### Messaging, Malware and Mobile Anti-Abuse Working Group

# TLS for Mail: M³AAWG Initial Recommendations

## Executive Summary

Recent disclosures regarding pervasive monitoring of email traffic have increased public interest in the technical measures that providers can deploy to protect user mail from eavesdropping. In this document, M³AAWG recommends three basic measures that messaging providers can implement relatively quickly in order to enhance the security and privacy of their users' mail.

## Introduction

This document has been kept brief and simple, targeting "low-hanging fruit" that can be implemented relatively quickly. M³AAWG recognizes that a short document cannot explore all the implications of an area as complex as this one, but we feel there is significant benefit in providing a recommended initial approach while additional technical documents are developed that expand on these recommendations.

This document focuses on measures that messaging providers can deploy. It does not attempt to address additional end user-controlled encryption options such as the use of PGP/GPG or S/MIME for privacy of message content, both in transit and at rest.

### *1) Protect mail flows between providers with opportunistic TLS*

TLS, created in 1999, is the successor to SSL. Due to a number of known security issues with SSLv2 and SSLv3, M³AAWG urges the industry to disable all versions of SSL. However, IT managers should be aware of how this may affect their users, especially those with older client software. Note that older versions of TLS have their own set of security issues.

By default, mail flows between providers are not encrypted. In normal use, TLS requires that an encryption/decryption key be based on an independent certificate. This has proven to be a significant barrier to adoption and use. However, most common Mail Transfer Agents (MTAs) can be instructed to attempt to negotiate opportunistic TLS session encryption*(1) by employing ad-hoc, session-based keys to protect MTA-to-MTA flows from eavesdropping on a best-effort basis.

***M³AAWG strongly encourages all operators to enable opportunistic TLS on all mail servers.***

One important limitation to note: SMTP is a hop-by-hop protocol, and since TLS works as part of a TCP connection that supports a direct SMTP session, opportunistic TLS also works on a hop-by-hop basis. If some hops in the message-delivery architecture deploy TLS but others do not, protection against eavesdropping will be correspondingly incomplete. That said, while opportunistic TLS is not perfect, it will help protect at least some traffic from passive attacks and we urge you to avoid the pitfall of letting a quest for the perfect derail you from realizing genuine incremental improvement.

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

If you have already implemented opportunistic TLS on your mail servers, you can review the opportunistic TLS offered to your users along the mail flow by visiting https://starttls.info/.

M[3]AAWG specifically urges you to ensure that your mail server uses TLS version 1.2,[2] rather than an earlier version and that it prefers cipher suites that offer forward secrecy.[3]

***2) Protect intracompany network traffic from eavesdropping***

Historically, internal provider network traffic over dedicated links has usually been assumed to be secure and thus has not been encrypted. Given what has been recently disclosed about the scale of pervasive network monitoring[4], that assumption is no longer warranted. M[3]AAWG urges you to encrypt all traffic within your own network infrastructure, whether with TLS or alternative cryptographic methods, just as we are now recommending that you use opportunistic TLS to encrypt MTA-to-MTA messaging traffic flowing over the Internet.

***3) Protect user passwords from eavesdropping (IMAPS/POPS/SMTP Submit/web email interface)***

Moreover, when users provide their user name and password to access their mailbox or to send a message, providers should use encryption to protect those credentials from interception too. This includes using:

- IMAP (or POP) with TLS
- Mail submission over port 465 with TLS or port 587 with STARTTLS
- Web email interface protected with TLS

## Conclusion

The Messaging, Malware and Mobile Anti-Abuse Working Group recommends that industry messaging providers enable the basic encryption technologies outlined in this paper as first-line defenses against eavesdropping on user messaging. These recommendations should be considered initial steps rather than comprehensive encryption guidance. M[3]AAWG is working to create additional guidance with respect to protecting user messaging.

## References


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


## Related RFCs

- 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, M[3]AAWG, mail security, TLS, SMTP, network traffic security, user password security, opportunistic TLS, eavesdropping, pervasive monitoring, transport layer security