SSH 를 이용한 보안 POP

Manish Singh, $<$yosh@gimp.org$>$ v1.0, 30 September 1998

임은재, eunjea@kldp.org 2000년 10월 27일

이 문서는 ssh 를 이용해 보안 POP 연결을 하는 방법을 설명한다.

목 차

제 1 절 소개

일반적인 POP 메일 연결은 매우 보안에 취약하다. 당신의 암호는 네트워크을 통해 깨끗한 텍스트(누구나 볼수 있는)로 날아간다. 공공 네트워크 (즉 대학교나 당신이 사용하는 ISP같은) 에서 누군가 당신의 암호를 알아 낼수 있는 스니퍼를 설치해 놓았는지도 모른다. 특히, 규칙적으로 메일을 첵크하는 메일첵커를 사용하는 경우 당신의 암호가 노출될 가능성은 더욱 높아진다.

이 암호로, 공격자는 당신의 메일 계정(개인정보와 기밀이 포함되 있을수 있는)에 접근할수 있으며, 또한 이 암호는 쉘 계정 암호와 동일한 경우가 많으므로, 더 많은 손실의 가능성도 있다.

우리는 이러한 단순한 암호인증(깨끗한 텍스트가 네트워크 상으로 흐르는) 대신에 암호화된 채널을 ssh 클라이언트를 통해 구현할수 있다.

APOP, KPOP, IMAP 등과 같은 보안 인증방법이 이미 있지만, ssh 를 사용하는 것은, 특별한 메일 클라이언트나 서버 지원을 필요로 하지 않는다 (서버에서 ssh 접속을 지원하는 것을 제외하고). 그리고, 또 한가지 당신의 트래픽은 ssh 에 의해 압축 전송되므로, 전화 모뎀 접속과 같은 느린 접속을 가진 사람들에게는 또 하나의 멋진 방법이다.

제 2 절 기초적인 기술

이 기술은 ssh 의 기본적인 특징중 하나이다 : *port forwarding*

당신은 ssh 클라이언트를 필요로 하는데 다음에서 구할수 있다.

`http://www.ssh.fi/` 와 미러들. RPM은 다음에서. `ftp://ftp.replay.com/pub/crypto/` 그리고 데비안 패키지는 이곳에. `ftp://non-us.debian.org/debian-non-US/` (그리고 각각의 미러들에서).

2.1 포트 포워딩 준비

포트 포워딩은 다음과 같이 한다:

```
ssh -C -f popserver -L 11110:popserver:110 sleep 5
```

이 명령에 대해 자세히 살펴 보자

`ssh`

ssh 클라이언트 실행 파일 그 자체 (모든 것을 가능케 해주는 마술 프로그램 :-)).

`-C`

이 것은 데이터 스트림의 압축을 가능하게 한다, 이것은 옵션이지만, 특히 전화 모뎀 사용자들에게는 유용하다.

`-f`

ssh 가 인증에 성공하고 포트 포워딩에 성공하고 나면, 다음 프로그램을 실행할수 있도록 백그라운드로 포크된다. 우리는 단지 ssh의 포트 포워딩 기능만을 사용할 것이므로 tty 는 필요없다.

`popserver`

우리가 접속할 POP 서버.

`-L 11110:popserver:110`

POP 서버 포트 110을 로컬 포트 11110으로 포워드 한다. 누구나 사용할수 있는 높은 숫자의 로컬 포트를 사용한다.

`sleep 5`

ssh 가 백그라운드로 포크된후, 이 명령을 실행한다. 이것은 당신의 메일 클라이언트가 로컬 포트에 접속할때 까지 접속을 유지하게 된다. 5초는 일반적으로 충분한 시간이다. (역자주: 당신의 시스템이 충분히 빠른 시스템이라면, 이 명령이 필요하지 않거나, 숫자를 줄일수 있다. 실험해 볼것)

이외에도 당신은 다른 ssh 의 적당한 옵션들을 사용할수 있다.

물론 이것은 POP 서버에서 sshd 도 지원해야 한다. 그러나 반듯이 쉘 계정을 가지고 있어야 하는 것은 아니다. 우리가 필요한 시간은 서버가 "텔넷 접속을 허용하지 않습니다"라고 표시하는 동안에도 충분히 확보할수 있다.

2.2 테스트 해보기

포트 포워딩을 위한 자세한 명령을 알아 보았다면 이제 실제로 테스트 해보자:

```
$ ssh -C -f msingh@popserver -L 11110:popserver:110 sleep 1000
```

popserver 는 POP 서버이다. 나의 로컬머신의 사용자 이름이 manish 이므로, msingh 라고 POP 사용자를 명시해 주었다. (만약 로컬과 원격 사용자 이름이 동일하다면 필요하지 않다.)

잠시후 다음과 같이 암호를 물어 올것이다:

```
msingh@popserver's password:
```

내 POP 암호를 입력 (만약 당신의 쉘 계정을 가지고 있고, 그 암호가 POP 암호와 다르다면 쉘계정의 암호를 입력해야 한다). 끝 ! 이제 다음과 같이 로컬 포트로 포워딩된 POP 서버로 접속을 해볼수 있다.

```
$ telnet localhost 11110
```

다음과 비슷한 결과를 보여야 한다:

```
QUALCOMM POP v3.33 ready.
```

꺄오! 되는데! 이제 데이터는 암호화되는 네트워크 상에 있게 된다. 유일하게 암호화 되지 않은 텍스트는 로컬 루프백 인터페이스 내 에서만 사용된다.

제 3 절 메일 소프트웨어와 같이 사용하기

이 섹션은 팝 클라이언트 소프트웨어를 ssh가 포워딩한 포트를 사용하도록 설정하는 것을 설명한다. 주된 초점은 fetchmail (에릭 레이몬드가 만든 훌륭한 프로그램) 에 맞추었다. fetchmail 은 다음에서 찾을수 있다.

http://www.tuxedo.org/\~{}esr/fetchmail/. 또한, fetchmail의 문서를 읽는 것도 당신에게 많은 도움을 줄것이다.

3.1 fetchmail 설정하기

이것은 나의 .fetchmailrc 파일이다.

```
defaults
        user msingh is manish
        no rewrite

poll localhost with protocol pop3 and port 11110:
        preconnect "ssh -C -f msingh@popserver -L 11110:popserver:110 sleep 5"
        password foobar;
```

간단하죠? fetchmail 은 이외에도 풍부한 옵션을 가지고 있으나, 여기서 중요한 것은 preconnect 와 poll 옵션이다.

우리는 POP 서버에 직접 접속않고 대신 로컬 호스트 11110 포트로 접속한다. preconnect 은 ssh 가 미리 접속을 해서 패치메일을 위해 포트 포워딩을 하고 5초동안 포트를 열어 놓는다. 이제 패치메일은 로컬 11110 포트로 접속하여 메일을 긁어오게 된다.

그래서 패치메일을 실행할때 마다, 당신은 암호입력을 해야한다. 만약 당신이 백그라운드(내가 하는 것처럼) 실행하고자 한다면, 이것은 불편하므로, 다음 섹션에서 이것을 해결하자.

3.2 모두 자동화 하기

ssh 는 사용자 인증을 여러 방법으로 할수 있다. 그중 한가지가 RSA public/private key pair 이다. 당신은 `ssh-keygen`를 사용해 인증키를 만들수 있다. 인증키는 passphrase 를 가질수 있으며, 그것은 공백일수 있다.

만약 당신의 머신이 안전하다고 생각된다면, 공백의 passpharase를 사용해라. 그리고 위와 같이 `.fetchmailrc` 를 설정한후 패치메일을 데몬모드로 실행하면 메일을 자동으로 받아올수 있다.

그러나, 만약 passphrase가 필요하다고 생각된다면, 좀더 복잡해진다. ssh 는 **agent** 에 의해 실행되어 지며, 등록키, 인증등을 ssh 접속이 이루어진 상태에서 해야한다. 그래서 나는 다음과 같은 스크립트를 사용했다.

`getmail.sh`:

```
#!/bin/sh
ssh-add
while true; do fetchmail --syslog --invisible; sleep 5m; done
```

모뎀 접속을 할때, 다음을 실행한다:

```
$ ssh-agent getmail.sh
```

이것은 나에게 passphrase를 한번 묻는다. 그리고, 매 5분마다 메일을 첵크하게 된다. 모뎀 접속이 끊어지면, ssh-agent 를 끝낸다. (나는 이것을 ip-up, ip-down 스크립트 에 넣었다.)

3.3 fetchmail을 사용하지 않는 방법

만약 패치메일을 사용하지 못하거나 사용하기 싫다면? Pine, Netscape 등의 메일 클라이언트들은 그들만의 POP 매카니즘을 가지고 있다. 그러므로, 패치메일의 사용을 고려해라! 그 편이 더 유연한 방법이다. 그리고 메일 클라이언트들은 그런 종류의 작동을 해서는 않된다. Pine 과 Netscape 은 로컬 메일 시스템을 사용하기 위해 설정될 수 있다.

그러나, 이렇게 하려면 당신의 메일 클라이언트들이 포워딩된 포트에 접속되어 있도록 충분한 여유 시간을 주어야 한다 (예를 들어 `sleep 100000000` 와 같은). 이것은 어쩌면 당신의 네트워크 관리자가 허용하지 않을지도 모른다.

두번째로, 몇몇 클라이언트 (넷스케입과 같은) 는 POP 서버의 포트가 110으로 하드 코딩되어 있다. 이것은 루트 권한으로 해당 포트로 포워딩을 해야 한다. 이것은 고민거리 이긴 하나, 작동은 할것이다.

제 4 절 기타

4.1 Disclaimer

이 문서에 대해 필자는 보증은 하지 않는다. 이것은 단지 자유로운 자원으로 제공된다.

ssh 와 같은 암호화 소프트웨어는 어떤 제한들(당신이 어디에 사는가)에 종속될지도 모른다. 어떤 나라들에서는, 당신에게 그런 소프트웨어들을 사용할 허가가 있어야 한다. 만약 당신이 이런 법률들에 대해 잘 알지 못한다면, 전문가와 상의해라.

이 문서에서 제공되는 정보의 사용은 당신의 메일 서비스 프로바이더에 의해 예기되지 않을수도 있다. 저자는 네트워크 서비스의 남용/오용을 조장하지 않고, 이 문서를 정보를 제공하는 목적으로만 제공한다. 만일 이 문서에 기술된 것이 메일 프로바이더의 서비스 합의에 위반되는지 확실하지 않다면 먼저 그것에 대해 정리할 필요가 있다.

4.2 저작권

4.3 도와주신 분들

ssh 포트 포워딩에 대해 알려준 Seth David Schoen `$<$schoen@uclink4.berkeley.edu$>$`에게 감사드린다.