Messaging, Malware and Mobile Anti-Abuse Working Group

TLS for Mail: M³AAWG Initial Recommendations

(메일에서의 TLS: M³AAWG 기본 권고 사항)

December 2014

www.m3aawg.org/TLSforMailBP-Korean

요약

최근 전자 메일 트래픽에 대한 광범위한 감시에 대해 폭로되면서 공급자가 사용자 메일을 보호하기 위해 제공 할 수 있는 기술적 조치에 대한 대중의 관심을 높였습니다. M³AAWG 는 본 문서를 통해 메시지 공급자가 사용자 메일의 보안 및 개인 정보 보호를 강화하기 위해 비교적 신속하게 구현할 수 있는 3 가지 기본 조치를 권고합니다.

서론

본 문서는 비교적 신속하게 구현될 수 있도록 간결하고 단순하게 작성되었습니다. 짧은 문서로 이러한 복잡한 영역의 모든 영향을 탐구할 수는 없겠지만, 추가적으로 관련된 확장 기술문서가 개발되는 동안 권고할 만한 기본적인 접근법을 제공할 수 있다는 큰 이점이 있다는 것이 M3AAWG 의 인식입니다.

본 문서는 메시징 제공 업체가 구현할 수 있는 조치를 중점적으로 다룹니다. 전송 중 혹은 유휴 상태의 메시지 내용의 개인 정보 보호를 위한 PGP/GPG 혹은 S/MIME 의 사용과 같은 추가적인 최종 사용자 제어 암호화 옵션은 다루지 않습니다.

1) 기회적 TLS(Opportunistic TLS)를 사용하여 공급자 간의 메일 흐름 보호

TLS 는 SSL 의 후속으로서 1999 년에 만들어 졌습니다. SSLv2 및 SSLv3 에 대한 여러 가지 알려진 보안 문제로 인해 M³AAWG 는 업계에 SSL 의 모든 버전을 사용하지 못하도록 촉구하고 있습니다. 그러나 IT 관리자는 이 문제가 사용자들, 특히 이전 클라이언트 소프트웨어를 사용하는 이들에게 어떤 영향을 미칠 수 있는지 알고 있어야 합니다. 이전 버전의 TLS 에는 자체적인 보안 이슈가 있음을 유의해야 합니다.

기본적으로 공급자 간의 메일 흐름은 암호화되지 않습니다. 일반적으로 TLS 를 사용하려면 각각의 독립적인 인증서에 기반한 암호화 및 복호화 키가 요구되는데 이 부분이 채택과 사용하는데 큰 장벽임이 입증되었습니다. 그러나 가장 일반적인 메일 전송 에이전트(MTA)는 MTA 에서 MTA 로의 흐름을 도청으로부터 보호하기 위해 임시 세션 기반 키를 사용하여 기회적 TLS 세션 암호화*(1)를 시도하도록 지시될 수 있습니다.

M³AAWG 는 모든 운영자가 모든 메일 서버에서 기회적 TLS 를 사용할 것을 강력히 권고합니다.

한가지 중요한 제한 사항: SMTP 는 hop-by-hop 프로토콜이며 TLS 는 직접 SMTP 세션을 지원하는 TCP 연결의 일부로 작동하기 때문에 기회적 TLS 도 hop-by-hop 기반으로 작동합니다. 메시지 전달 아키텍처의 일부 홉이 TLS 를 사용하더라도 다른 홉이 그러하지 않은 경우 도청에 대한 보호는 그에 따라 불완전하게 됩니다. 그러나, 기회적 TLS 가 완벽하지 않더라도, 적어도 일부 트래픽을 소극적 공격(passive attack)으로 부터 보호하는 데 도움이 될 것이며, 우리는 완벽을 추구하느라 진정한 점진적 개선으로부터 완전히 탈선하지 않기를 촉구합니다. 이미 메일 서버에 기회적 TLS 가 구현된 경우 https://ssl-tools.net/mailservers. [**Note:** link updated July 2018.] 를 방문하여 메일 흐름에 따른 사용자에게 제공되는 기회적 TLS 를 재확인 할 수 있습니다.

M³AAWG 는 특히 메일 서버에서 버전 1.2 이상의 TLS[2]를 사용할 것과 forward secrecy.[3] 를 제공하는 암호화 슈트(Cipher Suite)를 우선할 것을 권합니다.

2) 사내 네트워크 트래픽의 도청 방지

과거에는 전용 링크를 통한 내부 프로바이더 네트워크 트래픽이 일반적으로 안전하다고 간주되어 암호화되지 않았습니다. 그러나, 최근에 공개된 광범위한 네트워크 감시[4]의 규모를 고려하면 이러한 가정은 더 이상 보장되지 않습니다. M³AAWG 는 MTA-to-MTA 메시징 트래픽을 인터넷을 통해 암호화하기 위해 기회적 TLS 를 사용하도록 권고하는 것과 마찬가지로, TLS 또는 대체 암호화 방법을 사용하여 네트워크 인프라 내의 모든 트래픽을 암호화 할 것을 권합니다.

3) 도청으로부터 사용자 비밀번호 보호 (IMAPS/POPS/SMTP Submit/웹메일 인터페이스)

* See, for example, the "recipes" at https://bettercrypto.org/static/applied-crypto-hardening.pdf at section 2.3.

또한, 사용자가 메일박스에 액세스하거나 메시지를 보내기 위해 사용자 이름과 암호를 제공하는 경우 공급자는 해당 자격 증명이 누출되지 않도록 보호하기 위해 암호화를 사용하여야 합니다. 여기에는 아래의 사용이 포함됩니다:

- TLS 를 사용하는 IMAP(또는 POP)
- TLS 를 사용하는 포트 475 또는 STARTTLS 를 사용하는 포트 587 에 대한 메일 서브미션
- TLS 로 보호되는 웹메일 인터페이스

결론

The Messaging, Malware and Mobile Anti-Abuse Working Group 에서는 본 문서에 설명된 기본 암호화 기술을 업계 메시징 공급자가 사용자 메시징 도청에 대한 첫번째 방어 수단으로 사용할 것을 권고합니다. 이러한 권고 사항은 포괄적인 암호화 지침보다는 초기 단계로 고려되어야 합니다. M³AAWG 는 사용자 메시징 보호에 관한 추가 지침을 작성하기 위해 노력하고 있습니다.

참조

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

관련 RFC

- 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

Keywords: Messaging, Malware and Mobile Anti-Abuse Working Group, M³AAWG, mail security, TLS, SMTP, network traffic security, user password security, opportunistic TLS, eavesdropping, pervasive monitoring, transport layer security

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

M3AAWG087-Korean