Messaging, Malware and Mobile Anti-Abuse Working Group

Mail のための TLS: M3AAWG Initial Recommendations

December 2014

www.m3aawg.org/TLSforMailBP-Japanese

概要

最近のメールトラフィックの大規模監視に関する告発により、利用者のメールを盗聴から守るためにプロバイダが導入可能な技術的対策について一般の関心が高まっています。この文書では、セキュリティや利用者のメールのプライバシーを強化するために M3AAWG が推奨するプロバイダが比較的速やかに実現可能な 3 つの対策について記述します。

はじめに

本文書は、簡潔でシンプルにすることで、比較的すばやく、ざっくりと実現できるものを目指しています。M3AAWG としては本分野のような複雑な領域を短い文書ですべて説明できるとは考えてはいませんが、推奨の初期設定を提供することで、これらを拡張した更なる技術文書が作成されれば、大きな意味があると感じています。

本文書はメッセージングプロバイダが実装可能な手段にフォーカスするものであり、伝送中、保存中に関わらず、PGP/GPG や S/MIME のようなエンドユーザ側の暗号化オプションについて言及しようとするものではありません。

1) 日和見 TLS によるプロバイダ間のメール経路の保護

1999 年に作られた TLS は SSL を置き換えるもので、SSLv2 と SSLv3 には数多くの脆弱性問題があり、M3AAWG としてはすべてのバージョンの SSL を使用しないことを強く推奨しています。ただし、IT 管理者は、ユーザ、特に古いクライアントソフトウェアを使用しているユーザに対して、どういった影響があるのかは注意すべきで、TLS にも古いバージョンにはいくつかの脆弱性問題が存在するということにも留意すべきです。

デフォルトではプロバイダ間のメールの経路は暗号化されていません。通常、TLS は暗号化/複合化キーが独立した公開鍵証明書に基づいている必要があり、これが採用や利用にあたっての大きな障壁になっています。しかしながら、一般的なメール転送エージェント（Mail Transfer Agent: MTA）では、ベストエフォートで盗聴から MTA 間の経路を守るため

のセッション毎のアドホックなキーを採用することで、TLS セッション暗号化*(1)を利用できるかネゴシエーションするように設定することができます。

M³AAWG はすべてのメールサーバで日和見 TLS を有効にすることを強く奨励します

ひとつ重要な制限として、SMTP はマルチホップな中継プロトコルで、TLS は直接 SMTP セッションをサポートする TCP 接続の一部として動作するため、日和見 TLS もホップ単位で機能します。もし、メッセージ配送構成の内、いくつかのホップでは TLS が実装されているが、そのほかの部分で実装されていなければ、盗聴に対する保護としては相応に不完全となります。つまり、日和見 TLS は完璧なものではなく、少なくともいくらかのトラフィックを受動的な攻撃から保護するのを手助けするものです。少しずつ改善するようにすることから脱線し、完璧を目指すような沼に陥らないことを推奨します。

すでにメールサーバに日和見 TLS を導入済みであれば、https://ssl-tools.net/mailservers を訪れることでユーザに提供した日和見 TLS をメールフローに沿って確認できます。

特に、M³AAWG としてはメールサーバが TLS version 1.2[2] を使用しているかどうか確認することを強く推奨します。また、暗号スイートとして forward secrecy[3] を提供しているものを使用することがより望まれます。

2) 社内ネットワークにおける盗聴からの保護

歴史的に、専用線上の内部ネットワークトラフィックは通常安全であると仮定され暗号化されてきませんでしたが、最近暴露された大規模ネットワーク監視を考慮すると、この課程はもはや正しいとはいえません。M³AAWG としては、インターネット上の MTA 間のメッセージトラフィックに対して日和見 TLS を使用することを推奨しているのと同様に、TLS であれ、他の暗号化手段であれ、保有するネットワークインフラ内のトラフィックもすべて暗号化することを強く推奨します。

3) ユーザパスワードの盗聴からの保護 (IMAPS/POPS/SMTP Submit/web email interface)

加えて、メールボックスにアクセスしたり、メッセージを送信したりするために、利用者がユーザ名やパスワードを送信するとき、プロバイダはこれらの情報を傍受から守るために暗号化すべきです。これらには以下のものを使用することが含まれます。

- TLS を使用した IMAP (or POP)
- TLS を使用した port 465 や STARTTLS を使用した port 587 での認証
- TLS で保護されたウェブメールインターフェース

結論

M³AAWG はメッセージングプロバイダ業界に対して利用者のメッセージを盗聴から防御するための最前線として本文書で概説したような基本的な暗号技術を有効にすることを推

---

* https://bettercrypto.org/static/applied-crypto-hardening.pdf の at section 2.3. のレシピを参照

奨します。これらの推奨事項は包括的な暗号化ガイダンスとしてではなく、最初のステップとして考えるべきです。M³AAWG はユーザのメッセージを保護することに関して追加のガイダンスを作成することに取り組んでいます。

参考文献

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

関連 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

キーワード: 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

この文書は株式会社クオリティア（QUALITIA CO., LTD.）によって産業界への貢献を目的として翻訳されたものです。 https://www.qualitia.co.jp/

M3AAWG087-Japanese