Needham-Schroeder public-key の Scyhter による評価結果

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. Scyther の文法による記述

2.1. プロトコル仕様

```
protocol Needham-Schroeder-PublicKey(A, B, AS)
{
        role A
        {
                fresh Na: Nonce;
                var Nb: Nonce;
                send_1(A, AS, (A, B));
                recv_2(AS, A, (pk(B), B, {pk(B), B}sk(AS)));
                send_3(A, B, {Na, A}pk(B));
                recv_6(B, A, {Na, Nb}pk(A));
```

```
                send_7(A, B, {Nb}pk(B));

        }

        role B

        {

                fresh Nb: Nonce;

                var Na: Nonce;

                recv_3(A, B, {Na, A}pk(B));

                send_4(B, AS, (B, A));

                recv_5(AS, B, (pk(A), A, {pk(A), A}sk(AS)));

                send_6(B, A, {Na, Nb}pk(A));

                recv_7(A, B, {Nb}pk(B));

        }

        role AS

        {

                recv_1(A, AS, (A, B));

                send_2(AS, A, (pk(B), B, {pk(B), B}sk(AS)));

                recv_4(B, AS, (B, A));

                send_5(AS, B, (pk(A), A, {pk(A), A}sk(AS)));

        }

}
```

2.2. 攻撃者モデル

Scyther はデフォルトで Dolev-Yao モデルを想定しており、特に記載すべき項目はない。

2.3. セキュリティ要件

```
// ロールAのセキュリティ要件

claim_a1(A, Alive);

claim_a2(A, Weakagree);

claim_a3(A, Secret, Na);

claim_a4(A, Secret, Nb);

// ロールBのセキュリティ要件

claim_b1(B, Alive);

claim_b2(B, Weakagree);

claim_b3(B, Secret, Na);

claim_b4(B, Secret, Nb);

// ロールASのセキュリティ要件

なし。
```

3. Scytherによる評価結果

3.1. 出力

Scytherでの評価結果では、プロトコルに従わずプロトコルを完了させる手順が発見された。

```
claim id [Needham-Schroeder-PublicKey,a1], Alive       :        No
attacks within bounds.
claim id [Needham-Schroeder-PublicKey,a2], Weakagree   :At least 2
attacks.
claim id [Needham-Schroeder-PublicKey,a3], Secret(Na)  :        No
attacks within bounds.
claim id [Needham-Schroeder-PublicKey,a4], Secret(Nb)  :        No
attacks within bounds.
```

```
claim id [Needham-Schroeder-PublicKey,b1], Alive       :       No
attacks within bounds.
claim id [Needham-Schroeder-PublicKey,b2], Weakagree   :At least 2
attacks.
claim id [Needham-Schroeder-PublicKey,b3], Secret(Nb)  :At least 7
attacks.
claim id [Needham-Schroeder-PublicKey,b4], Secret(Na)  :At least 7
attacks.
```

3.2. 攻撃の解説

図 1.では、ロール A が演じる Charlie とロール AS を演じる Alice のやりとりが連動していないことが見てとれる。Alice は Charlie の要求に直接応えているわけではなく、Charlie の要求に矛盾しないデータ（実質的には同じデータ）を応答として返している。いずれの攻撃も、ロール AS のレスポンスがロール A 及びロール B の要求に応じたものではないことを示唆している。

4. 形式化

4.1. 方針

認証には Lowe による定義を含めて、いくつかのセキュリティ要件が定義されている。一方、元の文献では目標とするセキュリティ要件が定義されていない。そこで、本評価では、Scyther で選択可能な認証に関する性質すべてについて評価を行った。

4.2. 妥当性

Needham-Schroeder プロトコルは既に抽象化されている暗号プロトコルであり、モデル化（単純化など）は不要であった。

4.3. 検証ツールとの相性

プロトコル仕様、攻撃者モデルを記述するにあたって、特に制限はなかった。

セキュリティ要件を記述するにあたって、Scyther 内部では公開鍵は鍵サーバーなしに入手可能であるように形式化されているため、シーケンスのうち、公開鍵の配布に関する個所は正確に形式化されていない可能性がある。しかし、NSPK プロトコルでは、だれでも公開鍵を入手可能であるため、Scyther での評価と現実との差異はないと考えられる。

4.4. 検証ツール適用時の性能

検証時間は 0.8 秒だった。実行環境は以下のとおり。

✧　CPU：AMD Phenom X4 9750B (2.4GHz)

✧　メモリ：1.7GB

5. 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。

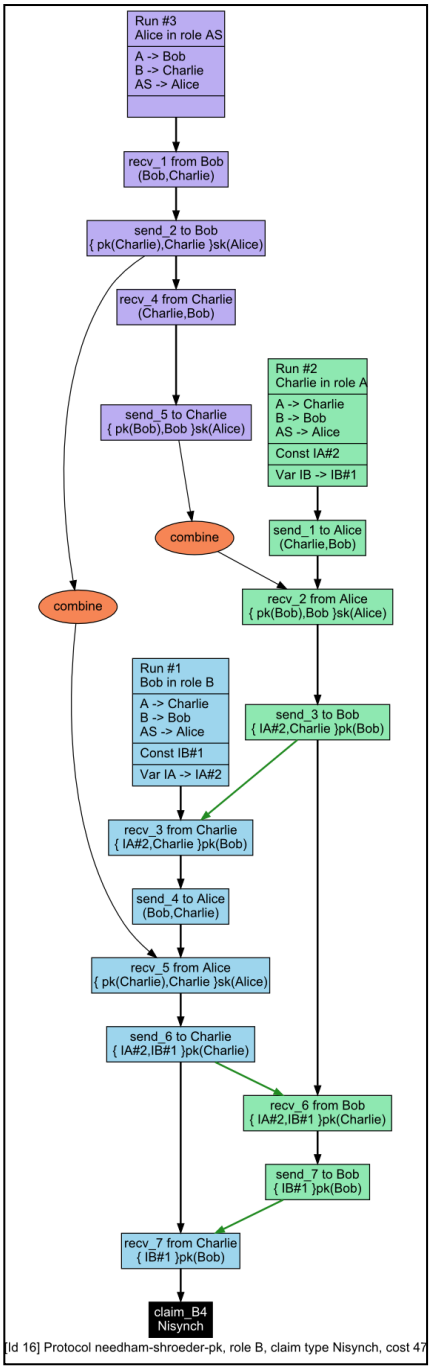

図. 1.　攻撃に関する解説