

暗号プロトコル評価結果

独立行政法人 情報通信研究機構

1. プロトコル名 : PKM

2. 関連する標準

IEEE Std 802.16e-2005

<http://standards.ieee.org/getieee802/download/802.16e-2005.pdf>

3. 使用したツール : Scyther

4. 評価の概要 : Scyther による評価では、weak agreement への攻撃の可能性が指摘されているが、ペイロードの改ざんがされるわけではないので、攻撃としての意味はない。

5. Scyther による評価

5.1. シーケンス記述

```
usertype String;
usertype Time;
hashfunction hmac;
hashfunction SHA;
macro KEK = SHA(AK);
const choice: Function;
const CryptoSuites: Function;
macro Cert-SS = pk(SS);
macro AuthRequest = (Cert-SS, SS); //12.1.1.4.10
macro AuthReply = ({AK, PS}pk(SS), sqn, BS); //12.1.1.4.13
macro KeyRequest = (sqn, hmac(sqn, AK)); //12.1.1.4.11
macro KeyReply-payload = (sqn, IV, {TEK, IV}KEK);
macro KeyReply = (KeyReply-payload, hmac(KeyReply-payload, AK));
//12.1.1.4.15
////////////////////////////////////
protocol PKMv1(SS, BS)
{
  /*****/
  role SS //peer
```

```

{
  /***/
  // variables
  // AK exchange
  var AK: Nonce; //authentication key
  var sqn: Nonce; //key sequence number
  var PS: Nonce; //random number used in PKCS#1 v2.1

  // TEK exchange
  var TEK: Nonce; //traffic encryption key
  var IV: Nonce; //IV for CBC-encryption mode

  /***/
  // sequence
  //---- 7.2.1: SS authorization and AK exchange ----
//   send_1(SS,BS, AuthInfo);
  send_2(SS,BS, AuthRequest);
  recv_3(BS,SS, AuthReply);
  //---- 7.2.2: TEK exchange
  send_4(SS,BS, KeyRequest);
  recv_5(BS,SS, KeyReply);

  /***/
  // security properties
}
/***/
role BS //server
{
  /***/
  // variables
  // AK exchange
  fresh AK: Nonce; //authentication key

```

```

fresh sqn: Nonce; //key sequence number
fresh PS: Nonce; //random number used in PKCS#1 v2.1

// TEK exchange
fresh TEK: Nonce; //traffic encryption key
fresh IV: Nonce; //IV for CBC-encryption mode

/*****/
// sequence
//---- 7.2.1: SS authorization and AK exchange ----
//   recv_1(SS,BS, AuthInfo);
recv_2(SS,BS, AuthRequest);
send_3(BS,SS, AuthReply);
//---- 7.2.2: TEK exchange
recv_4(SS,BS, KeyRequest);
claim(BS, Running, SS, AK);
claim(BS, Running, SS, TEK);
send_5(BS,SS, KeyReply);

/*****/
// security properties

}
}

```

5.2. 攻撃者モデル

Scyther はデフォルトで Dolev-Yao モデルの通信路を想定しているため、Scyther を利用した評価で攻撃者モデルについて記載すべき項目はない。

5.3. セキュリティプロパティの記述

本評価では、ロール BS によるロール SS の認証だけではなく、両側認証としてロール SS に関する性質についても評価を行っている。

5. 4. 検証結果

○評価ツールの出力

claim	PKMv1, SS	SKR_SS1 AK	Fail	[at least 2 attacks]
claim	PKMv1, SS	SKR_SS2 TEK	Fail	[at least 1 attack]
claim	PKMv1, SS	Alive_SS3	-	Fail [at least 1 attack]
claim	PKMv1, BS	SKR_BS3 AK	Ok	[no attack within bounds]
claim	PKMv1, BS	SKR_BS4 TEK	Ok	[no attack within bounds]
claim	PKMv1, BS	Alive_BS5	-	Ok [no attack within bounds]
claim	PKMv1, BS	Weakagree_BS6	-	Fail [at least 1 attack]
claim	PKMv1, BS	Commit_BS7	(SS, AK)	Fail [at least 1 attack]
claim	PKMv1, BS	Commit_BS8	(SS, TEK)	Fail [at least 1 attack]

○攻撃に関する解説

次ページの図は PKMv1 がロール BS について weak agreement を満たさない例である。ここで、ロール SS (Bob) はロール BS が Charlie だと想定して暗号プロトコルを実行しており、直接ロール BS と通信しているわけではない。

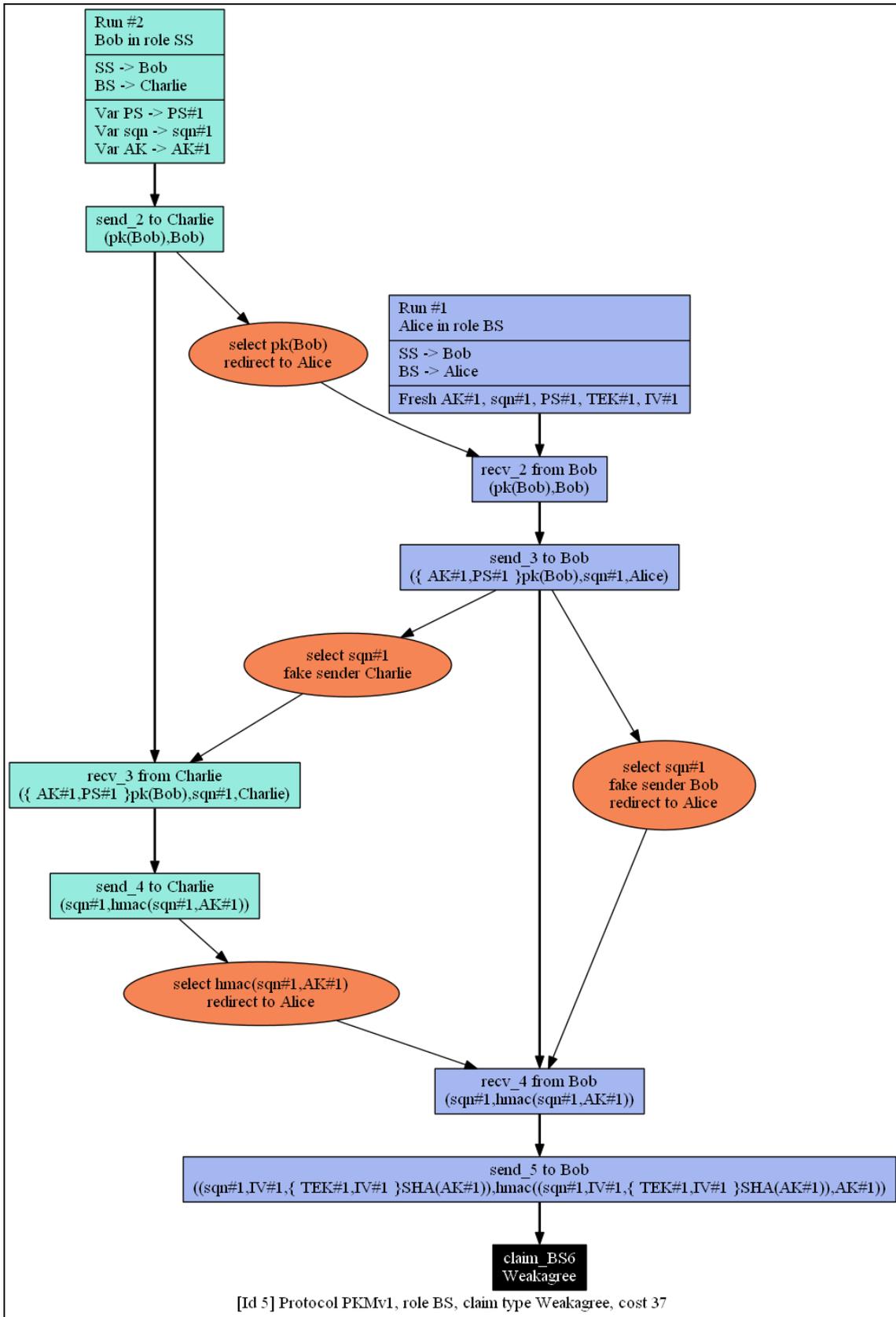


図 1. 攻撃に関する解説

5.5 モデル化

○モデル化プロセス

・AuthInfo メッセージはローカル BS が知らない認証局が作成している可能性がある証明書を送付しており、暗号プロトコルとしては無意味であるため省略した。

・PKM では、1 回の鍵交換で 2 つの鍵 TEK を交換する（うち 1 つは前回交換したもの）、評価時間が大幅に増加する上、1 回の鍵交換処理では妥当なモデル化が難しいため、1 つの鍵 TEK を交換するモデルとした。

5.6. モデル化の妥当性

交換するセッション鍵を 1 つとしたため、複数のセッションをまたがる場合の暗号プロトコルの安全性については妥当な評価となっていない可能性がある。ただし、PKMv1 では完全ななりすましが可能であり、このモデルの単純化が評価結果に大きな影響を与えることはないと考えられる。

5.7. 評価ツールとの相性

○暗号プロトコルの記述可能性

Scyther はローカル BS が知らない（可能性がある）認証局をモデル化することができない。しかし、これが評価結果に影響を与える可能性は小さい。

○セキュリティプロパティの記述可能性

特になし。

5.8. 評価ツールの性能

- ・ CPU : Intel Core2Duo E8400 3.0GHz
- ・ メモリ : 4GB
- ・ OS : Windows7 32-bit 版
- ・ 評価に要した時間 : 3 分 14 秒

5.9. 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