Secure IMAP (and POP3)

Roberto Cecchini

Roberto.Cecchini (at) fi.infn.it

도운이

김정수

pibonazi (at) semi.korea.ac.kr

v 2.6 18 December 2000 번역**: v 1.3 12 April 2001**

이 문서는 **stunnel**을 이용하여 SSL을 지원하지 않는 IMAP이나 POP3데몬이 SSL을 이용할 수 있게 하는 방법을 소개한다. 특히 POP3접속시 로그인 이름과 암호가 패킷상에 평문으로 누출되는 약점이 있는데, 이를 극복할 수 있는 좋은 수단이 될 수 있다. 본인이 약간의 설명이나 내용을 덧붙였다. 원문은 http://security.fi.infn.it/tools/stunnel/index-en.html 에서 볼 수 있다.

1. 서론

Netscape(IMAP)와 Outlook(IMAP 과 POP3)는 메일서버에 암호화된 접속(SSL)을 지원한다. 만일 IMAP서버가 이런 종류의 접속을 지원하지 않는다면 부분적인 해결책은 SSL wrapper를 쓰는 것이다. 여러가지가 많이 있지만, 나는 stunnel (http://www.stunnel.org)을 쓴다.

2. OpenSSL 설치

첫번째 일은 OpenSSL을 설치하는 것이다.

1. `tar` 파일을 `/usr/local` 에 푼다.
2. 다음과 같은 간단한 절차를 따르라(openssl-0.9.6a 기준이다).

```
$ ./config
$ make
$ make test
$ make install
```

3. 인증서 요청과 설치

주의: 이 절차들은 **.infn.it**에만 해당되는 것이다.

1. srv.cnf (http://security.fi.infn.it/tools/stunnel/srv.cnf) 를 `/usr/local/ssl/lib/` 에 복사한다(주: 이것은 지은이의 지역적 설정으로 OpenSSL의 초기 설정 파일인 `/usr/local/ssl/openssl.cnf` 을 이용하는것이 일반적 경우다.).
2. 인증서 요청을 생성한다.

```
> cd /usr/local/ssl/certs
> /usr/local/ssl/bin/openssl req -new -nodes -out req.pem \
 -keyout key.pem -config /usr/local/ssl/lib/srv.cnf

Using configuration from /usr/local/ssl/lib/srv.cnf
Generating a 1024 bit RSA private key
.....................+++++
.........................+++++
writing new private key to 'key.pem'
-----
You are about to be asked to enter information that will be
incorporated into your certificate request.
What you are about to enter is what is called
a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
%이제 당신의 인증서 요청(certificate request)에 기록될 정보를 물어볼 때이다.
%입력될 것은 구별되는 이름(Distinguished Name) 이나 DN으로 부른다.
%당신이 입력할 항목은 몇개 되지 않으며, 기본값을 취할때는 빈칸으로 대신할수 있다.
%만일 당신이 '.'를 입력한다면, 그 항목은 공백으로 남을것이다.

Country Name (2 letter code) [IT]:                                    %2-
문자 국가코
드
INFN (accettare il default!) [INFN]:                                  %도
메인명 같은데요?
Locality Name (p.e. Firenze) []:Firenze                               %지
역명
Organization Name (p.e. Sezione di Firenze) []:Sezione di Firenze     %기
관명
Server type [Server IMAP]:          %서버타입
Server name (p.e. postino.fi.infn.it) []:postino.fi.infn.it           %서
버이름
Email Address []:cecchini@fi.infn.it

> chmod 600 key.pem
```

`key.pem` 은 서버 비밀키(private key)를 평문으로 담고 있다!

3. `req.pem` 을 인증서를 보내줄 CA로 보낸다(참고: 자필 서명 인증서 생성 (http://kldp.org/HOWTO/html/SSL-RedHat-HOWTO/ssl-redhat-howto-3.html#AEN199): 서정룡님의 번역중 일부).

4. (에디터를 이용하여) `/usr/local/ssl/certs/stunnel.pem` 를 작성하는데, 이는 서버 비밀키와 서버 인증서를 담고 있다. 하나의 빈 줄을 두 부분 사이에 삽입하고, 또하나의 빈줄을 파일 가장 밑에다 삽입하라.

   역자주: 실제적으로 한줄이 별도로 첨가되지 않아도 잘 동작하였다. 따라서 지은이의 의도는 각 부분이 끝나고 다음줄로 넘어가라는 뜻으로 받아들이면 되겠다. 다음은 `stunnel.pem`의 내용의 예이다.

```
 -----BEGIN RSA PRIVATE KEY-----
 MIICXQIBAAK-
BgQDHkqs4YDbakYxRkYXIpY7xLXDQwULR5LW7xWVzuWmmZJOtzwlP   % 서버 비밀키 부분
 7mN87g+aaiQzwXUVndaCw3Zm6cOG4mytf20jPZq0tvWnjEB3763sorpfpOe/4Vsn   %
 VBFjyQY6YdqYXNmjmzff5gTAecEXOcJ8CrPsaK+nkhw7bHUHX2X+97oMNQIDAQAB
 AoGBAMd3YkZAc9LUsig8iDhYsJuAzUb4Qi7Cppj73EBjyqKR18BaM3Z+T1VoIpQ1
 DeXkr39heCrN7aNCdTh1SiXGPG6+fkGj9HVw7LmjwXclp4UZwWp3fVbSAWfe3VRe
 LM/6p65qogEYuBRMhbSmsn9rBgz3tYVU0lDMZvWxQmUWWg7BAkEA6EbMJeCVdAYu
 nQsjwf4vhsHJTChKv/He6kT93Yr/rvq5ihIAPQK/hwcmWf05P9F6bdrA6JTOm3xu
 TvJsT/rIvQJBANv0yczI5pUQszw4s+LTzH+kZSb6asWp316BAMDedX+7ID4HaeKk
 e4JnBK//xHKVP7xmHuioKYtRlsnuHpWVtNkCQQDPru2+OE6pTRXEqT8xp3sLPJ4m
 ECi18yfjxAhRXIU9CUV4ZJv98UUbEJOEBtx3aW/UZbHyw4rwj5N511xtLsjpAkA9
 p1XRYxbO/clfvf0ePYP621fHHzZChaUo1jwh07lXvloBSQ6zCqvcF4hG1Qh5ncAp
 zO4pBMnwVURRAb/s6fOxAkADv2Tilu1asafmqVzpnRsdfBZx2Xt4oPtquR9IN0Q1
 ewRxOC13KZwoAWtkS7l0mY19WD27onF6iAaF7beuK/Va
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 MI-
IECTCCA3KgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBujELMAkGA1UEBhMCVVMx   % 인증서 부분
 EzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1NlYXR0bGUxHzAdBgNVBAoT   %
 FkJsdXJkeWJsb29wIEluZHVzdHJpZXMxFjAUBgNVBAsTDUlTIERlcGFydG1lbnQx
 ITAfBgNVBAMTGEJvbWJhc3RpYyBULiBCbHVyZHlibG9vcDEoMCYGCSqGSIb3DQEJ
 ARYZYm9tYmFzdGljQGJsdXJkeWJsb29wLmNvbTAeFw0wMDA2MDYwMDUxMTRaFw0x
 MDA2MDQwMDUxMTRaMIG6MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3Rv
 bjEQMA4GA1UEBxMHU2VhdHRsZTEfMB0GA1UEChMWQmx1cmR5Ymxvb3AgSW5kdXN0
 cmllczEWMBQGA1UECxMNSVMgRGVwYXJ0bWVudDEhMB8GA1UEAxMYQm9tYmFzdGlj
 IFQuIEJsdXJkeWJsb29wMSgwJgYJKoZIhvcNAQkBFhlib21iYXN0aWNAYmx1cmR5
 Ymxvb3AuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDHkqs4YDbakYxR
 kYXIpY7xLXDQwULR5LW7xWVzuWmmZJOtzwlP7mN87g+aaiQzwXUVndaCw3Zm6cOG
 4mytf20jPZq0tvWnjEB3763sorpfpOe/4VsnVBFjyQY6YdqYXNmjmzff5gTAecEX
 OcJ8CrPsaK+nkhw7bHUHX2X+97oMNQIDAQABo4IBGzCCARcwHQYDVR0OBBYEFD+g
 lcPrnpsSvIdkm/eol4sYYg09MIHnBgNVHSMEgd8wgdyAFD+glcPrnpsSvIdkm/eo
 l4sYYg09oYHApIG9MIG6MQswCQYDVQQGEwJVUzETMBEGA1UECBMKV2FzaGluZ3Rv
```

```
bjEQMA4GA1UEBxMHU2VhdHRsZTEfMB0GA1UEChMWQmx1cmR5Ymxvb3AgSW5kdXN0
cmllczEWMBQGA1UECxMNSVMgRGVwYXJ0bWVudDEhMB8GA1UEAxMYQm9tYmFzdGlj
IFQuIEJsdXJkeWJsb29wMSgwJgYJKoZIhvcNAQkBFhlib21iYXN0aWNAYmx1cmR5
Ymxvb3AuY29tggEAMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEEBQADgYEAwEEk
JXpVXVaFTuG2VJGIzPOxQ+X3V1Cl86y4gM1bDbqlilOUdByUEG4YfSb8ILIn+eXk
WzMAw63Ww5t0/jkO5JRs6i1SUt0Oy80DryNRJYLBVBi499WEduro8GCVD8HuSkDC
yL1Rdq8qlNhWPsggcbhuhvpbEz4pAfzPkrWMBn4=
-----END CERTIFICATE-----
```

5. `req.pem` 과 `key.pem` 을 삭제하고, `stunnel.pem` 을 보호하라 (**chmod 600**). 지금 이 파일은 서버 비밀키를 평문으로 담고 있다.

4. stunnel 설치

다음과 같이 간단한 절차를 따른다(stunnel-3.14 기준).

```
$ ./configure
$ make
$ make install
```

5. 서버에서의 stunnel

stunnel을 데몬으로서 작동할 것을 권한다. 부트시에 다음 명령들을 이용한다. (두번째 명령은 오직 POP3 연결이 필요할 때만 이용한다.)

```
stunnel -d 993 -p /usr/local/ssl/certs/stunnel.pem -r localhost:imap
stunnel -d 995 -p /usr/local/ssl/certs/stunnel.pem -r localhost:pop
```

역자주: 여기서 **-d** 옵션과 **-r**옵션이 병행하는 것을 주의해 볼 필요가 있다. -d 옵션은 주어진 포트에 대하여 데몬모드로 작동하라는 뜻인데 예를 들어 POP3에서는 995번 포트를 감시하다가, SSL접속이 되면 그 내용을 복호화하여 pop3포트로 포워딩한다. 이 방법의 경우 반드시 상응하는 데몬도 같이 작동하고 있어야 하며 - 포워딩할 포트가 있어야 한다 - 모든 사용자가, SSL을 이용한 접속을 한다는 가정이 없기 때문에 그다지 효과적이지 못하다. 여기서 **-l**옵션을 이용한 두번째 방법을 생각해 본다.

```
stunnel -d 993 -p /usr/local/ssl/certs/stunnel.pem -l /usr/sbin/imapd
stunnel -d 995 -p /usr/local/ssl/certs/stunnel.pem -l /usr/sbin/ipop3d
stunnel -d 995 -p /usr/local/ssl/certs/stunnel.pem -
l /usr/local/lib/popper -- popper qpopper -s
```

이것은 주어진 포트를 감시하다가 접속되면, 그 내용을 복호화하여 **-l** 이 지정한 프로그램에 넘기라는 뜻이다. 여기서는 포워딩할 포트가 따로 필요없어 앞의 방법보다 효과적이다. Qualcomm (http://www.qualcomm.com)사의 qpopper처럼 실행할 프로그램이 옵션이 필요한 경우 3번째 예제처럼 **--** 뒤에 옵션을 준 완전한 형태로 쓰면 된다.

-L 옵션도 존재하는데, 차이점은 **-l** 옵션은 inetd 타입의 프로그램(ipop3d등)을 실행할때 사용되는 특별한 경우를 뜻한다. **-L**옵션의 경우 local pty를 열고 프로그램을 실행한다.

6. E-Mail 클라이언트(Unix) 설정

SSL을 지원하는 클라이언트(Netscape Messanger, Outlook, Pine etc)들에 대해서 오직 해 주어야 할 일은 그것들이 보안 접속(Secure connection)을 할 수 있도록 설정을 해 주는 것이다.

역자주: Netscape Messanger는 (v4.75까지)서버에 POP3접속시 SSL을 지원하지 않는다(설정의 SSL은 보내는 메일 서버의 설정이다).

여기서는 브라우저들이 서버 인증서를 발급한 CA의 인증서를 포함하는가의 여부는 꼭 필요하지 않다. 물론 서버 인증서를 포함한다면 더 좋다.

SSL을 지원하지 않는 메일 클라이언트들에 대해서는 다음과 같이 설정한다.

1. stunnel을 클라이언트에 설치한다.
2. 만일 당신이 서버 인증서(옵션이지만, 권한다)를 확인하기를 원한다면 서버 CA 인증서를 `/usr/local/ssl/certs/CAcert.pem` 에 복사한다. 그리고

```
> cd /usr/local/ssl/certs/
> ln -s CAcert.pem `/usr/local/ssl/bin/openssl x509 \ -noout -
hash < CAcert.pem`.0
```

3. 다음 명령으로 stunnel을 구동한다(통상적으로 시스템을 구동할때이다).

```
> stunnel -c -v 2 -d 143 -r imap_server:993
> stunnel -c -v 2 -d 110 -r pop3_server:995
```

여기서 **-v 2** 옵션은 2번(서버 인증서 확인시)에만 해당된다.

역자주: **-c**는 클라이언트 모드를 나타낸다. 클라이언트 모드에서는 **-d** 와 **-r**에 할당되는 포트 번호가 서버의 경우와 반대임을 볼 수 있다. **-d** 에서 할당된 포트에서 나오는 내용을 암호화하여 **-r**로 할당된 포트로 포워딩한후 서버와 통신을 한다고 이해하면 되겠다.

4. e-mail클라이언트가 imap(또는 pop3) 포트를 확인할 수 있도록 설정하라.

7. E-mail 클라이언트(Windows) 설정

SSL을 지원하는 클라이언트(예: Netscape Messanger, Outlook, Pine)들에 대해서 오직 해 주어야 할 일은 그것들이 보안 접속(Secure connection)을 할 수 있도록 설정을 해 주는 것이다.

역자주: Netscape Messanger는 (v4.75까지)서버에 pop3접속시 SSL을 지원하지 않는다(설정의 SSL은 보내는 메일 서버의 설정이다). Outlook Express 5는 서버에 POP3접속시 SSL을 지원한다.

여기서는 브라우저들이 서버 인증서를 발급한 CA의 인증서를 포함하는가의 여부는 꼭 필요하지 않다. 물론 서버 인증서를 포함한다면 더 좋다.

SSL을 지원하지 않는 메일 클라이언트들에 대해서는 다음과 같이 설정한다.

1. stunnel을 클라이언트에 설치한다.

   a. `winstun.zip` (http://security.fi.infn.it/stunnel/tools/winstun.zip) 을 다운로드한다.

   b. `ssleay32.dll`, `libeay32.dll`, `stunnel.exe` 을 같은 디렉토리에 푼다(원한다면 `dll`파일들은 `\windows\system`으로 옮겨도 된다).

2. stunnel을 다음 명령을 이용하여 실행하여라.

```
stunnel -c -d 143 -r imap_server:993
stunnel -c -d 110 -r pop3_server:995
```

3. e-mail클라이언트가 imap(또는 pop3) 포트를 확인할 수 있도록 설정하라.