hand, this growth also has a negative impact in the case of security. Bad practices in network happen frequently, such as carding. Because of this crime, security aspect in using of computer network has become a crucial matter.

Therefore, cryptography offers an alternative solution to overcome those problems. Cryptography is categorized as a science and an art which have a purpose to protect the message secrecy and security. The secrecy refers to message encryption, while the security refers to message delivery from sender to receiver.

In the case of message delivery, there are 3 aspects to be considered: user authentication, message authentication, and undeniable content of sender.

Hence, there are some techniques which are used to prevent phishing attack:

1. strong website authentication
2. mail server authentication
3. mail authentication via digital signature

2. Phishing

According to definition in [1], phishing, short for password harvesting fishing, is the luring of sensitive information, such as password and other personal information, from a victim by masquerading as someone trustworthy with a real need for such information.

Cyber criminals do phishing attack with the following ways:

1. They hijack users and send them to fraudulent websites of trusted brands such as well-known banks, online retailers, and credit card companies.
2. Phishing attacks use 'spoofed' e-mails to lure recipients into browse fraudulent websites. This technique usually exploits the email header using SMTP (simple mail transfer protocol).
3. The fraudulent websites are designed to fool recipients into divulging personal financial data. For the example credit card numbers, account usernames and passwords, and social security numbers.

Most of victims give positive response to the phishing attack with spoofing e-mail. As the result, a lot of consumers suffer various losses in the form of illegal credit card usage and stolen identity.

Here are the phishing statistics around the world [2]:

1. United States 35.0%
2. South Korea 16.0%
3. RRC 15.0%
4. Russia 7.0%
5. England 5.5%
6. Mexico 4.5%
7. Taiwan 2.5%

3. Technique Criteria for Preventing Phishing

Techniques which are used to prevent phishing attack have to fulfill these criteria [3]:

1. Minimize end-user training
2. Use of existing standards-based technologies
3. Unilateral deployment must add value
4. Must be cost-effective for both senders, recipients, and Internet infrastructure providers
5. Must be able to authenticate the sender of email

4. Strong Website Authentication

This technique uses a mechanism to strongly authenticate any users visiting a business web site using two-factor authentication. First factor is a request of username and password while the other is a challenging process from server side to client side via smart card. This technology tries to limit end-user training as much as possible [2].

The positive aspects of this technique are:

1. Phisher can not log into real site without the right physical token such as smart card, even if a user falls for a phishing attack
2. Users are given a stronger sense of trust in their transaction with business web site

The downsides of this technique are:

1. Set up time delays
2. Desktop software installation
3. High management costs
4. Potentially high cost per user
5. User needs to bring a smart card when doing a transaction

5. Mail Server Authentication

This technique uses enhanced DNS (domain name system) capabilities to verify the IP (internet protocol) address of sender's email server [2] [3].

The advantages of this technique are:

1. Easy to configure at senders mail servers
2. Makes it harder for phishers to be anonymous
3. Legitimate business email can be better identified in order to prevent any spamming attack

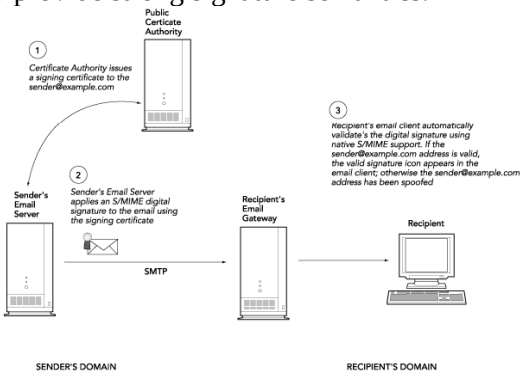
The disadvantages of this technique are:

1. Sender and recipient gateways are required to use these methods
2. SMTP sender is not visible to recipient ("From:" address still can be spoofed)
3. There will be a problem for anyone using 3rd party emailing services
4. It does not accommodate email forwarding

6. Mail Server Authentication via Digital Signature

This technique uses existing industry standard S/MIME digital signatures to sign outbound mail to provide signature verification at the gateway or email client [2] [3].

S/MIME is an asymmetric cryptography technique which is used to authenticate sender and provide strong signature semantics.



The followings are the stages to authenticate e-mail using S/MIME digital signature:

1. Authority in the trusted public certificate, such as VeriSign, Thawte, GlobalSign, publishes digital signature for each e-mail addresses.
2. Each sent e-mails will be inserted a digital signature with private key. This digital signature provides a way to prove the authentication of "From:" address.
3. The recipient will be equipped with S/MIME protocol whose function is to verify the digital signature. If it is valid then "From:" address is expressed as a valid as well. Therefore, the recipient can trust the email content.

The positive aspects of this technique are:

1. It would work without any additional software
2. "From:" address is impossible to spoof without detection
3. Phishers must register with a certificate authority to send phishing emails. It makes a stronger identity audit trail to prosecute phishers
4. Legitimate business email can better identified by end user

The downsides of this technique are:

1. Recipients still have to inspect the "From:" address for misleading domains
2. Not all email clients supports S/MIME
3. Recipients may not check certificate revocation status

4. Sender and recipient getaways must both understand S/MIME digital signatures if using gateway server to verify signatures

7. Conclusion

There is no methods that can perfectly overcome the phishing attack until this time. The strong website authentication technique provides high level authentication, but it is not easy to be used by end user. The mail server authentication technique can verify a sender domain, but it does not authenticate "From:" address. Moreover, it also cannot accommodate e-mail forwarding. The last technique, mail authentication via digital signature, accommodates a way to authenticate email address and prevent phishing and spamming attacks. However, based on the cost, it is not an effective one. Overall, for common users, it is recommended to use mail server authentication because it is the easiest among the others.

8. Reference

[1] http://en.wikipedia.org/wiki/Phishing, January 4th, 2006
[2] http://www.antiphishing.org/, January 6th, 2006
[3] http://www.itpapers.com/whitepaper.aspx?scname=Digital+Signatures&docid=130185, December 31st, 2005