LCA 2005

Fighting spammers with Exim and SA-Exim

http://marc.merlins.org/linux/talks/SA-Exim/

Marc MERLIN
marc_soft@merlins.org

The problem

- Do we really need to describe it?
- Spam Sucks!
- Fishing attacks can be very dangerous with unsuspecting users
- No, I didn't send you that windows virus, I don't run windows. Don't bounce it back to me.
- More generally, Joe Jobs
- Why would I know anything about it?

Why Exim?

- Sendmail could do it, but config sucks (also had other problems with speed and queue handling, although it's better now)
- Qmail? Go away troll (qmail accepts everything at SMTP time, frozen in time (1996?), dead code.
- Postfix is a quite good MTA with a definitely more secure model, but that model is a tradeof on speed and SMTP time functionality vs Exim (although postfix is slowly catching up)

What can you do about it?

- You can refuse a lot of junk and rejecting very little real mail, just by tuning exim
- You can mess with spammers with high volume senders by just putting a few delays in the SMTP responses (15s)
- Annoy people probing you, and prevent open http relays from sending mail through you:

```
# How many bad commands trigger a connection clause (exim 4.11 or better)
# (you need at least 4 for a STARTTLS session)
smtp_accept_max_nonmail = 7

# Number of unknown SMTP commands we accept before dropping the connection
smtp_max_unknown_commands = 1
```

```
# Extended callouts appeared in exim 4.11
# If a host is broken, for instance by refusing NULL mail froms, we bounce
# all their mail until they fix it. Let's only remember this for 5m
# (default is 3h)
callout_domain_negative_expire = 5m
# The usefulness of this option is unknown to me, default is 7d
callout_domain_positive_expire =  7d
# How long you cache a failed callout (default is 2h, but I prefer to not
# penalize someone who just fixed his mail)
callout_negative_expire = 5m
# How long we cache an address that was successfully checked. Let's not overload
# remote servers for nothing, 1 week should be enough (default is 1 day)
callout_positive_expire = 7d
# What random local part we use for testing (that way, you can find out hosts
# that accept any local part because they don't do SMTP time address
# verification
callout_random_local_part = callout-check-$primary_host_name-$tod_epoch

# This returns informative error messages when we reject Email based on
# syntax or other header checks (like exim 3 used to do by default)
smtp_return_error_details = true

# The maximum size of headers for a mail
header_maxsize = 128k

# The maximum size of a single header line
header_line_maxsize = 7k
```

Exim4 ACLs, a godsend

- Exim4 can apply ACLs at each phase of the SMTP connection
- SMTP connect / SMTP AUTH / VRFY / EXPN / STARTTLS / HELO / MAIL FROM / RCPT TO / DATA
- We apply ACLs after RCPT TO and DATA so that we can have as much information about the sender as possible, which we can then log if we reject the mail. Also, some broken MTAs don't properly deal with a rejection after HELO or MAIL FROM
- For instance, we reject bad HELO values after RCPT TO to know who the mail was from and who it was for

HELO checking

```
# In RCPT TO ACL:
  deny     message         = HELO/EHLO required by SMTP RFC
           condition       = ${if eq{$sender_helo_name}{}{yes}{no}}
           delay           = TEERGRUBE

## Forged HELOs

  deny     message         = Forged IP detected in HELO (it's mine) - $sender_helo_name
           hosts           = !+relay_from_hosts
           log_message     = Forged IP detected in HELO: $sender_helo_name
           condition       = ${if eq{$sender_helo_name}{$interface_address}{yes}{no}}
           delay           = TEERGRUBE

  deny     message         = Invalid domain or IP given in HELO/EHLO
          !condition       = ${if match{$sender_helo_name}{\\\.}{yes}{no}}
           delay           = TEERGRUBE

# If the user HELOs with an IP, we check it against the connecting IP's rev hostname
  deny    message          = Forged IP detected in HELO - $sender_helo_name != $sender_host_address
           hosts           = !+relay_from_hosts
           condition     = ${if match{$sender_helo_name}{\N^\d+(\.\d+){3}$\N} {yes}{no}}
           condition     = ${if eq{$sender_helo_name}{$sender_host_address} {no}{yes}}
           delay           = TEERGRUBE

  deny    message          = Forged hostname detected in HELO - $sender_helo_name
           # accept helo which is in local_domain if we relay or had smtp auth
           hosts           = !+relay_from_hosts
            !authenticated = *
           log_message     = Forged hostname detected in HELO - $sender_helo_name
           condition       = ${if match_domain{$sender_helo_name}{+local_domains} {yes}{no}}
           delay           = TEERGRUBE
```

Dictionary Attacks

```
  deny     message         = Only one recipient accepted for NULL sender
           senders         = :
           condition       = ${if >{$rcpt_count}{1} {1}}
           delay           = TEERGRUBE

.ifdef ALLOWEDRCPTFAIL
  drop    message= too many unknown users (${eval:$rcpt_fail_count+1} failed recipients)
           log_message     = Dictionary attack (${eval:$rcpt_fail_count+1} failed recipients).
          # remove 2 to match the actual number of max failed recipients requested
           condition       = ${if >{$rcpt_fail_count}{${eval:ALLOWEDRCPTFAIL-2}} {1}{0}}
          # we need to run the drop rule first, but add the last delay here
           delay           = ${eval:FAILEDRCPTDELAY*$rcpt_fail_count}s
           domains         = +local_domains
           hosts           = !+relay_from_hosts
          !authenticated = *
.endif

       # This won't work the 1st time: $rcpt_fail_count is incremented later
  deny     message         = unknown user
           log_message     = Teergrube: dictionary attack (${eval:$rcpt_fail_count+1} failed recipients)
           condition       = ${if >{$rcpt_fail_count}{0} {1}{0}}

          # In teergrube mode, we listen forever and delay more and more
          # delay the sender because people who do dictionary attacks can
          # reconnect and try again, so let's slow them down
           delay           = ${eval:FAILEDRCPTDELAY*$rcpt_fail_count}s
           domains         = +local_domains
          !verify   = recipient
```

Teergrubing

- Your resources vs the sender's
- On failure, try to hold the connection open as long as you can and/or just reply slowly on any error

```
   # Blacklist of envelope senders
  deny    senders         = +denyenvsenders
          message         = Sender $sender_address is blocked: ${lookup{$sender_address}
lsearch*@{BLOCKENVSEND1}{$value}{"unspecified reason"}}
          delay           = TEERGRUBE
```

```
captain.process@bananalotto.fr  "go away"

butlerc@pacbell.net       "I do not communicate with people who use permission-based e-
mail filtering tools."

.*@ebuyer.com             "what part of no spam didn't you understand?"
```

SMTP callouts: callbacks

- Invented by Philip Hazel in Exim 3.20 in November 2000 independently from Ian Jackson in SAUCE somewhat earlier
- Not specifically designed for anti-spam, but very useful for that too
- Do your env and header from addresses exist?
- Can I bounce to your env from later?
- Can my users reply to your header from?
- Callouts: callbacks vs callforwards. Callforwards go to you from one outside MX to an inside authoritative MX. Callbacks go to the sender

SMTP callbacks/callouts: Random

Callbacks work like this: lookup the MX(es) for the domain of the envelope/header from, and try to connect back to attempt a fake delivery (we first check if the server would accept anything, and cache the results either way)

```
Connecting to smtp5.domain.tld [10.10.10.10]:25 ... connected
220 smtp.domain.tld ESMTP
HELO mail1.merlins.org
250 smtp.domain.tld Hello magic.merlins.org [209.81.13.136], pleased to meet you
MAIL FROM:<>
250 2.1.0 <>... Sender ok
553 5.5.3 <callout-check-mail1.merlins.org-1109701303@domain.tld>... Invalid
RSET
250 2.0.0 Reset state
MAIL FROM:<>
250 2.1.0 <>... Sender ok
RCPT TO:<merlin@domain.tld>
250 2.1.5 <merlin@domain.tld>... Recipient ok
QUIT
```

SMTP callbacks/callouts: NoRandom

Some sites like yahoo try to stifle dictionary attacks by accepting any RCPT TO, but yet do reject known fake/abused yahoo Emails to save up on backend processing. Incidentally, they still help with SMTP callbacks.
You need to configure Exim to skip random callbacks with them

```
Connecting to mx3.mail.yahoo.com [64.156.215.7]:25 ... connected
220 YSmtp mta241.mail.scd.yahoo.com ESMTP service ready
HELO mail1.merlins.org
250 mta241.mail.scd.yahoo.com
MAIL FROM:<>
250 null sender <> ok
RCPT TO:<merlin@yahoo.com>
250 recipient <merlin@yahoo.com> ok
QUIT
```

SMTP callbacks/callouts: open accept

Other sites run unhelpful MTAs like qmail that are unable to verify recipients and accept everything, or an MTA that isn't authoritative for the list of recipients (offsite backup MX. This is where you would configure Exim callforwards)
These sites render SMTP callbacks mostly useless :(

```
HELO mail1.merlins.org
250
MAIL FROM:<>
250 null sender <> ok
RCPT TO:<callout-check-mail1.merlins.org-1109701443@domain.tld>
250 recipient <callout-check-mail1.merlins.org-1109701443@domain.tld> ok
```

SMTP callbacks/callouts: in action

mail from: police@fbi.gov
250 OK
rcpt to: marc@merlins.org
550-Verification failed for <police@fbi.gov>
550-Called: 204.11.0.66
550-Sent: RCPT TO:<police@fbi.gov>
550-Response: 550 <police@fbi.gov>: Recipient address rejected: This service is temporarily unavailable. Please contact the recipient via other means.
550 Sender verify failed

mail from: xdkpelaqc@madtui.com
250 OK
rcpt to: marc@merlins.org
451-could not connect to ns.madtui.com [8.7.146.81]: Connection refused
451-Could not complete sender verify callout for <xdkpelaqc@madtui.com>.
451-The mail server(s) for the domain may be temporarily unreachable, or
451-they may be permanently unreachable from this server. In the latter case,
451-you need to change the address or create an MX record for its domain
451-if it is supposed to be generally accessible from the Internet.
451 Talk to your mail administrator for details.

SMTP callbacks/callouts: Config

```
# Now, do basic address checking, that we forgo if the receipient is in a
# whilelist
deny    hosts           = !+localadds:!+hosts_disable_callback:*
        sender_domains = !+envdomain_disable_callback:!+domains_callback_norandom:*
        local_parts     = !+noenvfromcallback
       !verify = sender/callout=90s,random
       # We check a random address so that we know not to bother doing further
       # callbacks against sites that accept all addresses
        delay           = TEERGRUBE

# We do a separate callback for special hosts that we want to do callback
# on but that prevent random from working (yahoo for instance will refuse
# an RCPT on a known spammer, but will otherwise accept RCPT TOs non
# existing addresses (in an attempt to prevent dictionnary attacks against
# their user DB)
deny    hosts = !+localadds:!+hosts_disable_callback:*
        sender_domains = +domains_callback_norandom
        local_parts     = !+noenvfromcallback
       !verify = sender/callout=90s
        delay           = TEERGRUBE
```

SMTP callbacks/callouts: Caveats

- web site confirmation Emails
- bounces from internal unbounceable sources (mailer-daemon@you.cant.reach.this.domain.tld)
- postmaster callbacks: too many sites don't have postmasters anymore, too many false positives :(
- Idiots who block null envelope froms

```
220-rocmail.com ESMTP MDaemon 3.5.6 ready
220-RocSoft does not allow you to relay mail. No FakeMail
220-No SPAM, No USBE, No Telnet, Tchuessie!
220
helo foo
250 rocmail.com Hello foo, pleased to meet you
mail from: <>
550 Sorry, this server is configured to refuse this sort of mail (to combat the SPAM problem)
quit
221 See ya in cyberspace
```

Greylisting: Basics

- Greylisting tuplets are a combination of connecting IP, envelope From, envelope To
- Basic greylisting works by sending a 45x (temporary failure) to each tuplet that we haven't seen recently
- Each greylisted tuplet is then whitelisted, saved on disk, and we rely on the sender being a real MTA, and to try resending the mail later
- whitelisted tuplets are eventually cleaned up
- Basic greylisting suffers from a few problems, the biggest ones being all new mail being delayed, and mail from broken senders like legit send only websites, being lost.

SMTP time hints for SA

- You could use callbacks for scoring instead of rejection
- Same for errors like no reverse DNS for connecting IP
- You don't necessarily want to reject mail on DNS blacklists either (especially bl.spamcop.net)
- SA does support DNS blacklists, but you can give it other SMTP time hints that it can't otherwise know

```
warn   message = X-Broken-Reverse-DNS: no DNS for IP address $sender_host_address
       !verify = reverse_host_lookup
```

Combining tests for rejection

- What if we only decided on rejection after combining many tests, like SpamAssassin does
- But we want to do this at SMTP time, so that we can reject the mail then (no joe jobs)
- We also want to be able to save a copy of each rejected mail to study them and/or look for possible false positives
- Enter SA-Exim

SA-Exim Basics

- http://marc.merlins.org/linux/exim/sa.html
- SA-Exim was one of the first (the first?) implementations of SA at SMTP time with the goal of SMTP time filtering
- Runs after DATA and temp/permrejects there if appropriate
- Can use all the Exim and SA rejection/anti-spam hints
- Greylisting at the same time
- Teergrubing
- Optionally save mails with a certain score

SA-Exim Benefits

- No joe jobs, but notification to false positive senders since you send an SMTP time rejection
- Rejecting at SMTP time, even in DATA instead of RCPT TO, does get you off some spammer's lists.
- It becomes fairly safe to reject spams instead of filing them in a separate folder, since rejecting spams becomes joe job safe and can still save a copy for safety
- SA + greylisting: a marriage made in heaven
  - greylisting without the delays
  - No problem with VERP mailing lists (ever changing tuplet)
  - don't delay SMTP callbacks and your outgoing mail (greylisting at DATA, not RCPT To)
  - Save/capture Emails from broken servers that only send once

SA-Exim Caveats

- MS Exchange and others are stupid: 550 after RCPT TO or DATA can be interpreted as user unknown. The helpful error string we send back is discarded
  - at least they get some notification / mostly safe after DATA?
- There are rumours that some somewhat legitimate SMTP servers do not check/wait for a return code after sending their “.” in DATA
  - those are typically the same servers that wouldn't process any kind of rejection anyway
- Usual greylisting caveats: mail delays and some pseudo-legits senders never resend
  - at least SA-Exim doesn't greylist and delay most Email
  - send once and ignore RFCs senders can be an acceptable loss

SA-Exim Setup: Checklist

- You need Exim 4.11 or better, with the dynamically loadable local_scan (default in most linux deb or rpm packages), or SA-Exim compiled within your Exim source
- SA-Exim works with just about any SpamAssassin, although SA 3.0 or better is recommended for Greylisting (SA-Exim ships with an SA 3.0 module, and you won't have to patch your copy of SA)
- SA-Exim uses spamc to talk to SA, so it is completely independent from the SA code base, but you need spamc/spamd installed (technically a bit slower, but more flexible/independent from spamd versions)

SA-Exim Setup: Exim & SA

- Setup spamd to run with no privileges, without access to users' home directories, and give it its own location

```
spamd --max-children 50 --daemonize --username=nobody
        --nouser-config –helper-home-dir=/var/spool/spamassassin/
```

- If you are using modularized local_scan, tell exim to use sa-exim.so (works out of the box on debian)

```
local_scan_path = /usr/lib/exim4/local_scan/sa-exim.so
```

- Configure SA to output the right headers:

```
report_safe             0
use_terse_report        1                       # for SA < 3.x
rewrite_subject         1
subject_tag             SPAM: _HITS_:

add_header              all Report _REPORT_     # for SA > 3.0
rewrite_header          Subject SPAM: _HITS_:
```

SA-Exim Setup: Exim4.conf

- Configure Exim to interface with SA-Exim:

```
localpartlist nosarej = CONFDIR/acls/destwhitelist

# check_rcpt ACL:
  warn     message       = X-SA-Do-Not-Rej: Yes
           local_parts   = +nosarej:postmaster:abuse

  warn     message       = X-SA-Do-Not-Run: Yes
           hosts         = +relay_from_hosts

  warn     message       = X-SA-Do-Not-Run: Yes
           authenticated= *

# You'll want to strip SA headers for messages that aren't local
# This means you should strip them at least in the remote_smtp transport
#
# Let's remove these headers if the message is sent remotely
headers_remove = "X-SA-Do-Not-Run:X-SA-Exim-Scanned:X-SA-Exim-Mail-From:X-SA-
Exim-Rcpt-To:X-SA-Exim-Connect-IP"

# On most multiuser systems, you'll probably also want to remove
# X-SA-Exim-Rcpt-To on all local deliveries to protect Bcc privacy
```

SA-Exim Setup: SA-Exim.conf

```
# X-SA-Exim-Rcpt-To on all local deliveries to protect Bcc privacy
SAEximRunCond: ${if and {{def:sender_host_address} {!eq {$sender_host_address}
{127.0.0.1}} {!eq {$h_X-SA-Do-Not-Run:}{Yes}} } {1}{0}}
SAEximRejCond: ${if !eq {$h_X-SA-Do-Not-Rej:}{Yes} {1}{0}}

SAmaxbody: 256000
SATruncBodyCond: 0
SARewriteBody: 0

SAteergrube: 25.0
SAteergrube: ${if and { {!eq {$sender_host_address}{204.80.101.251}} {!eq
{$sender_host_address}{216.109.84.130}} } {25.0}{1048576}}
SAteergrubetime: 900
SAteergrubeSavCond: 1
SAteergrubesave: /var/spool/sa-exim/SAteergrube

SApermreject: 11.0
SAtempreject: 3.0
SAtemprejectoverwrite: 1

SAgreylistiswhitestr: GREYLIST_ISWHITE
SAgreylistraisetempreject: 6.5

SAspamacceptsave: /var/spool/sa-exim/SAspamaccept
```

SA-Exim In Action: Teergrubing

```
helo
mail from
rcpt to
data
354 Enter message, ending with "." on a line by itself
(...)
Spam message with spam keywords and/or blacklisted stuff
.
451- wait for more output
451- wait for more output
(... one line every 10 secs, 15 minutes elapse ...)
450 Please try again later
```

- but.... spammers have become wiser: many have built in timeouts and won't wait longer than 20-30 seconds
- they also don't resend typically
- that said, it's good news for greylisting: if they don't resend, we don't get the spam. If they do, we delay them.

SA-Exim In Action: Log Samples

SA: Action: Not running SA because SAEximRunCond expanded to false (Message-Id: 1D8kXQ-00075S-Cn). From <merlin@mydomain.org> (local) for justincfi@email.com

SA: Action: check skipped due to message size (1543640 bytes) and SATruncBodyCond expanded to false (Message-Id: 1D8klD-0008PW-9A). From <nicomaster69@yahoo.com> (host=web30908.mail.mud.yahoo.com [68.142.200.161]) for vincent@domain.tld

SA: Action: scanned but message isn't spam: score=-6.2 required=7.0 (scanned in 7/7 secs | Message-Id: E1D8kCT-00056S-NP@webatwork5.cheapdomainsuk.com). From <nobody@webatwork5.cheapdomainsuk.com> (host=216-239-45-4.google.com [216.239.45.4]) for marc_bts@mydomain.org

SA: Debug: Writing message to /var/spool/sa-exim/SAtempreject/new/20050308113004.gxusaxnjms@homepostal.com
SA: Action: temporarily rejected message: score=9.0 required=7.0 trigger=3.0 (scanned in 18/18 secs | Message-Id: 20050308113004.gxusaxnjms@homepostal.com). From <n.1199.6148271@homepostal.com> (host=mail13.homepostal.com [208.53.12.45]) for xavier@domain.tld

SA: Debug: Writing message to /var/spool/sa-exim/SApermreject/new/1110309009_20050308190940.71ED2580134E@smtp.efrei.fr
SA: Action: permanently rejected message: score=38.9 required=7.0 trigger=11.0 (scanned in 18/18 secs | Message-Id: 20050308190940.71ED2580134E@smtp.efrei.fr). From <49NJNQR@aisp.net> (host=smtp.efrei.fr [194.2.204.37]) for marcefrei@mydomain.org

SA: Debug: Writing message to /var/spool/sa-exim/SAteergrube/new/RSDWZZHANNKFKETQKFSYKCRN@yahoo.com
SA: Action: teergrubed sender for 30 secs until it closed the connection: score=50.0 required=7.0 trigger=25.0 (scanned in 18/18 secs | Message-Id: RSDWZZHANNKFKETQKFSYKCRN@yahoo.com). From <fiuczl@hananet.net> (host=NULL [222.121.213.138]) for marc_f@mydomain.org

SA-Exim In Action: Greylisting by Example

3 delivery attempts during greylisting:

2005-03-07 15:31:29 1D8Rgy-0005sE-9P SA: Debug: Writing message to /var/spool/sa-exim/SAtempreject/new/422CE42E.00001E.03440@PASCAL
2005-03-07 15:31:29 1D8Rgy-0005sE-9P SA: Action: temporarily rejected message: score=5.4 required=7.0 trigger=3.0 (scanned in 8/8 secs | Message-Id: 422CE42E.00001E.03440@PASCAL). From <noble.p@domain2.tld> (host=postfix3-2.domain2.tld [213.228.0.169]) for vincent@domain.tld
2005-03-07 15:31:43 1D8RhF-0004yK-2j SA: Debug: Writing message to /var/spool/sa-exim/SAtempreject/new/422CE42E.00001E.03440@PASCAL
2005-03-07 15:31:43 1D8RhF-0004yK-2j SA: Action: temporarily rejected message: score=5.4 required=7.0 trigger=3.0 (scanned in 9/9 secs | Message-Id: 422CE42E.00001E.03440@PASCAL). From <noble.p@domain2.tld> (host=postfix1-c.domain2.tld [213.228.0.79]) for vincent@domain.tld
2005-03-07 15:50:19 1D8RzF-00065j-EC SA: Debug: Writing message to /var/spool/sa-exim/SAtempreject/new/422CE42E.00001E.03440@PASCAL
2005-03-07 15:50:19 1D8RzF-00065j-EC SA: Action: temporarily rejected message: score=5.4 required=7.0 trigger=3.0 (scanned in 9/9 secs | Message-Id: 422CE42E.00001E.03440@PASCAL). From <noble.p@domain2.tld> (host=postfix1-c.domain2.tld [213.228.0.79]) for vincent@domain.tld

Successful delivery after trying more than 30mn later:

2005-03-07 16:15:37 1D8SNj-0005LN-O9 SA: Action: scanned but message isn't spam: score=3.9 required=7.0 (scanned in 8/8 secs | Message-Id: 422CE42E.00001E.03440@PASCAL). From <noble.p@domain2.tld> (host=postfix1-c.domain2.tld [213.228.0.79]) for vincent@domain.tld

SA-Exim In Action: Greylisting Config

SpamAssassin config:

```
loadplugin Greylisting /usr/share/perl5/Mail/SpamAssassin/Plugin/Greylisting.pm
header GREYLIST_ISWHITE eval:greylisting("( 'dir' => '/var/spool/sa-exim/tuplets'; 'method' => 'dir';
'greylistsecs' => '1800'; 'dontgreylistthreshold' => 11; 'connectiphdr' => 'X-SA-Exim-Connect-IP';
'envfromhdr' => 'X-SA-Exim-Mail-From'; 'rcpttohdr' => 'X-SA-Exim-Rcpt-To'; 'greylistnullfrom' => 1;
'greylistfourthbyte' => 0 )")
describe GREYLIST_ISWHITE The incoming server has been whitelisted for this recipient and sender
score GREYLIST_ISWHITE  -1.5
priority GREYLIST_ISWHITE 99999
```

Whitelist tuplet:

```
magic:/var/spool/sa-exim/tuplets/213/228/0/noble.p@domain2.tld# cat vincent@domain.tld
1110238289
Status: Whitelisted
Last Message-Id: <422CE42E.00001E.03440@PASCAL>
Whitelisted Count: 1
Query Count: 4
SA Score: 5.355
```

What's missing / TODO

- Get a full featured exim config that you can tweak from http://marc.merlins.org/linux/exim/#conf
- If you care about viruses/malware, you could/should configure exiscan too
- For SA-Exim:
  - Go beyond SURBL, and greylist body URLs
  - Do per-user SA runs with the exiscan 45x trick

Are you a good sysadmin,
or programmer?

Need a job?
(Silicon Valley, Sydney, Santa Monica, Zürich, New York, India)

Email: marc_jo@merlins.org

Questions