공개키 암호화 알고리즘을 이용한 웹 기반 메일 시스템의 개발 및 구현

하 경 재 , 문 철 곤
경 남 대 학 교 컴퓨터 공학과
kjha@kyungnam.ac.kr. gone98@mail.com.kyungnam.ac.kr

(Development of Web-Based Mail-System using the Public-key Encryption Algorithm)

Kyung-Jae Ha , Cheol-Gon Moon

요 약

웹에 기반한 메일 서비스의 급속한 성장으로 인하여 전자 메일은 인터넷을 이용하는 많은 사용자들의 주요 정보 교환수단이 되었다. 현재의 웹에 기반한 메일 시스템에서 SMTP 프로토콜을 이용하여 메일을 전송할 경우, 전송되는 메시지는 아무런 보안 조치도 취해지지 않은 상태로 전송된다. 그러므로 네트워크에 연결된 내,외부의 침입자에 의하여 정보가 도청될 경우 쉽게 정보가 해석될 수 있는 문제점이 있다. 본 논문에서는 웹 상에서의 메일 서비스로 전자메일을 전송할 경우 데이터부분을 암호화하여 전송함으로써 외부의 침입자에 의해 전송데이터가 가로채지더라도 해독하지 못하도록 하였으며 받은 전자메일에 대하여 원래의 데이터로 복호화 할 수 있는 웹 기반 메일 시스템을 개발하였다. 이를 위하여 보안기능이 강화된 MIME 인코딩 알고리즘을 제안하고 이를 응용한 웹 기반 메일 서비스 및 클라이언트 어플리케이션을 구현하여 실제로 데이터 도청 시 메일 메세지가 보호될 수 있음을 보였다.

1.서론

1990년대 중반 이후 웹에 기반한 전자 메일 서비스는 그 사용성의 편리함과 무료라는 장점으로 대부분의 인터넷 서비스 사용자들이 이용하게 되었다. 이러한 웹 기반의 전자 메일 서비스는 인터넷이라는 개방된 네트워크를 통해 전달되기 때문에 제3자에 의하여 패킷이 쉽게 가로채질 수 있으며 이 경우 메일의 데이터나 첨부된 내용이 쉽게 해석되어질 수 있다.

전자 메일의 전송규약은 1982년에 발표된 RFC 821/822 와 멀티미디어 데이터의 전송을 위한 MIME (Multipurpose Internet Mail Extentions)을 제안한 RFC 1341/1342이 있으며 이후 전자 메일의 보안에 관한 관심과 그 필요성이 높아짐에 따라 보안에 그 초점을 둔 새로운 POP3 가 개발되었다.[1][2].이러한 전자 메일 자체의 규약으로는 제 3자에 의한 해석 가능성을 막을 수 없기 때문에 중요한 데이터를 첨부한 메일의 경우 암호화하여 전송해야할 필요가 있다. 이러한 암호화 기술로는 대칭키 암호 알고리즘과 비대칭키 암호 알고리즘이 주로 사용되며 그 효율성과 보안성을 위해 두 가지 알고리즘을 결합하여 사용한다.[3]

본 논문에서는 이러한 암호화 알고리즘을 사용하여 보안성을 높인 웹 기반의 전자메일 시스템의 개발 및 구현을 목적으로 하였다. 멀티미디어 데이터를 위한 MIME 규약 및 메일 전송시 SMTP를 준수하였으며 타 메일 서비스와의 호환을 위해 암호화 되지 않은 메일의 전송시 디지털 서명을 첨부하였다.

본 논문의 구성은 2 장에서 암호화 관련 기술에 대해 알아본 뒤 본 논문에 적용될 암호화 알

고리즘에 대해서 설명하며 3장에서는 구현된 웹 기반 암호화 전자메일 시스템의 동작을 보였다. 4장에서는 결론 및 향후연구 방향을 제시한다.

2. 전자 메일 데이터의 암호화

2.1 암호화 알고리즘

암호화 알고리즘은 암호화와 해독에 필요한 키에 따라 크게 대칭형 알고리즘과 비대칭형 및 단 방향성의 해쉬함수로 나뉜다. 대칭키 암호의 경우 송신측에서 사용한 비밀키가 수신측에서도 복호화를 위해 사용되는 경우로 DES, IDEA,RC5 등이 있다. 이 경우 암호화된 데이터의 전송 전에 비밀키가 공유되어야 하므로 키 관리에 문제점이 발생하나 비대칭키 알고리즘에 비하여 매우 빠른 속도를 보인다. 이에 반해 비대칭키 알고리즘은 송신측에서 공개된 키로 암호화하여 전송한 데이터를 수신측에서 보유한 비밀키로 다시 복호화하는 알고리즘으로서 키의 공유가 없으므로 키의 교환과 관리는 수월하나 그 속도가 느리다는 단점이 있다. 일반적으로 비대칭키 알고리즘은 RSA로 대표된다. 또한 해쉬(hash) 함수의 경우 임의의 크기를 입력으로 받아 고정된 출력으로 변환해 주며 MD5 (Message Digest #5), SHA(Secure hash Algorithm)등이 있다.[4]

2.2 적용 알고리즘

전자 메일은 그 데이터의 크기가 대용량일 경우가 많으므로 암호화하는데 걸릴 시간을 고려해야 한다. 비대칭형 알고리즘인 RSA의 경우 보안성은 우수하지만 대칭형 알고리즘인 DES보다 속도가 현저히 느리다.[5] 따라서 일반적으로 이 두 알고리즘을 결합하는 방법이 바람직하다. 그러므로 RSA 알고리즘으로 먼저 비밀키를 생성하고 그 키를 사용하여 DES 알고리즘을 적용한 암호화 방법을 사용한다. 메일 데이터의 인코딩 알고리즘은 MIME 표준 인코딩 방법인 Base64를 사용하였다[6]. Base64 의 경우 3개의 문자로 이루어진 24bit의 입력을 받아서 4개의 문자를 생성해 낸다. 이때 인코딩된 4 byte의 데이터는 첫 번째와 세번째의 데이터가 그 뒤 데이터의 일부 정보를 가지고 있으므로 암호화시 두 번째 네 번째 데이터는 암호화 대상에서 제외하였다. 이렇게 함으로써 암호화 하는데 걸리는 시간과 암호화된 데이터를 크기를 줄일 수 있다. 이렇게 암호화된 데이터를 전송하면 수신측에서는 미리 전송 받은 비밀키를 사용하여 DES에 사용된 키를 복호화 하고 다시 복호화된 키를 사용하여 메일 데이터를 해독한다. 이 과정은 다음과 같이 나타낼 수 있다.

1. DES 알리즘을 적용을 위한 비밀키 생성
   Key(C) = M^E mod N.
   E , N: 공개키
2. Base64로 인코딩 된 데이터를 DES로 암호화
   Enc(Data)=DES(Key,Base64(1,3))
   Base64(1,3): 첫 번째와 세 번째 데이터
3. 암호화된 데이터를 비밀키와 함께 전송
   Send(Key, Enc(Data))
4. 수신 측에선 개인키를 사용하여 복호화
   Data=DES(Key,Enc(Data))

따라서 해커나 여타 다른 사용자에 의해 메시지가 전송 중 누출되더라도 수신자의 비밀키를 알 수 없으므로 데이터의 해석이 불가능하다.

3. 웹 기반의 암호화 메일 시스템 구현

본 논문에서 제안 된 시스템은 Linux를 기반으로 하여 C언어 및 PHP가 사용되었으며 데이터베이스는 MySQL을 사용하였다. 또한 아파치 웹서버와 인터넷 익스플로러 5.0을 사용하였다. 제안 시스템과 달리 암호화를 지원하지 않는 일반 웹 기반 메일시스템과의 호환을 위해 옵션을 제공하며 따로 전자 서명을 할 수 있는 기능을 추가하였다.

본 시스템의 암호화 부분 중 인코딩된 데이터를 암호화한 부분은 다음과 같다.

```
34563s24312612532q34323034532w34321r3
4321D67459v16756w98945M24539y987860
4517823756b19878O10434q67301t90771M1
9235K45980w23112778665825676D12333M
90998t46258N38789m33452z98909q45433r1
0768T28768C88767s36785O66778/29870A3
4366z56844L22678T24578Z21557s
```

그림1. 암호화된 데이터

암호화된 전자메일의 표시를 위해 다음과 같이 MIME 규약을 확장 하였으며 이를 이용하여 받은 전자 메일이 해당 시스템으로 암호화 되었는지의 여부를 판별할 수 있다. 또한 DES알고리즘에 사용된 비밀키가 메일 데이터와 함께 전송 되어야 하므로 서명 파일과 함께 첨부 파일 형태로 전송된다.

```
Content-Type: Enc/Dec-RSA_KEY;
        charset= ks_c_5601-1987
Content-Transfer-Encoding: Base64
X-MIME-ENC: RSA-DES-Encoder
```

그림2. 확장된 MIME 규약

사용자 정보의 보안을 위해 보낸 사람과 같은 메일 헤더 정보 또한 DES 알고리즘으로 암호화 될 수 있도록 하였으며 첨부 파일별로 암호화의 여부를 결정할 수 있도록 하였다.

4. 결론

본 논문에서는 일반적인 웹 기반 전자 메일 시스템의 보안상 문제점을 지적하고 이를 해결하기 위한 방안을 제시하였다. 전자 메일을 암호화 시킴으로써 비록 메일 데이터가 가로채지더라도 수신측이 아닌 이상 그 해독이 불가능하도록 하였다. 효율적인 암호화 기법을 위하여 대칭형 알고리즘과 비대칭형 알고리즘을 결합하여 사용하였으며 암호화된 데이터의 크기 및 암호화 속도의 향상을 위해 인코딩 데이터의 절반만을 암호화 대상으로 하였다.

본 논문의 향후 과제로서 DES보다 효율적인 알고리즘의 도입과 각 비밀키의 생성 및 보관, 관리에 관하여 향상된 사용자 편리성의 제공을 위해 좀 더 많은 연구를 하고자 한다. 또한 이와 같은 메일 데이터의 암호화를 지원하는 전자 메일 시스템이 전무하므로 앞으로 각 웹 기반 전자 메일 시스템 간의 암호화 및 보안에 관한 표준 규약의 제정 역시 시급하다 하겠다.

[참고 문헌]

[1] Jonathan B.Postel , "Smple Mail Transter Protocol", RFC 821,1982

[2] David H. Crocker , "Standard for the format of ARPA Internet Text Messages." RFC 822, 1982

[3] A.J. Mebezes, P.C. van Oorschot, S.A.ran st -one, Handbook of Applied Cryptography, CRC Press, 1997

[4] R.L. Rivest, "The MD5 Message Digest Algorithm"

[5] Bruce Schneier,"APPLIED CRYPTOGRAPHY ", SECOND EDITION, WILEY. 1996

[6] N.Freed & N.Borenstein,"MIME(Multi-purpose Internet Mail Extensions) Part One: Mechanisams for Specifying and Describing the Format of Internet Message Bodies,"RFC 1521, 1993