일회성키를 이용한 전자우편 보안 프로토콜

장준교(*), 이상하(*), 김동규(*)
(*)아주대학교 컴퓨터공학과

A proposed E-mail Security Protocol using One-time key

Jun-kyo Jang(*), Sang-ha Yi(*), Dong-kyoo Kim(*)
(*) Dept of Computer Engineering, Ajou University

요 약

전 세계가 정보화 열풍을 겪고 있는 시점에서, 엄청난 사용자들이 다양한 인터넷 서비스 중 전자우편 서비스를 생활의 일부분으로 사용하고 있다. 그러나 기존의 전자우편 서비스만을 제공하는 환경하에서는 많은 보안 위협요소 들이 존재하고 있으며 전자우편 서비스의 사용에 많은 제약과 노출 위험 가능성을 안고 있다. 이러한 문제점들을 극복하기 위한 노력들이 이미 기울여져 다양한 방법으로 해결책을 제시하고 있지만 아직 완전한 형태의 결과물이 나오지 못하고 있다. 그 중 대표적인 PEM은 구현의 어려움으로 인하여 보편화 되지 못하고 있으며, 또 다른 제품인 PGP는 키인증 등의 문제점을 안고 있는 실정이다. 또한 이들 제품들은 전자우편 보안 요구사항 들을 모두 충족시켜주지 못한다는 문제점들도 안고 있다.

본 논문에서는 위에서 언급했던 제품들이 안고 있는 문제점들을 극복할 수 있는 다른 해결책을 내 놓기 위해 모든 보안 요구사항을 만족할 수 있고 사용하기 편리한 전자우편 보안 프로토콜을 설계하였다. 이를 위해 비대칭키 방식인 키 분배 서버를 이용하며, 하부 사용자는 키 분배 서버에 의존해 기밀성 및 무결성등 정보보호 서비스를 제공 받을 수 있다.

1 서론

정보화 사회로의 전향이 이루어 지면서, 오늘날 다양한 변화들이 빠르게 발생하고 있다. 전에는 컴퓨터관련 전공을 한 사람이 아니면, 사용하지 않았던 다양한 인터넷 서비스들을 일반인들도 자연스럽게 사용하고 있으며 더욱더 보편화되어져 생활의 일부분으로 자리매김 하고 있다. 이들 서비스들 중 하나인 전자우편서비스도 이러한 분위기에 편승해 컴퓨터를 사용하는 사람이면 누구나 활용하고 사용하는 도구로 받아들여지고 있다.

하지만 이러한 전자우편서비스 사용의 폭증과 더불어 나타나는 문제점도 적지않게 발생하고 있다. 전자우편서비스를 개인적인 서신 교환목적으로 사용하든, 또는 회사업무의 일환으로 공문이나 안내문 등을 작성해 발송하는 경우든 간에 이들 전자우편 들은 봉투에 넣어져 밀봉되는 일반적인 편지와는 달리 보내는 곳의 주소뿐만 아니라 내용까지도 노출되어지는 구조를 가지고 있기 때문에 작성되어져 전송되어지는 과정에서 엿보여지 탈취 및 변조되어질 가능성을 안고 있다. 이러한 이유로 인하여 전자우편시스템의 정보보호서비스를 제공해야 할 필요성이 대두된다.

인터넷에서 전자우편의 정보보호 취약성을 보완하고 개선하기 위한 노력이 일치 감치 기울여져 1993년 2월에 IETF(Internet Engineering Task Force)의 PEM(Privacy Enhanced Mail) WG과 IRTF(Internet Research Task Force)의 PSRG(Privacy and Security Research Group)의 공동 연구로 PEM에 대한 RFC문서를 발표하였다[3]

또한 1991년에 필립짐머만(Philip R Zimmermann)이 만들어 발표한 PGP(Pretty Good Privacy)는 여러 차례 개정을 거쳐 사용되어지고 있으며[4], PEM의 형태를 따르지는 않지만 비밀성, 변조/위조/부인방지 등의 추구하는 목표는 동일하며, 전자메일의 보호뿐만 아니라 일반 파일에 대한 암호화도 가능하고, 개인 사용자들에 무료로 배포되어 널리 보급됨으로써 실질적인 표준(defacto standard)의 구실을 하고 있다. 하지만 PEM이나 PGP는 전자우편 시스템에서 요구하는 정보보호서비스 중 수신자 부인방지 서비스와 재 전송 방지 서비스들을 충족시켜 주지 못하는 실정이며[5][6], 이를 위한 계속적인 연구가 필요하다.

본 논문에서는 이러한 문제점들을 개선하려는 목적으로 전자우편 정보보호 요구사항 들을 모두 충족시키는 새로운 전자우편 보안 프로토콜을 제시하기 위해 공개키 방식을 사용하는 키 분배 서버(KDS : Key Distribution Server)를 이용하며 이로 인해 사용자는 대칭키 방식만을 이용하고 필요 시 키 분배 서버로부터 일회성키를 분배 받아 작동할 수 있도록 설계되었다[1]

2 전자우편 정보보호 서비스 요구사항

인터넷의 전자우편 서비스는 메시지를 작성하는 사용자는 작성된 메시지가 원하는 수신자만이 읽을 수 있기를 바라며 또한 수신자는 수신된 메시지가 수신자가 알고 있는 실제 송신자로부터 온 메시지임을, 보내진 메시지가 변조되지 않았음을 확신할 수 있기를 바란다. 또한 송신자나 수신자가 송신 또는 수신 사실을 부인하는 일이 발생하지 않기를 바란다.

이러한 송신자와 수신자간의 욕구를 모두 만족시켜주기 위해서 요구되어지는 전자우편 정보보호서비스를 우선 도출해봄으로써 설계되어질 전자우편 보안 프로토콜에 부가되어져야 하는 정보보호서비스의 범위를 정할 수 있을 것이다.

첫 번째로, 수신자 A가 메시지를 수신하였을 때 수신된 메시지가 정말로 송신자 A로부터 보내진 메시지인지를 수신자는 확인할 수 있어야 할 것이다. 그렇지 않다면 불법 사용자 B가 송신자 A인 듯이 행동함으로써 수신자 A를 속일 수 있게 된다. 이러한 문제를 방지할 수 있는 정보보호서비스를 사용자 인증 서비스라고 한다[2]

두 번째로, 송신자가 보낸 메시지가 원하지 않는 객체에게 건네어지더라도 메시지의 내용은 노출되어지지 않도록 하는 기밀성 서비스가 제공되어져야만 송신자가 원하는 수신자만이 메시지를 읽을 수 있도록 하는 것을 보장할 수 있다.

세 번째로, 수신자가 수신한 메시지가 전송도중 권한 없는 객체에 의해 변조되었다면 이러한 사실을 수신자는 확인할 수 있어야 한

다 이러한 서비스를 무결성 서비스라고 한다

네 번째로, 송신자 부인방지 서비스로써 송신자가 메시지를 수신자에게 전송한 후, 해당 메시지 전송사실을 부인할 수 없도록 하여야만 수신자는 수신 메시지에 대해 아무런 의심 없이 받아들일 수 있을 것이다.

다섯번째로, 송신자도 자신이 보낸 메시지가 수신자에 의해 열람되어진 후에 수신사실을 거부할 수 없도록 하여야만 믿고 보낼 수 있게 된다. 이러한 서비스를 수신자 부인방지서비스라고 한다.

여섯번째로, 수신자가 송신자로부터 수신한 정보를 제3자에게 전달하고 제3자는 이 정보를 조작하여 송신자로부터 수신한 정보임을 주장하지 못하게 하는 메시지 재전송 방지 서비스도 제공되어져야 한다.

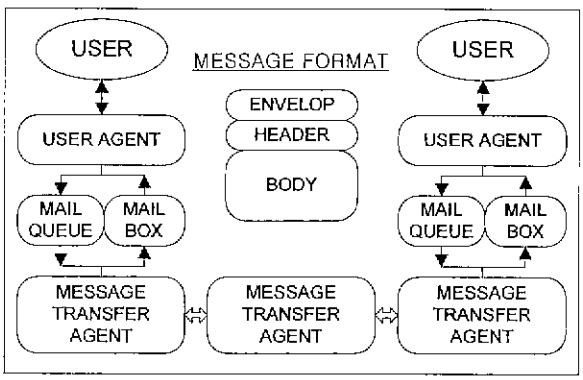
위에서 언급한 여섯 가지의 정보보호서비스가 제공되어져야만 전자우편 서비스를 사용하는 사용자들은 비밀을 유지해야 하는 정보들이나 집단의 이익과 직결되는 정보들에 대해서도 안심하고 전자우편 서비스를 이용할 수 있게 될 것이다.

3 전자우편시스템의 구성

인터넷에서 사용자가 전자우편 서비스를 사용하여 메일을 송수신하는 과정을 [그림 1]에서 표현하고 있다. [그림 1]을 보면 알수 있듯이 전자우편시스템은 크게 UA(User Agent)와 MTA(Message Transfer Agent)로 구성된다[7][8].

UA는 사용자가 보낼 메시지를 작성하고, 받은 메시지를 확인하는 작업을 수행하며, MTA는 UA로부터 메시지를 전달 받아 원하는 목적지까지 전달하는 역할을 담당한다. 이때 사용되는 프로토콜이 SMTP를 따르도록 되어있다. 전자우편 시스템은 온라인 형태로 통신이 이루어지는 것이 아니라 우선 UA가 작성한 메시지를 MTA에 넘겨주면 MTA는 목적지 주소를 확인한 후 라우팅을 통해 다음 경로를 결정한다. 그런 다음 MTA와 연결을 맺고 해당 메일을 전달하고 연결을 끊는 방식으로 반복되어져 최종 목적지 MTA까지 도착하게 되는 store and forward 방식을 따르고 있으며 해당 메일을 메일박스에 저장해 두었다가 수신자가 메일을 확인하기 위해 UA를 기동 시킬 때 메일박스로부터 수신된 메일을 가져와 보여주는 방식으로 작동한다[9]

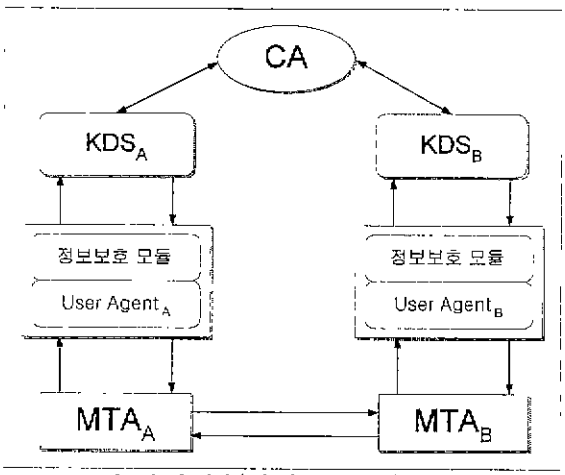
그렇기 때문에 일반적인 연결지향 방식과는 달리 통신 양단간에 먼저 연결을 맺기 위한 절차가 생략되어짐으로 보안 프로토콜도 다른 방법으로 접근 되어지야 한다



[그림 1] 전자우편 시스템

4 전자우편 정보보호 프로토콜

본 논문에서 제안하는 프로토콜의 전체 프레임워크를 도시하면 [그림 2]와 같다. 우선 정당한 사용자는 키 분배 서버와의 대칭키를 가지고 있으며, 키 분배 서버는 공개키 하부 구조(PKI Public Key Infrastructure)에 의해 비대칭키 방식을 따른다고 가정한다.



[그림 2] 전자우편 정보보호 프레임워크

정당한 송신자가 UA에서 수신자에게 보낼 메시지를 작성한 후 정보보호 모듈을 통해 H(M)을 발생시키고 수신자와 송신자 ID를 키 분배 서버에게 전달한다.

- 송신자→KDS$_A$: $ID_{송}$, $ID_{수}$, H(M)

키 분배 서버는 이들을 수신후에 분쟁이 발생시 사용하기 위해 송신자 부인 방지 영수증으로 저장하고, 세션키 $K_{session}$를 생성후 다음과 같은 정보를 구성하여 송신자 정보보호 모듈에게 전달한다

- KDS$_A$→송신자 : $\{K_{session}\}K_{KDSA,송신자}$, $\{K_{session}, ID_{송}, ID_{수}\}K_{KDSBpub}$, $[H(M)]K_{KDSAprIv}$

정보보호 모듈은 수신자에게 보낼 안전한 형태의 메시지를 구성하여 MTA에게 건달한다.

- 송신자→MTA : $\{M\}K_{session}$, $\{K_{session}, ID_{송}, ID_{수}\}K_{KDSBpub}$, $[H(M)]K_{KDSAprIv}$

이 정보는 여러 MTA를 거쳐 최종적으로 수신자에게 전달된다. 수신자는 수신된 메시지를 확인하기 위해서는 자신의 도메인내에 있는 키 분배 서버를 통하여야만 가능하다 우선 수신자가 수신한 메시지의 내용은 다음과 같다.

- 송신자→수신자 : $\{M\}K_{session}$, $\{K_{session}, ID_{송}, ID_{수}\}K_{KDSBpub}$, $[H(M)]K_{KDSAprIv}$

이들 정보 중 $\{K_{session}, ID_{송}, ID_{수}\}K_{KDSBpub}$, $[H(M)]K_{KDSAprIv}$를 키 분배 서버에게 전달한다.

- 수신자→KDS$_B$: $\{K_{session}, ID_{송}, ID_{수}\}K_{KDSBpub}$, $[H(M)]K_{KDSAprIv}$

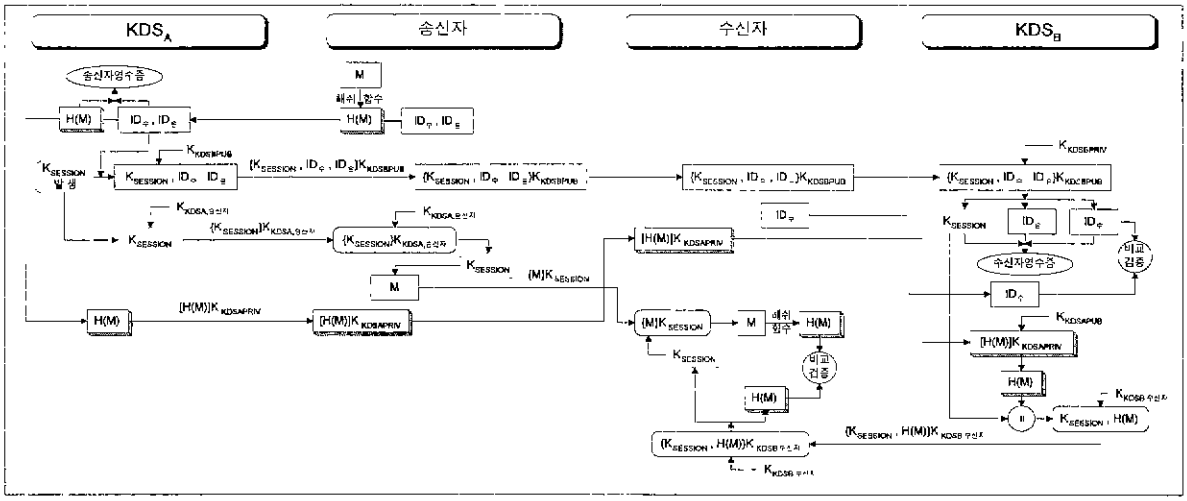
키 분배 서버는 자신의 비밀키를 이용해 $\{K_{session}, ID_{송}, ID_{수}\}K_{KDSBpub}$를 복호화 하여 $K_{session}$, $ID_{송}$, $ID_{수}$를 얻는다 또한 키 분배 서버 A의 비대칭키를 이용해 H(M)도 얻어낸다. 그런 다음 수신자 부인방지를 위해 $ID_{송}$ $ID_{수}$, H(M)를 저장하고 다음과 같은 정보를 수신자의 정보보호 모듈에게 전달한다

- KDS$_B$→수신자 : $\{K_{session}, H(M)\}K_{KDSB\ 수신자}$

수신자 정보보호 모듈은 위의 정보를 자신의 비밀키로 복호화한 후 $K_{session}$, H(M)을 얻어내고 세션키를 이용해 메시지를 복호화한후 해쉬함수를 이용해 무결성을 검증하고 문제가 없다면 UA를 통해 수신자 메시지를 확인할 수 있도록 해준다 [그림 3]은 프로토콜의 전체 시나리오를 나타낸다.

4.1 기밀성 서비스

본 논문에서 설계한 전자우편 보안 프로토콜에서는 송신자가 전달하는 메일에 대한 기밀성 서비스를 제공하기 위해서 키 분배 서버로부터 일회성키를 할당 받아 메시지를 암호화하며, 일회성키를 수신자에게 전달하기 위해 수신자의 키 분배 서버의 비대칭키로 암호화하여 전달한다 수신자가 일회성키를 획득하는 과정은 수신자의



[그림 3] 전자우편 정보보호 프로토콜 시나리오

키 분배 서버의 비대칭키로 암호화되어있는 토큰을 전달하여 토큰 내에 저장된 일회성키를 돌려 받음으로써 이루어진다

4.2 무결성 서비스와 전자서명

송신자는 전달할 메시지를 암호화할 뿐만 아니라 무결성 서비스를 제공하기 위해 일방향 함수를 이용하여 메시지의 해쉬값을 얻어내고 이것을 송신자 키 분배 서버의 비밀키로 전자서명 한다. 이때 수신측에서는 수신자의 키 분배 서버에서 메시지의 해쉬값의 전자서명을 확인하고 수신자측에게 해쉬값을 전달하면 수신측에서는 수신된 메시지의 해쉬값과 일치하는지를 확인함으로써 메시지가 전달도중 변경됐는지의 여부를 확인한다[1]

4.3 송신자 부인방지와 수신자 부인방지 서비스

수신자가 수신한 메시지에 대해 송신자가 송신사실을 부인할 때, 수신자는 송신자 키 분배 서버에 이의 증재를 요청한다. 송신자 키 분배 서버는 수신자로부터 증재를 원하는 메시지를 전달 받고 해당 메시지의 해쉬값을 얻어낸 후 자신의 데이터베이스에 동일한 송신지 영수증이 존재하는지를 확인함으로써 이를 증명한다.

송신자가 송신한 메시지에 대해 수신자가 수신사실을 부인할 때도 또한 동일한 방법을 이용한다. 송신자는 수신자 키 분배 서버에 증재를 요구한다. 수신자 키 분배 서버는 송신자로부터 증재를 원하는 메시지를 전달 받고 해당 메시지의 해쉬값을 얻어낸 후 자신의 데이터베이스에 동일한 송신자 영수증이 존재하는지를 확인함으로써 수신자가 수신사실을 부인할 수 없도록 한다

4.4 메시지 재전송 방지 서비스

메시지 재전송은 수신자가 송신자로부터 수신한 정보를 제3자에게 전달하고 제3자는 이 정보를 조작하여 송신지로부터 수신한 정보임을 주장하는 경우이다. 하지만 본 논문에서 제안한 전자우편 정보보호 프로토콜은 자신이 수신한 수신사실을 주장하기 위해선 키 분배 서버에 저장되어있는 수신 사실 증명서가 존재하여야 하기 때문에 사실여부를 키 분배 서버에 증재함으로써 확인되어질 수 있다

5 결론

본 논문에서 제안하고 있는 전자우편 보안 프로토콜은 전자우편 보안 요구 사항인 사용자 인증 서비스, 기밀성 서비스, 무결성 서비스, 송신자/수신자 부인 방지 서비스, 메시지 재전송 방지 서비스 모두를 제공할 수 있도록 설계되어져 기존의 전자우편 정보보호 서비스의 일환으로 개발된 PGP나 PEM에서 제공되어지지 못했던 수신자 부인방지 서비스, 메시지 재전송 방지 서비스까지도 수립하고 있어 PGP와 PEM의 문제점을 해결하고 있다

또한 비대칭키 방식을 이용하는 키 분배 서버를 이용하여 하부 사용자는 단지 해당 도메인내에 있는 키 분배 서버와의 대칭키만을 가지고 작동됨으로써 공개키 기반구조를 간소화 시킬 수 있었다.

본 논문에서 제안하고 있는 전자우편 보안 프로토콜은 국책과제인 "분산통신망환경 통합 정보보호서비스 소프트웨어 기술" 개발에서 무연결지향 통신상에서의 정보보호 서비스 방법을 전자우편 보안에 적용한 것이다 이러한 취지에서 앞으로 하부엔진에 독립적인 응용프로그램을 개발할 수 있도록 하기 위해 전자우편 시스템에서 UA 부분에 간단히 IDUP GSS-API 함수만을 삽입함으로써 정보보호서비스를 받을 수 있도록 할 수 있는 API를 만들어 제공할 수 있어야 할 것이다.

참고문헌

[1] 김동규, 장준교외, 분산통신망 환경 통합정보보호서비스 소프트웨어 기술, 정통부 2차년도 연구개발보고서, 1998, 1.
[2] 김동규, 장준교외, 분산통신망 환경 통합정보보호 서비스 소프트웨어 기술, 정통부 1차년도 연구개발보고서, 1996, 1
[3] 강명희외, "인터넷 메일 시스템에서의 정보보호 서비스 구현," 한국통신정보보호학회 논문지, 제7권, 제2호, pp 107~122, 1997. 6
[4] Simon Garfinkel, "PGP Pretty Good Privacy", O'Relly& Associates 1995
[5] S.Kent, "Privacy Enhancement for Internet Electronic Mail, Part2 : Certificate-Based Key Management", RFC 1422, 1993
[6] Patriciu,V V ,"Security Solutions for Email Transmissions in Computer Networks",Proceedings of CONTI'94 International Conference, Bucharest, Romania. 1995.
[7] J.Postel, "Simple Mail Transfer Protocol", RFC 821, 1982.
[8] J.Linn, "Privacy Enhancement for Internet Electronic Mail, Part1 Message Encryption and Authentication Procedures", RFC 1421, 1993
[9] D.Balenson, "Privacy Enhancement for Internet Electronic Mail, Part3 : Algorithms, Modes, and Identifiers", RFC 1423, 1993
[10] B Kaliski, "Privacy Enhancement for Internet Electronic Mail, Part4 : Key Certificate and Related Services", RFC 1424, 1993