Columbia Linux User's Group

Jason W. Dixon

7/14/04

Introduction

- Purpose
  - Secure Email Transmission
  - Proof of Identity (Authentication)
  - Defended Resources (Bandwidth, Storage, etc)
- Goals
  - Full Authentication/Encryption between Clients and Server
  - Security with Convenience
  - “Hands-off” Operational Design
  - Protection without Intervention

Layered Design

- SMTP/TLS
- RBL/SBL
- Content Filtering
- Virtual Users
- POP/IMAP/TLS
- Webmail/SSL

Mail Delivery (SMTP)

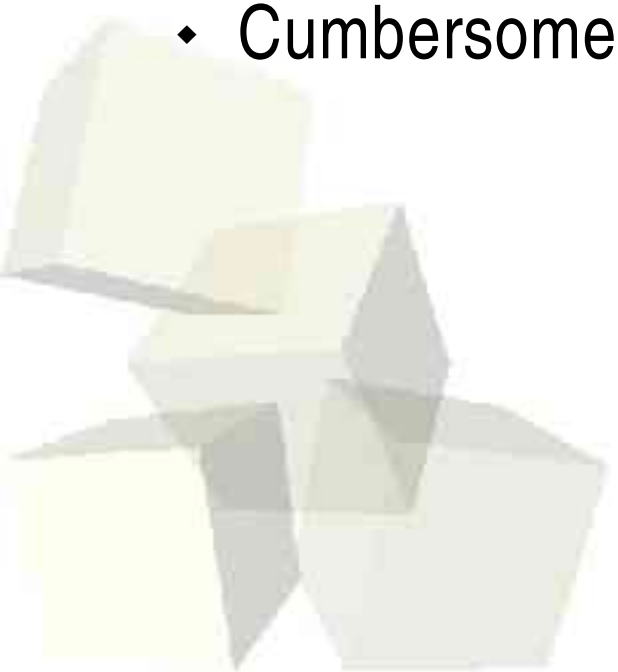
- Postfix
- Virtual Users w/MySQL
- Cyrus-SASL (SMTP AUTH)
- OpenSSL
- PostfixAdmin (User Administration)
- Source/Content Filtering

Postfix

- Fast, Secure, Simple
- Sendmail compatible
- Supports Procmail
- Maildir or mbox
- Chroot-able
- Real-time Blackhole Lists (RBL)
- Blacklisting (deny by source)
- Whitelisting (approve by source)
- Greylisting (acting on peer behavior)

- Cyrus-SASL
  - Authentication Library
  - Supports passwd, pam, krb4, sasldb, SQL, LDAP, authdaemond, others
- OpenSSL
  - Free
  - Self-signed Certificates
  - Might require manual client import unless signed by root CA
- Virtual Users w/MySQL
  - No shell accounts
  - Easy to Administer
  - Can be difficult to enforce quotas

- Amavisd-new
  - MTA interface to content checkers
  - Secure, Modular, Fast
  - Can modify mail headers
  - Chroot-able
  - Black/white/grey-listing
  - Cumbersome configuration
- SpamAssassin
  - Header Analysis
  - Text Analysis
  - Supports RBL/SBL's
  - Supports distributed hash databases like Vipul's Razor
- Vipul's Razor
  - Distributed Hash Database
  - Collaborative
  - Very Effective



Courier-IMAP

- Supports POP3/IMAP and TLS/SSL
- Authdaemond supports passwd, PostgreSQL, MySQL, CRAM/MD5, LDAP, others
- Can use same SSL cert as Postfix
- Maildir only
- Easy Configuration

- PostfixAdmin
  - Requires PHP, Apache, MySQL
  - Fast, Simple
  - Doesn't support quotas

Installation

```
####################
Cyrus-SASL
####################

tar zxf cyrus-sasl-2.1.18.tar.gz
cd cyrus-sasl-2.1.18/

./configure --disable-checkapop --disable-otp \
--disable-srp --disable-krb4 --disable-gssapi \
--disable-anon –with-authdaemond=/var/run/courier-imap

make

make install

rm -rf /usr/lib/sasl2

ln -s /usr/local/lib/sasl2/ /usr/lib/sasl2

echo '/usr/local/lib' >> /etc/ld.so.conf

ldconfig
```

Installation (cont'd)

```
####################
Courier-IMAP
####################

useradd jason
passwd jason
su jason -
cd

mkdir $HOME/rpm
mkdir $HOME/rpm/SOURCES
mkdir $HOME/rpm/SPECS
mkdir $HOME/rpm/BUILD
mkdir $HOME/rpm/SRPMS
mkdir $HOME/rpm/RPMS
mkdir $HOME/rpm/RPMS/i386

echo "%_topdir    $HOME/rpm" >> $HOME/.rpmmacros

rpmbuild -ta courier-imap-3.0.3.20040424.tar.bz2

sudo rpm -ivh /home/jason/rpm/RPMS/i386/courier*rpm
```

Installation (cont'd)

```
####################
Postfix
####################

useradd postfix
groupadd postdrop
tar zxf postfix-2.1.0.tar.gz
cd postfix-2.1.0/

make -f Makefile.init makefiles 'CCARGS=-DHAS_MYSQL \
-I/usr/include/mysql' 'AUXLIBS=-L/usr/lib/mysql \
-lmysqlclient -lz -lm' 'CCARGS=-DHAS_PCRE \
-I/usr/include/pcre' 'AUXLIBS=-L/usr/lib -lpcre' \
'CCARGS=-DUSE_SASL_AUTH -I/usr/local/include/sasl' \
'AUXLIBS=-L/usr/local/lib -lsasl2'

make

make install

... continued ...
```

Installation (cont'd)

(Questions during make install)

```
install_root: [/]
tempdir: [/tmp]
config_directory: [/etc/postfix]
daemon_directory: [/usr/libexec/postfix]
command_directory: [/usr/sbin]
queue_directory: [/var/spool/postfix]
sendmail_path: [/usr/sbin/sendmail]
newaliases_path: [/usr/bin/newaliases]
mailq_path: [/usr/bin/mailq]
mail_owner: [postfix]
setgid_group: [postdrop]
html_directory: [no]
manpage_directory: [/usr/man]
readme_directory: [no]
```

Installation (cont'd)

```
####################
Clamav
####################

http://dag.wieers.com/packages/clamav/
rpm -ivh clamav*rpm clamav-db*rpm clamd*rpm
chkconfig clamd on
service clamd start


####################
SpamAssassin
####################

http://dag.wieers.com/packages/spamassassin/
rpm -ivh spamassassin*rpm
chkconfig spamassassin on
service spamassassin start


####################
Vipul's Razor
####################

http://dag.wieers.com/packages/razor-agents/
rpm -ivh razor-agents*rpm
```

Installation (cont'd)

```
####################
Amavisd-new
Prerequisites
####################

http://dag.wieers.com/packages/perl-Archive-Zip/
http://dag.wieers.com/packages/nomarch/
http://dag.wieers.com/packages/arc/
http://dag.wieers.com/packages/unarj/
http://dag.wieers.com/packages/unrar/
http://dag.wieers.com/packages/zoo/
http://dag.wieers.com/packages/lzo/
http://dag.wieers.com/packages/lzop/
http://dag.wieers.com/packages/freeze/

rpm -ivh perl-Archive-Zip*rpm nomarch*rpm arc*rpm \
unarj*rpm unrar*rpm zoo*rpm lzo*rpm freeze*rpm

... continued ...
```

- Installation (cont'd)

```
Manual perl modules:

Compress::Zlib
IO::Zlib
Archive::Tar
IO::Stringy
Mail-Tools
Unicode::Map
Unicode::String
MIME-Tools
Convert::TNEF
Convert::UUlib
MIME::Base64
Net::Server
Net::SMTP
Digest::MD5
Time::HiRes
Unix::Syslog

tar zxf <package>.tar.gz
cd <package>
perl Makefile.PL
make && make test && make install
```

- Installation (cont'd)

```
####################
Amavisd-new
####################

http://www.ijs.si/software/amavisd/#download
tar zxf amavisd-new-20030616-p10.tar.gz
cd amavisd-new-20030616

cp amavisd /usr/local/sbin/
cp amavisd.conf /etc/

echo '/usr/local/sbin/amavisd start' >> /etc/rc.local
```

Installation (cont'd)

```
####################
PostfixAdmin
####################

http://high5.net/postfixadmin/
tar zxf postfixadmin-2.0.4.tgz
mv postfixadmin-2.0.4/ /var/www/html/postfixadmin

chown -R apache:apache /var/www/html/postfixadmin

chmod 640 /var/www/html/postfixadmin/*.[php|css]
chmod 640 /var/www/html/postfixadmin/admin/*.[php|css]
chmod 640 /var/www/html/postfixadmin/users/*.[php|css]
chmod 640 /var/www/html/postfixadmin/templates/*.[php|css]

mysql -p < /var/www/html/postfixadmin/DATABASE.TXT
```

- Installation (cont'd)

```
####################
Squirrelmail
####################

http://www.squirrelmail.org/download.php
tar zxf squirrelmail-1.4.2.tar.gz
mv squirrelmail-1.4.2/ /var/www/html/squirrelmail

cd /var/www/html/squirrelmail/conf
perl conf.pl

... continued ...
```

- Installation (cont'd)

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Server Settings

General
-------
1.  Domain                 : dixongroup.net
2.  Invert Time            : false
3.  Sendmail or SMTP       : Sendmail

A.  Update IMAP Settings   : localhost:143 (courier)
B.  Change Sendmail Config : /usr/sbin/sendmail

R   Return to Main Menu
C.  Turn color on
S   Save data
Q   Quit

Command >>
```

Configuration Examples – Postfix (main.cf)

```
... snip ...

mydestination = localhost.$mydomain, $myhostname
home_mailbox = Maildir/
virtual_gid_maps = static:501
virtual_mailbox_base = /var/spool/postfix/virtual
virtual_alias_maps = mysql:/etc/postfix/mysql_virtual_alias_maps.cf
virtual_mailbox_domains = mysql:/etc/postfix/mysql_virtual_domains_maps.cf
virtual_mailbox_maps = mysql:/etc/postfix/mysql_virtual_mailbox_maps.cf
virtual_mailbox_limit = 51200000
virtual_minimum_uid = 501
virtual_transport = virtual
virtual_uid_maps = static:501
smtpd_use_tls = yes
smtpd_tls_key_file = /etc/postfix/mailkey.pem
smtpd_tls_cert_file = /etc/postfix/mail_signed_cert.pem
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_sasl_auth_enable = yes
smtpd_sasl_local_domain = $myhostname
smtpd_sasl_security_options = noanonymous
smtpd_client_restrictions =
   check_sender_access hash:/etc/postfix/sender_access,
   permit_sasl_authenticated
smtpd_recipient_restrictions =
   check_recipient_access hash:/etc/postfix/recipient_access,
   permit_mynetworks,
   permit_sasl_authenticated,
   reject_unauth_destination
```

Configuration Examples – Postfix (master.cf)

```
... snip ...

# The amavisd-new interface
#
smtp-amavis unix -      -       -       -       2       smtp
        -o smtp_data_done_timeout=1200
        -o disable_dns_lookups=yes

127.0.0.1:10025 inet n  -       -       -       -       smtpd
        -o content_filter=
        -o local_recipient_maps=
        -o relay_recipient_maps=
        -o smtpd_restriction_classes=
        -o smtpd_client_restrictions=
        -o smtpd_helo_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o mynetworks=127.0.0.0/8

... snip ...
```

Configuration Examples – Postfix (Virtual Users)

```
# mysql_virtual_alias_maps.cf
user = postfix
password = postfix
hosts = 127.0.0.1
dbname = postfix
table = alias
select_field = goto
where_field = address

# mysql_virtual_domains_maps.cf
user = postfix
password = postfix
hosts = 127.0.0.1
dbname = postfix
table = domain
select_field = description
where_field = domain

# mysql_virtual_mailbox_maps.cf
user = postfix
password = postfix
hosts = 127.0.0.1
dbname = postfix
table = mailbox
select_field = maildir
where_field = username
```

Configuration Examples – Postfix (MySQL schema)

```
CREATE TABLE admin (
  username varchar(255) NOT NULL default '',
  password varchar(255) NOT NULL default '',
  created datetime NOT NULL default '0000-00-00 00:00:00',
  modified datetime NOT NULL default '0000-00-00 00:00:00',
  active tinyint(4) NOT NULL default '1',
  PRIMARY KEY  (username),
  KEY username (username)
) TYPE=MyISAM COMMENT='Postfix Admin - Virtual Admins';

CREATE TABLE alias (
  address varchar(255) NOT NULL default '',
  goto text NOT NULL,
  domain varchar(255) NOT NULL default '',
  created datetime NOT NULL default '0000-00-00 00:00:00',
  modified datetime NOT NULL default '0000-00-00 00:00:00',
  active tinyint(4) NOT NULL default '1',
  PRIMARY KEY  (address),
  KEY address (address)
) TYPE=MyISAM COMMENT='Postfix Admin - Virtual Aliases';

... continued ...
```

Configuration Examples – Postfix (MySQL schema)

```
CREATE TABLE domain (
  domain varchar(255) NOT NULL default '',
  description varchar(255) NOT NULL default '',
  aliases int(10) NOT NULL default '-1',
  mailboxes int(10) NOT NULL default '-1',
  maxquota int(10) NOT NULL default '-1',
  created datetime NOT NULL default '0000-00-00 00:00:00',
  modified datetime NOT NULL default '0000-00-00 00:00:00',
  active tinyint(4) NOT NULL default '1',
  PRIMARY KEY  (domain),
  KEY domain (domain)
) TYPE=MyISAM COMMENT='Postfix Admin - Virtual Domains';

CREATE TABLE domain_admins (
  username varchar(255) NOT NULL default '',
  domain varchar(255) NOT NULL default '',
  created datetime NOT NULL default '0000-00-00 00:00:00',
  active tinyint(4) NOT NULL default '1',
  KEY username (username)
) TYPE=MyISAM COMMENT='Postfix Admin - Domain Admins';

... continued ...
```

Configuration Examples – Postfix (MySQL schema)

```
CREATE TABLE log (
  timestamp datetime NOT NULL default '0000-00-00 00:00:00',
  username varchar(255) NOT NULL default '',
  domain varchar(255) NOT NULL default '',
  action varchar(255) NOT NULL default '',
  data varchar(255) NOT NULL default '',
  KEY timestamp (timestamp)
) TYPE=MyISAM COMMENT='Postfix Admin - Log';

CREATE TABLE mailbox (
  username varchar(255) NOT NULL default '',
  password varchar(255) NOT NULL default '',
  name varchar(255) NOT NULL default '',
  maildir varchar(255) NOT NULL default '',
  quota int(10) NOT NULL default '-1',
  domain varchar(255) NOT NULL default '',
  created datetime NOT NULL default '0000-00-00 00:00:00',
  modified datetime NOT NULL default '0000-00-00 00:00:00',
  active tinyint(4) NOT NULL default '1',
  PRIMARY KEY  (username),
  KEY username (username)
) TYPE=MyISAM COMMENT='Postfix Admin - Virtual Mailboxes';
```

- Configuration Examples – Cyrus-SASL (smtpd.conf)

```
pwcheck_method: authdaemond
authdaemond_path: /var/run/authdaemon.courier-imap/socket
```

Configuration Examples – Amavisd-new (amavisd.conf)

```
... snip ...

$sa_local_tests_only = 0;   # (default: false)
$sa_auto_whitelist = 1;    # turn on AWL (default: false)
$sa_timeout = 30;           # timeout in seconds for a call to SpamAssassin
$sa_mail_body_size_limit = 150*1024; # don't waste time on SA if mail is larger
$sa_tag_level_deflt  = 1.0; # add spam info headers if at, or above that level
$sa_tag2_level_deflt = 3.0; # add 'spam detected' headers at that level
#$sa_kill_level_deflt = $sa_tag2_level_deflt; # triggers spam evasive actions
$sa_kill_level_deflt = 5.5; # triggers spam evasive actions
$sa_dsn_cutoff_level = 10;  # spam level beyond which a DSN is not sent,
$sa_spam_subject_tag = '***SPAM*** ';   # (defaults to undef, disables)
$sa_spam_modifies_subj = 0; # may be a ref to a lookup table, default is true

@av_scanners = (
['Clam Antivirus-clamd',
  \&ask_daemon, ["CONTSCAN {}\n", "/var/amavis/clamav/clamd.socket"],
  qr/\bOK$/, qr/\bFOUND$/,
  qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
);

@av_scanners_backup = (
  ['Clam Antivirus - clamscan', 'clamscan',
    '--stdout --disable-summary -r {}', [0], [1],
    qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],
);
```

- Configuration Examples – SpamAssassin (/etc/mail/spamassassin/local.cf)

```
# These values can be overridden by editing ~/.spamassassin/user_prefs.cf
# (see spamassassin(1) for details)

# These should be safe assumptions and allow for simple visual sifting
# without risking lost emails.

required_hits 5
rewrite_subject 1
subject_tag [SPAM]
report_safe 0
```

- Configuration Examples – Courier-IMAP (authdaemonrc)

```
authmodulelist="authpwd authmysql"
authmodulelistorig="authcustom authcram authuserdb authldap authpgsql authmysql authpwd"
daemons=5
version="authdaemond.mysql"
authdaemonvar=/var/run/courier-imap
```

Configuration Examples – Courier-IMAP (authmysqlrc)

```
MYSQL_USERNAME          postfix
MYSQL_DATABASE          postfix
MYSQL_CRYPT_PWFIELD     password
MYSQL_UID_FIELD         '501'
MYSQL_GID_FIELD         '501'
MYSQL_USER_TABLE        mailbox
MYSQL_LOGIN_FIELD       username
MYSQL_MAILDIR_FIELD     maildir
MYSQL_NAME_FIELD        name
MYSQL_OPT               0
MYSQL_PASSWORD          postfix
#MYSQL_PORT             0
MYSQL_QUOTA_FIELD       quota
MYSQL_SERVER            127.0.0.1
MYSQL_SOCKET            /var/lib/mysql/mysql.sock
MYSQL_HOME_FIELD        '/var/spool/postfix/virtual'
```

Configuration Examples – Courier-IMAP (imapd)

```
... snip ...

ADDRESS=127.0.0.1
PORT=143
MAXDAEMONS=40
MAXPERIP=8
PIDFILE=/var/run/imapd.pid
TCPDOPTS="-nodnslookup -noidentlookup"
AUTHMODULES="authdaemon"
# DEBUG_LOGIN=0   - turn off login debugging
# DEBUG_LOGIN=1   - turn on login debugging
# DEBUG_LOGIN=2   - turn on login debugging + log passwords too
DEBUG_LOGIN=0
IMAP_CAPABILITY_TLS="$IMAP_CAPABILITY AUTH=PLAIN"
IMAP_DISABLETHREADSORT=0
IMAP_CHECK_ALL_FOLDERS=0
IMAP_TRASHFOLDERNAME=Trash
IMAP_EMPTYTRASH=Trash:7
IMAP_MOVE_EXPUNGE_TO_TRASH=0
HEADERFROM=X-IMAP-Sender
IMAPDSTART=YES

... snip ...
```

Configuration Examples – Courier-IMAP (imapd-ssl)

```
SSLPORT=993
SSLADDRESS=0
SSLPIDFILE=/var/run/imapd-ssl.pid
IMAPDSSLSTART=YES
IMAPDSTARTTLS=TLS
IMAP_TLS_REQUIRED=1
COURIERTLS=${bindir}/couriertls
TLS_PROTOCOL=SSL3
TLS_STARTTLS_PROTOCOL=TLS1
TLS_CERTFILE=/etc/courier-imap/courier.crt
TLS_VERIFYPEER=NONE
```

Configuration Examples – Courier-IMAP (pop3d)

```
PIDFILE=/var/run/pop3d.pid
MAXDAEMONS=40
MAXPERIP=4
AUTHMODULES="authdaemon"
AUTHMODULES_ORIG="authdaemon"
DEBUG_LOGIN=0
POP3AUTH="LOGIN CRAM-SHA1"
POP3AUTH_ORIG="LOGIN CRAM-MD5 CRAM-SHA1"
POP3AUTH_TLS="LOGIN PLAIN"
POP3AUTH_TLS_ORIG="LOGIN PLAIN"
PORT=110
ADDRESS=0
TCPDOPTS="-nodnslookup -noidentlookup"
POP3DSTART=NO
```

Configuration Examples – Courier-IMAP (pop3d-ssl)

```
SSLPORT=995
SSLADDRESS=0
SSLPIDFILE=/var/run/pop3d-ssl.pid
POP3DSSLSTART=YES
POP3_STARTTLS=YES
POP3_TLS_REQUIRED=1
COURIERTLS=${bindir}/couriertls
TLS_PROTOCOL=SSL3
TLS_STARTTLS_PROTOCOL=TLS1
TLS_CERTFILE=/etc/courier-imap/courier.crt
TLS_VERIFYPEER=NONE
```

THE END

Thanks for attending!