基于 Qmail+LDAP 的大规模邮件系统的安全设计*

陈 三 忠
(深圳大学现代教育技术与信息中心, 广东 深圳 518060)

摘 要: 讨论了基于 LDAP 的 Qmail 平台的安全邮件系统的实现和应用问题。首先介绍了 SSL/TLS (安全套接字层/安全传输层) 的模型, 分析并给出了基于 LDAP 的 POP、SMTP、IMAP 的邮件服务协议安全的解决方法, 讨论了 LDAP 协议的安全设计等相关问题。运用 Stunnel 和 OpenSSL 等开源软件包实现安全设计。

关键词: SSL/TLS; LDAP; Qmail; 认证
中图分类号: TP393.08 文献标识码: A 文章编号: 0529-6579 (2002) S1-0035-03

邮件在 Internet 中传输过程中有两个重要数据要防止被窃听: 邮件本身和用户密码。用户在下载邮件和 MTA 之间传输邮件都有被窃听的机会, 因为邮件系统本身默认的是明文传输方式。超大规模邮件系统一般由服务器群组成, 包括数个甚至数十个 SMTP、POP、IMAP、LDAP 等服务器, 构成高可用、高容量、可容错、可负载均衡的邮件系统, 服务器之间的信任连接和用户邮件的安全传输的问题是值得研究和分析。本文以基于 LDAP 认证的 Qmail 邮件系统平台为例, 给出 POP3、IMAP、SMTP、LDAP 的安全传输的具体实现。

1 SSL/TLS 的介绍

SSL (Secure Socket Layer) 是 NetScape 公司设计的主要用于 web 的安全传输协议。这种协议在 WEB 上获得了广泛的应用。IETF (http://www.ietf.org) 将 SSL 作了标准化, 即 RFC2246, 并将其称为 TLS (Transport Layer Security), 从技术上讲, TLS1.0 与 SSL3.0 的差别非常微小。为加强数据的传输安全, 特别是敏感的口令数据的传输安全, 可采用公开密钥算法对传输数据进行加密。对 SMTP、POP、IMAP 和 LDAP 协议的传输, 可使用 SSL/TLS (安全套接字层/安全传输层), 保证数据传输的安全, 通过在 SMTP、POP 服务器上安装 CA, 保证服务器之间的相互鉴别, 防止假冒的服务器。

1.1 SSL/TLS 主要提供下面功能

数据加密: 客户机/服务端 session 的加密;

服务器的身份鉴定: 客户机可以鉴定服务器的真实性;

客户机的身份鉴定: 服务器可以鉴定客户机的真实性;

数据的完整性: 保证数据在传输过程中不会被修改, 防止受到 "man in the middle" 式的攻击。

1.2 SSL 的协议结构

SSL 是一个介于应用协议与 TCP 之间的一个可选层, 其位置大致如下:

POP IMAP SMTP HTTP LDAP

SSL

TCP

IP

以 http 为例, 如果利用 SSL 协议来访问网页, 其步骤如下:

用户: 在浏览器的地址栏里输入 https://www.xxx.com

HTTP 层: 将用户需求翻译成 HTTP 请求, 如

GET /index.htm HTTP/1.1
Host www.sslserver.com

* 收稿日期: 2002-03-21
作者简介: 陈三忠 (1968-), 男, 工程师; E-mail: chensz@21cn.com

SSL 层：借助下层协议的的信道安全的协商出一份加密密钥，并用此密钥来加密 HTTP 请求。TCP 层：与 web server 的 443 端口建立连接，传递 SSL 处理后的数据。接收端与此过程相反。SSL 在 TCP 之上建立了一个加密通道，通过这一层的数据经过了加密，因此达到保密的效果。

下面要用到 OpenSSL（http://www.openssl.org），它是 SSL 协议的执行库的开放源码，它包括了 SSL 库文件和一些加密工具。

2 邮件协议的安全传输

2.1 POP Over SSL/TLS

POP 的默认端口是 110，对应的加密端口是 995，首先在 POP 服务器上安装 stunnel（http://stunnel.mirt.net）：

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

然后，在 POP 服务器上运行 stunnel，下面给出运行示例：

```
#!/bin/sh
exec /usr/local/bin/tcpserver -R -v -c 50 \
        -l pop3.szu.edu.cn \
        192.168.0.3 995 \
        /usr/local/sbin/stunnel -f \
        -p /etc/ssl/stunnel.pem \
        -l /var/qmail/bin/qmail-popup -- qmail
        -popup \
        pop3.example.com \
        /var/qmail/bin/auth pop \
        /var/qmail/bin/qmail-pop3d Maildir 2>&1
```

2.2 SMTP Over SSL/TLS

在 SMTP 服务器安装 stunnel，参见上面方法，以下给出 SMTP Over SSL 的运行示例：

```
#!/bin/sh
QMAILDUID=`id -u qmaild`
NOFILESGID=`id -g qmaild`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
exec /usr/local/bin/softlimit -m 2000000 \
    /usr/local/bin/tcpserver -v -R -l 0 -x /etc/tcp.smtp.cdb -c "$MAXSMTPD" \
    -u "$QMAILDUID" -g "$NOFILESGID" 0 smtp /usr/local/sbin/stunnel -p -f
/etc/pem/smtp.pem -N smtp -l/var/qmail/bin/qmail-smtpd 2>&1
```

2.3 IMAP Over SSL/TLS

我们的 IMAP 服务器采用 Courier-IMAP（http://www.inter7.com/courierimap）软件包，它支持 SSL，还需要在 IMAP 服务器上安装了 OpenSSL 和 stunnel 软件包。

stunnel 通过侦听 IMAPS 端口（port 993：IMAP over SSL），将数据解密再转发至 143 端口，实现 IMAP Over SSL/TLS，首先确认 /etc/services 中是否有如下内容，没有则添加：

```
imap 143/tcp #imap4
imaps 993/tcp #imap4 over SSL
```

安装 stunnel，并启动：

```
#stunnel -d 993 -r 143
```

现在，客户端就可以通过 IMAPS 协议与 IMAP 服务器实现 IMAP over SSL。

3 目录服务的安全设计 LDAP Over SSL

基于 SSL 的 ldap 协议称为 ldaps，OpenLDAP1 仅支持 LDAP v2，而 LDAP v2 不支持 SSL/TLS（包括其它一些加密机制），在 master 和 slave 之间，Ldap Server 和 Ldap Client 之间数据是明文传输，那么很容易通过侦听通讯，被有心人获得关键数据和密码；OpenLDAP2 支持 LDAP v2 和 LDAP v3，LDAP v3 相对于 LDAP v2 最重要的是添加了对传输层安全（TLS，Transport Layer Security）的支持及增加了认证方法 SASL。

为了使得 OpenLDAP1 支持密文传输，我们可以通过外部程序 stunnel，进行 SSL tunnelling。

3.1 OpenLDAP1 下的 SSL/TLS

首先安装 OpenSSL：

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

再安装 stunnel；

stunnel 使用的 CA（Certification Authority）：

```
/usr/local/ssl/certs/stunnel.pem
```

stunnel.pem 通过下面步骤生成：

```
$ openssl req -new -x509 -days 365 -nodes -
        config stunnel.cnf \
        -out stunnel.pem -keyout stunnel.pem
```

```
$ openssl gendh 512 >> stunnel.pem
```

成功安装完毕，启动 slapd：

```
# /usr/local/libexec/slapd
```

启动 stunnel：

```
# /usr/local/sbin/stunnel -r ldap -d 636 \
-p /usr/local/ssl/certs/stunnel.pem
```

LDAPS 通常使用 636 端口。

在客户端模式下，需要启动：

```
# stunnel -c -d 636 -r ldapserver.yourorg.com:636
```

这样，客户端与服务端之间实现 LDAP Over SSL。

另外，slurpd 本身并没有 SSL 的能力，在 master 上需要使用客户端的模式：

```
# stunnel -c -d 9636 -r ldapreplica.yourorg.com:636
```

在 master LDAP server 的 slapd.conf，设置：

```
replica host=localhost:9636
```

3.2 OpenLDAP2 下的 SSL/TLS

对于 OpenLDAP2，因其本身就支持 StartTLS [RFC2830] 和 LDAP over SSL (ldaps://)，首先安装 OpenSSL，在编译 OpenLDAP 时加入对 SSL 的支持，就可以实现 Over SSL：

编译安装支持 TLS 的 OpenLDAP：

```
env CPPFLAGS=-I/usr/local/ssl/include LDFLAGS=-L/usr/local/ssl/lib \
./configure --with-tls
make depend
make
make test
make install
```

启动基于 SSL 的 LDAP 服务：

```
./slapd -d1 -h "ldaps://0.0.0.0/"
```

这样，ldap 服务器就实现了对 SSL/TLS 的支持。OpenLDAP2 的 slurpd 支持 Start TLS。

当然，为了密码的更安全，你甚至可以采用 Kerberos 认证，将用户密码放在 Kerberos 数据库中，其它的信息譬如 uid、homedirectory、mailMessageStore、mailHost 等等放在 LDAP 的数据库中，MIT Kerberos V 可以帮助你实现这个目的。

参考文献：

[1] http://www.linux.org/docs/ldp/howto/LDAP-Implementation-HOWTO/index.htmlLdap Implementation HOWT Roelvan Meer Giuseppe Lo Biondo

[2] http://web.mit.edu/kerberos/www/

[3] http://www.lifewithqmail.org/ldap/

[4] http://rfc.net/rfc2830.html LDAPv3: Extension for Transport Layer Security

[5] http://www.openldap.org

[6] http://www.openssl.org

[7] http://www.inter7.com/courierimap/

[8] http://stunnel.mirt.net

Security of the Large Scale Email Service Application Based on Qmail and LDAP

CHEN San-zhong

(Education Technology and Information Center,
Shenzhen University, Guangdong, Shenzhen 518060, China)

Abstract: This paper discusses the security of the large scale email service application based on Qmail and LDAP. Firstly, the author focuses on the targets, principles, and security strategy based on open SSL and SSL tunnelling technology, and how to settle such as POP and SMTP and IMAP protocol over SSL, etc.

Key words: SSL/TLS; LDAP; Qmail; authentication