2016 年 秋 村井研 TERM 最終
MTA-STS : SMTP MTA Strict Transport Security を用い暗号化された電子メール通信経路の確立とその実装

尾崎周也 (shuya) *　　親 中島博敬 (nunnun) †
shuya@sfc.wide.ad.jp　　nunnun@sfc.wide.ad.jp

概要

本研究は SMTP におけるクライアント-MTA 間の通信において中間者攻撃の脆弱性が存在する問題に着目し, IETF UTA Working Group で審議中の MTA STS(SMTP MTA Strict Transport Security)[1] を JavaScript にて実装した. なお本実装は MTA-STS のポリシーでメールを送信する初めての実装物である.

1　背景

SMTP は WWW 以前から使用されているメール配送プロトコルの標準技術だ. SMTP は当初の仕様から今日まで改善が続けられており現在も使用されている. 電子メールは配送されるまでに 1 つまたは複数の MTA を経由して配送されるが, その通信経路は必ずしも暗号化されていない問題がある. [図 1]

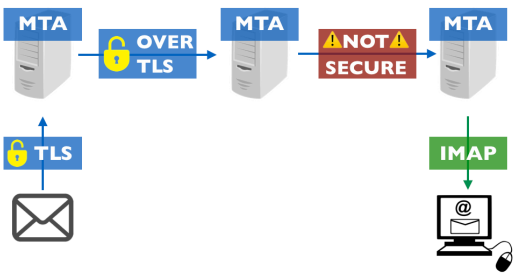

図 1　電子メールの配送経路

STARTTLS 拡張で通信経路の暗号化は行われるが, 日和見暗号化であるため能動的な攻撃を防ぐことは難しい. つまり中間者攻撃には脆弱である. ここに 2 つの攻撃例を示す.

- POODLE 攻撃
- DNS Poisoning

1.1　POODLE 攻撃

POODLE 攻撃とは暗号化された通信から脆弱性をつき情報を盗み出す攻撃だ. 現在はトランスポート層における通信秘匿技術として TLS1.2 の使用が推奨されておりほとんどのサーバやブラウザは TLS1.2 に対応している. しかし全てのサーバ, ブラウザが対応しているとは限らない. そのため互換性を確保するために古い暗号方式での通信リクエストを受ける場合がある. その際, SSL3.0 のようなセキュリティホールが既知化したプロトルで通信をすることが可能となる. このプロトコルのダウングレードを悪用して中間者攻撃を行うのが POODLE 攻撃である.

1.2　DNS Poisoning

DNS Poisoning も考えられる.DNS 応答が偽造・改竄されているサーバに接続した場合, ユーザは意図しない接続先に誘導される. DNSSEC で正当性が証明されない限りそのサーバが意図したものかユーザは判断することができない.

2　研究目的

以上から本研究では中間者攻撃に脆弱である SMTP の現状を問題とし, SMTP-STS によるセキュアな MTA 間通信を実現することを目的にする.

*慶應義塾大学 総合政策学部
†慶應義塾大学 政策・メディア研究科

3　関連技術

3.1　HTTP Strict Transport Security

HSTS は Web サーバがブラウザに対して現在のアクセス以降は HTTP ではなく HTTPS での接続を強制するセキュリティ機構である．SMTP-STS の考えはこれに基づく．

3.2　DNS-based Authentication of Named Entities(DANE)

DANE はドメイン (DNS) とそれに証明書を発行する証明局との紐付けを明確化するセキュリティ機構だ．DANE によってサーバの応答の正当性を担保することができる．

4　提案手法

本研究では上記の問題を解決するために MTA-STS を実装する.MTA-STS は SMTP の中間者攻撃への脆弱性から検討されている新しいセキュリティ機構であり, IETF UTA Working Group で審議中だ.[1]MTA-STS の技術的特徴は 2 点に集約される．

- STARTTLS での通信を強制する．
- 通信経路が暗号化されていなかった場合は報告する, またはメールの受け取りを拒否する．

5　実装

実装はインターネットドラフトで定義されているもののうち, 接続の検証部分を実装した．本実装は WebPKI の取得と DNS からの MTA-STS レコードの取得, 認証に用いられる SSL 証明書の検証を行う．

実装環境としては OS は CentOS6.7 を使用し, 実装言語は JavaScript, クロスプラットフォームは Node.js, MTA は Exim を利用した．システムの構成は次の通りである。

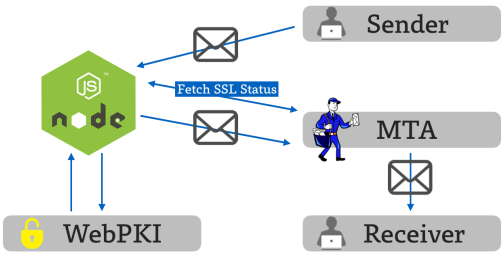

図 2　システム構成図

6　評価

実際に本実装を使用しメールの送信を行い, 認証が正しく行われるかを検証した．MTA-STS ポリシーを保持しかつ運用されている MTA にはメールが送信でき, ポリシーを持たない MTA にはメールが送信できないことを確認した．

7　まとめ

本研究は初めて MTA-STS の認証部分の実装を行なった．実装の過程の中で実運用されているメールサーバの多くは MTA-STS をサポートしていないこと, サポートしていたとしてもドラフトの定義通りに運用されていないことが明らかになった．

参考文献

[1] D. Margolis et al, “SMTP Strict Transport Security”, Internet Draft, March 2016. https://tools.ietf.org/html/draft-margolis-smtp-sts-01

[2] A. Malatras etal, “Technical Recommendations for Improving Security of Email Communications”, MIPRO 2016/ISS

[3] 上野宣. (2005) 『今夜わかるメールプロトコル』翔泳社.