EAP-AKA 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 Method for 3rd Generation Authentication and Key Agreement

- ✧ 機能

  移動体通信（3G）における認証モジュール IM を用いた相互認証・鍵交換プロトコル。暗号として IM に組み込まれた AKA アルゴリズムを利用する。

- ✧ 関連する標準

  RFC4187（http://www.ietf.org/rfc/rfc4187.txt）

2. プロトコル仕様

EAP-AKA のプロトコル仕様の概要を解説する。

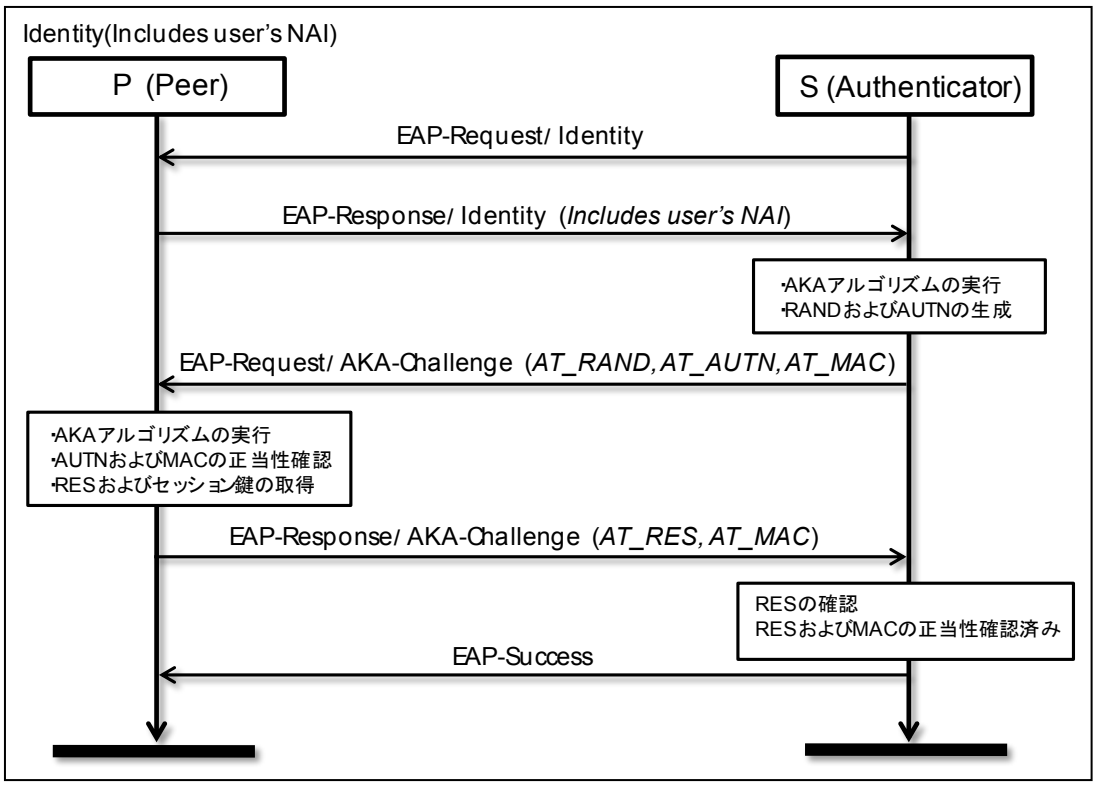

図 1. シーケンス図

2.1. EAP 全般について

EAP パケットは以下の 4 種類のフィールドで構成される。

- ✧ Code：パケットの種類を特定するための定数。Request, Response, Success, Failure の 4 種類がある。
- ✧ Identifier：Request と Response を対応させるためのフィールド。
- ✧ Length：パケット全体の長さ。
- ✧ Data：任意のペイロードであり、RFC3748 の中では規定されない。

Code フィールドが Request もしくは Response の場合、さらに以下のとおり。

- ✧ Type：Request/Response で運ぶペイロードの種類を指定するフィールド。RFC3748 では 8 個の値が指定されており、デフォルトの認証方式は MD5-Challenge もしくは One Time Password である。EAP 上で拡張方式による認証を行う場合には、Type フィールドで認証方式を指定する。
- ✧ Type-Data：Type で指定された型のペイロード。

2.2. EAP-AKA について

EAP-AKA は、きちんと認証を行う full authentication procedure に加えて、再認証方式などいくつかの暗号プロトコルを定義している。本評価では、full-authentication procedure を評価対象とする。以下、EAP-AKA における Data フィールドのペイロードについて説明する。上記のシーケンス図におけるメッセージのペイロードは以下のとおりである。

- ✧ 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 を含む。
- ✧ メッセージ 3：EAP-Request/AKA-Challenge
  Data フィールドは RAND, AUTN, MAC の 3 つの値を含む。
  - ➢ RAND：Authenticator（以下、ロール A）が生成する乱数
  - ➢ AUTN：認証用データ。AKA では、シーケンス番号 XOR AK、アルゴリズム及び鍵を指定する情報（AMF)、MAC を含むとしている。AK=f5(事前共有鍵, RAND)
  - ➢ MAC：EAP ペイロード全体に対する MAC 値。計算には事前共有鍵を用いる。
- ✧ メッセージ 4：EAP-Response/AKA-Challenge
  Data フィールドは RES の値を含む。

- RES：チャレンジ RAND に対するレスポンス。RES=f1(事前共有鍵, RAND)

なお、f1, f2, f5 はそれぞれに定義された関数である。

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-AKA については、以下のように記述されている。

- Mutual authentication: Yes
- Integrity protection: Yes
- Replay protection: Yes
- Confidentiality: Yes, except method-specific success and failure indications
- Key strength: EAP-AKA supports key derivation with 128-bit effective
- Dictionary attack protection: N/A (Section 12.5)
- Session independence: Yes (Section 12.4)

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

EAP-AKA 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_AKA.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。