

Mail Scanning a la Open Source

Boris Quiroz Q.

<http://boris.penguin.cl>

CC by- nc- nd/2.0/cl



¿Software Libre?

- Nos permite:
 - Usarlo.
 - Copiarlo.
 - Modificarlo.
 - Distribuido libremente.
- Software Libre == Open Source?

¿Porque Software Libre?

- Respeto a las libertades del usuario.
- Puede ser estudiado y modificado.
- Con su estudio ayudamos al crecimiento de la comunidad.
- Nos permite publicar una nueva version mejorada.

Virus: La mas antigua de las amenazas

- Programa que puede infectar a otros programas.
- Según lo que infectan: Archivos, Booteo, etc.
- Según su comportamiento: Uniformes, Poliformicos, Metamorficos, etc.
- Porque no todo es perfecto...

Lo de ahora, Spam

- Correo electronico no solicitado.
- Publicidad, cadenas, etc.
- Perdida de tiempo del usuario.
- Utilizacion innecesaria de recursos del servidor.

¿Cuanto cuesta el Spam?

- 70% a 80% de los correos es SPAM, con un crecimiento mensual del 18%.
- De ellos, el 5% contiene Malware.
- Costo total del Spam = U\$20.5 Billones.
- Costo total de Virus = U\$55 Billones.

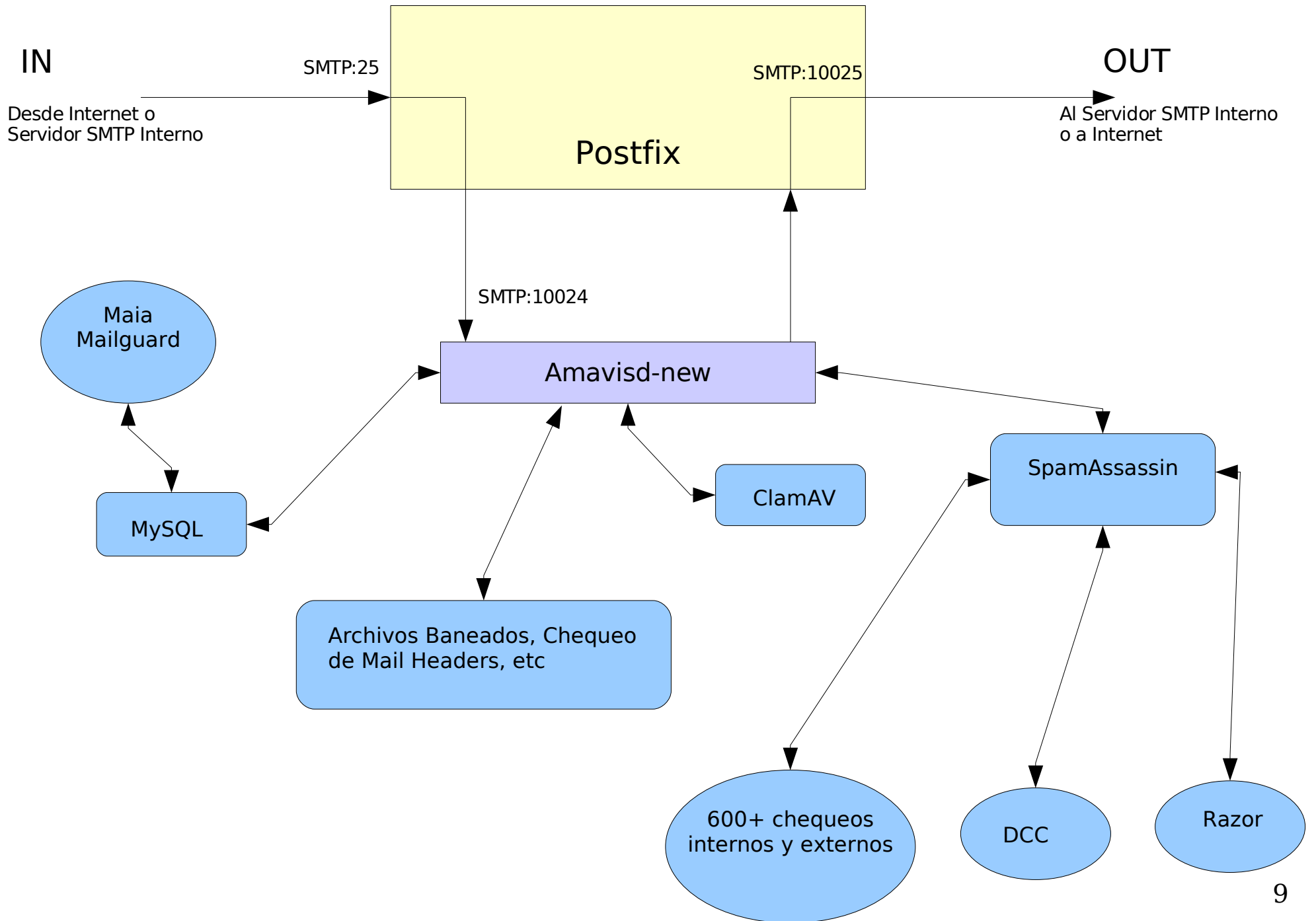
Fuente: ePrivacy Group.

Ingredientes.

- ClamAv
- SpamAssassin
- Razor2, DCC
- Amavisd-new
- Postfix || Sendmail
- Maia Mailguard
- Linux, Apache, MySQL, PHP

Tareas y Funciones

- Deteccion de Virus.
- Reconocimiento de Spam.
- Envio a cuarentena y/o bloqueo de e-mails.
- Manejo de Procesos.



ClamAV

- Funciona en línea de comando y como demonio.
- 33.000+ virus, worms y troyanos.
- Participación activa de la comunidad.
- 5^{to} mejor AntiVirus.
- Base de datos actualizada.



<http://www.clamav.net>

SpamAssassin

- Analizador de correos electronicos.
- Utiliza 5 criterios de analisis:
 - Inspeccion de Cabeceras.
 - Analisis del Mensaje.
 - Black Lists.
 - Bayesian.
 - Hashing.



<http://spamassassin.apache.org>

AntiSpam HowTo

- DNSBL: Domain Name Service Block Lists.
- RHSBL: Right Hand Side Block Lists.
- Analizadores reciben puntuacion.
- Puntuacion tipica: 5,0.

Ejemplo de Puntuacion

Cada regla aporta “evidencia” para la puntuacion final, la cual se compara con la puntuacion definida por el usuario.

<u>Score</u>	<u>Rule Name</u>	<u>Rule Description</u>
3.511	PYZOR_CHECK	Listed in Pyzor (http://pyzor.sourceforge.net/)
2.101	BAYES_90	Bayesian spam probability is 90 to 99%
1.113	RCVD_IN_SBL	Received via a relay in the Spamhaus Block List
1.047	RAZOR2_CHECK	Listed in Razor2 (http://razor.sourceforge.net/)
0.876	RAZOR2_CF_RANGE_11_50	Razor2 gives confidence between 11 and 50%
0.705	MSGID_FROM_MTA_HEADER	Message-ID was added by a relay
0.336	HTML_WEB_BUGS	Image tag intended to identify you
0.320	MIME_HTML_ONLY	Message only has text/html part MIME parts
0.100	HTML_MESSAGE	HTML included in message
0.100	SPAMCOP_URI_RBL	URI's domain appears in sc.surbl.org
10.209		

Bloqueo y/o Cuarentena

- Encargado: Amavisd-new.
- Metodos de discriminacion:
 - Usuarios.
 - Dominios.
 - Black Lists.
 - White Lists.
 - Puntuacion de Spam.
 - Virus, spam y/o adjuntos.

Maia Mailguard

- Desarrollado por Renaissoft.
- Nacio como una interfaz para administrar filtros de contenido.
- Actualmente se considera un Sistema para el manejo de virus y spam.
- Desarrollado en Perl, PHP y SQL.
- Sus informante es Amavisd-new.



<http://www.renaisssoft.com>

Maia Mailguard

- Maia permite a los usuarios:
 - Filtrar contenidos.
 - Crear listas de confianza.
 - Liberar y/o enviar correos a cuarentena.
 - Reportar Spam.
 - Confirmar status de sus correos.
- Bayesian comparte la informacion a las redes de colaboracion.

Procesos de Administracion






Current protection level: Custom

- Off
- Low
- Medium
- High

**Custom levels are in use:
Use settings screen to manage, or choose a preset level above.

[Change Level](#)

Cache Contents

 [Report/Confirm]	You have 18 items in your ham cache. Click here to help train the filter, or to report a spam message that was missed.
 [Report/Rescue]	You have 84 items in your spam cache. Click here to report it, or to rescue a message that was mistakenly blocked.
 [Delete/Rescue]	You have 3 items in your virus cache. Click here to delete it, or to rescue a message that was mistakenly blocked.
 [Delete/Rescue]	You have 0 items in your banned-file cache. Click here to delete it, or to rescue a message that was mistakenly blocked.
 [Delete/Rescue]	You have 0 items in your bad-header cache. Click here to delete it, or to rescue a message that was mistakenly blocked.

[Delete all items](#)

85168 SPAM items have been blocked for you **4289** Viruses have been blocked for you

200938 Spam items blocked systemwide **12568** Viruses blocked systemwide

Procesos de Administracion

Statistics for All Users											
Items				Score			Size (kB)			Bandwidth/day	
Mail Type	Count	Items/day	Pct	Min	Max	Avg	Min	Max	Avg	MB	Cost (\$CDN)
Suspected Ham	8357	128.3	1.7%	-20.523	4.981	-1.123	0.6	4412.0	19.5	2.45	0.018
Confirmed Ham	32596	66.2	6.8%	-21.893	21.904	-1.075	0.3	4882.4	12.1	0.78	0.006
False Positives	551	1.1	0.1%	3.692	108.147	7.801	0.6	213.6	20.8	0.02	0.000
Suspected Spam	26261	273.5	5.5%	0.000	140.542	27.685	0.3	207.4	5.6	1.49	0.011
Confirmed Spam	200938	408.4	41.7%	0.000	232.153	34.001	0.3	254.9	4.1	1.65	0.012
False Negatives	707	1.5	0.1%	-16.032	73.710	4.478	0.4	1259.2	19.7	0.03	0.000
Whitelisted Items	196947	407.7	40.9%	-	-	-	0.3	4778.4	7.9	3.15	0.023
Blacklisted Items	54	0.4	0.0%	-	-	-	0.7	25.0	10.2	0.00	0.000
Viruses/Malware	12568	26.4	2.6%	-	-	-	0.7	2299.2	44.8	1.15	0.008
Banned Attachments	2290	5.0	0.5%	-	-	-	0.8	682.0	33.5	0.16	0.001
Invalid Mail Headers	80	0.2	0.0%	-	-	-	0.3	1507.8	55.9	0.01	0.000
Oversized Items	30	0.1	0.0%	-	-	-	5018.7	23338.2	6786.0	0.42	0.003
Efficiency 99.46% False Positive 0.23% False Negative 0.30% Sensitivity 99.65% PPV 99.73% Specificity 98.34% NPV 97.88%											

Procesos de Administracion

Address: uj@univision.com	
Virus Scanning	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Detected viruses should be...	<input type="radio"/> Labeled <input checked="" type="radio"/> Quarantined <input type="radio"/> Discarded
Spam Filtering	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Detected spam should be...	<input type="radio"/> Labeled <input checked="" type="radio"/> Quarantined <input type="radio"/> Discarded
Add a prefix to the subjects of spam?	<input type="radio"/> Yes <input checked="" type="radio"/> No
Add X-Spam: Headers when Score is >=	<input type="text" value="-999.000"/>
Consider mail 'Spam' when Score is >=	<input type="text" value="5.000"/>
Quarantine Spam when Score is >=	<input type="text" value="5.000"/>
Attachment Type Filtering	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Mail with dangerous attachments should be...	<input type="radio"/> Labeled <input checked="" type="radio"/> Quarantined <input type="radio"/> Discarded
Bad Header Filtering	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Mail with bad headers should be...	<input type="radio"/> Labeled <input checked="" type="radio"/> Quarantined <input type="radio"/> Discarded

Procesos de Administracion

E-mail address or domain to add:

List to add to:

Whitelist Blacklist

Add to List

Address	Whitelist	Blacklist	Remove
akhan@example.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
ldavis@example.com	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
tmoore@example.com	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>

Update Reset

System Configuration

Enable auto-creation of user accounts? [?]	<input type="radio"/> Yes <input checked="" type="radio"/> No
Enable tracking of false negatives? [?]	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable tracking of statistics? [?]	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable virus scanning? [?]	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable spam filtering? [?]	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable banned file attachment checks? [?]	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable checks for invalid mail headers? [?]	<input checked="" type="radio"/> Yes <input type="radio"/> No
Enable spam-trap accounts? [?]	<input checked="" type="radio"/> Yes <input type="radio"/> No
Mail size limit (bytes): [?]	<input type="text" value="500000"/>
Oversized items should be... [?]	<input type="radio"/> Accepted <input checked="" type="radio"/> Rejected

Paths & Ports

Mail installation directory: [?]	<input type="text" value="/usr/local/apache/htdocs/mail"/>
Administrator's contact e-mail address: [?]	<input type="text" value="jsmith@example.com"/>
Downstream SMTP server (MTA-TX): [?]	<input type="text" value="localhost"/>
Downstream SMTP port number: [?]	<input type="text" value="10025"/>
Encryption key file (optional): [?]	<input type="text" value="/var/amavis/afblowfish.key"/>

Cache Expiry & Quarantine Reminders

Expiry period for quarantined mail (days): [?]	<input type="text" value="10"/>
Expiry period for cached ham (days): [?]	<input type="text" value="5"/>
E-mail reminder threshold (items): [?]	<input type="text" value="100"/>
E-mail reminder threshold (size): [?]	<input type="text" value="500000"/>
E-mail reminder template file: [?]	<input type="text" value="/var/amavis/mail/templates/reminder.tpl"/>
Mail login URL for e-mail reminders: [?]	<input type="text" value="http://www.example.com/mail/"/>

On the Horizon...

- Todas las aplicaciones continúan con su desarrollo.
- Desarrollo de nuevos features de Maia:
 - “Grey Lists”
 - Maia Network
 - Nuevo sistema de reportes.
- Se espera un crecimiento sostenido del Spam en los próximos años.

¿Preguntas?

