2016 年 秋 村井研 TERM 中間
SMTP-STS : SMTP 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 SMTP STS(SMTP Strict Transport Security)[1] を JavaScript にて実装する. 実装物と既存実装物の相互運用テストを行うとともに, その有用性と問題点を考察する.

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に至る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]

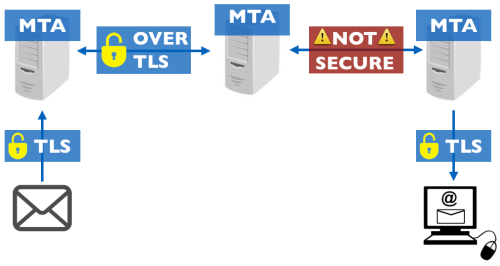

図 1　電子メールの配送経路

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

関連技術は 2 点あげられる.

3.1 HTTP Strict Transport Security (HSTS)

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 SMTP-STS を実装する.SMTP Strict Transport Security (SMTP-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]SMTP-STS の技術的特徴は 2 点に集約される.

- メールプロバイダが特定の認証 (DANE) が有効な TLS 接続上でメールの配送ができることを宣言する.
- 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

実装は特定の機能,TLS 接続の認証の部分にしぼった MVP を実装する予定だ. また 2 つの方法を考えている.

1. Haraka プラグインとして実装する
2. 既存実装を JavaScript で再実装する

Haraka とは Node.js で実装された OSS の SMTP サーバであり, この拡張機能としての実装を目指す. 既存実装を再実装するという点では, 現在 GitHub 上にある実装物 (go,python の 2 つ) は最新のドラフトを反映していないものだ. 本研究ではドラフトを反映させた実装を目指す.

6 評価

評価は実装物と既存実装間で疎通がとれるかに設定する.

7 展望

先述したように本研究では MVP のみの実装を行う.MVP のみを実装する理由は SMTP-STS の土台技術である DNSSEC が正常動作しているサーバが現時点ではまだ少ないためだ.[2] 本研究の MVP と既存実装との疎通が確認された後, ドラフトに従い SMTP-STS の他の機能の実装を行う予定だ.

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] DNSSEC name and shame! https://dnssec-name-and-shame.com/