Needham-Schroeder public-key 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

  Needham-Schroeder public-key

- ✧ 機能

  公開鍵サーバを用いた相互認証プロトコル。

- ✧ 関連する文書

  R.Needham and M.Schroeder, ″Using encryption for authentication in large networks of computers,″ Communications of the ACM, 21(12), December 1978.

2. プロトコル仕様

Needham-Schroeder public-key のシーケンス図を示す。

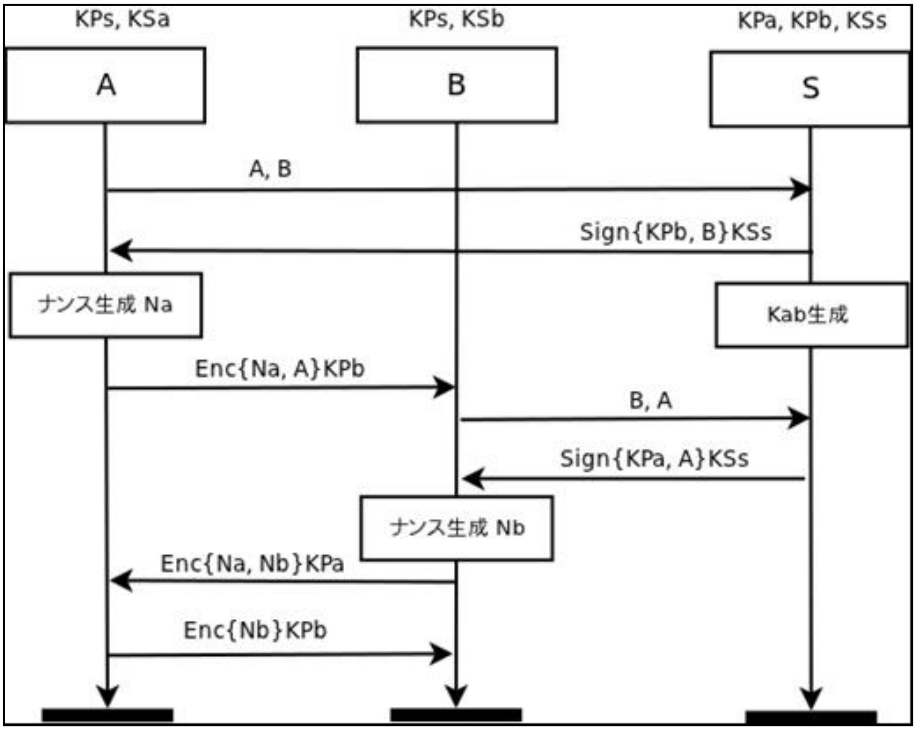

図 1. シーケンス図

3. 攻撃者モデル（自然言語による記述）

基本情報の関連する文書にて、“all communication paths, and thus can alter or copy parts of messages, replay messages, or emit false material. While this may seem an extreme view, it is the only safe”と述べられているため、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）

基本情報の関連する文書にて、相互認証を目的としていることが記述されているが、それ以上の記載は見当たらない。

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

以下の文献に攻撃法が紹介されている。

- Gavin Lowe, “An attack on the Needham-Schroeder public key authentication protocol,” Information Processing Letters, 56(3), pp.131--136, November 1995.
- SPORE (Security Protocol Open Repository)
  http://www.lsv.ens-cachan.fr/Software/spore/nspk.html

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。