EAP-TTLS の概要

国立研究開発法人 情報通信研究機構

1. 基本情報

✧ 名前

Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)

✧ 機能

EAP において、TLS を用いて使用する暗号アルゴリズムのネゴシエーションとサーバ認証・鍵交換を実現し、ユーザ名とパスワードを用いてクライアント認証を実現すること目的としたプロトコル。

✧ 関連する標準

RFC5281 (https://tools.ietf.org/html/rfc5281)

2. プロトコル仕様

EAP-TTLS のプロトコル仕様の概要を解説する。EAP-TTLS では、ピア（クライアント)、アクセスポイント、TTLS サーバ、アプリケーションサーバの 4 つのロールが設定されている。EAP-TTLS では、EAP の Type フィールドが EAP-TTLS に設定される。以下、EAP-TTLS の Data フィールドのペイロードについて説明する。なお、アクセスポイントと TTLS サーバは、受信したパケットのメッセージを転送するだけの場合があり、この場合、シーケンス図中では paththrough と表記されている。以下では、転送されるメッセージのペイロードについては説明しない。

✧ メッセージ 1：EAP-Request/Identity

Data フィールドは何も含まない。

✧ メッセージ 2：EAP-Response/Identity

Data フィールドはピアの ID を含んでも良いが、プライバシ保護の観点から含まなくても良い。

✧ メッセージ 3：EAP-Request/TTLS (TLS Start)

Data フィールドは「Start ビット」を含む。

✧ メッセージ 4：EAP-Response/TTLS (TLS client_hello)

- TLS client_hello：以下のペイロードを含む。
  - クライアントのバージョン。
  - 乱数 client_random
  - [セッション ID session-id]
  - 利用可能な暗号スイートのリスト。
  - 利用可能なハッシュ関数のリスト。

✧ メッセージ 5：EAP-Request/EAP-TTLS (TLS server_hello, TLS certificate, [TLS server_key_exchange], TLS certificate_request, TLS server_hello_done)

- TLS server_hello：以下のペイロードを含む。
  - サーバのバージョン。
  - 乱数 server.random
  - セッション ID session-id（生成方法は後述）
  - 選択された暗号スイート cipher_suite
  - 選択されたハッシュ関数 compression_method
- TLS certificate：以下のペイロードを含む。
  - 公開鍵証明書、方式としては、RSA、DHE-DSS、DHE-RSA、DH-DSS、DH-RSA がある。
- TLS server_key_exchange：オプションであり、クライアントが premaster secret を変更するために十分な情報を certificate ペイロードが含まない場合にのみ用いられる。
  - 鍵交換アルゴリズム。
  - 公開パラメータとサーバの暫定的な公開鍵。
- TLS server_key_exchange：オプションであり、クライアントが premaster secret を変更するために十分な情報を certificate ペイロードが含まない場合にのみ用いられる。
  - 鍵交換アルゴリズム。
  - 公開パラメータとサーバの暫定的な公開鍵。
- TLS certificate_request：以下のペイロードを含む。
  - 利用可能な証明書のリスト。
  - 利用可能な認証局のリスト。
  - TLS server_hello_done：定数

✧ メッセージ 6：EAP-Response/EAP-TLS (TLS certificate, TLS client_key_exchange,

TLS certificate_verify, TLS change_cipher_spec, TLS finished)

- TLS certificate：ピアの公開鍵証明書
- TLS client_key_exchange：premaster secret を共有するためのデータ。RSA を用いる場合にはサーバの公開鍵で暗号化された premaster secret。DH を用いる場合には公開する値 g^x である。
- TLS certificate_verify：メッセージ 3～5 の TLS メッセージに対する署名値。
- [TLS change_cipher_spec]：OPTIONAL。暗号スイートのスペックを変更するための値。
- TLS finised メッセージは鍵共有が成功したことを確認するための verify_data を含む。

  Verify_data=PRF(master_secret, finished_label,
  MD5(handshake_message)+SHA1-128(handshake_message))
  Finished_label：固定値「client finished.」である
- Handshake_message:メッセージ 3～6 の TLS メッセージすべてを結合したデータ。

✧ メッセージ 7：EAP-Request/EAP-TTLS (TLS change_cipher_spec, TLS finished)

- TLS certificate：ピアの公開鍵証明書
- TLS finised メッセージは鍵共有が成功したことを確認するための verify_data を含む。
  - Verify_data=PRF(master_secret, finished_label,
    MD5(handshake_message)+SHA1-128(handshake_message))
  - Finished_label：固定値「client finished.」である。
  - Handshake_message:メッセージ 3～7 の TLS メッセージすべてを結合したデータ。

✧ メッセージ 8：EAP-Response/EAP-TLS (Challenge)

- ピアの username を暗号化したデータ。TLS では、MAC then ENC で暗号化を行う。
- 認証用の EAP-TLS_challenge を暗号化したデータ
  - EAP-TLLS_challenge = PRF-nn(master_secret,
    “”ttls challenge”, client_random+server_random)
  - EAP-TTLS では、TTLS サーバが AAA サーバに master_secret を転送するための方法は記述されていない。

✧ メッセージ 9：EAP-Success

Data フィールドは何も含まない。

鍵階層は以下のとおり。

- Master_secret
  = PRF(pre_master_secret, “master_secret”, client_random+server_random)
- MAC 鍵||暗号化鍵
  = PRF(master_secret, “key expansion”, server_random+client_random)

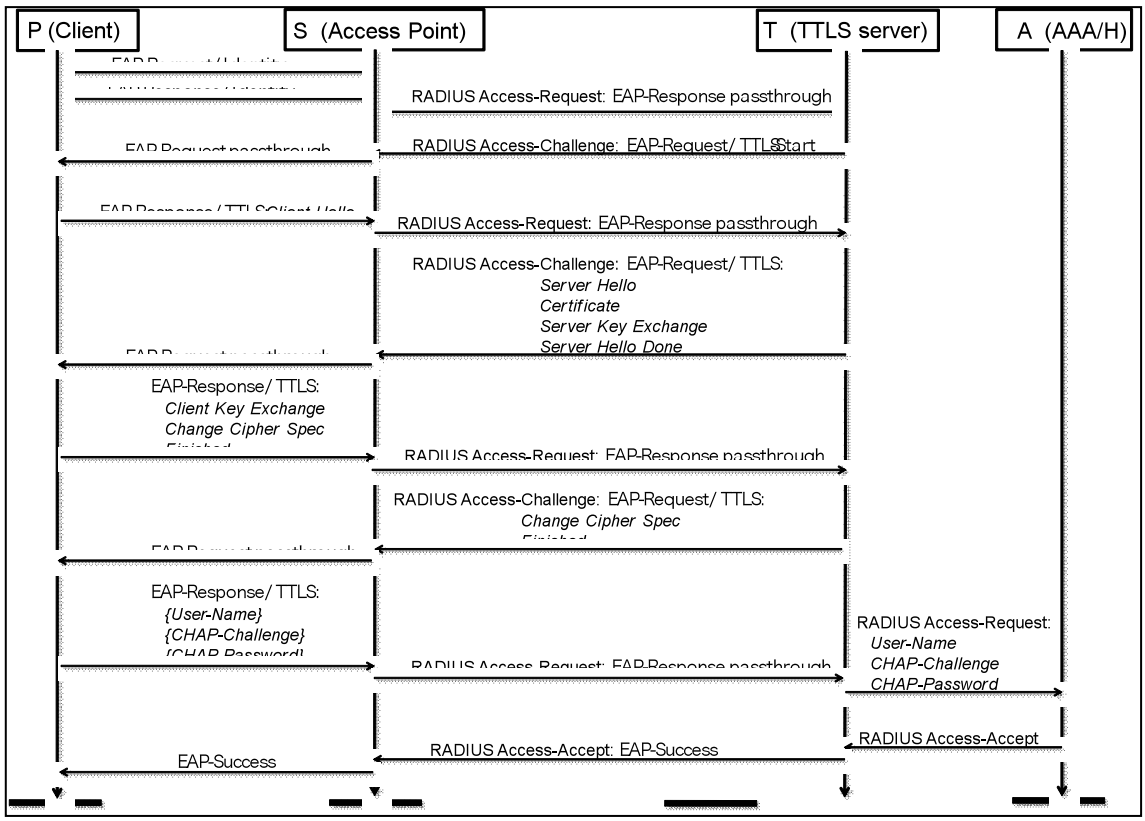

図 1. シーケンス図

3. 攻撃者モデル（自然言語による記述）

攻撃者として Dolev-Yao モデルを想定する。すなわち、通信の盗聴、改ざん、遮断、再送が可能とする。

4. セキュリティ要件（自然言語による記述）

RFC3748 では、暗号プロトコルの安全性について記述するためにいくつかの例を示しており、多くの場合これに従ってセキュリティプロパティが記述される。EAP-TTLS については、以下のように記述されている。

- Ciphersuite negotiation: Yes

- Mutual authentication: Yes, in recommended implementation
- Integrity protection: Yes
- Replay protection: Yes
- Confidentiality: Yes
- Key derivation: Yes
- Key strength: Up to 384 bits
- Dictionary attack prot.: Yes
- Fast reconnect: Yes
- Cryptographic binding: No
- Session independence: Yes
- Fragmentation: Yes
- Channel binding: No

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

EAP-TTLS について、現時点で知られている脆弱性はない。

5.2. 形式手法に基づく検証

AVISPA による評価結果が

http://www.avispa-project.org/library/EAP_TTLS_CHAP.html

に掲載されている。

6. 備考

本文書は、**総務省「暗号・認証技術等を用いた安全な通信環境推進事業に関する実証実験の請負　成果報告書**」からの引用である。