Yahalom-Paulson'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

  Paulson's strengthened 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

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

2. プロトコル仕様

Yahalom-Paulson's modified は Yahalom のバリエーションの 1 つである。元論文では、脆弱性が指摘されている。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。

Yahalom-Paulson's modified は、最後のメッセージにロール B が生成するナンスを追加するなどして、安全性の強化を目指したプロトコルである。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）

上述の元論文で、“Like most such models, it includes a spy who is in control of all communications.”と述べており、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-Paulson's modified のセキュリティ要件について詳しく述べていない。しかし、Yahalom プロトコルと同じく、以下の性質が成り立つことが期待されていると考えられる。

- 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。

また、これに加えて、Yahalom-Paulson's modified の脆弱性（セッション間の独立性）を満たすことが期待されている。

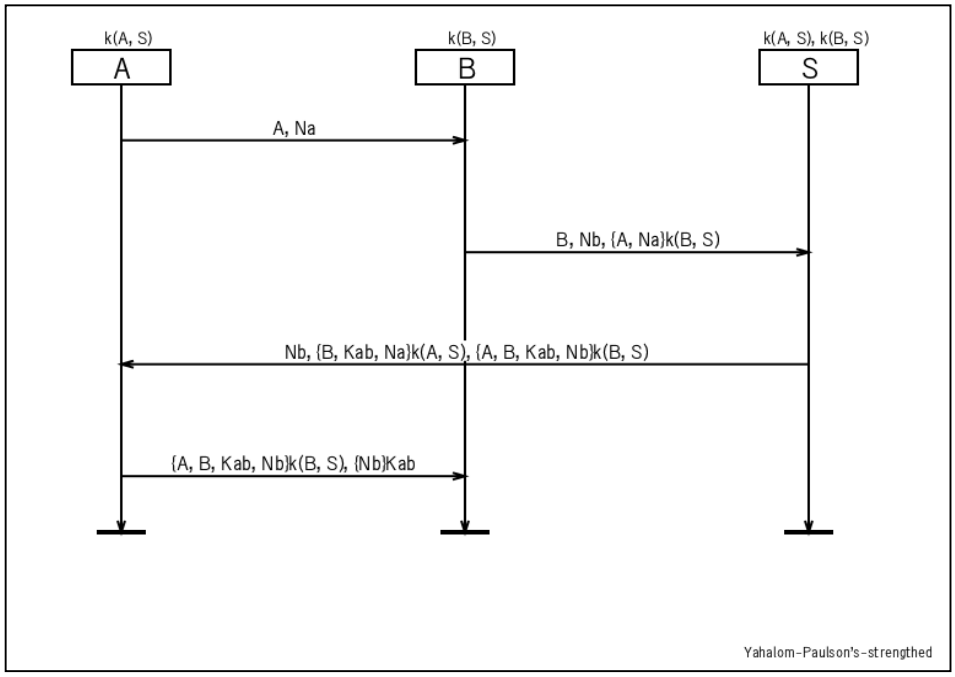

図 1.　シーケンス図

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

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

Paulson は、以下の文献の中で、Isabelle/HOL を用いて本プロトコルを評価している。

- 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。