[6-12] # 안전한 전자 메일 서비스(PC-MHS)를 위한 제안

o송유진 ,이민규,이재호,김대웅
한국 전자 통신 연구소

Proposal for secure services of PC-MHS

Youjin-Song,Minkyu-Lee,Jaeho-Lee,Daeung-Kim
Electronics and Telecommunications Research Institute

요 약

본 논문은 안전한 전자 메일 서비스를 제공하기 위한 메일 서명 통신방식에 대하여 제안한다. 통신 네트워크를통해 전자 메일을 송수신할 때 사용자의 정당성(Validation) 을 확인하고 메일 통신문의 위조,변경등을 검출하는 인증(Authentication) 기술을 검토하는 바, 전송 정보나 축적 정보의 안전성 확보책으로서 대표적인 공개키 인증 방식인 RSA암호 방식을 사용한 중재 서명 방식을 전자 메일 시스템에 적용하는 것을 제안한다. 본 논문에서 적용되는 메일 서명 통신 방식은 메시지 복원법과 인증자 조회법의 혼합 방식을 이용하며 중재자를 매개로 하는 중재 서명 방식을 기본으로 하는 구조이다.이와 같은 관점에서 메일 서명 통신의 기본 방식은 송신자와 수신자는 중재자를 매개하여 통신하고 중재자는 송신자가 보낸 메일을 암호화하여 수신자에게 보낸다. 수신자는 그 암호문에 디지탈 서명을 한 후 중재자에게 되돌려 보낸다. 다음에 중재자는 송신자에게 메일 서명문을 보냄과 동시에 수신자에게 암호화 키를 보내는 방식이다.

I. 서론

정보화 사회가 발전하고 중요한 정보가 통신 네트워크를 통해 송수신 됨에 따라 컴퓨터 네트워크 사용자의 정당성(Validation)을 확인하고 통신문의 위조,변경등을 검출하는 인증(Authentication)기술이 중요시 되고 있다. 이에 따라 전송정보나 축적 정보의 안전성 확보책 으로서 대표적인 공개키 인증 방식인 RSA(Rivest,Shamir,Adleman)암호 방식을 사용한 디지탈 서명(Digial Signature) 방식을 전자 메일 시스템에 적용하는 것을 제안한다. 본 논문에서 제안하는 방식은 전자 메일 서비스를 안전하게 제공하기 위한 중재 서명 방식(Arbitrated Digital Signature)을 적용한 메일 서명 통신 방식이다. 본 논문에서는 이와같은 관점으로부터 송신자와 수신자는 중재자(통신업자)를 매개하여 통신하고 중재자는 송신자가 보낸 메일을 암호화하여 수신자에게 보낸다. 수신자는 그 암호문에 디지탈 서명을 한 후 중재자에게 되돌려 보낸다. 다음에 중재자는 송신자에게 메일 서명문을 줌과 동시에 수신자에게 암호화 키를 보낸다. 본 논문의 구성은 1장은 서론, 2장은 메일 서명 통신을 위한 기본 방식및 중재 서명 방식의 구조에대해 논하고 3장에서는 메일 시스템에 서명 방식을 적용하기 의한 제안 방식의 기본 구조및 조건,안전성등을 논하고 4장에서 마무리 짓고자 한다.

II. 안전성을 위한 디지탈 서명 방식

1. 메일 안전성을 위한 서명 방식

디지탈 서명이란 송신자가 비밀키로 메일 통신문에 암호처리를 하여 메일 서명문을 생성해서 보내고 수신자가 그 메일 서명문을 근거로 상대의 메일 내용이 정당한것인가를 확인하는 방식이다. 즉 평문의 송신자와 평문이 위조,변경되지 않은 것을 증명하는 인증 기술이다.

이러한 디지탈 서명 방식에는 직접 서명 (True signature) 과 중재 서명 (Arbitrated signature) 2 가지 방식이 있는 바 안전성 관점에서 서명방식의 조건은 다음을 만족시켜야 한다.

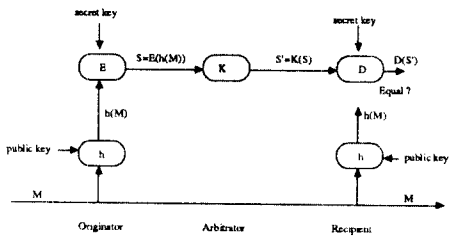
(1) 메일 서명문이 제3자에 의해 위조 , 변경될수 없다.

(2) 메일 서명문이 수신자에 의해 위조, 변경될수 없다.

(3) 수신자의 메일 서명 사실을 송신자가 부정할수 없다.

즉 디지탈 서명의 기본 조건인 메일 내용의 위조 유무및 송신자의 정당성을 인증할 수 있어야 한다.

공개키 암호법을 사용한 직접 서명방식은 위의 조건 1과 2를 만족하나 메시지 복원법 (Message Recovery Method) 를사용하기 때문에 복원된 메시지가 의미있는 것인가 어떤가를 판정하는 의미처리의 문제가 있다.이 의미 처리 문제에 대해서는 아직 해석적으로 평가되거나 지적되지 않고 있는 실정이다. 한편, 인증자 조회법(Authenticator Verification Method)은 의미 처리가 필요 없지만 보통 관용 암호법을 기본으로 하기 때문에 비밀키의 분배가 필요하다. 따라서 안전성 조건을 만족하고 의미 처리와 키 배분 문제를 효율적으로 해결할 수 있는 혼합 방식즉 관용 암호법을 기본으로 하는 인증자 조회법과 공개키 암호화법에 의한 메시지 복원법을 혼합한 방식을 메일 서명 통신 방식에 적용한다. 본 논문에서 제안하는 메일 서명 통신 방식은 공개키 암호화방식을 근간으로 하는 혼합 방식으로서 중재 서명 방식을 구성하는 영역으로서 적용 될 수 있다. 중재 서명 방식을 이용한 메일 서명 통신 방식의 정보 흐름도는 그림 <2-1> 과 같다.



<그림2-1> 중재 서명 방식을 이용한 메일 서명 통신 방식의 정보 흐름도

2. 서명 방식의 분류및 특징

종래의 서명 방식을 디지탈 서명에 사용되는 암호화법,메일 서명문의 검사법,디지탈 서명 방식의 구성법의 관점으로 부터 분류하고 그 특징을 간단히 서술한다.

가. 암호화법

디지탈 서명을 행하기 의해 사용되는 암호화법으로서 관용 암호화법(Conventional cryptography)과 공개키 암호화법(Public key cryptosystem)이 있다.

(1) 관용 암호화법
관용 암호화법이란 암호화키와 복호화키가 동일하고 그 키를 각각 비밀로 하는 암호호화법으로서 대표적인 관용 암호화법은 DES(Data Encryption Standard) 방식이 있다.

(2) 공개키 암호화법

공개키 암호화법이란 송수신자의 암호화키와 복호화키가 각 각 다르며 암호화키는 공개하고 복호화키만을 비밀로하는 암호화법이다. 공개키암호화법에 의한 중재 서명 방식에서는 송신자만이 비밀로 갖고 있는 키를 사용해서 암호화및 복호화를 행하고 서명문을 생성하기 때문에 조건 1,2가 만족되며 중재자가 공통키로 송신자의 서명문을 인증하므로 조건3을 만족 시킬 수 있다.대표적인 공개키 암호화법으로서 RSA(Rivest,Shamir,Adleman)법과 R(Rabin)법이 있다. RSA법은 모든 메시지에 대하여 서명이 가능한 장점을 갖지만 암호화,복호화의 계산량이 많다는 단점이 있는 반면 R법은 모든 메시지에 대해 서명이 가능하지 않다는 잔점도 있지만 암호화 계산량이 적다는 장점이 있다.

나. 검사법

(1) 메시지 복원법

메시지 복원법(Message recovery method)이란 송신자가 메시지에 암호화를 행해서 서명문의 일종인 메일 서명문(Signed Message)으로 변환해서 수신자에게 보낸다. 그 다음에 수신자는 송신되어진 메일 서명문에 복호화를 행해서 원 메시지를 복원한다.

(2) 인증자 조회법

인증자 조회법이란 송신자가 암호처리 h(hash function)를 행해서 서명문의 일종인 인증자(Authenticator)로 변환하여 그대로 메시지와 함께 수신자에게 보낸다. 그 다음에 수신자는 원 메시지에 동일한 암호처리 h를 행하여 얻어진 인증자를 생성하여 송신되어진 인증자와 조회하는 방식이다. 인증자 조회법은 검증(Verification) 이라고도 한다.

다. 구성법

(1) 직접 서명

직접 서명(True signature)이란 수신자가 직접 메시지의 정당성을 인증하는 것으로 분쟁이 발생하는 경우만 판정자에 의해 판단을 내리는 방식이다.

(2) 중재 서명

중재 서명이란 송신자와 수신자 이외의 제3자인 중재자가 메시지의 정당성을 인증하고 그 결과를 수신자에게 알리는 방식이다. 즉, 신뢰할 수 있는 중재자를 개입하여 인증을 행하는 방식이 중재 서명 방식이다.

III. 전자 메일 시스템에의 서명 방식 적용

1. 메일 서명 통신의 기본 방식및 구조

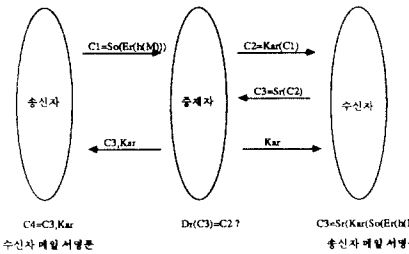
중재 서명 방식을 이용한 메일 서명 통신 방식이 만족해야 할 기본 조건은 다음과 같다.

(1) 수신자 의 디지탈 서명 사실을 송신자가 부정할 수 없는 조건

(2) 메일 서명문이 수신자에 의해 위조,변경될 수 없는 조건

(3) 메일 서명문이 제3자 에 의해 위조,변경될 수 없는 조건

이러한 기본 조건을 만족하는 메일 서명 통신 방식의 기본 구조는 <그림3-1>과 같다.

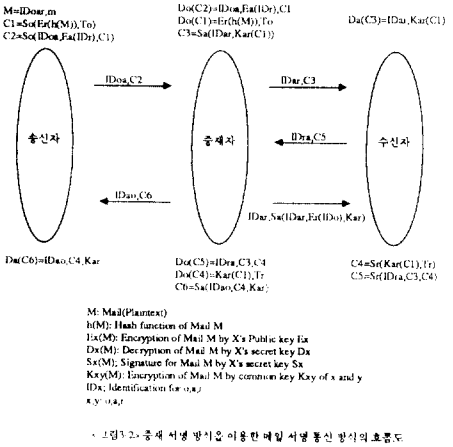


<그림3-1> 메일 서명 통신 방식의 기본 구조

본 논문에서 제안하는 메일 서명통신 방식의 기본 원리를 설명한다. 메일 통신에 앞서 송신자 (originator,o) ,수신자 (recipient,r) 및 중재자 (arbitrator,a) 는 공개키 암호화 시스템 (Publickey Cryptosystem)의 암호화키 Ex(x=o,r,a) 그리고 복호화키 Sx를 작성하고 암호화키 는 공개 화일(예를 들면 , 전화 번호부등) 에 등록하며 , 복호화키는 각 사용자 즉, 송신자,수신자,중재자가 비밀로 보관한다.본 논문에서는 X의 공개키 Ex에 의해 메일 M의 암호화를 Ex(M),X의 비밀키 Sx에 의해 메일 M의 복호화 또는 메일 M에의 서명을 Sx(M),X와 Y간의 공통키 Kxy에 의한 메일 M의 암호화를 Kxy(M)으로 표시한다. 단 ,x,y는 o,r,a중의 하나이다.이러한 표시를 기본으로 해서 메일 서명 통신을 할때 송신자는 메일 M을 수신자의 공개된 암호화키로 암호화Er(M)하고 나이가 자신의 비밀 복호화키로 서명한 메일문 So(M)을 중재자에게 보낸다.송신자로부터 메일 서명문을 받은 중재자는 그 메일문을 수신자가 모르는 공통키로 암호화하여 수신자에게 보낸다. 이 시점에서는 수신자는 공통키 Kar을 모르기 때문에 메일 서명문의 내용이나 송신자를 알 수 없다.그리고 수신자는 중재자로부터 온 메일문에 비밀 복호화키 Sr로 디지탈 서명하여 중재자에게 되돌린다.중재자는 수신자로부터 온 디지탈 서명문이 서명여부를 확인하고 수신자에게 공통키를 보내 준다.수신자는 중재자로부터 온 공통키로 메일 내용을 확인하고 송신자의 서명을 확인할 수 있다.중재자는 또한 수신자로부터 온 메일 서명문과 중재자의 공통키를 송신자에게 보낸다. 이 수신자 서명문을 통해 원 메일과 대조하여 수신자의 메일 위조,변경 여부를 확인할수 있다.

2. 메일 서명 통신 방식의 정보 흐름

본 논문에서 제안하는 메일 서명 통신 방식의 정보 흐름도는 <그림3-2> 와 같다. 그림에서 보는 바와 같이송신자(Originator)는 원 메시지m과 송신자, 중재자및 수신자의 ID를 메일로서 작성하고 이 메일에 인증자 h와 수신자 공개키로 암호화 한후 서명한다. 그리고 이 송신자 메일 서명문과 함께 수신자 식별 정보(ID)를 중재자 공개키로 암호화한 서명문을 중재자에게 송신한다. 서명문을 수신한 중재자는 송신자의 메일 서명문을 복호화 한 후 중재자와 수신자의 공통키로 암호화하여 서명해서 수신자에게 보낸다. 중재자 서명문을 받은 수신자는 공통키로 서명한 메일 서명문을 중재자에게 되 돌린다. 이때 , 중재자는 공통키를 송수신자에게 배분하여 수신자는 이 공통키로서 송신자 메일 서명문을 복호화할 수 있다. 그리고 중재자는 수신자가 서명한 메일 서명문을 공통키로 서명하여 송신자에게 보낸다. 이 메일문을 송신자는 복호화하여 보관함으로써 수신자의 부정 행위를 방지할 수 있다.



<그림3-2> 중재 서명 방식을 이용한 메일 서명 통신 방식의 흐름도

3. 메일 서명 통신 방식의 안전성

본 논문에서 제안하는 메일 서명 통신 방식은 전자 메일이 제 3자및 수신자에 의해 위조,변경 될 수 없고 수신자의 메일 서명 사실을 송신자가 부정 할 수 있는 부정 행위에 대해 안전성을 부여할 수 있다. 즉, 제 3자및 수신자에 의한 메일 자체의 위조,변경등은 송수신자가 각각 메일에 서명함으로써 부정 행위 방지가 가능 할 것이다.그리고, 수신자에 의한 수신 사실의 부정은 송신자가 수신자 메일 서명문을 보관함으로서 방지할 수 있고 송신자에 의한 송신 사실의 부정은 수신자가 송신자 메일 서명문을 보관함으로서 방지할 수 있다.

IV. 결언

본 논문에서는 RSA 암호에 근거한 중재 서명 통신 방식을 도입한 메일 서명 통신 방식을 제안하였다. 제안한 방식의 특징은 다음과 같다.

(1) 공개키 암호화법을 사용한 중재 서명 방식으로 구성된다.

(2) 인증자 조회법과 메시지 복원법을 병용한 혼합 방식이다.

(3) 중재자가 공통키를 사용함으로써 송수신자간의 키 배분이 불필요하다.

제안된 메일 서명 통신 방식을 전자 메일 시스템 (PC-MHS)에 적용 하기 위해서 신뢰할 수 있는 중재자 서명을 위한 중재자 선정과 혼합 방식의 적용으로 인한 구현상의 검토가 요구된다.

또한, 향후 본 논문에서 제안된 메일 서명 통신 방식의 효율성및 안전성 평가와 개인 식별 정보(Identity)에 근거한 인증 방식을 적용한 시스템의 검토가 요구된다.

참고 문헌

1. W. Diffie and M. Hellman, "New directions in cryptography", IEEE Trans. Information Theory, Vol.IT-22, No.6, pp.644-654, Nov. 1976

2. R.L.Rivest,A.Shmir and L.Adleman, "A method for obtaining digital signature and public-key cryptosystem", Comm. ACM, Vol.21, No.2, pp120-126,Feb.1978

3. S.G.Akl, "Digital signature: a tutorial survey", IEEE Computer,pp.15-24, Feb.1983

4. D.E.Denning, "Protecting public keys and signature keys", IEEE Computer, pp27-35, Feb.1983

5. D.W.Davis, "Applying the RSA digital signature to electronic mail", IEEE Computer,pp55-62, Feb.1983

6. "Data Encryption Standard", FIPS Pub. 46 National Bureau of Standards, Washington,D.C.,Jan.1977

7.D.E.Denning, "Cryptography and data security", Addison-Wesley,1982

8. 小山謙二,"公開鍵暗号による高速かつ安全なディジタル署名法", 信学論, Vol. J67-D No.3, pp305-312, 1984

9. 田中良明, 内田孝則, 秋山稔,"暗号を用いた内容証明, 配達証明サービス", Vol. J70-D No.2, pp.423-431, 1987