Yahalom-BAN simplified 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

  BAN simplified 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

  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-BAN simplified は元論文で指摘された Yahalom の問題を解決した暗号プロトコルである。Yahalom 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-BAN simplified 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暗号プロトコルである。

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。

また、これに加えて、Yahalom-BAN simplified はセッション間の独立性を実現するために提案された暗号プロトコルである。

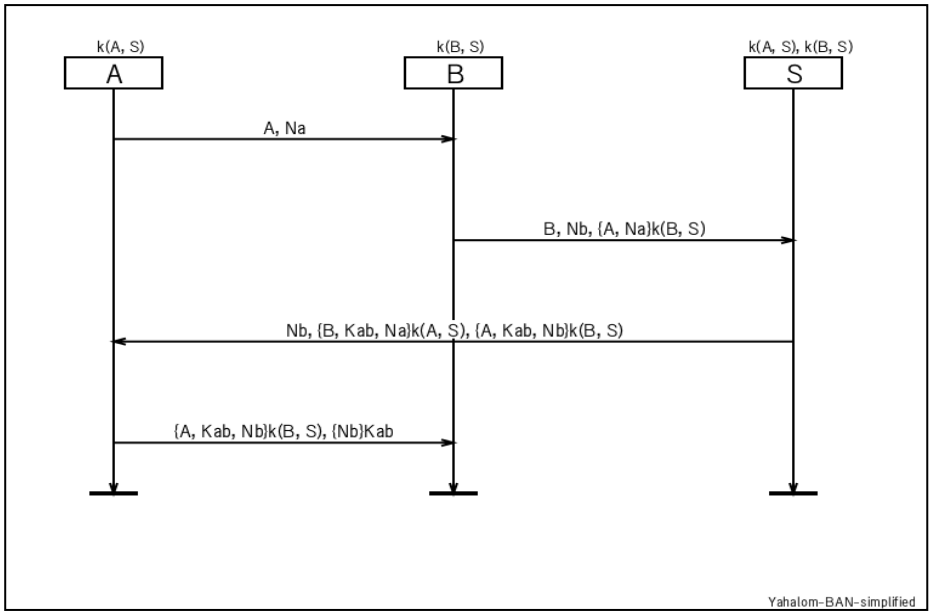

図 1. シーケンス図

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

以下の文献で、Yahalom-BAN simplified に対して中間者攻撃及びリプレイ攻撃が可能であることを指摘している。

- Paul Syverson, “A taxonomy of replay attacks,” In Proceedings of the 7th IEEE Computer Security Foundations Workshop, pp. 131-136, IEEE Computer Society Press, 1994.

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。