暗号プロトコル評価対象の概要

独立行政法人　情報通信研究機構

1.プロトコル名：Extensible Authentication Protocol Method for Global System for Mobile Communications(GSM) Subscriber Identity Modules

2.関連する標準：RFC4186 (http://www.ietf.org/rfc/rfc4186.txt)

3.暗号プロトコル仕様

Extensible Authentication Protocol Method for Global System for Mobile Communications(GSM) Subscriber Identity Modules(以下、EAP-SIM) について解説する。

3.1.暗号プロトコルの概要と目的

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いないこと、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。

シーケンス図

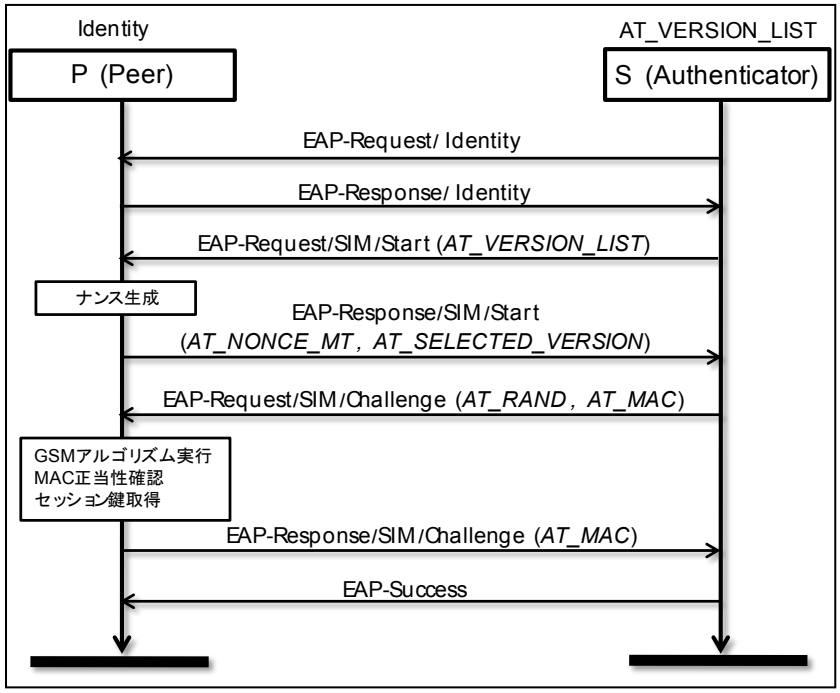

図 1.シーケンス図

○EAP-SIM

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/SIM/Start
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。
- MAC=HMAC-SHA1-128(Kaut, EAP パケット, NONCE-MT)
MAC 用の事前共有鍵 Kaut は SIM に格納された秘密情報から生成される。
・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。
- MAC=HMAC-SHA1-128(Kaut, EAP パケット, SRES の繰り返し)
・メッセージ 7：EAP-Success
Data フィールドは何も含まない。

○鍵階層
・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)

4.評価の環境

4.1.攻撃者モデル（自然言語による記述）

インターネットプロトコルでは、Dolev-Yao モデルの想定が一般的である。

4.2.セキュリティプロパティ（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、以下の性質を持つと主張されている。

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)

4.3.暗号プロトコルに関して知られている結果

〇脅威/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。

〇Formal Method 等による検証：

http://www.avispa-project.org/library/EAP_SIM.html に AVISPA による評価結果が掲載されている。

5.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。