

Kerberos with forwardable ticket の Scyther 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

The Kerberos Network Authentication Service (V5), Kerberos with forwardable ticket

◇ 機能

信頼できる第三者機関 (TTP, Trusted Third Party) の存在を前提とする、オープンなネットワークにおけるサーバ・クライアント間でのネットワーク認証・鍵交換プロトコル。特徴は認証後にクライアントの IP アドレスを変更可能であること。暗号として共通鍵暗号を利用。

◇ 関連する標準

RFC4120 (<https://www.ietf.org/rfc/rfc4120.txt>)

2. Scyther の文法による記述

2.1. プロトコル仕様

```
usertype SessionKey;
usertype Time;
usertype String;
usertype Option;
const IP-addr: Function;
const DNS: Function;
inversekeys(IP-addr, DNS);
protocol Kerberos-forwardable-ticket(C, A, G, S)
{
    role C
    {
        fresh T2: Time;
        fresh FORWARDABLE: Option;
```

```

        fresh T1: Time;
        fresh N2: Nonce;
        fresh N1: Nonce;
        fresh U: String;
        var Texpire2: Time;
        var Texpire1: Time;
        var Kcs: SessionKey;
        var Kcg: SessionKey;
        var Tstart2: Time;
        var Tstart1: Time;
        var Tcg, Tcs1, Tcs2: Ticket;

        send_1(C, A, (U, G, N1));
        recv_2(A, C, (C, Tcg, {G, Kcg, Tstart1, Texpire1,
N1}k(C, A)));

        send_3(C, G,
                (IP-addr(C), S, N2, Tcg, {C, T1}Kcg,
FORWARDABLE));

        recv_4(G, C, (U, Tcs1, {S, Kcs, Tstart2, Texpire2,
N2}Kcg));

        send_5(C, G, (IP-addr(C), S, N2, Tcs1, {C, T1}Kcg));
        recv_6(G, C, (U, Tcs2, {S, Kcs, Tstart2, Texpire2,
N2}Kcg));

        send_7(C, S, (Tcs2, {C, T2}Kcs));
        recv_8(S, C, {T2}Kcs);
    }
    role A
    {
        fresh Texpire1: Time;
        fresh Kcg: SessionKey;
        fresh Tstart1: Time;
        var N1: Nonce;

```

```

    var U: String;
    recv_1(C, A, (U, G, N1));
    send_2(A, C,
           (C,
            {U, C, G, Kcg, Tstart1, Texpire1}k(A, G),
            {G, Kcg, Tstart1, Texpire1, N1}k(C, A)));
}
role G
{
    fresh Texpire2: Time;
    fresh Kcs: SessionKey;
    fresh Tstart2: Time;
    var Texpire1: Time;
    var FORWARDABLE: Option;
    var T1: Time;
    var Kcg: SessionKey;
    var N2: Nonce;
    var U: String;
    var Tstart1: Time;
    recv_3(C, G,
           (IP-addr(C), S, N2,
            {U, C, G, Kcg, Tstart1, Texpire1}k(A, G),
            {C, T1}Kcg, FORWARDABLE));
    send_4(G, C,
           (U,
            {IP-addr(C), U, C, S, Kcs, Tstart2,
             Texpire2, FORWARDABLE}k(G, S),
            {S, Kcs, Tstart2, Texpire2, N2}Kcg));
    recv_5(C, G,
           (IP-addr(C), S, N2,
            {IP-addr(C), U, C, S, Kcs, Tstart2,
             Texpire2, FORWARDABLE}k(G, S),

```

```

        {C, T1}Kcg));
    send_6(G, C,
           (U,
            {IP-addr(C), U, C, S, Kcs, Tstart2,
Texpire2, FORWARDABLE}k(G, S),
            {S, Kcs, Tstart2, Texpire2, N2}Kcg));
    }
    role S
    {
        var Texpire2: Time;
        var T2: Time;
        var FORWARDABLE: Option;
        var Kcs: SessionKey;
        var U: String;
        var Tstart2: Time;
        recv_7(C, S,
              ({IP-addr(C), U, C, S, Kcs, Tstart2,
Texpire2, FORWARDABLE}k(G, S),
              {C, T2}Kcs));
        send_8(S, C, {T2}Kcs);
    }
}

```

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 C のセキュリティ要件
claim_c1(C, Secret, Kcg);
claim_c2(C, Secret, Kcs);
claim_c3(C, Weakagree);
// ロール A のセキュリティ要件
claim_a1(A, Weakagree);
// ロール G のセキュリティ要件

```

```
claim_g1(G, Secret, Kcg);
claim_g2(G, Weakagree);
// ロール S のセキュリティ要件
claim_s1(S, Secret, Kcs);
claim_s2(S, Weakagree);
```

3. Scyther による評価結果

3.1. 出力

Scyther での評価結果では、セッション鍵の漏洩の可能性が指摘されているが、通常 Kerberos ではサーバ間の階層構造は固定されており、また、サーバが不正な行動をとることは想定されていない。そのため、サーバの不正が無制限においては問題にならない。

```
claim id [Kerberos-forwardable-ticket, C1], Secret(Kcg) : No attacks
within bounds.
claim id [Kerberos-forwardable-ticket, C2], Secret(Kcs) : No attacks
within bounds.
claim id [Kerberos-forwardable-ticket, C3], Weakagree : At least 1
attack.
claim id [Kerberos-forwardable-ticket, A1], Weakagree : Exactly 1
attack.
claim id [Kerberos-forwardable-ticket, G1], Secret(Kcg) : No attacks
within bounds.
claim id [Kerberos-forwardable-ticket, G2], Weakagree : At least 1
attack.
claim id [Kerberos-forwardable-ticket, S1], Secret(Kcs) : At least 14
attacks.
claim id [Kerberos-forwardable-ticket, S2], Weakagree : At least 15
attacks.
```

3.2. 攻撃の解説

以下の図では、Kerberos with forwardable ticket において、ロール C とロール S で共有されるセッション鍵 Kcs がロール S については Secret を満たさない例を示している。ただし、Kerberos では、サーバ間の階層構造は固定されており、また、サーバが不正な行動をとることは想定されていない。この結果は Kerberos の安全性がサーバの信頼性に依拠し

ているという設計者の意図に合致したものとなっており、通常の運用の際は問題ない。なお、図では攻撃者がロール A を演じている。ロール A はセッション鍵 Kcs を暗号化している鍵 Kcg を自分で生成できるので、ロール G が生成するセッション鍵 Kcs を入手できる。

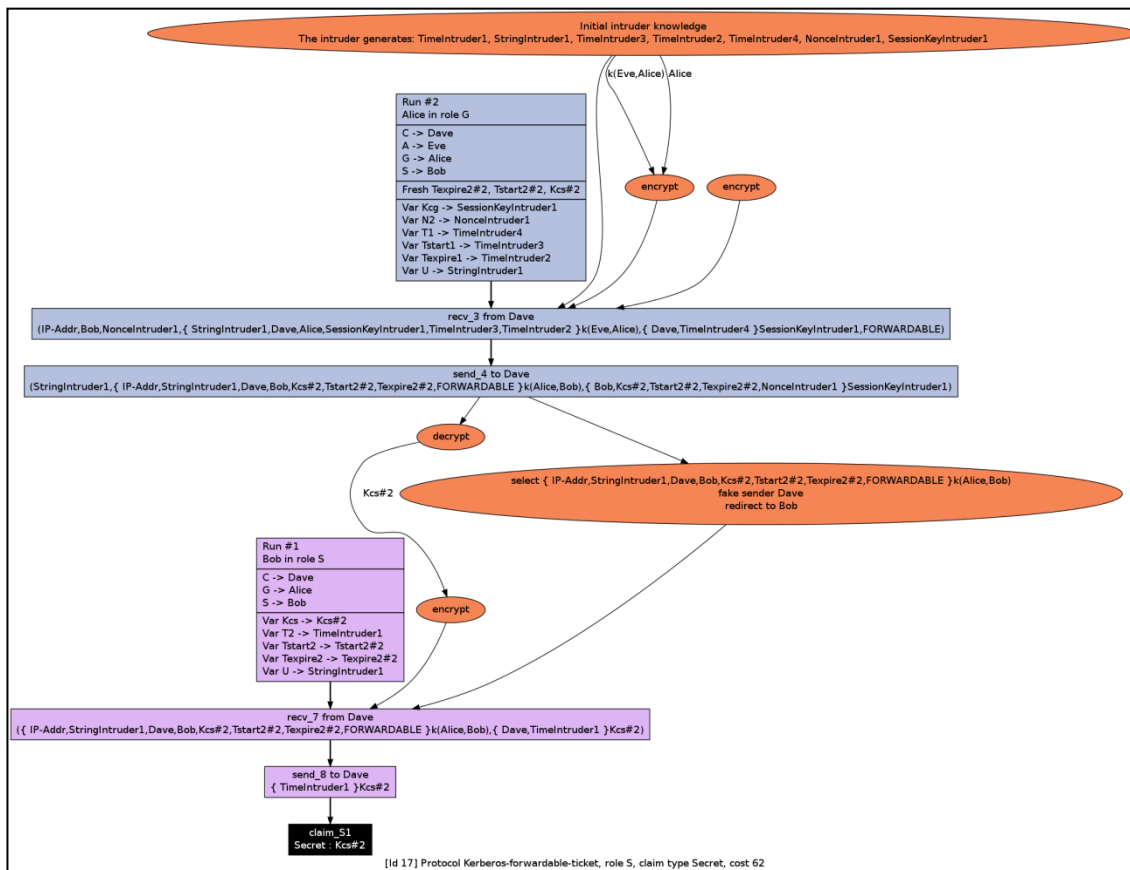


図. 1. 攻撃に関する解説

4. 形式化

4.1. 方針

Kerberos では、チケットの有効期限を時刻情報で記述している。形式化では、Time という型を宣言し、時刻情報に関する変数を Time 型として記述した。

4.2. 妥当性

Kerberos では、サーバの不正行為を想定していないと思われる。Scyther では、攻撃者の能力を制限することができないため、仕様が目的としている安全性を評価できていない可能性がある。ただし、上述の結果では、Kerberos の安全性がサーバの信頼性に依拠しているという設計者の意図に合致したものとなっており問題ない。

4.3. 検証ツールとの相性

プロトコル仕様の記述にあたって、形式化では時刻情報について Time という型を宣言し

ているが、時刻の整合性をチェックしているわけではなく、基本的にナンスとして取り扱われる。

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、暗号プロトコルの目的は、サーバによるクライアントの片側認証及びセッション鍵（チケット）の交換であることより、Kcsに関する秘匿性及びクライアント - サーバ間で non-injective agreement が成立していれば良いと思われる。また、RFC4120 中では、時刻情報を盛り込むことで、リプレイ攻撃を防げるとしている。したがって、クライアント - サーバ間で injective agreement が満たされていることが望ましい。

Scyther では、injectivity を評価することができない。しかし、評価の結果、with forwardable ticket は Weakagreement を満たさないため、これが問題となることはなかった。

4.4. 検証ツール適用時の性能

検証時間は約 4 時間だった。実行環境は以下のとおり。

- ◇ CPU : Intel Xeon E5502 (1.87GHz) 4CPU(SMP)
- ◇ メモリ : 48GB
- ◇ Scyther v1.1

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。