Messaging, Malware and Mobile Anti-Abuse Working Group
(Grupo de trabajo de Mensajería, Malware y Anti – Abuso Móvil)

Recomendaciones iniciales de M³AAWG para abordar una posible amenaza Man-in-the-Middle

Julio 2015

URL de referencia para este documento: www.m3aawg.org/MITM-Recommendations-Spanish

Introducción

La comunidad de mensajería ha logrado un progreso impresionante en cuanto a la fomentación del despliegue de las criptografías oportunistas (de mejor esfuerzo) del tráfico de correo electrónico. Las criptografías oportunistas, como se describe en los documentos TLS for Mail: M³AAWG Initial Recommendations and IETF Opportunistic Security: Some Protection Most of the Time**,** no son necesariamente seguras contra los ataques Man-in-the-Middle (MITM) o ataques de intermediario "hombre en el medio".

Para entender por qué esto es verdad, es necesario considerar el qué ocurre normalmente cuando las criptografías oportunistas no pueden ser negociadas adecuadamente. En ese caso, las transmisiones MTA-to-MTA (mail-transfer-agent to mail-transfer-agent / de agente de transferencia de correo a agente te transferencia de correo) , normalmente, ceden terreno al envío del tráfico de correo electrónico sin formato, es decir, totalmente sin cifrar. En consecuencia, la elección del proveedor se encuentra entre tolerar el cifrado de mejor esfuerzo o dejarlo sin cifrar en absoluto. Eso no sería una gran elección y este documento asume que la TLS oportunista es la opción preferente. Habiendo dicho esto, aunque la criptografía oportunista protege los mensajes durante la transmisión del remitente al receptor, sigue siendo posible para el agresor MITM impersonalizar el destino previsto con un certificado auto-firmado.

Este breve documento describe la situación MITM y varios métodos que los malos ejecutores pueden usar para gestionar los ataques y cubrir todos los componentes para disuadir estos ataques. Esto también introduce a una nueva tecnología, DANE (DNS-based Authentication of Named Entities), que puede ayudar a los proveedores de mensajería a validar que se están comunicando con el destino previsto al usar SSL/TLS.

Mitigar los ataques Man-in-the-Middle (MITM)

En los ataques MITM, los adversarios se interponen ellos mismos entre el remitente del mensaje y el previsto receptor de este:

Todos los siguientes métodos han sido usados por los malos ejecutores para interferir entre remitentes y receptores. La lista no debe ser considerada exhaustiva:

1. ARP spoofing[1].
2. Servidores Rogue DHCP servers[2].
3. Web Cache Communication Protocol (WCCP)[3] (Protocolo de comunicación de caché web).
4. Web Proxy Autodiscovery Protocol (WPAD)[4] (Protocolo de auto-descubrimiento Proxy Web).
5. Puntos de acceso inalámbrico WiFi falsificados (puntos de acceso "evil twin")[5].
6. DNS envenenado[6].
7. Inyección de ruta [7].
8. Dispositivos físicos (en línea) de interceptación de tráfico de red.

Este discurso no tiene en cuenta los ataques de interceptación que están ejecutados en el propio punto final, ni tampoco considera los ataques Man-in-the-Browser o similares. Como con cualquier tecnología, sin unos puntos finales seguros no se puede garantizar una seguridad de datos general.

Riesgos de los ataques MITM

Si los adversarios son capaces de ejecutar con éxito un ataque MITM contra el tráfico de red de texto no cifrado, pueden interceptar el tráfico, modificarlo y/o impersonalizar partes de la comunicación. Si el trafico está cifrado en el trayecto, pero el punto final no está criptográficamente protegido ante los ataques MITM, un adversario puede ejecutar muchos ataques del mismo tipo tanto contra este tráfico cifrado como ante el tráfico de texto sin formato. Por lo tanto, es extremadamente importante que las transmisiones criptográficamente protegidas, también sean protegidas contra los ataques MITM.

En un mundo ideal, el tráfico sería protegido por los usuarios de principio a fin implementando PGP/GPG o S/MIME y también se protegería el tráfico de servidor a servidor con SSL/TLS. Pero la mayoría de los usuarios no usan ni PGP/GPG ni S/MIME. Esto convierte al cifrado de servidor a servidor aún más esencial. Los proveedores de mensajería que quieren impedir los ataques MITM pueden ayudar a proteger el tráfico de servidor a servidor usando métodos donde:

1. Todos los servidores de correo se identifican a sí mismos usando un certificado de confianza a nivel mundial. Es decir, el servidor usa un certificado firmado por una autoridad de confianza certificada a nivel mundial.
2. El nombre de los servidores corresponden al nombre de uno de los domain para el que fue creado el certificado (combinación del servidor y el certificado).
3. Protocolo de comprobación del Estado de un Certificado En línea o The Online Certificate Status Protocol (OCSP) y/o Lista de renovación de certificados o Certificate Revocation List (CRL) ha sido verificado y el certificado no ha sido anulado.

---

1 ARP spoofing, http://en.wikipedia.org/wiki/ARP_spoofing
2 Rogue DHCP, http://en.wikipedia.org/wiki/Rogue_DHCP
3 Web Cache Communication Protocol, http://en.wikipedia.org/wiki/Web_Cache_Communication_Protocol
4 Web Proxy Autodiscovery Protocol, http://en.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol
5 Evil twin (wireless networks), http://en.wikipedia.org/wiki/Evil_twin_%28wireless_networks%29
6 DNS spoofing, http://en.wikipedia.org/wiki/DNS_spoofing
7 Kim Zitter, "Revealed: The Internet's Biggest Security Hole," *Wired Magazine*, August 26, 2008, http://www.wired.com/2008/08/revealed-the-in/

4. El certificado no ha sido usado antes de ser válido y después de haber caducado.
5. El certificado es firmado usando una firma estándar en la industria (SHA-2)[8].
6. El certificado cubre un fuerte par de claves (2048- or 4096-bit RSA).
7. La creación y la recepción del respaldo de un servidor de correo electrónico es la versión más reciente del protocolo TLS (TLS 1.2 en el momento de la creación de este documento).
8. Los servidores se ponen mutuamente de acuerdo en usar el conjunto de cifrado "ciph er suite" que admita el secreto a futuro[9] para intercambiar claves (normalmente Ephemeral Diffie-Hellman [EDH][10] o Elliptic curve Diffie-Hellman Ephemeral [ECDHE])[11]).
9. Un fuerte cifrado simétrico es negociable (idealmente AES-128 or AES-256).

Si *alguna* de las procedentes condiciones no son realizadas entre el MTA emisor y el MTA receptor, el servidor que lo envía no debería transmitir el mensaje al MTA receptor.

Disposición de los mensajes que no pueden ser transportados de forma segura

¿Cómo puede el mensaje no entregable ser procesado de forma segura si el servidor emisor no puede transmitir el mensaje al servidor receptor previsto? Las opciones pueden incluir hipotéticamente:

1. El mensaje puede ser rechazado directamente y devuelto al remitente para procesarlo, suponiendo que el portador emisor y el portador receptor lleguen a un acuerdo de que no pueden intercambiar mensajes de forma segura mientras que la conexión siga establecida. Los mensajes que NO PUEDEN ser entregados de forma segura deben NO ser rebotados al aparente cuerpo de mensaje del remitente (debido a la posibilidad de un falso remitente aparente).
2. Alternativamente, el mensaje puede ser temporalmente puesto en cola y después retirado, una o más veces, lo que ayuda a abordar la no entregabilidad transitoria.
3. Después de proceder con los pasos anteriores (1) o (2), el mensaje puede ser descartado sumariamente. Esto asume que el remitente tiene un mecanismo de confirmación de entrega a nivel de aplicación para detectar las entregas silenciosas en caso de que estas ocurran.

   En general, los mensajes que no pueden ser entregados deben ser manejados de manera consistente de acuerdo con las recomendaciones que se encuentran en la Sección 3.8 de M[3]AAWG Sender Best Common Practices[12].

Direcciones futuras con DANE

DNS-based Authentication of Named Entities (DANE[13, 14]) es una propuesta de IETF para un método que permite que los certificados se vinculen a los nombres del DNS usando DNSSEC. DANE permite a una página web especificar el certificado que utiliza y que debe ser visto por las terceras personas que interactúan con la página web. La identidad de ese certificado debe ser especificado por registros especiales incluidos en el DNS. DNSSEC permite a terceros confiar en los registros DANE que son publicados en el DNS. El DANE será explorado con más detalle y por separado en otro documento del M[3]AAWG.

---

8 SHA-2, https://en.wikipedia.org/wiki/SHA-2
9 Forward secrecy, http://en.wikipedia.org/wiki/Forward_secrecy
10 Diffie-Hellman key exchange, https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
11 Elliptic curve Diffie-Hellman, https://en.wikipedia.org/wiki/Elliptic_curve_Diffie-Hellman
12 M[3]AAWG Sender Best Common Practices, Version 3.0, Updated February 2015, https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_BCP_Ver3-2015-02.pdf
13 RFC 6698: https://tools.ietf.org/html/rfc6698
14 RFC 7218: https://tools.ietf.org/html/rfc7218

Conclusión

Hacer uso de las criptografías oportunistas como se ha descrito en TLS para Correo: TLS for Mail: M³AAWG Initial Recommendations es una excelente manera de empezar a proteger el tráfico del correo electrónico entre proveedores. De todas formas, no está diseñado para impedir los ataques Man-in-the-Middle. The Messaging, Malware and Mobile Anti-Abuse Working Group recomienda que los proveedores de la industria de la mensajería usen los principios descritos en este documento para luchar contra los ataques MITM, prestando más atención a los certificados y el vigor de estos. Es decir, vinculando una identidad a un par de claves criptográficas. Estas directrices no están destinadas a ser consideradas exhaustivas y M³AAWG está trabajando en la creación de una guía adicional para mejorar la protección de la mensajería del usuario.

Fuentes

[1] ARP spoofing, http://en.wikipedia.org/wiki/ARP_spoofing

[2] Rogue DHCP, http://en.wikipedia.org/wiki/Rogue_DHCP

[3] Web Cache Communication Protocol, http://en.wikipedia.org/wiki/Web_Cache_Communication_Protocol

[4] Web Proxy Autodiscovery Protocol, http://en.wikipedia.org/wiki/Web_Proxy_Autodiscovery_Protocol

[5] Evil twin (wireless networks), http://en.wikipedia.org/wiki/Evil_twin_%28wireless_networks%29

[6] DNS spoofing, http://en.wikipedia.org/wiki/DNS_spoofing

[7] Kim Zitter, "Revealed: The Internet's Biggest Security Hole," *Wired Magazine*, August 26, 2008, http://www.wired.com/2008/08/revealed-the-in/

[8] SHA-2, https://en.wikipedia.org/wiki/SHA-2

[9] Forward secrecy, http://en.wikipedia.org/wiki/Forward_secrecy

[10] Diffie-Hellman key exchange, https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

[11] Elliptic curve Diffie-Hellman, https://en.wikipedia.org/wiki/Elliptic_curve_Diffie-Hellman

[12] M³AAWG Sender Best Common Practices, Version 3.0, Updated February 2015 https://www.m3aawg.org/sites/maawg/files/news/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

[13] RFC 6698: The DNS-Based Authentication of Named Entities (DNS) Transport Layer Security (TLS) Protocol: TLSA, https://tools.ietf.org/html/rfc6698

[14] RFC 7218: Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE), https://tools.ietf.org/html/rfc7218

Este documento ha sido traducido al español como un servicio público por GeeksForLess Inc.

M³AAWG097-Spanish