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

  Internet Key Exchange Protocol Version 2 (IKEv2)

- ✧ 機能

  IPsec の前に実行する相互認証・鍵交換プロトコル。 IKEv1 との互換性は確保されていない。 暗号化方式として 3DES、ハッシュ関数として SHA-1 が規定されている。

- ✧ 関連する標準

  RFC5996 (https://tools.ietf.org/html/rfc5996)

2. プロトコル仕様

IKEv2 のシーケンスを図 1 に示す。

3. 攻撃者モデル（自然言語による記述）

RFC5996 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。

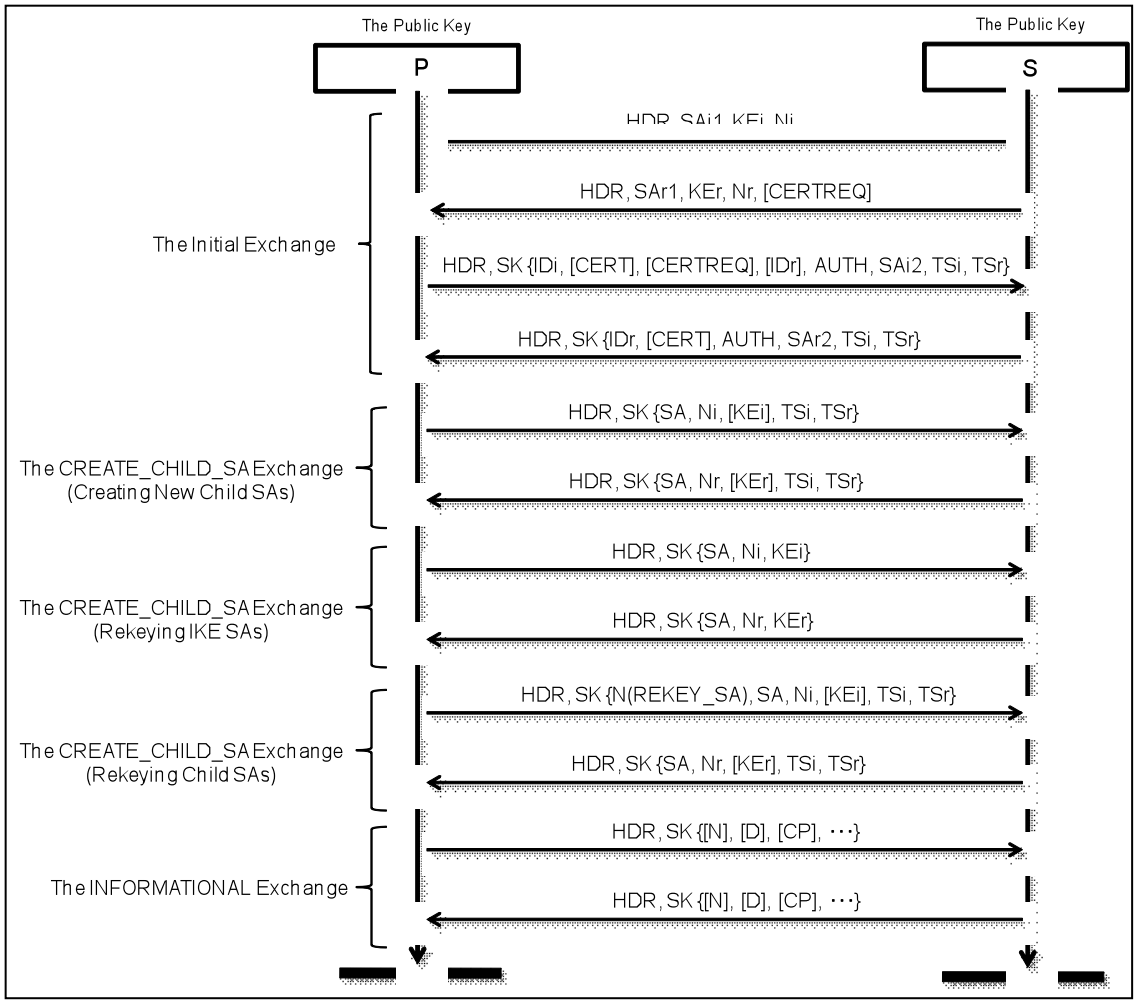

図 1. シーケンス図

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

RFC5996 の「5. Security Considerations」において、以下の脆弱性が指摘されている。

①追加の Diffie-Hellman 交換なしでの CREATE_CHILD_SA の使用による繰り返しの再入力では、すべての SA にとって単一キーの暗号解読に対する脆弱性を生む。

②イニシエータが認証される前に、IKE_SA_INIT と IKE_AUTH exchanges が始まると、結果として、安全ではないネットワーク上に置かれた場合に、この暗号プロトコル実装を完全に堅牢にする必要がある。

③事前共有鍵を使用する場合に、パスワードや名前、または他の低エントロピーソースから共有化される秘密を導出すると、辞書攻撃やソーシャルエンジニアリング攻撃の対象となる。

④次の AUTH ペイロードのサブシーケンスを保護するための共有鍵を生成しない EAP 認証方

式を使用する場合は、特定の中間者攻撃及びサーバ偽装攻撃が可能である。

5.2. 形式手法に基づく検証

AVISPA による評価結果が以下に掲載されている。

- http://www.avispa-project.org/library/IKEv2-DS.html
- http://www.avispa-project.org/library/IKEv2-DSx.html
- http://www.avispa-project.org/library/IKEv2-MAC.html
- http://www.avispa-project.org/library/IKEv2-MACx.html
- http://www.avispa-project.org/library/IKEv2-CHILD.html

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。