EAP-SIM 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 Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)

✧ 機能

FDD-TDMA 方式で実現されている第二世代携帯電話規格 (GSM) における SIM を用いた相互認証・鍵交換プロトコル。

✧ 関連する標準

RFC4186 (https://www.ietf.org/rfc/rfc4186.txt)

2. プロトコル仕様

GSM では、チャレンジ・レスポンスによる片側認証が実装されている。しかし、相互認証のメカニズムが提供されておらず、セッション鍵が 64 ビットしかないことから、EAP-SIM により相互認証及び 128 ビットの鍵配布を実現する。

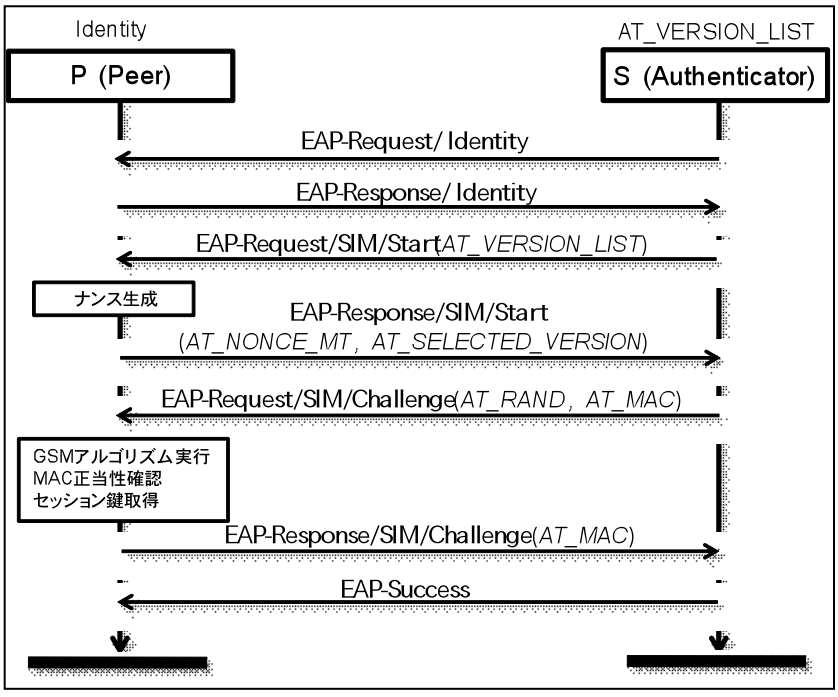

図 1. シーケンス図

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-SIM について

EAP-SIM 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。また、MAY で記述されている属性値は省略する。以下、EAP-SIM における Data フィールドのペイロードについて説明する。EAP-SIM では、EAP の Type フィールドを SIM に設定する。また、EAP-SIM では、さらに Subtype と Reserved というフィールドが設定されている。Subtype フィールドの値は EAP-AKA [RFC4187]から引用している。Full authentication procedure では、Start, Challenge の 2 つの値を用いる。本評価では、Reserved フィールドの値については言及しない。上記のシーケンス図におけるメッセージのペイロード（属性値）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/SIM/Start
  Data フィールドはサーバが利用可能な暗号方式のリスト
  (VersionList) を含む。
- ✧ メッセージ 4：EAP-Response/AKA-Challenge
  Data フィールドは、ピアが選択した暗号方式 (SelectedVersion)、

ピアが生成するナンス NONCE_MT の値を含む。

✧ メッセージ 5：EAP-Request/SIM/Challenge

Data フィールドは、サーバが生成するナンス RAND を含む。また、EAP パケット、NONCE_MT と事前共有鍵から生成した MAC 値を含む。

✧ メッセージ 6：EAP-Response/SIM/Challenge

Data フィールドは、EAP パケット、ナンス RAND と事前共有鍵から生成した MAC 値を含む。

✧ メッセージ 7：EAP-Success

Data フィールドは何も含まない。

2.3. 鍵階層について

✧ Ki：SIM に格納されている鍵

✧ SRES ,Kc：Ki と RAND から生成される値

- SRES|Kc = GSM の乱数生成機能(RAND, Ki)

✧ MK：マスター鍵

- MK=SHA1(ピア ID, Kc の繰り返し, NONCE-MT, VersionList, SelectedVersion)

✧ Kaut：MAC 生成用鍵

- Kaut=PRF-SHA1(MK)

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-SIM については、以下のように記述されている。

- Mutual authentication: Yes (Section 12.3)
- Integrity protection: Yes (Section 12.9)
- Replay protection: Yes (Section 12.9)
- Confidentiality: Yes
- Key derivation: Yes
- Dictionary attack protection: N/A (Section 12.7)
- Cryptographic binding: N/A

- Session independence: Yes (Section 12.6)

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

EAP-SIM 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_SIM.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。