

Analysis of Perusal Confirmation of Sharp Mail

Hankyu Joo

Hallym University
hkjoo@hallym.ac.kr

Abstract

Sharp Mail was developed as a substitute for existing email systems and possesses several novel features. One such feature is the ability to generate a circulation confirmation document, which is to provide legal evidence of sent and received email. The crucial aspect of this document is perusal confirmation. Perusal confirmation certifies that the intended receiver of the message has read it. In this study, perusal confirmation is analyzed to determine whether it always contains correct information. This paper shows that perusal confirmation is not guaranteed always to contain correct information.

Keywords: *safety analysis, electronic mail system, Sharp Mail, non-repudiation*

1. Introduction

Electronic mail systems have been used widely for many years. National IT Industry Promotion Agency (NIPA) of Korea has developed a new electronic mail system protocol known as Sharp Mail as a substitute for the existing email systems [1]. The Korean Ministry of Science, ICT, and Future Planning requires now using Sharp Mail in many areas.

Sharp Mail was developed to provide several features such as swiftness, convenience, transmitter and receiver authentication, transmission, receipt and perusal confirmation, and to issue a circulation confirmation document. Transmission, receipt, and perusal confirmation are provided in the circulation confirmation document. A circulation confirmation document provides legal evidence of transmitted, received, and read email that is, the email is regarded as true until counterevidence is presented [3].

This study analyzes perusal confirmation to determine whether a circulation confirmation document containing perusal confirmation can be used as legal evidence. A perusal confirmation certifies that the receiver of the message has read the message. Perusal confirmation is designed to provide non-repudiation that is the receiver cannot deny that he has read the message. For a circulation confirmation document to be used as legal evidence a perusal confirmation should always contain correct information – perusal confirmation should be generated for each read message and should not be generated for any message that has not been read. The findings of this study show that perusal confirmation is not always guaranteed to contain correct information.

2. Sharp Mail System and Perusal Confirmation

Sharp Mail is a new electronic mail system protocol and is described in [1]. Sharp Mail system has been developed and implemented [2].

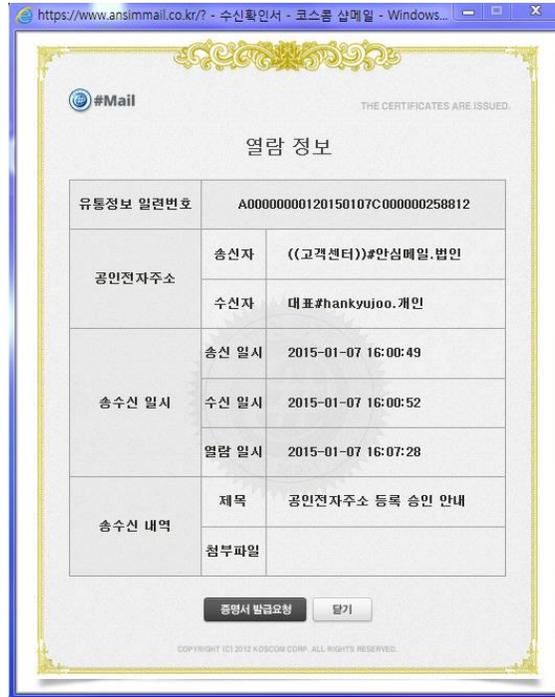


Figure 1. Perusal Confirmation (Original Korean Version)

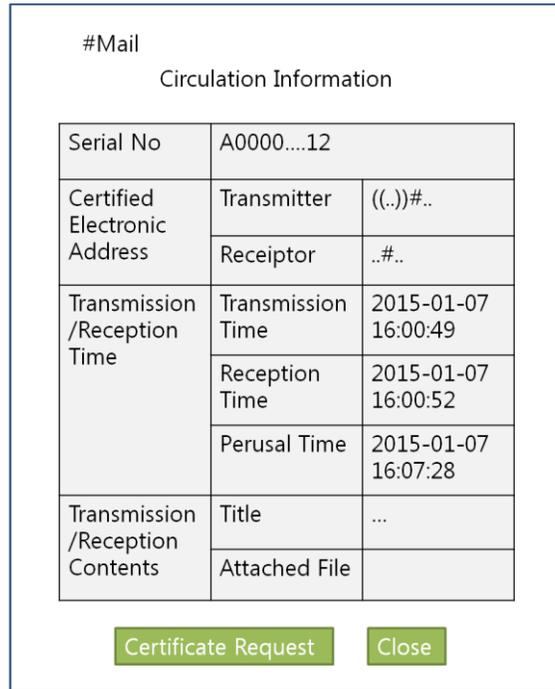


Figure 2. Perusal Confirmation (Translated)

Sharp Mail is supposed to provide features such as swiftness, convenience, transmitter and receiver authentication, transmission, receipt, and perusal confirmation, and to issue a circulation confirmation document. Perusal confirmation is crucial

feature of the Sharp Mail system. Perusal confirmation certifies that the intended receiver has read the message. Perusal confirmation information is also included in the circulation confirmation document. Generating perusal confirmation is described in [1, 4, 5]. Figure 1 and Figure 2 show the actual perusal confirmation of the Sharp Mail system [2].

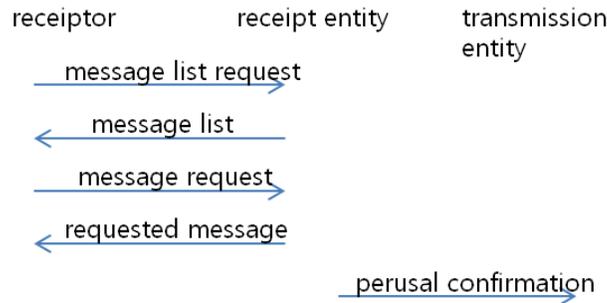


Figure 3. Normal Perusal Confirmation Generation Protocol (Perusal Confirmation is Generated Immediately After the Requested Message is Transmitted)

The major entities involved in generating perusal confirmation are transmission entity, receipt entity, a receipt client, receptor (receiver is called receptor in [1, 4, 5]), and circulation certification server. The transmission entity is similar to the mail server of the message transmitter. The receipt entity is similar to the mail server of the message recipient. The receipt client is similar to the mail client (such as Outlook or webmail client) of the message recipient. The receptor is the user who is the message recipient. In this study, because the receipt client is entirely under the control of the receptor, the receipt client is not distinguished from the receptor. The circulation certification server retains perusal confirmation and generates a circulation confirmation document, which contains the perusal information, whenever requested. Perusal confirmation is generated by the receipt entity.

Figure 3 and Figure 4 show the message receipt and perusal confirmation generation process. When the receipt entity receives a message from the transmission entity, the message is saved in the post-box of the receptor. The receptor requests a message list after user authentication. The receipt entity transmits the message list from the receptor post-box to the receptor. When the receptor requests a specific message to peruse, the receipt entity transmits the requested message to the receptor. The receptor transmits an acknowledgement to the receipt entity after he peruses the requested message. The receipt entity generates perusal confirmation immediately after the message is transmitted as Figure 3 indicates, or upon receipt of the receptor's acknowledgement, as indicated in Figure 4. The receipt entity then transmits the generated perusal confirmation to the transmission entity. The transmission entity verifies the perusal confirmation and request storing the perusal confirmation to the circulation certification server. The circulation certification server generates circulation confirmation document, which contains the perusal information, whenever it is requested.

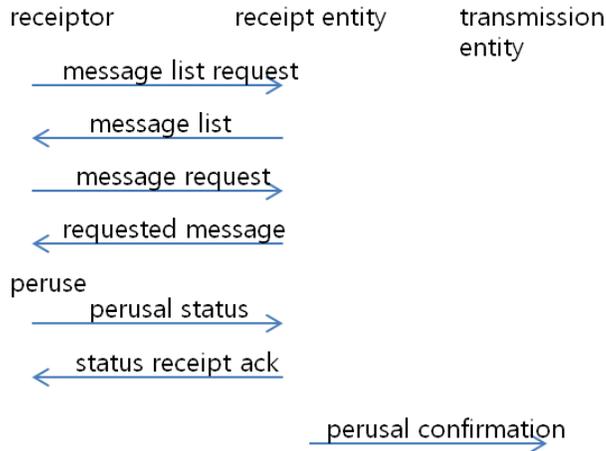


Figure 4. Normal Perusal Confirmation Generation Protocol (Perusal Confirmation is Generated after a Perusal Status Message from the Receptor is Obtained)

Perusal confirmation should always contain correct information in order to provide non-repudiation when necessary. Whenever the receptor reads a message, the perusal confirmation should be generated. If the receptor has not read the message, the perusal confirmation should not be generated.

3. Analysis of Perusal Confirmation

Figure 5 and Figure 6 show the possible problems caused during the generation of a perusal confirmation.

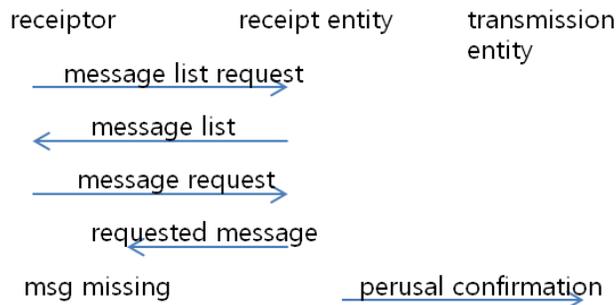


Figure 5. Abnormal Perusal Confirmation Generation Protocol (In Case Perusal Confirmation is Generated Immediately after the Requested Message has been Transmitted)

If a perusal confirmation is generated immediately after the requested message is transmitted, the perusal confirmation may still be generated in case the receptor has not perused the message as illustrated in Figure 5. The message may not be read by the receptor because of the network problem or receipt client problem. Non-repudiation cannot be achieved and the perusal confirmation may be generated for messages that have not been read.

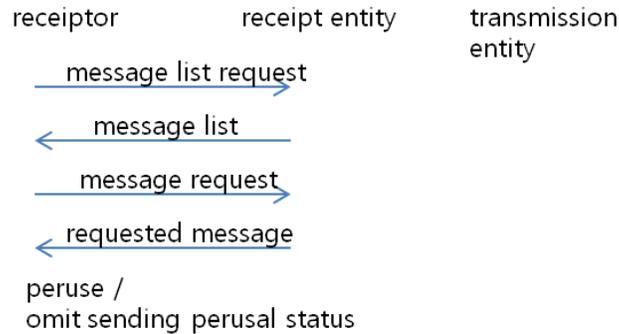


Figure 6. Abnormal Perusal Confirmation Generation Protocol (In Case Perusal Confirmation is Generated after Perusal Status Message from the Receptor has been Obtained)

If the perusal confirmation is generated upon the receipt of the acknowledgement from the receptor, the perusal confirmation may still not be generated although the receptor has read the message as illustrated in Figure 6. The receptor may omit sending the acknowledgement after he or she reads the message. If the acknowledgement has not been received, the receipt entity cannot generate a perusal confirmation. The receptor may read the message without a perusal confirmation having been generated.

The perusal confirmation is not guaranteed to contain correct information. It may be generated for messages that have not been read by a receptor or may not be generated for messages that have been read by a receptor. Because perusal confirmation may contain incorrect information, a Sharp Mail circulation confirmation document may have incorrect information, as well.

4. Conclusion

Sharp Mail is an electronic mail system that possesses several notable features. One such feature is generating circulation confirmation document which is designed to give legal evidence. The crucial aspect of a circulation confirmation document is perusal confirmation, which certifies that the intended receiver of a message has read it. A perusal confirmation is to be generated whenever the receiver has read the message. The perusal confirmation is not to be generated if the receiver has not read the message.

However, this study's findings show that the perusal confirmation may be generated for messages that have not been read by a receiver or the perusal confirmation may not be generated for messages that have been read by a receiver. Because perusal confirmation may contain incorrect information, a Sharp Mail circulation confirmation document may contain incorrect information, as well. Therefore, such a circulation confirmation document of Sharp Mail will be unable to provide legal evidence.

References

- [1] NIPA, "Trustworthy e-Document Circulation Framework Specification", NIPA-TS-CCD-OVERVIEW vol. 2.4, (2013) July.
- [2] "Koscom: Ansim Mail", <https://www.ansimmail.co.kr/kpost/index.html>.
- [3] Ministry of Law, "Framework Act on Electronic Documents and Transactions", Act no. 11461, (2012) June.
- [4] NIPA, "e-Document Circulation Confirmation Technical Specification", NIPA-TS-CCD-CONFIRMATION vol. 2.4, (2013) July.

- [5] NIPA, "e-Document Circulation Client Technical Specification", NIPA-TS-CCD-CLIENT, vol. 2.0, (2013) July 2013.

Author



Hankyu Joo received his B.Sc. degree in Computer Science from Hallym University, Korea, in 1988. He received his M.S. and Ph.D. degrees in Computer Science and Engineering from Arizona State University in 1994 and 1998, respectively. He worked for the Electronics and Telecommunications Research Institute, Korea, from 1999 to 2000. He is a professor of Computer Engineering at Hallym University. His research interest includes information security and software engineering.