Implementación de los criterios de calidad y seguridad en el correo electrónico con Sendmail

Implementation of Quality and Security Criteria in e-mail with Sendmail

Pedro R. Benito da Rocha

Resumen

Explicación de cómo aplicar las tecnologías de cifrado, filtrado y directorio para dotar a un servicio de correo electrónico de fiabilidad y seguridad, traduciendo este esfuerzo en una mayor confianza en el servicio por parte del usuario, que conoce y utiliza directa o indirectamente las tecnologías más actuales aplicadas a un servicio "tradicional" como es el de correo electrónico. Se expone un caso práctico con Sendmail, uno de los servidores de correo electrónico más extendidos, de forma que los administradores del servicio puedan aplicar de forma práctica los contenidos del artículo a su entorno real de trabajo.

Palabras clave: Calidad en el servidor de correo electrónico con Sendmail.

Summary

Explanation is given on how to apply the ciphering, filtering and directory technologies to endow to a reliable and secure e-mail service. This effort will mean a greater service confidence on the part of the user who is the one who knows and uses, direct or indirectly, today's technologies applied to a "traditional" service as considered e-mail. A practical case using Sendmail is exposed –being it one of the more widely known e-mail servers– for Service Administrators to apply in a practical way the content described in the artide.

Keywords: Quality on the e-mail Server with Sendmail.

Veremos algunos de los criterios de calidad y seguridad aplicados al correo electrónico, y más concretamente a la implementación que hace Sendmail de su servidor SMTP en su versión libre

1.- Introducción

El servicio de correo electrónico ha sufrido relativamente pocos cambios a lo largo de los años; aun así, sigue siendo uno de los más utilizados por los usuarios de la red. En una red cada día más sujeta a ataques y a intromisión de la privacidad, el correo electrónico no puede ser ajeno a las nuevas circunstancias, ya que los usuarios cada vez demandan un servicio mejor y más seguro sin perder flexibilidad y utilidad.

En este artículo intentaremos mostrar algunos de los criterios de calidad y seguridad aplicados al correo electrónico, y más concretamente a la implementación que hace Sendmail de su servidor SMTP en su versión libre, por ser una de las más extendidas en la red. No obstante, todo lo aquí presentado se puede aplicar a otras implementaciones de servidores SMTP como Postfix, si bien la capacidad de filtrado con Postfix aún no llega a la integración de los filtros con el servidor que tiene Sendmail.

2.- Criterios de calidad

Los criterios de calidad aplicados al correo electrónico están claramente identificados por tres factores: seguridad, fiabilidad y servicio al usuario. Actualmente en la comunidad RedIRIS se ha puesto en marcha la iniciativa PACE de calidad en el correo electrónico (Red Académica de Correo Electrónico), la cual es una buena referencia a la hora de diseñar un servicio de correo electrónico moderno y eficiente.

La implementación de los criterios de calidad se va a realizar en el MTA, ya que así el impacto es mucho menor que si se tomaran medidas solamente en el lado del cliente

En la implementación de Sendmail los criterios de calidad que se van a observar son: el uso de cifrado para dar mayor seguridad a las comunicaciones, el uso de un servidor de directorio para almacenar los datos de usuario para así conseguir una mayor flexibilidad y fiabilidad, y el uso de distintos filtros y reglas para evitar la utilización indebida o malintencionada de nuestro servidor SMTP.

Todos estos criterios transmiten al usuario la sensación de calidad en el servicio de correo, al poder apreciar mejoras no recibiendo virus, spam, etc., e incrementando su confianza al tener la seguridad de que sus mensajes son privados.

3.- Implementación de los criterios de calidad

Como se desprende de lo visto hasta ahora, la implementación de los criterios de calidad se va a realizar en el MTA, ya que así el impacto es mucho menor que si se tomaran medidas solamente en el lado del cliente, como por ejemplo cifrado por el mismo (PGP, etc.) o colocación de filtros antispam. Paralelamente se consigue una independencia del cliente, y de la situación de movilidad del usuario, al no tener que configurar e instalar programas cada vez que cambia de cliente de correo.

3.1.- Cifrado

Los mensajes de correo electrónico normalmente viajan en plano por la red. Los que salen de nuestra institución hacia Internet viajan por una red insegura quedando expuesto su contenido a la vista de terceros. La solución a esta circunstancia pasa por cifrar el canal de comunicaciones, de tal manera que el mensaje no pueda ser visualizado por terceras personas que estén escuchando en la red.

Para implementar el cifrado, existe una extensión SMTP llamada STARTTLS, mediante la cual el servidor SMTP ofrece la posibilidad de usar un canal cifrado para el envío del mensaje tal y como se describe en el RFC 2487. Sendmail dispone de esta extensión sin necesidad de añadir ningún parche ni plug-in, y para ello utiliza las librerías de libre distribución OpenSSL.

3.2.- Servicio de directorio

Uno de los mayores problemas con los que se enfrenta un administrador de correo es el creciente número de usuarios a los que se ha de dar servicio. El mantenimiento de dichas cuentas de usuario implica cada vez más tiempo y más personal, así como el trabajo de mantener la consistencia de los datos de usuario en los distintos servidores. El servidor de directorio permite ser un servicio de autenticación centralizada con todas las ventajas que esto conlleva, como por ejemplo:

- Los datos siempre son consistentes al existir una única base de datos, o en el caso de LDAP la replicación de datos es automática y casi instantánea en todos los servidores.
- Los cambios en los datos de usuario son inmediatos. El usuario percibe que cuando cambia su contraseña de correo lo hace automáticamente en todos los servidores, de forma transparente.
- El mantenimiento de datos es más simple para el administrador, ya que agregar un nuevo servidor al sistema no implica abrir de nuevo todas las cuentas.
- Los servidores de directorio permiten autentificar usuarios por red usando protocolos seguros.

En resumen, un servidor de directorio permite la implementación de un sistema de contraseña única de forma sencilla.

3.3.- Filtrado

3.3.1.- El correo basura

Como ya hemos comentado, el correo no solicitado (también llamado spam o correo basura) que inunda con mayor frecuencia los buzones de los usuarios es un problema cada vez mayor. Este problema implica al servicio de correo electrónico de dos formas:

a) Los usuarios reciben correo que no desean, es molesto y da una mala sensación del servicio
b) Consume recursos del sistema

Cuando además se utiliza el servidor de correo de una institución para enviar correo a otros servidores (lo que se denomina open-relay) el daño es mayor, ya que no sólo se consumen recursos del sistema: ancho de banda, cpu, disco,... sino que también el servidor de correo será incluido en listas negras como fuente de correo basura, con lo cual el correo legítimo de nuestros usuarios se verá afectado al ser bloqueado por los servidores de destino.

Para evitar el open-relay, los servidores SMTP actuales cuentan con las llamadas reglas anti-relay, que evitan el uso de un servidor de correo por parte de terceros para reenviar correo no solicitado. Esto plantea un problema nuevo: ¿qué ocurre con los usuarios que están fuera de nuestra institución? La respuesta es simple: autenticación del emisor. Para implementar la autenticación de usuarios existe una extensión SMTP llamada SMTP-AUTH que se explica en el RFC 2554. La mayoría de servidores SMTP incluido Sendmail ofrecen esta posibilidad. Al usar esta extensión, todos los usuario autentificados pueden usar el servidor SMTP para enviar mensajes fuera de la institución sin estar físicamente en ella, lo que se conoce como relay o reenvío.

Si bien las reglas anti-relay evitan el uso de un servidor como fuente de correo no solicitado, no evitan el problema de la llegada de este tipo de correo a nuestro servidor. Para esto existen otros filtros llamados filtros anti-spam de los cuales hay varios tipos:

- Listas negras. Se basan en listas de servidores que han sido denunciados como fuente de spam. Cuando el servidor recibe un mensaje comprueba la procedencia del mismo, y en caso de provenir de un servidor incluido en una lista negra bloquea el mensaje y este no llega al buzón del usuario. Un ejemplo de listas negras es el proyecto PUAS de RedIRIS
- Filtros por contenido. Estos filtros analizan el contenido del mensaje y, mediante patrones más o menos complicados, marcan el mensaje como "bueno" o como "spam"

Ambas soluciones tienen el inconveniente de dar a veces falsos positivos, es decir, bloquean mensajes legítimos. Es por esto por lo que no todos los usuarios desean este tipo de soluciones.

3.3.2.- Filtros antivirus

Otro tipo de filtros son los filtros antivirus. Este tipo de filtros bloquea o incluso limpia los mensajes que contienen virus. Prácticamente todos los antivirus comerciales están desarrollando versiones de sus productos que funcionan a nivel de MTA.

4.- Implementación de los criterios de calidad usando Sendmail

La implementación de los criterios de calidad con Sendmail se debe hacer en dos pasos: la compilación y la configuración.

Para evitar el open-relay, los servidores SMTP actuales cuentan con las llamadas reglas anti-relay, que evitan el uso de un servidor de correo por parte de terceros para reenviar correo no solicitado

Una vez compilado e instalado Sendmail se puede proceder a la creación de una configuración de Sendmail propia adaptada a las necesidades de cada institución

En el primer paso, se indican las características y las posibilidades del servidor en general, y en el segundo se seleccionan las características aplicadas a un caso concreto.

4.1.- Compilación de Sendmail

La compilación por defecto no activa algunas de las características de Sendmail como por ejemplo la autenticación, el cifrado o el soporte para el servidor de directorio LDAP. Mediante un sencillo fichero de configuración se puede hacer que Sendmail tenga integradas dichas características.

El fichero en cuestión se llama site.config.m4 y ha de residir en el directorio devtools/Site/ de la distribución de Sendmail.

```
APPENDDEF(`confENVDEF', `-DSASL -DSTARTTLS -DMILTER')
APPENDDEF(`conf_sendmail_LIBS', `-lssl -lcrypto -lsasl')
APPENDDEF(`confMAPDEF', `-DLDAPMAP')
APPENDDEF(`confLIBS', `-lldap -llber')
```

Figura 1: Fichero de configuración para compilar Sendmail

En este fichero se añade soporte para las siguientes opciones:

- Librerías SASL: para añadir autenticación a Sendmail usando SMTP-AUTH
- Librerías SSL: para añadir cifrado usando STARTTLS
- Librerías LDAP: para añadir soporte de directorio LDAP a Sendmail

Como se puede observar, Sendmail utiliza varias librerías para dar soporte a los distintos criterios de calidad mencionados anteriormente. Dichas librerías son:

- SASL: provee de mecanismos de autenticación
- OpenSSL: añade capacidad de cifrado usando SSL
- OpenLDAP: para poder usar un servidor de directorio como un "mapa" o base de datos para almacenar las distintas configuraciones

Una vez creado el fichero site.config.m4 se compila e instala Sendmail como indica el manual. La ventaja de haber usado un fichero de configuración reside en que dicho fichero es reutilizable si deseamos actualizar la versión de Sendmail.

4.2.- Configuración de Sendmail

Una vez compilado e instalado, se puede proceder a la creación de una configuración de Sendmail propia adaptada a las necesidades de cada institución.

Tradicionalmente se editaba el fichero de configuración directamente. En cambio aquí se propone otro método mucho más sencillo, que ayuda a entender mejor la configuración de Sendmail sin tener que aprenderse complicadas reglas.

El método consiste en la creación de un fichero m4, el cual al ser procesado por dicha herramienta genera el fichero sendmail.cf, que es el utilizado por el servidor. A continuación se muestra un fichero de configuración m4 completo, que veremos con más detenimiento posteriormente.

```
divert(-1)
# Fichero de configuración m4 para sendmail.cf
#
# Autor: Pedro R. Benito da Rocha (pedro@ubu.es)
# Versión: 1.1
# Última modificación: 08/10/2001
divert(0)dnl
include(`/usr/local/src/sendmail-8.12.8/cf/m4/cf.m4')dnl
VERSIONID(`@relay.ubu.es.mc 2.0 (ubu.es) 08/10/2001')dnl
OSTYPE(linux)dnl
DOMAIN(generic)dnl
define(`ALIAS_FILE', `/etc/mail/aliases')dnl
FEATURE(`access_db', `hash -T<TMPF> /etc/mail/access_db')dnl
TRUST_AUTH_MECH(`LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `LOGIN PLAIN')dnl
define(`confDEF_AUTH_INFO')dnl
FEATURE(`no_default_msa')dnl
FEATURE(`authinfo')dnl
FEATURE(`nouucp', `nospecial')dnl
FEATURE(`mailertable', `hash /etc/mail/mailertable')dnl
FEATURE(`loose_relay_check')dnl
FEATURE(`enhdnsbl', `dnsbl.dominio.com', `',`t')dnl
define(`CERTDIR', `/etc/certs/')dnl
define(`confCACERT_PATH', `/etc/certs/')dnl
define(`confCACERT', `/etc/certs/ca.crt')dnl
define(`confSERVER_CERTPATH', `/etc/certs/')dnl
define(`confSERVER_CERT', `/etc/certs/r maquina.dominio.es.crt')dnl
define(`confSERVER_KEY', `/etc/certs/ maquina.dominio .es.key')dnl
define(`confCLIENT_CERT', `/etc/certs/ maquina.dominio .es.crt')dnl
define(`confCLIENT_KEY', `/etc/certs/ maquina.dominio .es.key')dnl
define(`confMAX_MESSAGE_SIZE', `52428800')dnl
INPUT_MAIL_FILTER(`tamiz-milter',`S=inet:5555@maquina.dominio.es, T=S:30s;R:30s;E:5m')dnl
MAILER(local)dnl
MAILER(smtp)dnl
```

Figura 2: Fichero de configuración m4 para Sendmail

Este fichero, al que se llamará sendmail.mc, contiene las directivas necesarias para implementar los criterios de calidad antes descritos. Para generar el fichero de configuración de Sendmail a partir del fichero sendmail.mc se debe dar la siguiente orden: m4 sendmail.mc > sendmail.cf que produce un fichero sendmail.cf listo para ser utilizado.

4.2.1.- Autenticación (SMTP-AUTH)

Una vez compilado Sendmail con las opciones de autenticación de cliente, para activarlo basta con indicarle los métodos que debe utilizar para dicha autenticación.

Las directivas de autenticación de usuario en fichero sendmail.mc son:

```
TRUST_AUTH_MECH(`LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `LOGIN PLAIN')dnl?
```

Donde se definen los mecanismos "LOGIN" y "PLAIN" como los mecanismos válidos de autentificación. Estos mecanismos los implementa la librería SASL.

Para la autenticación, Sendmail utiliza la librería SASL, que permite utilizar varios métodos para realizar la autenticación efectiva del usuario

Ventajas:

- Ambos mecanismos son los usados por los clientes más comunes.
- Son fáciles de configurar.

Inconvenientes:

- La autenticación se produce en plano, es decir no está cifrada.

Cualquier cliente que sea capaz de usar SMTP-AUTH podrá pues enviar mensajes incluso estando fuera de la institución, recordemos que Sendmail permite el reenvío (relay) de mensajes a usuarios autentificados.

4.2.2.- Conexión a un servidor de directorio

Para la autenticación, Sendmail utiliza la librería SASL, que permite utilizar varios métodos para realizar la autenticación efectiva del usuario. Si se emplea SASL con el módulo PAM como autentificador, SASL se encarga de llamar a PAM indicando que la autenticación es para el servicio SMTP. Si a esto se añade el uso del programa PAM-LDAP de Padl Software se acaba de conectar Sendmail con un servidor LDAP como fuente de la autenticación. La ventaja de utilizar Sendmail con la librería SASL es su gran flexibilidad a la hora de autentificar usuarios.

Para generar la conexión Sendmail – SASL – PAM -LDAP se requiere la configuración de tres ficheros:

a) El fichero /usr/lib/sasl/Sendmail.conf. Cuyo contenido es una única línea que indica el método de autenticación. En nuestro caso dicha línea es: pwcheck_method:pam
b) El fichero /etc/pam.d/smtp. Configurado según se indica en el programa PAM-LDAP
c) El fichero /etc/ldap.conf. Configurado según se indica en el manual de OpenLDAP, indicando el servidor ldap y la base del árbol. También se puede añadir cifrado indicando los certificados a usar

```
#%PAM-1.0
auth       sufficient   /lib/security/pam_ldap.so
auth       required     /lib/security/pam_unix_auth.so try_first_pass
account    sufficient   /lib/security/pam_ldap.so
account    required     /lib/security/pam_unix_acct.so
```

Figura 3: Fichero de configuración smtp para PAM

```
host ldap.dominio.es
base dc=dominio,dc=es
ssl start_tls
tls_cacertfile /etc/certs/ca.crt
tls_cacertdir /etc/certs
tls_cert /etc/certs/ldap.dominio.es.crt
tls_key /etc/certs/ldap.dominio.es.key
```

Figura 4: Fichero de configuración LDAP

4.2.3.- Cifrado

Las siguientes líneas del fichero sendmail.mc hacen referencia al cifrado:

```
define(`CERTDIR', `/etc/certs/')dnl
define(`confCACERT_PATH', `/etc/certs/')dnl
define(`confCACERT', `/etc/certs/ca.crt')dnl
define(`confSERVER_CERTPATH', `/etc/certs/')dnl
define(`confSERVER_CERT', `/etc/certs/relay.dominio.es.crt')dnl
define(`confSERVER_KEY', `/etc/certs/relay.dominio.es.key')dnl
define(`confCLIENT_CERT', `/etc/certs/relay.dominio.es.crt')dnl
define(`confCLIENT_KEY', `/etc/certs/relay.dominio.es.key')dnl
```

En ellas se detalla la ubicación de los certificados, tanto de los raíz como de los certificados cuando actúa como servidor y cliente.

Para que Sendmail utilice el cifrado, aparte de compilarlo con las opciones antes descritas, basta con indicarle la ruta donde se han instalado los ficheros con los certificados. Dichos certificados pueden generarse con la herramienta OpenSSL o bien ser proporcionados por terceros, siendo totalmente compatible con los certificados comerciales.

Otra ventaja de usar cifrado se refleja al autentificar usuario, ya que como se ha dicho los métodos de autenticación LOGIN y PLAIN autentifican en plano, y añadir cifrado al canal de comunicaciones no compromete las contraseñas de los usuarios.

Para que Sendmail utilice el cifrado, aparte de compilarlo con las opciones antes descritas, basta con indicarle la ruta donde se han instalado los ficheros con los certificados

4.2.4.- Reglas anti-relay

En las versiones más modernas de Sendmail, las reglas anti-relay vienen activadas por defecto, no siendo necesaria ninguna configuración extra para activarlas.

4.2.5.- Filtros antispam

Para combatir el spam Sendmail proporciona una serie de filtros y reglas de acceso configurables por el administrador que se activan mediante la directiva FEATURE(`access_db') del fichero sendmail.mc.

Con dicha directiva se activa el uso de una base de datos llamada access_db que reside en el directorio /etc/mail, en la cual se definen las reglas de acceso al servidor SMTP.

4.2.6.- Listas negras

Las listas negras se implementan mediante servidores DNS en los que se almacena la dirección IP del servidor que ha sido denunciado como open-relay o como fuente de correo basura.

En el fichero de configuración que se está tratando aparece en la siguiente línea:

```
FEATURE(`enhdnsbl', `dnsbl.dominio.com', `',`t')dnl
```

En la cual se define que dnsbl.dominio.com va a ser el dominio a través del cual se van a realizar las consultas DNS para saber si un servidor está bloqueado o no.

Se pueden definir varias listas negras, que se evaluarán en el orden en el que se indiquen. Por ejemplo, si deseamos usar las listas de RedIRIS PUASSOFT y PUASHARD se debería añadir a la configuración las siguientes líneas:

Para adaptar el correo electrónico a la nueva situación, se ha de planificar un servicio adaptado a las nuevas tecnologías que permita la aplicación de criterios de calidad que redunden en un mejor servicio

```
FEATURE(`enhdnsbl', `puassoft.rediris.es', `Bloqueado por PUASSOFT',`t')dnl
FEATURE(`enhdnsbl', `puashard.rediris.es', `Bloqueado por PUASHARD',`t')dnl
```

En las cuales se configuran las zonas puassoft.rediris.es y puashard.rediris.es respectivamente.

4.2.7.- Filtros antivirus

Existen varios filtros antivirus para Sendmail, algunos basados en mailers y otros basados en el motor de filtrado de Sendmail: Milter que es un conjunto de librerías que proporciona capacidades de filtrado a Sendmail, es una solución propietaria de Sendmail y de momento los filtros que usan Milter solamente funcionan con este producto.

Uno de los filtros más sencillos es Tamiz, desarrollado por la Universidad de Zaragoza, el cual permite independientemente de la solución antivirus adquirida, rechazar los mensajes que contengan virus. Tamiz soporta los antivirus más populares de manera que unido a su sencillez hacen de este filtro una herramienta ideal para evitar la entrada de virus a través del correo electrónico.

Para activar un filtro Milter, se utiliza la directiva INPUT_MAIL_FILTER del fichero sendmail.mc. En la siguiente línea se muestra como activar el filtro Tamiz para Sendmail.

```
INPUT_MAIL_FILTER(`tamiz-milter',`S=inet:5555@maquina.dominio.es,v T=S:30s;R:30s;E:5m')dnl
```

Se pueden definir tantos filtros Milter como se desee, teniendo en cuenta que se aplicarán en el orden en el que se han definido.

5.- Conclusiones

El correo electrónico es una herramienta de trabajo ampliamente usada por las personas conectadas a Internet. Esta herramienta ha sufrido pocos cambios desde su inicio, pero no puede ser ajena a los problemas derivados del uso masivo de la red. Para adaptarlo a la nueva situación, se ha de planificar un servicio adaptado a las nuevas tecnologías que permita la aplicación de criterios de calidad que redunden en un mejor servicio.

Las técnicas de filtrado y cifrado aplicadas al correo electrónico le dotan de la seguridad que el usuario reclama, si bien el problema del correo basura aún se encuentra lejos de una solución definitiva.

El otro gran problema es el creciente número de usuarios al que aplicar técnicas de autenticación y configuración centralizadas como parte imprescindible para dotar al servicio de agilidad y eficiencia.

El servidor SMTP Sendmail no ha sido ajeno a estos cambios y ha evolucionado para soportar estas nuevas técnicas en el correo electrónico, de tal forma que continúa siendo una solución válida para ofrecer un servicio de calidad.

Pedro R. Benito da Rocha
(pedro@ubu.es)
Universidad de Burgos
Área de sistemas del Servicio de Informática y Comunicaciones