Yahalom-Lowe's modified 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

  Lowe's modified version of Yahalom

- ✧ 機能

  共通鍵暗号の鍵サーバを用いた相互認証・鍵交換プロトコル。

- ✧ 関連する文書

  Gavin Lowe, "Towards a completeness result for model checking of security protocols," Technical Report 1998/6, Dept. of Mathematics and Computer Science, University of Leicester, 1998.

2. プロトコル仕様

Yahalom-Lowe's modified は Yahalom のバリエーションである。以下にシーケンス図を示す。

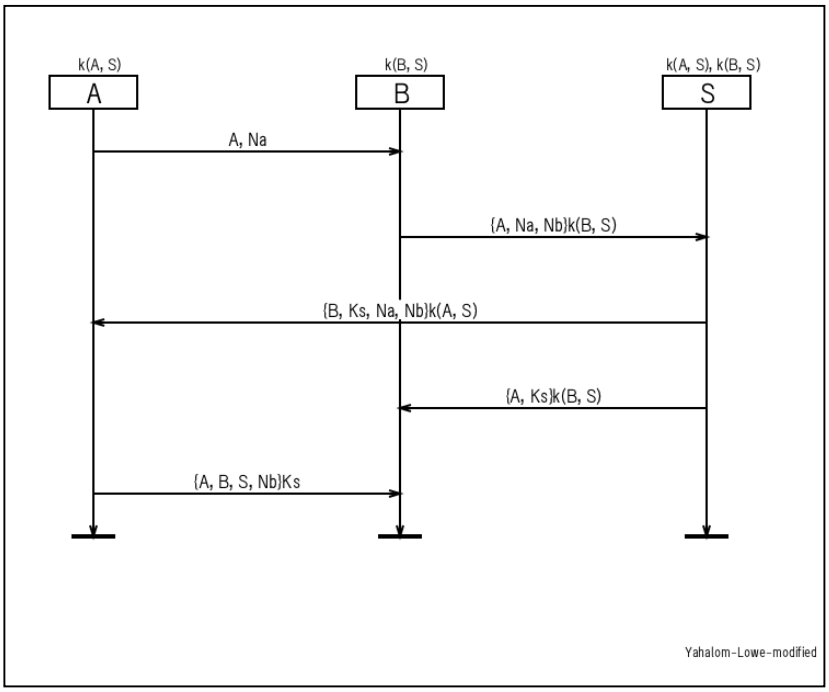

図 1. シーケンス図

3. 攻撃者モデル（自然言語による記述）

上述の元論文では、“this intruder is assumed to have complete control over the communications network, and so can intercept messages, and introduce new messages into the system using information from messages he has previously seen.”と述べており、攻撃者として Dolev-Yao モデルを想定している。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）

上述の元論文では、Yahalom-Lowe's modified について、特別なセキュリティ要件を定義していない。そこで、Yahalom と同じく、以下が成り立つことを期待する。

- セッション鍵 Kab が正しく配布されたこと。
- ロール A とロール B は互いの存在を確認できたこと。

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

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

上述の元論文で、モデルチェックツール FDR を用いて検証している。

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。