IKE-SIG 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 Internet Key Exchange (IKE)

- ✧ 機能

  IPsec の前に実行する鍵交換プロトコル。認証に電子署名を使用。

- ✧ 関連する標準

  RFC2409 (https://tools.ietf.org/html/rfc2409)

2. プロトコル仕様

IKE Phase 1 では、Main モード（標準モード: 実装必須）と Aggressive モード（簡易モード）の 2 種類がある。また、Phase 1 における認証方式として、署名による認証、公開鍵暗号による認証、改良公開鍵暗号による認証、既知の共有鍵による認証の 4 つの方式が定められており、IKE-PSK では署名を使用する。図 1 に、署名による認証を用いた Main モードの暗号プロトコルを示す。

3. 攻撃者モデル（自然言語による記述）

RFC2409 ではリプレイ攻撃などを想定しているが、本文書では、より強い攻撃者として 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）

- ➢ 認証：エンティティ P とエンティティ S はお互いに通信相手が誰であるかを正しく確認することができ、攻撃者によりなりすまされない。
- ➢ 鍵交換：エンティティ P とエンティティ S の共有するセッション鍵が想定されていないエンティティに対して秘匿されていることが必要である。

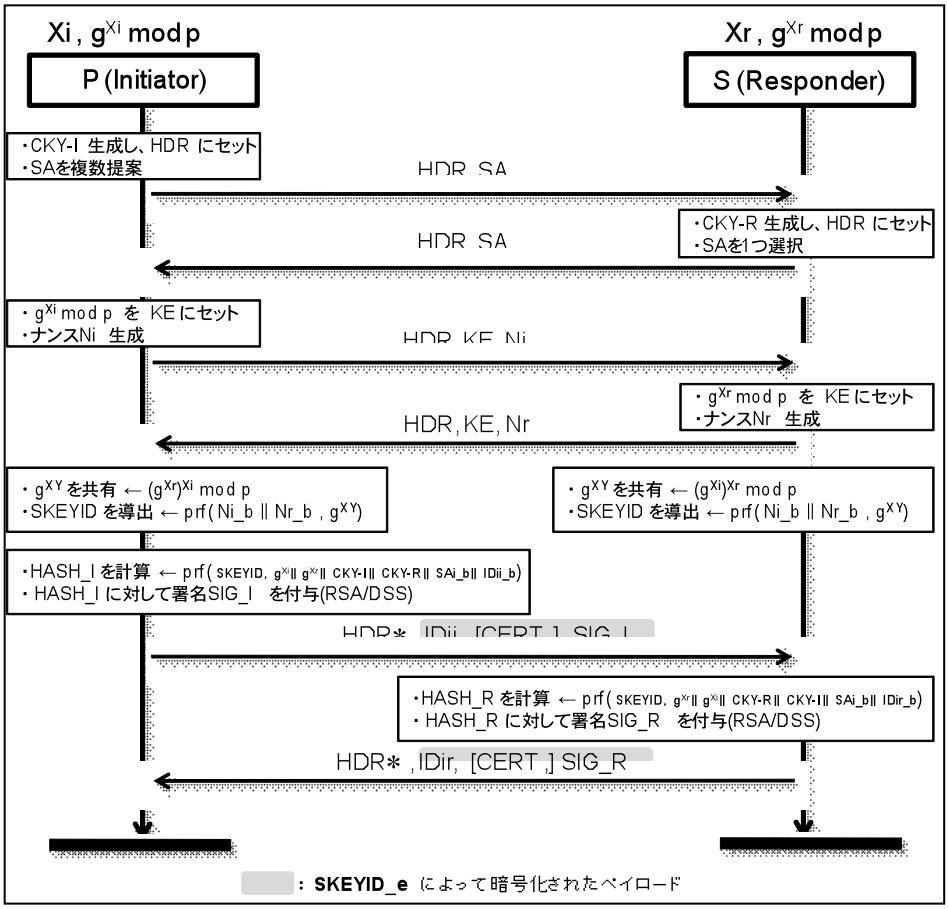

図 1. シーケンス図

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

RFC2409 における「10. Security Consideration」において、Quick モードを使用しての鍵交換の繰り返しによって、Diffie-Hellman 共有鍵のエントロピーが減少するなど、セキュリティについての考慮事項が記載されている。

5.2. 形式手法に基づく検証

Scyther による評価結果が以下で実施されている。

Cas Cremers, “Key exchange in IPsec revisited: Formal analysis of IKEv1 and IKEv2,” http://www.cosic.esat.kuleuven.be/esorics2011/slides/Session_06_Cryptography_Protocol_Analysis/1410_Cremers.pdf.

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。