POP3 보안을 위한 사용자 인증과 암호화 통신

이 형 승, 허 신
한양대학교 전자계산학과

User authentication and Secure communication for POP3 Security

Hyoung-Seung Lee, Shin Heu
Dept. of Computer Science and Engineering, Hanyang University

요 약

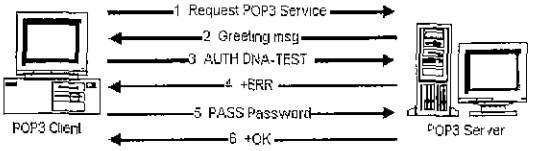
인터넷의 빠른 성장으로 인해 E-mail은 특정 부류만의 사람이 사용하는 것이 아니라 일반 대중에게도 널리 사용되는 생활의 일부분이 되었다. 현재의 POP3 구조에서는 원격 접속을 시도할 경우 사용자의 ID와 Password는 암호화가 안된 상태로 전송된다. 이러한 것 때문에 여러 보안 공격의 대상이 될 수 있으며 여러 보안 문제를 발생시키고 있다. 본 논문에서는 기존의 POP3에서 PASS라는 명령어를 통한 사용자 인증 과정에서 나타나는 문제점을 지적하고 이를 방지하기 위한 새로운 인증 방법을 One-Time Password System을 이용해서 제시하고 구현하고자 한다 또한 One-Time Password System을 이용해 불법적인 방법으로 알아낸 암호의 재사용을 방지했다. 또한 암호화 통신을 위해 관용 암호화 방식의 IDEA 알고리즘을 이용했으며, 키 분배와 관리 문제는 One-Time Password System에서 생성한 키를 IDEA의 비밀키로 사용함으로써 해결했다

1. 서 론

메일 프로그램이 작동하고 있는 클라이언트 측의 컴퓨터와 메일 서버 사이에서 메일을 관리하기 위해 규정된 프로토콜이 POP3이다. 현재의 POP3 구조에서는 원격 접속을 시도할 경우 사용자 ID와 Password는 암호화가 안된 상태로 전송된다 [1][4] 즉, 도청을 통해서 다른 사용자의 암호를 쉽게 빼낼 수 있다는 보안 문제를 야기 시킨다. 본 논문에서는 사용자 인증 과정에서 나타나는 이러한 문제를 없애기 위해 기존의 PASS라는 명령어를 사용하여 사용자 암호를 서버에게 전송하는 인증 방법이 아니라 One-Time Password 방식을 이용한 사용자 인증 방법을 제시하고 구현하는 것이다. One-Time Password 방식을 구현하는 방법은 여러 가지가 있으나 이곳에서는 Challenge-Response방식을 이용하고자 한다. 또한 사용자를 인증하는 인증 절차뿐만 아니라, 클라이언트와 서비시이의 주고 받는 메시지에 대한 보안도 가능하게끔 하였다 제안하는 보안 구조는 POP3 프로토콜을 확장시켜 클라이언트에 대한 인증과, 데이터 무결성 보장, 재사용 방지, 데이터 비밀성 문제를 해결할 수 있다.

2. 기존 POP3의 문제점

아래 그림은 POP3가 일반적으로 행하는 인증 절차를 나타낸 것이다. 그림에서 1, 2번은 클라이언트가 메일 서비스를 받기 위해 서버와 110번 포트를 통해 TCP 연결을 시도하는 과정을 나타낸 것이다. 그림에서 3번은 클라이언트가 서버에게 USER이라는 POP3 명령어를 이용해서 사용자 ID를 서버에게 전달하는 절차를 나타낸 것이고, 4번은 서버 측에서 해당 사용자 ID를 조사해 ID가 존재한다면 "+OK" 메시지를 그렇지 않은 경우엔 "-ERR" 메시지를 클라이언트 측에 보내게 된다 그림에서 5번은 클라이언트가 서버 측에게 자신의 암호를 POP3 명령이 PASS를 사용해서 보내게 된다 그런데 이기서 문제가 발생할



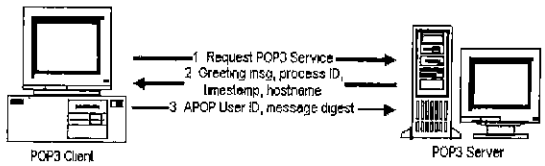
<그림 1 POP3 서버의 사용자 인증 절차>

수 있다 즉 PASS라는 명령어를 이용해서 사용자의 암호를 전송하는 경우 도청을 통해 암호를 알아낼 수 있으며, 이것은 사용자 암호가 암호화가 되지 않은 상태로 전송되기 때문이다[1]

3. 관련 연구

관련 연구로는 APOP이라는 새로운 명령어를 이용한 인증과 Kerberos 시스템을 사용하는 AUTH 인증이 있다.

APOP 인증은 challenge-response 방식을 이용한다. 이 방식은 기존의 POP3 에서 나타난 문제점인 네트웍상의 사용자 암호 노출은 해결했다 하지만 POP3 서버에서 사용자 암호를 알고 있어야만 한다[2] 즉, 사용자 암호를 plaintext로 등록을 시켜두어야 한다. 이 점은 아주 큰 문제점을 야기 시킬 수 있다 기존의 시스템에서는 사용자 암호를 Hashing function에 통과시킨 값을 가지고 있다는 것을 고려해볼 때 아주 위험한 생각이다. 하지만 이 방식을 이용하는 것은 서버의 보안이 네트웍상의 보안보다는 더욱 견고하다는 믿음과 함께, 서버에서의 보안 문제가 발생하더라도 네트웍 상에서 사용자 암호가 빠져나가는 것을 막아보자는 의도이다[2]. 아래 그림은 APOP의 인증



<그림 2. POP3 APOP 인증 절차>

절차를 나타낸 것이다. 또한 APOP의 경우 기존의 USER/PASS를 이용해서 사용자 인증을 할 수가 없다.

Kerberos를 이용하는 AUTH 방식은 아래에 나온 예처럼 인증을 위해 AUTH라는 명령어를 사용한다. 또한 이 방법은 클라이언트와 서버가 둘 다 지원하는 인증 방법을 협상할 수 있도록 한다.

Examples:
S: +OK POP3 server ready
C: AUTH KERBEROS_V4
S: + AmFYig==
C: BAcAQU5EUkVXLkNNVS5FRFUAOCAsho84kLN3/IJmrMG+25a4DT+nZImJjnTNHJUtxAA-o0KPKfHEcAFs9a3CL5Oebe/ydHJUwYFdWwuQ1MWiy6IesKvjL5rL9WjXUb9MwT9bpObYLGOK1lQh
S: + or//EoAADZI=
C: DiAF5A4gA+oOIALuBkAAmw==
S: +OK Kerberos V4 authentication successful
...
C: AUTH FOOBAR
S: -ERR Unrecognized authentication type

서버는 특별한 AUTH 유형을 제공할 필요가 없다. 즉 모든 AUTH 협상이 실패했을 때 기존의 POP3 인증 방법을 이용해서 클라이언트를 인증할 수 있다 하지만 이 방법도 클라이언트 측에서 기능을 제공하지 못하면 무용지물이다. Kerberos처럼 클라이언트와 서버가 인증을 위해 협상을 할 수는 있으나 실제 메일 클라이언트는 여러 협상 방법을 통해 인증을 하지는 않는다 그러므로 클라이언트와 서버가 기존의 POP3 서버에서 행하는 인증 방법처럼 단일화된 방법으로 인증을 하면서 암호화 기능만을 추가하는 것이 더욱 효과적일 것이라고 할 것이다. 즉, 기존의 POP3 처럼 사용자 인증을 위해 사용자의 개인 정보를 스스로 관리하지 않아도 되며, 메일 클라이언트와 서버에 암호화 기능을 추가함으로써 기존 POP3 인증 과정을 해결하고자 하는 것이다.

4. 제안한 보안 모델

4.1 적용된 관련 기술

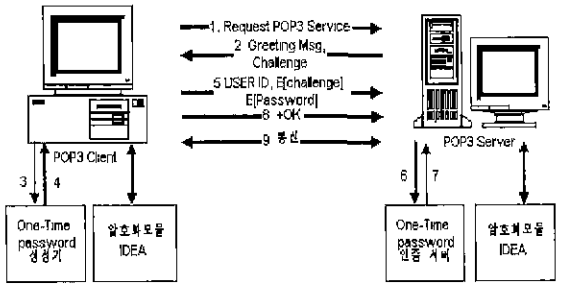
본 논문에서 안전한 인증 방법을 제공하기 위해 One-Time Password 방식을 채용했다. POP3에 인증을 받기 위해 동일한 암호를 매번 사용하는 기존의 암호 인증 시스템의 문제점은 네트웍을 통해서 POP3에 인증을 받고자 할 때 발생한다. 암호는 네트웍을 도청함으로써 쉽게 알아낼 수 있으며, 이렇게 알아낸 암호는 불법적 재사용이 가능하다. One-Time Password 시스템은 로그인 할 때마다 항상 다른 암호를 사용하도록 함으로써 이러한 문제점을 해결하고 있다 따라서 침입자가 네트웍 도청을 통해서 One-Time Password를 알아냈다 할지라도 더 이상 사용할 수 없다[9]. 또한 APOP의 경우 POP3에 사용자 정보를 두어 또 다른 보안 위험을 안고 있으나, 이 방법은 그러한 위험에서도 자유롭다 또한 한 단계 더 나아가 메시지 암호화 통신을 위한 키를 자연스럽게 분배하게 됨으로써 키 분배의 문제점도 해결할 수 있다 이러한 One-Time Password 시스템을 구현하기 위한 방법은 여러 가지가 있으나 Time-Stamp 방식을 이용하고자 하는 경우 시스템간의 동기화가 필요하여, 본 논문에서는 Challenge-Response방식을 사용한다. 클라이언트 쪽에서 인증을 요구하면, 서버는 임의의 Challenge를 생성해서 사용자에게 전송한다. 사용자는 PIN과 Challenge를 이용해서 서버에 전송할 원 타임 패스워드를 생성하고, 서버에게 Response메시지를 보낸다. 서버는 동일한 Challenge와 등록된 사용자 정보를 이용해서 원 타임 패스워드를 생성한 후 사용자가 전송한 Response와 비교하여 사용자를 인증을 하는 방식이다[2]

또한 암호화 통신을 위해 관용 암호화 방식을 사용한다 이 방식은 공개키 암호화 방식보다 상대적으로 처리 속도가 빠르며, 메시지를 암호화/복호화 하는데 사용하는 키가 동일하다는 점이다. 따라서 메시지의 암호화와 복호화를 위해 키의 분배 문제가 발생한다 본 논문에서는 One-Time Password 시스템에서 생성하는 원 타임 패스워드를 암호화 통신을 위한 비밀키로 사용함으로써 키 분배 및 관리 문제를 해결하였다. 또한 원 타임 패스워드를 관용 암호화 알고리즘의 비밀키로 사용함으로써 좀 더 향상된 안정성을 제공할 수 있을 것이다.

4.2 제안한 보안 모델

본 논문에서는 기존 인증 방법의 문제점을 제시하고 이러한 문제를 해결하기 위한 새로운 인증 방법을 제시하고 암호화 통신을 위한 키를 분배하고자 한다. 본 논문에서는 One-Time Password 방식을 이용해서 위의 문제를 막고, 암호화 통신이 가능하도록 하기 위해 관용 암호화 방식인 IDEA방식을 사용하며 IDEA의 비밀키는 One-ime Password의 세션 키를 사용했다. 그리고 APOP에서 문제점으로 지적되고 있는 사용자 암호 관련 문제를 이 논문에서는 해결하고자 한다.

아래 그림은 본 논문에서 제안하고자 하는 보안 모델에 대한 POP3 인증 절차를 그림으로 나타낸 것이다. 그림에서 1, 2번은 기존의 POP3 구조와 같이 클라이언트가 메일 서비스를 받기 위해 서버와 110번 포트를 통해 TCP 연결을 시도하는 과정을 나타낸 것이다 단지, 서버에서는 Greeting msg를 보낼 때 서버에서 생성한 Challenge를 함께 클라이언트에게 보낸다. 그러면 클라이언트에서는 사용자 ID와 Challenge를 사용해서 클라이언트 OTPc(One-Time Password)를 생성한다. 이 생성된 암호를 이용해서 Challenge와 사용자 메일 암호를 암호화한다. 그런 후 사용자 ID와 암호화된 Challenge, 그리고 암호화된 사용자 메일 암호를 함께 서버에게 보낸다. 그러면 POP3 서버는 One-Time Password 인증 서버에게 인증을 요구한다 인증 서버는 OTPs를 생성하고 암호화된 Challenge를 복호화해 서버에서 생성한 임의의 Challenge와 동일하면 사용자를 인증한다. 이렇게 함으로써 기존의 POP3 에서 PASS라는 명령어를 통해 암호를 전송할 때 발생한 문제점을 없앴다. 또한 APOP 방식과



<그림 3 제안한 POP3 인증 절차>

달리 사용자 암호를 Plaintext로 둘 필요성도 없다 또한 메시지 암호화 통신을 위해 키의 교환도 자연스럽게 이루어, APOP에서처럼 암호화 통신을 위해 새로운 키를 교환해야하는 불편한 점도 개선될 것이다 또한 암호화 통신을 위해 관용 암호화 방식의 IDEA 알고리즘을 이용했으며, 키 분배와 관리 문제는 One-Time Password System에서 생성한 키를 IDEA의 비밀키로 사용함으로써 해결했다. 즉, 키의 분배가 잘 이루어져 보낼 메시지를 암호화할 수 있는 모든 조건이 갖추어졌다 본 논문에 대한 구현 작업은 지금 진행중이다.

5. 결론

기존의 POP3 구조에서는 클라이언트가 사용자 인증을 위해 사용자 ID와 Password를 서버에게 전송해야 했고, 또한 사용자 암호에 대해 암호화가 이루어지지 않아 암호가 쉽게 노출될 수 있는 위험성이 있었으나, 본 논문에서는 사용자 인증 과정에서 나타나는 이러한 문제를 없애기 위해 기존의 PASS라는 명령어를 사용하여 사용자 암호를 서버에게 전송하는 인증 방법이 아니라 One-Time Password 방식을 이용한 사용자 인증 방법을 제시하고 구현하는 것이다. One-Time Password 방식을 구현하는 방법은 여러 가지가 있으나 이곳에서는 Challenge-Response방식을 이용하고자 한다. 또한 사용자를 인증하는 인증 절차뿐만 아니라, 클라이언트와 서버사이의 주고받는 메시지에 대한 보안도 가능하게끔 하였다. 또한 APOP 처럼 POP3에서 사용자 암호를 알 필요성도 없으며, POP3에서 사용자에 대한 정보를 관리할 필요성도 없다.

참 고 문 헌

[1] 김종희, 허 신, "사용자 정보 암호화를 이용한 Secure-POP3의 개발," 정보과학회 논문지(C) 1997.12

[2] Larry J, Hughes, Jr. "Actually Useful Internet Security Techniques", New Riders, 1995.

[3] Martin Ababi, Roger Needham, "Prudent Engineering Practice for cryptographic Protocols", SRC research report, June 1, 1994.

[4] J Myers, "Post Office Protocol - Version 3" Canegie Mellon, May 1996.

[5] 송상현 외 5인, "웹 보안을 위한 사용자 인증과 암호화 통신 구현", JCCI'97, 1997.

[6] 권도균, "WWW 보안과 전자화폐," http://sharon.comeng.chungnam ac.kr/~dolphin/ws3/content/B2/.

[7] J. Linn, "Privacy Enhancement for Internet Electronic Procedures, Oct 02 1993.

[8] N. Haller, "The S/Key One-Time Password System", RFC 1760, Bellcore, February 1995.

[9] N. Haller, "One-Time Password System", RFC 1938, Bellcore, May 1996.