배달 및 내용증명이 가능한 전자 문서의 교환

황보성°, 이임영
순천향대학교 공과대학 정보기술공학부
e-mail : hbs@sec-cse.sch.ac.kr

Exchange of Electronic Document with Certification of Delivery and Contents

Bo-Sung Hwang°, Im-Yeong Lee
Division of Information Technology Engineering, College of Engineering, Soonchunhyang University

요 약

인터넷 환경의 발달에 의해 네트워크상의 콘텐츠의 전송이 활발해 지고 있다. 그 대표적인 예가 대중적으로 일반화되어 있는 전자메일일 것이다. 하지만 전자메일이 보다 일반화되고 보안상의 위협을 제거하기 위해선 전송되는 메일에 대한 내용증명과 배달증명이 가능해야 한다. 따라서, 본 논문에서는 먼저 내용증명과 배달증명이 가능한 기존의 방법들을 분석하고, 양사용자사이에 문서를 교환할 수 있는 새로운 방법을 제안한다.

1. 서론

인터넷의 발달과 더불어 전자문서의 교환은 이제 일상적인 모습이 되었다. 특히, 전자메일은 기업이나 개인의 사회 활동 가운데에서 중요한 역할을 차지하는 통신 수단이 되었다. 하지만, 인터넷상의 전자문서의 교환은 수신자에게 배달이 되었는지, 그 시간은 언제인지, 내용이 어떠한지 등에 대한 증명이 확실치 않아 분쟁 발생시 위와 같은 것들을 증명하는데 어려움이 따르게 된다. 따라서, 기존의 우편 제도에서 제공되고 있는 배달 및 내용 증명 서비스를 적용함으로써 사용자들에게 보다 안전한 전자문서의 교환을 제공할 수 있고, 분쟁 발생시 발급된 배달증명과 내용 증명을 통해 분쟁을 해결할 수 있을 것이다. 배달증명과 내용증명의 사전적 의미는 다음과 같다.[1]

- 배달증명

  수취인에게 우편물을 배달 또는 교부한 경우 그 사실을 배달 우체국에서 증명하여 발송인에게 통지해주는 제도로써 등기로 취급하는 우편물에 한하여 이용 가능하며, 발송시 발신자가 배달 증명을 청구하거나 필요시 사후에도 청구 가능하다. 배달 우체국은 수령증을 발신자에게 교부한다.

- 내용증명

  방송인이 수취인에게 어떤 내용의 문서를 언제 발송하였다는 사실을 우편관서가 공적으로 증명하는 제도로써 우편물의 문서 내용을 후일의 증거로 남길 필요가 있을 경우 이용되는 제도로 우체국의 보관용, 수취인에게 보내는 원본 그리고 발송인 보관용을 상호간에 우체국의 도장으로 표시를 하며, 수취인이 수취를 거부할 경우가 있으므로 내용 증명이라는 표시를 우편물에는 하지 않는다. 배달 증명과 동일하게 발신자는 우체국으로부터 수령증을 수령한다.

본 논문의 2장에서는 기존에 소개된 방식들을 분석하고 3장에서는 새로운 방법을 제안한다. 마지막으로 4장에서는 결론을 맺도록 한다.

2. 기존 방식의 고찰

본 장에서는 [1]에 소개된 TUA(Tanaka, Uchida and Akiyama)방식과 Nakao방식을 소개한다.

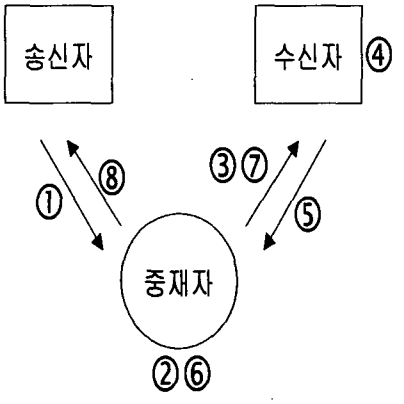
2.1 TUA 방식[2]

본 방식에서 송신자는 수신자의 공개키로 암호화된 메시지를 중재자에게 제공하고 중재자는 이를 수신자에게 제공하고 수신자는 자신이 암호문을 받았다는 증거를 중재자에게 제출 후 복호화할 수 있는 키를 중재자로부터 얻을 수 있다.

(1) 시스템 파라메터
- K : 세션키
- M : 송신자로부터 수신자에게 전송되는 메세지

- s, P_s : 송신자의 비밀키와 공개키
- r, P_r : 수신자의 비밀키와 공개키
- a, P_a : 중재자의 비밀키와 공개키
- $E_x(M)$: 키 x를 이용해 메시지 M을 암호화
- S_x : x의 서명

(2) 프로토콜



[그림 1] TUA 방식

① 송신자는 중재자에게 C1 = $S_s[E_{Pr}(M)]$을 계산해 전송한다. M은 수신자의 공개키로 암호화되었기 때문에 중재자도 그 내용을 알 수 없다.

②③ 중재자는 송신자의 서명을 확인하고 세션키 K를 생성한다. 생성된 세션키 K를 이용해 C1을 암호화하여 이것을 수신자에게 전송한다.

$$C2 = E_K[C1]$$

④⑤ 수신자는 C2를 받더라도 K를 알지 못함으로 C1을 알 수 없다. 수신자는 세션키 K를 중재자로부터 얻기 위해 C2 대한 서명문 C3(S_r[C2])을 중재자에게 제공한다. 중재자는 수신자로부터 서명되어있는 C3를 제공받음으로 해서 수신자가 메시지를 받았다는 배달 증명을 할 수 있다.

⑥ 중재자는 C3의 서명을 확인하고 ③에서 전송한 C2와 일치하는지 확인한다.

⑦ ⑥의 과정이 옳다면, 중재자는 수신자에게 세션키 K를 전송한다. 수신자는 K와 자신의 비밀키를 통해 메시지 M을 획득한다.

⑧ 중재자는 송신자에게 세션키 K와 C3를 제공함으로써 배달 증명이 가능하다.

2.2 Nakao 방식[3]

이 방식은 내용증명을 위해 일련번호와 해쉬함수를 이용하고 있으며, 배달증명은 중재자가 직접 송신자에게 통보한다.

(1) 시스템 파라메터
- n : 문서에 대한 일련번호
- H : 해쉬함수

다른 파라메터는 2.1에 설명되어있는 것과 같다.

(2) 프로토콜

① 송신자는 전송할 메시지에 서명해(C=S_s[M]) 중재자에게 전송한다.

② 중재자는 서명과 메시지를 확인한다. 그리고, 메시지에 대한 일련번호 n과 H(C)를 생성해 보관한다. n과 H(C)는 후에 내용증명에 이용된다.

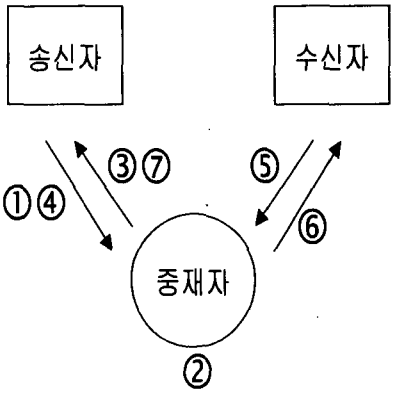
③ 중재자는 n과 S_a[n]을 송신자에게 전송한다.

④ 송신자는 n의 서명을 확인하고 다음을 중재자에게 전송한다.

$$n, S_a[n], S_s[M]$$

⑤⑥ 중재자는 메시지의 전송을 수신자에게 알리면 수신자는 자신의 패스워드를 통해 중재자에 접속 후 M을 수신한다.

⑦ 수신자가 M을 수신 후 중재자는 송신자에게 배달 증명을 통지한다.



[그림 2] Nakao 방식

만약, 송신자가 중재자에게 내용증명을 요구할 때 중재자에게 n, S_a[n], S_s[M]을 제공한다. 중재자는 다음을 확인해 옳다면 내용증명을 통지한다.

$$n = S_a[n], C = H[S_s[M]]$$

3. 제안 방식

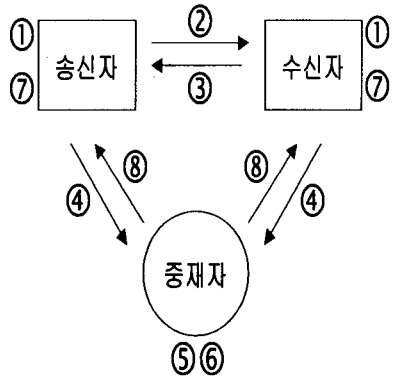
기존의 방식들은 송신자가 수신자에게 메시지를 보내는 경우에 한해서만 배달 및 내용증명이 가능한 프로토콜을 제안하였다. Off-line상의 모든 행위가 On-line상으로 이동함에 따라 송수신자 양방향으로 문서를 교환하는 프로토콜이 필요하고, 교환되어 지는 문서에 대한 배달 및 내용 증명 또한 필요할 것이다. 따라서 본 제안 방식에서는 송수신자들 사이에 문서를 교환하고 그에 대한 내용 및 배달 증명이 가능한 프로토콜을 제안한다.

(1) 시스템 파라메터

- K_s, K_r : 송신자와 수신자에 의해 생성된 세션키
- M_1, M_2 : 송신자와 수신자사이에 교환되어지는 문서들
- t : 타임스템프
- DES_s, DES_r : 교환되는 메시지에 대한 요약

다른 파라메터는 2.1에 설명되어있는 것과 같다.

(2) 프로토콜



[그림 3] 제안 방식

① 송수신자는 자신의 메시지를 교환하기 위해 세션키 K_r과 K_s을 생성한다.

② 송신자는 C1을 다음과 같이 생성해 수신자에게 제공한다. 메시지 M_1은 송신자가 생성한 세션키 K_s에 의해 암호화되어 있다.

$$C1 = S_s[A, R, t, E_{Ks}[M_1], DES_s]$$

③ 수신자는 문서에 대한 요약(DES_s)를 확인하고 C2을 생성해 송신자에게 제공한다. 메시지 M_2은 수신자가 생성한 세션키 K_r에 의해 암호화되어 있다.

$$C2 = S_s[S, H(M_1), E_{Kr}[M_2], DES_r]$$

④ 송수신자 모두 요약서를 확인하고 자신들이 요청한 것과 같다면 각 세션키를 중재자의 공개키로 암호화해 전송한다.

$$S_s[C2, E_{Ps}[K_s]], S_r[C1, E_{Ps}[K_r]]$$

⑤ 중재자는 C1과 C2를 확인 후 ④에서 제공받은 각각의 세션키로 M_1과 M_2를 복호화한다. 또한, 메시지들과 요약서가 일치하는지 검증해 송수신자가 잘못된 메시지를 보내었는지 검증할 수 있다.

⑥ ⑤의 과정이 옳다면, 중재자는 송수신자가 각각의 메시지를 확인할 수 있도록 세션키들을 공개디렉토리에 공개한다.

$$S_a[E_{Ps}[K_r]], S_a[E_{Pr}[K_s]]$$

⑦ 송수신자는 공개디렉토리를 통해 중재자의 서명과 자신의 공개키로 암호화된 세션키를 얻어 각각 메시지 M_1, M_2을 얻는다.

⑧ 배달 및 내용증명을 통지한다.

만약, 송신자가 C2를 받지 못한다 할지라도 C1안의 메시지 M_1은 세션키 K_s로 암호화되었기 때문에, K_s을 알지 못하는 수신자는 메시지를 알 수 없다. 송수신자사이에 교환되는 메시지는 암호화되었기 때문에 그 메시지의 정당성(요약서와 일치하는 메세지인지)을 당사자들은 알 수 없다. 중재자는 ⑤의 과정에서 서로간 요구하는 문서에 대한 요약서와 실제 복호화된 메시지를 확인함으로써 메시지의 정당성을 확인할 수 있다.

또한, 중재자는 ⑤의 과정에서 메시지를 확인함으로써 메시지에 대한 내용증명이 가능하고 ⑥의 과정에서 메시지를 풀 수 있는 세션키(K_r, K_s)를 각각의 공개키로 암호화하고 중재자의 비밀키로 서명해 공개 디렉토리에 공개함으로써 배달증명이 가능할 것이다.

4. 결론

지금까지 본 본문에서는 네트워크상의 교환되는 문서에 대한 내용 증명과 배달 증명을 설명하였다. 그리고 기존에 소개된 방식들을 분석하고 송수신자들 사이에 문서를 교환하고 그에 대한 내용 및 배달증명이 가능한 새로운 프로토콜을 제안하였다.

보안상의 위협과 분쟁시 효율적인 해결을 위해 네트워크상에서 전송되어지는 콘텐츠들에 대한 내용 및 배달증명에 대한 필요성은 증가하게 될 것이다. 또한, 서로간의 콘텐츠교환에 따른 공정한 교환[4]에 대한 많은 연구가 필요할 것이다.

참고문헌

[1] 박춘식, "배달 및 내용증명이 가능한 전자메일", 통신정보보호학회학술지, 제7권 제4호, pp.73-84. 1997

[2] Y.Tanaka, T.Uchida and M.Akiyama, "Content and Deliver Certification Service Using Cryptography in Electoric Mail", IEICE, Vol. J70-D, No,2, pp.423-431, 1987

[3] K.Nakao, "Applying Cryptography to Contents -certified Service", The 2nd CIS, 1985.

[4] N.Aoskan, Victor Shop and Michael Waider, "Optimistic Protocols for Fair Exchange", In 4th ACM Conference on Computer and Communication Security, pp6-17, 1997