データ保護・誤送信防止のメール技術とは?

~パスワード付きzip添付メール問題を考える~

2021.02.25

SAKURABA Shuji

JPAAWG / IAjapan / ASPC / IIJ

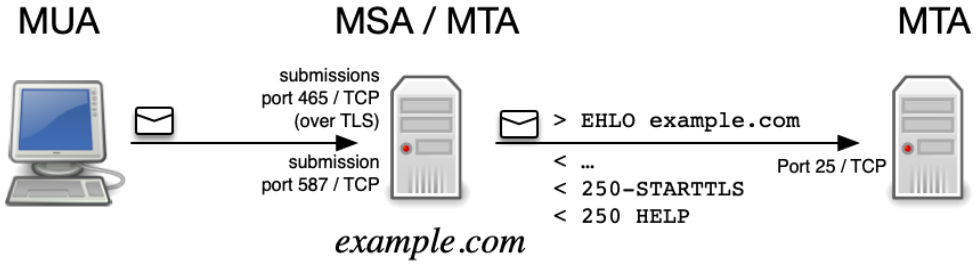
JPAAWG

データ保護のメール技術

- 配送経路の暗号化技術
  - STARTTLS
  - over TLS
  - DANE 関連
- 配送経路暗号化のための技術
  - MTA-STS
  - TLSRPT

SMTP における暗号化技術
TLS

- SMTP (Simple Mail Transfer Protocol)
  - メール投稿 (submission): MUA → MSA
  - メール配送 (mail transfer): MSA/MTA → MTA
- 暗号化手法 (TLS: Transport Layer Security)
  - SMTP セッション中に STARTTLS コマンドを利用
  - TLS セッションから開始 (現在は submissions: port 465 でのみ利用)
    - port 465/tcp は URD (URL Rendezvous Directory for SSM) でも利用
    - smtps (SMTP over TLS) は非推奨だが歴史的経緯から IANA で submissions として再割り当て



SMTP: Simple Mail Transfer Protocol (RFC5321)
MUA: Mail User Agent
MTA: Mail Transfer Agent
MSA: Mail Submission Agent

メールの配送経路の暗号化
STARTTLS

- STARTTLS の普及率
  - Google 透明性レポート (https://transparencyreport.google.com/safer-email/overview)
    - 送信メール 92%, 受信メール 94% (2020.11.25-2021.02.23)
  - 国内での調査
    - 送信メール 69.6%, 受信メール 62.5% (2020.10)

- STARTTLS の課題
  - 受信側が STARTTLS に対応していなければ TLS 配送 (経路暗号化) が行われない → opportunistic encryption protocol
  - 中間者 (man-in-the-middle) が受信側の応答から “250-STARTTLS” を省いたり，一旦 SMTP を終端するなどの手法により，送信側から平文でのメール配送を行わせる → downgrade or interception attacks

メールの配送経路の暗号化
MTA-STS/TLSRPT

- MTA-STS (SMTP MTA Strict Transport Security, RFC8461)
  - 受信側 (ドメイン) が TLS に対応しているかを事前に把握

    _mta-sts.example.com. IN TXT "v=STSv1; id=20160831085700Z;"
  - TLS 通信できなかった場合の対応動作を示す

    https://mta-sts.example.com/.well-known/mta-sts.txt

version: STSv1
mode: enforce
mx: *.example.net
max_age: 604800

- TLSRPT (SMTP TLS Reporting, RFC8460)
  - 送信側が受信側に STARTTLS 等の実施結果を報告する仕組み
  - メールあるいは https による報告 (enforce 設定等でメールが届かない場合もあるため)

_smtp._tls.example.jp. IN TXT "v=TLSRPTv1; rua=mailto:reports@example.jp”
_smtp._tls.example.jp. IN TXT “v=TLSRPTv1; rua=https://reports.example.jp/v1/tlsrpt”

  - フォーマットは JSON 形式 (gzip 圧縮することが望ましい)

メールの配送経路の暗号化
TLSRPTの例


```
{"organization-name":"Google Inc.",
 "date-range":{
     "start-datetime":"2021-02-22T00:00:00Z",
     "end-datetime":"2021-02-22T23:59:59Z"},
 "contact-info":"smtp-tls-reporting@google.com",
 "report-id":"2021-02-22T00:00:00Z_jpaawg.org",
 "policies":[{
     "policy":{
             "policy-type":"sts",
             "policy-string":[
                 "version: STSv1",
                 "mode: testing",
                 "mx: mx.jpaawg.org",
                 "mx: *.jpaawg.org",
                 "max_age: 604800"],
             "policy-domain":"jpaawg.org"},
     "summary":{
             "total-successful-session-count":0,
             "total-failure-session-count":1},
     "failure-details":[{
             "result-type":"validation-failure",
             "sending-mta-ip":"209.85.219.178",
             "receiving-ip":"59.106.222.112",
             "receiving-mx-
hostname":"mx.jpaawg.org",
             "failed-session-count":1}]}]}
```

メールの配送経路の暗号化
DANE (DNS-based Authentication of Named Entities)

- 解決しようとする課題
  - 現在の CA (Certificate Authorities) モデルの課題
  - 中間者攻撃 (Man-in-the-middle attacks)
  - TLS downgrade 攻撃
- DANE 概要
  - DNS を利用して証明書や公開鍵等を公開 (RFC6698, RFC7672)
    - DNSSEC が必須, TLSA RR を利用
  - プロトコル毎に設定 (TLS に対応しているかを判断することが可能)
    - TLSA レコードは _<port>._<protocol>.<hostname> に設定
    - 4つのパラメータ (certificate usage, selector, matching type, certificate association data)

```
_25._tcp.mail.ietf.org.      IN TLSA  3 1 1 0C[…]D6
_443._tcp.www.ietf.org.  IN TLSA  3 1 1 0C[…]D6
```

DANE 関連技術

- RFC7672 (Proposed Standard)
  - SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)
- RFC7929 (Experimental)
  - DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP
    - DNS の RR として OPENPGPKEY を利用
- RFC8162 (Experimental)
  - Using Secure DNS to Associate Certificates with Domain Names for S/MIME
    - DNS の RR として SMIMEA を利用