

Introduction of the S25R anti-spam system

ASAMI Hideo

deo@gabacho-net.jp

<http://www.gabacho-net.jp/en/anti-spam/>

Aug 29, 2009

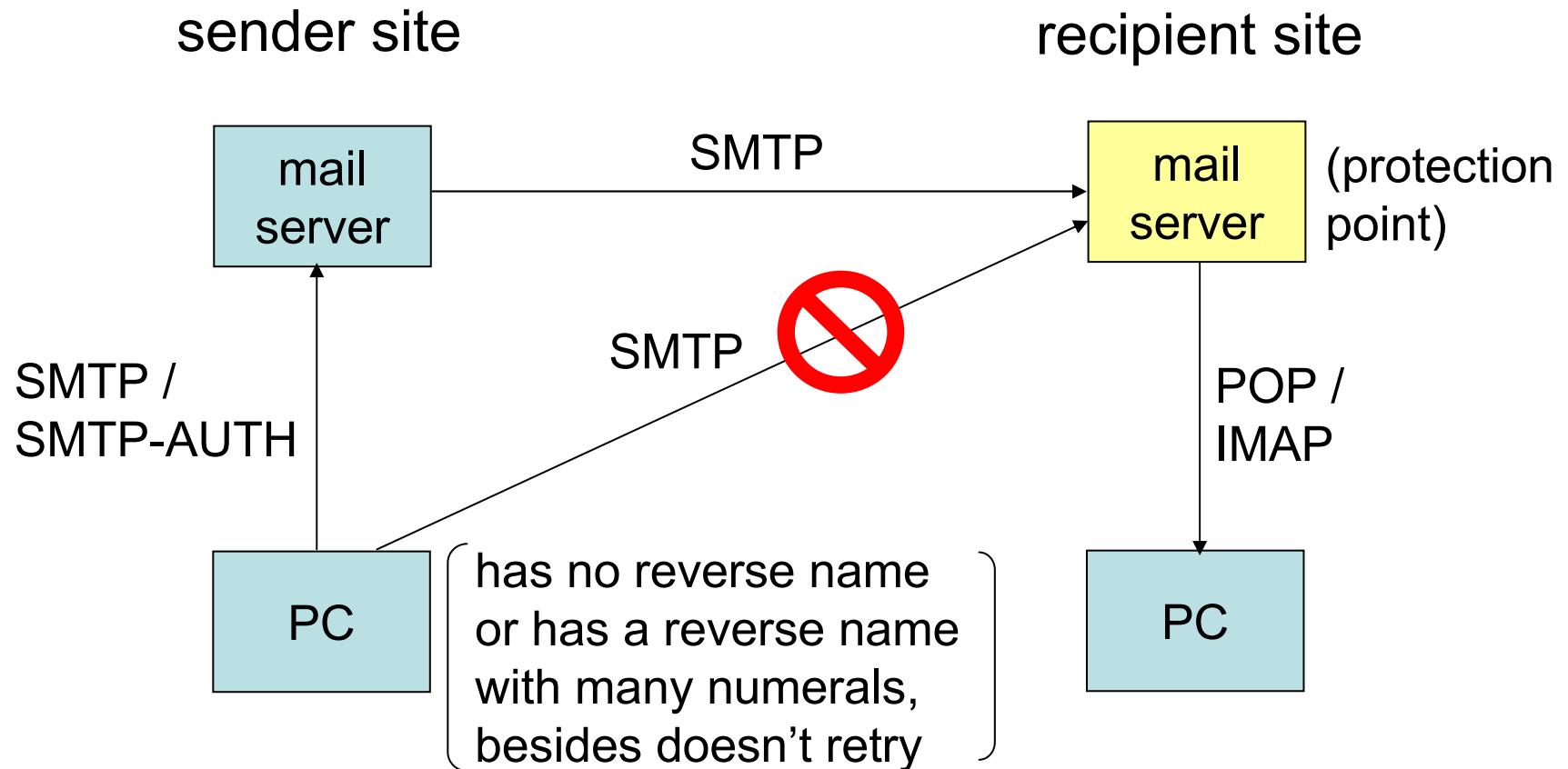
What is S25R?

The **S**elective SMTP **R**ejection Anti-spam System
(port **25**)

Gist of the action

- Rejects receiving mail returning a retry request (response code “450”) when the client host is supposed to be an end-user’s computer being based on its reverse name.
- Receives mail by whitelisting the host when a mail server is misidentified and so retry accesses are found.

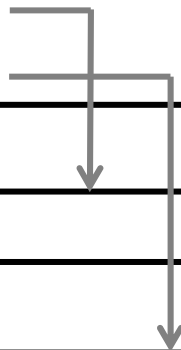
Concept of mail route restriction



How to configure

/etc/postfix/main.cf

```
smtpd_client_restrictions =  
  permit_mynetworks,  
  check_client_access regexp:/etc/postfix/white_list,  
  check_client_access regexp:/etc/postfix/rejections
```



/etc/postfix/white_list

```
permission conditions for mail servers misidentified
```

/etc/postfix/rejections

```
rejection conditions for end-user's computers not blocked by the following conditions  
/^unknown$/ 450 reverse lookup failure, be patient  
/^[^.]*[0-9][^0-9.]+[0-9].*¥./ 450 S25R check, be patient  
/^[^.]*[0-9]{5}/ 450 S25R check, be patient  
/^( [^.] +¥. )?[0-9][^.] *¥. [^.] +¥. . +¥. [a-z]/ 450 S25R check, be patient  
/^[^.]*[0-9]¥. [^.] * [0-9] - [0-9] / 450 S25R check, be patient  
/^[^.] * [0-9] ¥. [^.] * [0-9] ¥. [^.] +¥. . +¥. / 450 S25R check, be patient  
/^(dhcp|dialup|ppp|[achrsvx]?dsl) [^.] * [0-9] / 450 S25R check, be patient
```

Examples of blocked host names

unknown

evrtwa1-ar3-4-65-157-048. evrtwa1. dsl-verizon. net

pcp04083532pcs. levtwn01. pa. comcast. net

398pkj. cm. chello. no host. 101. 169. 23. 62. rev. coltfrance. com

wbar9. chi1-4-11-085-222. dsl-verizon. net

d5. GtokyoFL27. vectant. ne. jp

dhcp0339. vpm. resnet. group. upenn. edu PPPbf708. tokyo-ip. dti. ne. jp

Comparison of spam blocking rates

DNSBL	50--60%?
E-mail reputation	about 70%
Bayesian filter	80--90%
S25R	97--99%

You must NOT ...

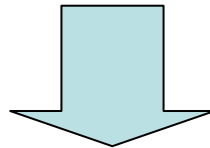
- specify “REJECT” (the response code “554”).
- leave retry accesses without watching the mail log.
 - * Retry period is 5 days by default setting of Postfix or sendmail (= given period for acceptance).
 - * Some mail servers stop retry in about 2 days.
 - * It is hard to accept mail servers which stop retry in about an hour. It is recommended to install the published white list or greylisting (such as Rgrey).

False positive rate

about 13% without a white list

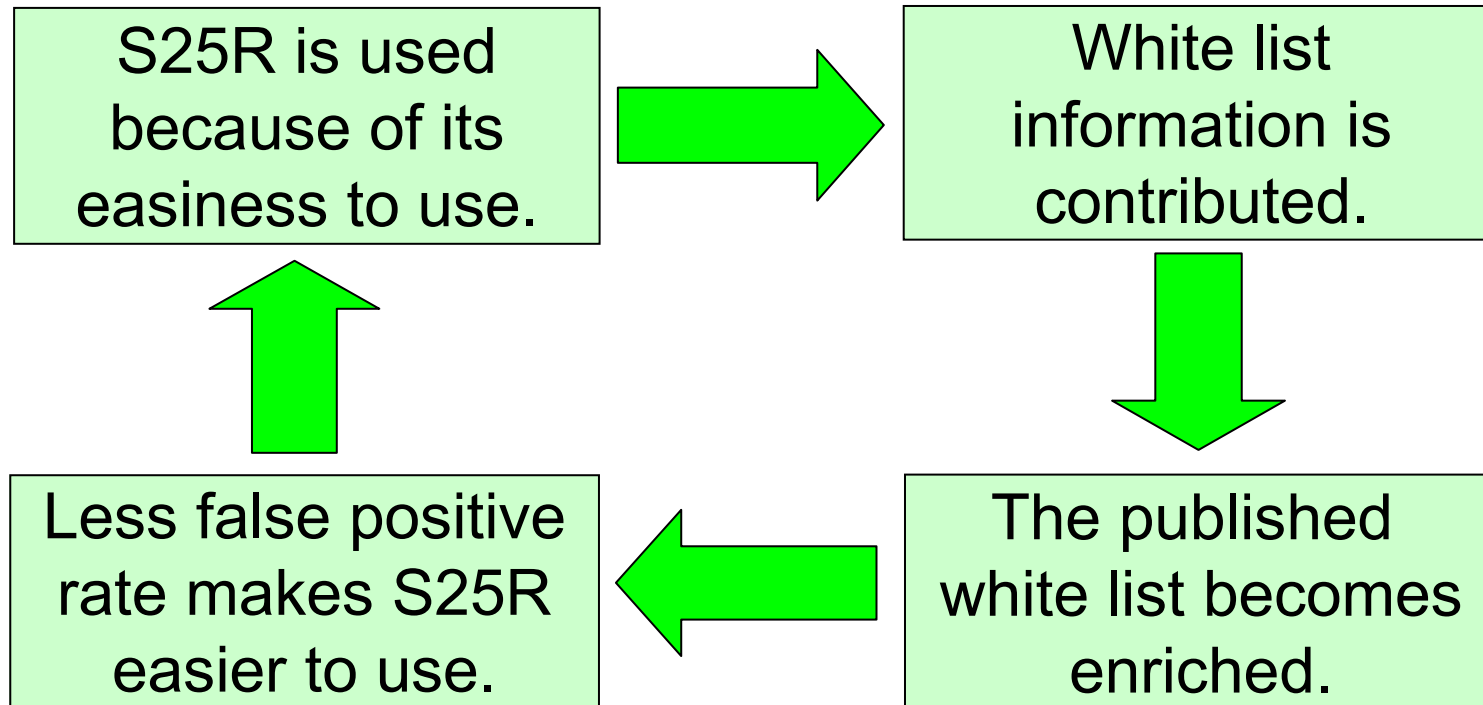
Major cases that legitimate mail servers are blocked by S25R

- reverse lookup failure / paranoid test error
- reverse host names including a serial number assigned by an ISP which has many subscriber lines
- reverse host names including a serial number assigned by a company which has many servers



The false positive rate reduces as the white list becomes enriched.

Virtuous circle of the white list



The published white list: now includes about 700 items

Log sorting script for finding retry accesses easily

- Retry accesses (with the same IP address, sender address and recipient address) are shown as lines in a sequence.
=>Whitelist the host if the sequense shows behavior of a legitimate mail server.

Generally, it retries for 30 mintes or more at an interval of 1 munute or more.

- An access which is not retried is shown as a single line separated by a blank line.
=>You can ignore it.
- Estimated message count (nealy equal to the number of spam messages which might have been received if they were not blocked) is displayed.
=>You can use it for statistics.

Automatic acceptance of hosts in false positives

Acceptance of hosts in false positives can be automated by using greylisting or tarpitting together with S25R.

	manual	automatic
merits	<ul style="list-style-type: none">•Additional software is not needed (in case of Postfix).•Stringent against retried spam accesses.	<ul style="list-style-type: none">•Few labor is needed for watching.•Acceptance succeeds even if the retry period is short.
demerits	<ul style="list-style-type: none">•Much labor is needed for watching.•Acceptance may fail if the retry period is shorter than the watching interval.	<ul style="list-style-type: none">•Additional software is needed.•Retried spam accesses may cheat the protection system (greylisting reduces 1% in the spam block rate).

Development by other volunteers

for Postfix	Rgrey Starpit taRgrey
for qmail	S25R application patch for qmail Qgrey s25rtarpitgreylist
for sendmail	smtp_wrapper application with milter
for XMail	application with XMailCFG
for mail clients	filter configuration for Becky! (by myself) Becky! S25R spam filter MailUtl3

Praises for S25R

- Surprising effectiveness! Legitimate mail can be received correctly.
- We had been in trouble over disk exhaustion by spam. We were survived.
- We can never abandon it.
- We recommend S25R for the customers of our hosting service.

Criticisms against S25R

criticisms	answers
Some legitimate mail servers don't have a reverse name.	You can receive mail by whitelisting while retry accesses are coming.
Some legitimate mail servers have a revers name with many numarals.	You can receive mail by whitelisting while retry accesses are coming.
It excludes mail servers with a dynamic IP address.	I hope such mail servers send out mail through your ISP's mail server.
Don't reject accesses selfishly on nothing but the result of reverse lookup.	Wait for whitelisting in the recipient site. It is mistaken operation if they leave retry accesses.
It is not useful but for a personal site.	The published white list has become useful for large sites.
Receiving defers.	Using greylisting or tarpitting reduces deferment. You shouldn't use it if you dislike even a little deferment.
Retry request loads the sender sites with the disk resource.	There is no problem even if mail stays in the sending queue. Loads on the Internet relay lines reduces.

Why has S25R spread?

The number of sites applying it: estimated to be over 1000

- High effectiveness.
- Free of charge.
- High skill is not needed for installation and operation.
- You don't need to ask anything of sender sites.
- The published white list has become enriched by contributors.
- Using greylisting and tarpitting was put into practice.
- It has become applicable for also qmail, sendmail and XMail.
- Besides the name is good?

Demand for ISPs: the service which enables users of connection with one IP address to assign their own reverse name

Appendix: The teachings to foresee the future prospects

People who first criticized things which have spread

AGAWA Hiroyuki	...	Shinkansen
ITOKAWA Hideo	...	VTR for home use
pros and semipros of computers	...	Windows



Things which satisfy the public needs
with continuous efforts shall win.