EAP-IKEv2 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

  The Extensible Authentication Protocol-Internet Key Exchange Protocol version 2 (EAP-IKEv2) Method

- ✧ 機能

  AP (Access Point) peer と EAP server 間の相互認証・鍵交換プロトコル。

- ✧ 関連する標準

  RFC5106 (https://www.ietf.org/rfc/rfc5106.txt)

2. プロトコル仕様

EAP-IKEv2 のプロトコル仕様の概要を解説する。RFC5106 では以下が記述されている。

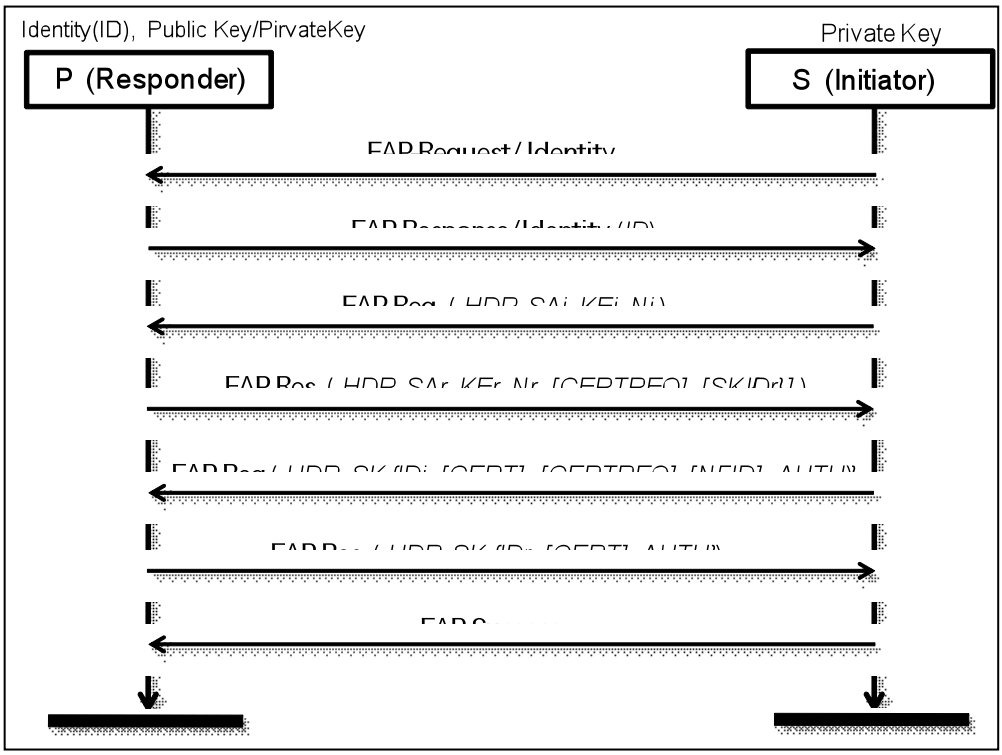

図 1. シーケンス図

✧ Figure 1: EAP-IKEv2 Full, Successful Protocol Run (p.7)

✧ Figure 2: Fast Reconnect Protocol Run (p.10)

✧ Figure 3: Error Handling in case of Unsupported D-H Value (p.14)

本評価では、正常系である Figure 1：EAP-IKEv2 Full, Successful Protocol Run (p.7) を対象とする。EAP-IKEv2 プロトコルは EAP 上で IKEv2 鍵交換プロトコルを実行し、ペイロードや鍵導出の方法は IKEv2 に準拠している。

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-IKEv2 については、以下のように記述されている。

- Ciphersuite negotiation: Yes
- Mutual authentication: Yes
- Integrity protection: Yes
- Replay protection: Yes
- Confidentiality: Yes
- Key derivation: Yes (see Section 5)
- Key strength: Variable
- Dictionary attack prot.: Yes (see Section 10.7)
- Fast reconnect: Yes (see Section 4)
- Crypt. binding: N/A
- Session independence: Yes (see Section 10.10)
- Defragmentation: Yes (see Section 10.11)
- 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-IKEv2 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_IKEv2.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。