Messaging, Malware and Mobile Anti-Abuse Working Group

M³AAWG Initial Recommendations for Addressing a Potential Man-in-the-Middle Threat
(M³AAWG 잠재적인 중간자 위협에 대처하기 위한 기본 권고 사항)

July 2015

http://www.m3aawg.org/MITM-Recommendations-Korean

소개

메시징 커뮤니티는 이메일 트래픽의 기회적(Opportunistic(best effort)) 암호화의 사용을 장려하는 부분에서 인상적인 진전을 이루었습니다. 그러나, 문서 TLS for Mail: M³AAWG Initial Recommendations 와 IETF Opportunistic Security: Some Protection Most of the Time 에 기술된 기회적 암호화는 MITM(Man-in-the-Middle) 공격(중간자 공격)에 대해 반드시 안전한 것은 아닙니다.

왜 이것이 사실인지 이해하려면, 기회적 암호화가 적절히 사용 될 수 없는 경우 보통 어떤 일이 일어날지 생각해 볼 필요가 있습니다. 이런 경우, MTA(메일 전송 에이전트) 에서 MTA 로의 전송에서 보통 전자 메일 트래픽을 일반 텍스트로 보내게 됩니다. 즉 전혀 암호화되지 않습니다. 결국, 공급자가 선택할 수 있는 것은 최적의 암호화를 허용하거나 혹은 전혀 암호화를 하지 않거나 입니다. 이는 선택지가 부족함을 의미하며, 본 문서에서는 기회적 TLS 를 우선적인 옵션으로 가정합니다. 그러나 기회적 암호화가 발신자에서 수신자로 메시지를 전송하는 동안 메시지를 보호하더라도, 자체 서명된 인증서를 가진 MITM 공격자가 의도된 대상으로 가장하는 것이 가능합니다.

본 문서에서는 간단하게, MITM 상황과 나쁜 행위자들이 MITM 공격을 수행하기 위해 사용할 수 있는 다양한 방법을 설명하고, 이러한 공격을 막기 위한 요소들을 다룹니다. 또한 새로운 기술인 DANE(DNS-based Authentication of Named Entities)를 소개합니다. DANE 는 메시징 공급자가 SSL/TLS 를 사용할 때 의도된 대상과 통신하고 있는지 확인하는 데 도움이 될 수 있습니다.

MITM (Man-in-the-Middle) 공격 완화

MITM 공격에서, 공격자(Adversary)는 메시지의 발신자와 최초 의도된 수신자 사이에 끼어듭니다 :

아래의 방법들은 모두 공격자가 보낸 사람과 받는 사람 사이에 끼어들기 위해 사용되었습니다. 이 목록에 공격방법이 전부 망라된 것으로 간주해서는 안됩니다 :

1. ARP 스푸핑[1]
2. 악성 DHCP 서버 (Rogue DHCP servers)[2]
3. Web Cache Communication Protocol (WCCP)[3]
4. Web Proxy Autodiscovery Protocol (WPAD)[4]
5. 스푸핑 된 WiFi 무선 액세스 포인트 ("evil twin" 액세스 포인트)[5]
6. DNS 중독 (DNS poisoning)[6]
7. BGP 라우트 인젝션[7]
8. 물리적(인라인) 네트워크 트래픽 인터셉션 디바이스

이 논의는 엔드 포인트 자체에서 실행되는 인터셉션 공격을 고려하지 않으며 Man-in-the-Browser 공격 등도 고려하지 않습니다. 어떤 다른 기술과 마찬가지로 보안 엔드 포인트가 없으면 일반 데이터 보안을 보장 할 수 없습니다.

---

[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://wwwwired.com/2008/08/revealed-the-in/

MITM 공격의 위험

만약 공격자가 일반 텍스트 네트워크 트래픽에 대한 MITM 공격에 성공한다면 해당 트래픽을 도청하거나 수정하고 통신 당사자로 위장 할 수 있습니다. 이동(transport) 중의 트래픽이 암호화(encrypted) 되더라도 엔드 포인트가 MITM 공격으로부터 암호화적 보호(cryptographically protect)가 되지 않는 경우, 공격자는 일반 텍스트 트래픽에 대해 동일한 공격을 여러 번 할 수 있습니다. 따라서 전송(transmission)의 암호화적 보호(cryptographically protect)를 통해 MITM 공격에 대해 보호하는 것이 매우 중요합니다.

이상적인 환경이라면, 트래픽은 PGP/GPG 또는 S/MIME 의 사용자 구현에 의해 종단 간(end-to-end)에 보호되며 서버와 서버 간의 트래픽도 SSL/TLS 로 보호됩니다. 그러나 대부분의 사용자는 PGP/GPG 나 S/MIME 을 사용하지 않습니다. 따라서 MITM 공격에 덜 취약한 서버 간 암호화가 더 중요합니다. MITM 공격을 막으려는 메시징 제공 업체는 다음과 같은 방법을 사용하여 서버 간의 트래픽을 보호 할 수 있습니다 :

1. 모든 메일 서버가, 자신의 식별을 위해 전 세계적으로 신뢰할 수 있는 인증서를 사용. 즉, 각 서버는 전 세계적으로 신뢰할 수 있는 인증 기관에서 서명 한 인증서를 사용.
2. 서버의 이름은 인증서가 발급 된 도메인 이름 중 하나를 사용. (서버와 인증서가 서로 일치)
3. 온라인 인증서 상태 프로토콜(OCSP) 및/또는(and/or) 인증서 폐지 목록 (CRL)을 확인하고, 인증서가 해지되어 있지 않음을 확인.
4. 인증서가 유효화 되기 전이나 만료 되지 않았는지 확인.
5. 인증서는 산업 표준 (SHA-2) 서명을 사용하여 서명되어 있을 것.[8].
6. 인증서는 강력한 (2048 또는 4096 비트 RSA) 키 쌍을 가질 것.
7. 발신 메일 서버와 수신 메일 서버가 TLS 프로토콜의 가장 최신 버전을 지원할 것. (이 문서가 발행 된 시점에는 TLS 1.2).

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

8 서버는 키 교환 (일반적으로 Ephemeral Diffie-Hellman [EDH][9] 또는 Elliptic Curve Diffie-Hellman Ephemeral [ECDHE][10])을 위해 forward secrecy[11]을 지원하는 cipher suite 사용에 상호 동의.

9 강력한 대칭 암호를 사용. (이상적으로 AES-128 또는 AES-256)

송신 MTA 와 수신 MTA 간에 위의 조건 중 하나라도 만족하지 않으면 송신 서버는 수신 MTA 에 메시지를 전송해서는 안됩니다.

안전하게 전달할 수 없는 메시지 처리

송신서버가 의도한 수신서버로 메시지를 전송할 수 없는 경우 배달 불가능한 메시지를 안전하게 처리하는 방법은 무엇일까요? 옵션에는 다음 항목들을 가정할 수 있습니다.

1. 발신 호스트와 수신 호스트가 연결되어 있는 동안 안전하게 메시지를 교환 할 수 없다는 합의에 도달했다는 가정하에서, 메시지는 처리를 위해 즉시 거부되어 송신자에게 반송 될 수 있습니다. 안전하게 배달 될 수 없는 메시지는 메시지 본문상의 송신자에게 반송되어서는 안됩니다. (스푸핑된 발신자일 가능성 때문).
2. 그 대신, 메시지를 일시적으로 대기시킨 다음, 한 번 이상 재 시도하여 일시적인 배송 불가 문제를 해결할 수 있습니다.
3. 위의 단계 (1) 또는 (2) 중 하나를 진행한 후에는 메세지를 즉시 삭제할 수 있습니다. 이는 발신자가 응용 프로그램 수준에서 묵시적 배달실패가 발생했을 때 이를 검출할 수 있는 배달 확인 메커니즘을 갖추고 있는 것으로 가정합니다.

일반적으로, 배달 불가 메시지는 M3AAWG Sender Best Common Practices Section 3.8 에 있는 권고 사항에 따라 처리해야 합니다.

DANE 의 향방

DNS-based Authentication of Named Entities (DANE[12, 13])는 DNSSEC 를 사용하여 인증서를 DNS (Domain Name Server) 이름에 바인딩 할 수 있는 방법에 대한 IETF 제안입니다. DANE 를 사용하면

[9] Diffie-Hellman key exchange, https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange
[10] Elliptic curve Diffie-Hellman, https://en.wikipedia.org/wiki/Elliptic_curve_Diffie-Hellman
[11] Forward secrecy, http://en.wikipedia.org/wiki/Forward_secrecy
[12] RFC 6698: https://tools.ietf.org/html/rfc6698
[13] RFC 7218: https://tools.ietf.org/html/rfc7218

사이트에서 사용하는 인증서를 지정할 수 있으며 해당 사이트와 상호 작용하는 서드파티에서 볼 수 있습니다. 해당 인증서의 신원은 DNS 에 포함 된 특수 레코드에 의해 지정됩니다. DNSSEC 는 서드파티가 DNS 에 게시 된 DANE 레코드를 신뢰할 수 있게 해줍니다. DANE 는 별도의 M3AAWG 문서에서 보다 자세히 탐구 될 것입니다.

결론

TLS for Mail: M[3]AAWG Initial Recommendations (TLS for Mail: M3AAWG 기본 권고 사항) 에서 설명된 기회적 암호화를 사용하는 것은 공급자 간의 전자 메일 트래픽 보호를 시작하는 훌륭한 방법입니다. 그러나 이것은 보다 정교한 MITM (Man-in-the-Middle) 공격을 막도록 설계되지 않았습니다. The Messaging, Malware and Mobile Anti-Abuse Working Group 에서는 업계의 메시징 공급 업체가 MITM 공격을 막기위해 인증서와 그 인증서의 유효성에 대한 보다 세심한 주의를 기울이면서 본 문서에 설명된 원칙을 사용할 것을 권고합니다. 인증서의 유효성에 대한 검증은 신원을 암호화 된 키 쌍과 연결 함으로서 가능합니다. 이 지침들은 포괄적으로 간주되도록 의도되지 않았으며, M3AAWG 는 사용자 메시징 보호를 개선하기 위한 추가적인 지침을 작성하기 위해 노력하고 있습니다.

참조

[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

This document was translated as a public service by Qualitia Co., Ltd.

M³AAWG097-Korean