SMTP Strict Transport Security（SMTP STS）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（総合政策学部/村井純研究室 KUMO研究グループ）

慶應義塾

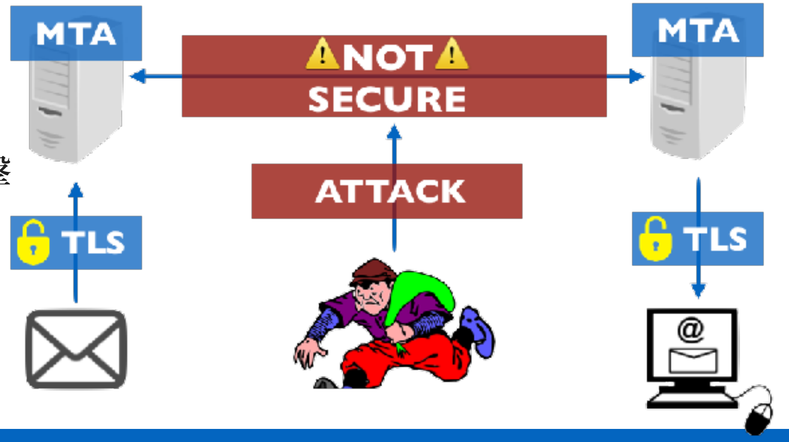
概要

SMTP Strict Transport Security(SMTP STS)とはメールの通信経路においてTLSプロトコルの利用をサーバに強制することで危険な通信経路からの電子メール配送を拒否するインターネット標準化過程にあるプロトコルである。本研究ではSMTP STSをJavaScriptを用いて実装し、その有用性と問題点を明らかにすると共に従来の電子メール配送方法について考察する。

1. 背景

SMTPは標準的な電子メールを転送するプロトコルであり様々な暗号化が施されている。例えばSTARTTLS拡張はSMTPセッションのTLS上での確立を可能とする。しかし以下のような場合はその安全性を保証できない。(i)POODLE攻撃 (ii)MTA間の通信の暗号化が有効でない場合［図１］

上記の例は中間者攻撃に対して脆弱であり、通信経路すべてを暗号化する電子メールの転送方法の確立が求められておりIETFで審議がされている。



［図１］
メール配送での中間者攻撃

2. SMTP STS

SMTP STSは電子メールの転送経路のすべてをTLS上で行うことを強制することでの課題の解決を志向する。これは既にRFC 6797で規定されたHTTP Strict Transport Securityの技術を応用するものである。

3. 関連技術

類似技術にDANEプロトコルがある。ルート認証局に依存しないDNSSECを用い出自と完全性を保証する。一方、SMTP STSは証明を認証局に依存す

4. 実装

本研究ではJavaScriptを用いてSMTP STSの実装を行う。実装物で実際に電子メールを使用することでSMTP STSの有用性と課題を明らかにする。

5. 参考文献

[1] IETF “SMTP Strict Transport Security draft-margolis-smtp-sts-00” https://tools.ietf.org/html/draft-margolis-smtp-sts-00#section-1
[2] Richard Blum. (2001) “*Open Source E-mail Security*”. Sams.

SMTP Strict Transport Security(SMTP STS)を用いてセキュアな方法でメールを送ろうっていう話です。中間者攻撃を防ぐために必要になります。
具体的には通信経路をTLSにのせることを強制するプロトコルです。

類似技術はこんなのがあります
https://ja.wikipedia.org/wiki/HTTP_Strict_Transport_Security