Yahalom 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

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

M.Burrows, M.Abadi, and R.Needham, “A Logic of Authentication,” Research Report 39, Digital Equipment Corp. Systems Research Center, Feb. 1989.

2. プロトコル仕様

Yahalom のシーケンス図を示す。ユーザは鍵サーバとの間で事前に鍵を共有していると仮定する。なお、上述の元論文では、BAN ロジックという論理記述と論理変換を用いて Yahalom プロトコルの安全性を証明することを試みている。

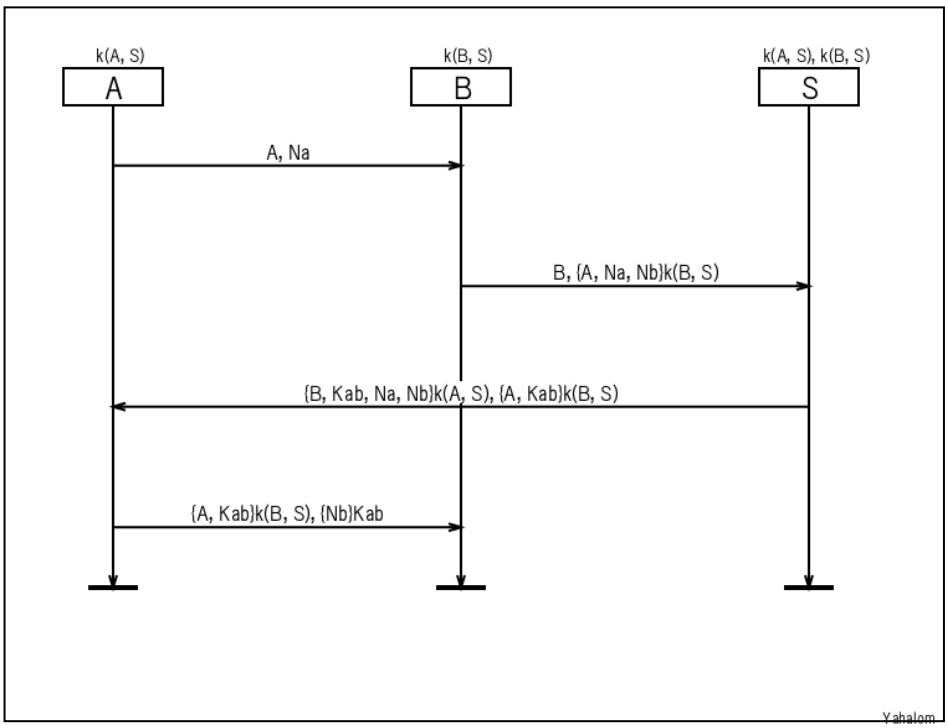

図 1. シーケンス図

3. 攻撃者モデル（自然言語による記述）

上述の元論文で、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、以下の性質が成り立つことを BAN ロジックを使って証明している。

- 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

上述の元論文では、Yahalom について１つの脆弱性を指摘している。暗号プロトコルの最後にロール A からロール B に送信されるメッセージは、ロール B が生成したナンスを含まないデータと、ロール A が復号できるデータで構成されている。したがって、ロール A-B 間で、複数のセッションを行う場合、ロール A は前のセッションで取得したメッセージから、次のセッションの最後のメッセージを偽造できる。

5.2. 形式手法に基づく検証

Paulson は、以下の文献の中で、Isabelle/HOL を用いて Yahalom を評価している。

- Lawrence C. Paulson, “Relations between secrets: Two formal analyses of the yahalom protocol,” J. Computer Security, 2001.

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。