M³AAWG

(*Grupo de Trabajo Anti-Abuso vía Mensajería, Malware y Móvil*)

TLS para Correo: Recomendaciones Iniciales de M³AAWG

www.m3aawg.org/TLSforMailBP-Spanish

Resumen Ejecutivo

Las recientes filtraciones sobre el monitoreo masivo del tráfico de correo electrónico han incrementado el interés público acerca de las medidas técnicas que los proveedores de este servicio pueden implementar, con el fin de proteger los mensajes de los usuarios frente al riesgo de interceptación. En este documento, M³AAWG recomienda tres medidas básicas que los proveedores pueden implementar de una manera relativamente rápida para fortalecer la seguridad y la privacidad de sus usuarios.

Introducción

Este documento es breve y simple, enfocándose en medidas cuya implementación no es muy compleja. M³AAWG reconoce que un documento corto no puede explorar todas las implicaciones de una área tan compleja como esta, sin embargo existe un beneficio significativo al ofrecer este acercamiento inicial a las medidas sugeridas, mientras otros documentos técnicos más detallados son desarrollados.

Este documento se concentra entonces en medidas que los proveedores de mensajes pueden implementar. Este documento no intenta abordar opciones de cifrado de datos controladas por el usuario, como PGP/GPG o S/MIME, que ofrecen privacidad para el contenido del mensaje, tanto cuando está en tránsito como cuando permanece archivado.

1) Protección del tráfico de correo electrónico entre los proveedores mediante el uso de opportunistic TLS (StartTLS).

TLS, creado en 1999, es el sucesor de SSL. Debido a un número de problemas de seguridad conocidos en SSLv2 y SSLv3, M³AAWG invita a la industria a desactive todas las versiones de SSL. Sin embargo, los encargados de las áreas de tecnología deben entender cómo esto puede afectar a sus usuarios, especialmente a aquellos que aún utilicen software viejo. Vale la pena recordar que algunas versiones antiguas de TLS tienen sus propios problemas de seguridad.

El tráfico de correo entre proveedores no es cifrado por defecto. En su uso normal, TLS requiere que la llave de cifrado y descifrado sea basada en un certificado independiente. Esto se ha convertido en una barrera significativa que dificulta su adopción y uso. Sin embargo, los Agentes de Transferencia de Correo (MTAs) más comunes pueden ser configurados para que intenten negociar sesiones de opportunistic TLS[*(1)] empleando llaves únicas por sesión, con el fin de proteger el tráfico entre MTAs del monitoreo del que pueden ser objeto, empleando para el efecto un mejor esfuerzo.

M³AAWG invita con insistencia a todos los operadores a implementar opportunistic TLS en todos sus servidores de correo.

---

[*] Ver, por ejemplo, las "recetas" en https://bettercrypto.org/static/applied-crypto-hardening.pdf sección 2.3.

Una limitación que se debe resaltar: SMTP es un protocolo paso-a-paso y, puesto que TLS funciona como parte de la conexión TCP que soporta una sesión directa de SMTP, *opportunistic TLS* también funciona de la misma forma, paso-a-paso. Si se ha implementado *opportunistic TLS* en algunos de los pasos que hacen parte de la arquitectura de envío de los mensajes, pero esa implementación no abarca la totalidad del proceso, la protección contra el monitoreo será incompleta. De cualquier manera, mientras que *opportunistic TLS* no es perfecto, por lo menos ayudará a proteger una parte del tráfico frente a ataque pasivos y M[3]AAWG invita a los proveedores de servicios a ver los beneficios incrementales reales que pueden existir, así la implementación no sea del todo perfecta o completa.

Si usted ya ha implementado *opportunistic TLS* en sus servidores de correo, visite el sitio web disponible en https://ssl-tools.net/mailservers [Nota: enlace actualizado el 2018 de julio] para verificar el nivel de protección que su implementación está ofreciendo a sus usuarios.

M[3]AAWG específicamente sugiere que la versión que se utilice en los servidores de correo sea TLS 1.2[(2)], y no alguna versión anterior, y que se utilicen algoritmos de cifrado que ofrezcan *forward secrecy*[(3)].

2) Proteger el tráfico en la red interna para evitar que sea monitoreado

Históricamente, el tráfico sobre vínculos dedicados en las redes internas se ha entendido como seguro y, por lo tanto, no se ha cifrado. Sin embargo, debido a recientes revelaciones sobre el alcance del monitoreo masivo en las redes[(4)], ese entendimiento debe ser replanteado. M[3]AAWG sugiere que todo el tráfico en la infraestructura de las redes internas sea cifrado, bien sea utilizando TLS u otros métodos criptográficos, además de recomendar el uso de *opportunistic TLS* para cifrar el tráfico de correo entre MTAs a través de Internet.

3) Proteger las contraseñas de los usuarios frente al monitoreo (IMAPS/POPS/SMTP Submit/interfaces web de correo)

De manera adicional, cuando los usuarios ingresan su nombre de usuario y su contraseña para acceder a su buzón de correo o para enviar un mensaje, los proveedores de servicios deberían usar cifrado para evitar la interceptación de esas credenciales. Esto es posible utilizando:

- IMAP (o POP) con TLS
- Envío de correo por el puerto 465 con TLS o a través del puerto 587 con StartTLS
- Interfaz web de correo protegida con TLS

Conclusión

El Grupo de Trabajo Anti-Abuso vía Mensajería, Malware y Móvil recomienda que la industria de proveedores de servicios de correo electrónico implementen tecnologías básicas de cifrado de datos, como una primera línea de defensa contra el monitoreo de los mensajes de sus usuarios. Estas recomendaciones deben considerarse como pasos iniciales, no como guías completas sobre criptografía. M[3]AAWG está trabajando en el desarrollo de guías adicionales relacionadas con la protección de las comunicaciones de los usuarios.

Referencias

1. Bettercypto.org, Applied Crypto Hardening, section 2.3 "Practical recommendations: Mail Servers," https://bettercrypto.org/static/applied-crypto-hardening.pdf at section 2.3.

2. TLS version 1.2, http://en.wikipedia.org/wiki/Transport_Layer_Security#TLS_1.2

3. Forward Secrecy, http://en.wikipedia.org/wiki/Forward_secrecy

4. MUSCULAR (DS-200B) surveillance program, http://en.wikipedia.org/wiki/MUSCULAR_%28surveillance_program%29

RFCs Relacionadas

- RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2," http://tools.ietf.org/html/rfc5246
- RFC 7258, "Pervasive Monitoring Is an Attack," http://tools.ietf.org/html/rfc7258