L-035

鍵交換プロトコルの安全性の検証ポイントに関する検討

A Study on Verification Points of Security for Key Exchange Protocols

太田 陽基 † 清本 晋作 † 田中 俊昭 †
Haruki Ota Shinsaku Kiyomoto Toshiaki Tanaka

1 まえがき

暗号プロトコルの安全性を客観的に検証する手法として，計算量理論にもとづいて安全性を証明する手法とフォーマル検証にもとづく手法が提案されている．前者の手法として，Bellare, Pointcheval, Rogaway は認証及び鍵交換プロトコルに対して，識別不可能性にもとづく安全性のフォーマルなモデル（以降，BPR モデルと呼ぶ）を最初に導入し [1]，本分野における後に続く多くの研究の基盤となった．しかしながら，これらの手法は，プロトコルごとの安全性証明を必要とするという問題がある．それに対し，後者の手法には，Dolev-Yao モデル [2] などの特化型状態探索にもとづく手法を始めとする多くの手法が提案されてきた．しかしながら，これらの手法は，安全性検証に多くの時間を要する，必ずしも自動化されていない，という問題がある．

著者らは，BPR モデルにもとづく鍵交換プロトコルの安全性検証手法を提案し，各安全性を効率的にチェックするための検証ポイントを示した [3]．その際，著者らは受動的攻撃安全，能動的攻撃安全，オフライン辞書攻撃安全，既知鍵攻撃安全，weak forward secrecy の 5 つの安全性に関する検証ポイントを示した．一方，鍵交換プロトコルに対し，検出不可能なオンライン辞書攻撃安全 [4]，未知鍵共有攻撃安全 [5]，strong forward secrecy [1]，weak backward secrecy [6] も必要であることが提唱された．本稿では，鍵交換プロトコルに対する提案手法を再度述べ，新たに上記の 4 つの安全性に関する検証ポイントを示す．

2 既存モデル

Bellare らは現実の攻撃をモデル化することにより，計算量理論にもとづく認証・鍵交換プロトコルの評価手法を定式化し，いくつかの提案した認証・鍵交換プロトコルの安全性を証明した [1]．Bellare らは上記の証明を行う上で，鍵交換プロトコルの “semantic security” という新しい安全性の概念を導入した．Bellare らの研究以降，鍵交換プロトコルに対し，セキュリティ要件に応じて，この概念に対する 9 つの安全性が提唱された．そのうち，1 節にて述べた 5 つの安全性に関しては，文献 [3] において示したため，本稿では以下の 4 つの安全性のみ取り扱う．

- semantic security
  攻撃者はセッション鍵に関するどんな情報も得ることができない．すなわち，攻撃者はセッション鍵と乱数を多項式時間で区別することができない．

(a) 検出不可能なオンライン辞書攻撃安全
パスワードが登録されているパーティは，攻撃者がパスワードを問い合わせていることを検出可能でなくてはいけない．

(b) 未知鍵共有攻撃安全
あるパーティが正しいと思っているパーティとは別のパーティとセッション鍵を共有することができてはいけない．

(c) strong forward secrecy
攻撃者がパーティの長期鍵及び内部状態を得ることができたとしても，それ以前に共有されたセッション鍵を得ることはできない．

(d) weak backward secrecy
攻撃者がパーティの内部状態を得ることができたとしても，そのセッション以降に共有されたセッション鍵を得ることはできない．

ただし，長期鍵，パスワードを使用しない場合, (c) , (a) の安全性はそれぞれ要求されない．また，forward secrecy と backward secrecy に関し，攻撃者が長期鍵と内部状態の両方を得られる場合を strong モデル，どちらか一方（前者は長期鍵，後者は内部状態）しか得られない場合を weak モデルと呼ぶ．

3 安全性検証手法

本稿では，2 ユーザ同士かまたはサーバとクライアント間で鍵交換を行う 2 者間の鍵交換プロトコルのみを対象とする．ここで，鍵交換プロトコルの安全性を検証する上で，以下を前提とする．

- 共通鍵やパスワードを使用している場合，2 パーティはあらかじめ同じ共通鍵やパスワードを何らかの安全な手順で共有しておき，その手順に脆弱性はない．
- 公開鍵を使用している場合，各パーティは認証局などの第三者機関との間において公開鍵証明書の正当性を確認することができ，その手順に脆弱性はない．
- 暗号プリミティブは危殆化していない．危殆化した暗号プリミティブが使用されている場合，検証プログラムはこの鍵交換プロトコルを安全でないと判定し，検証処理を終了する．

以下の手順により，検証プログラムが鍵交換プロトコルの安全性を検証する．

(1) 検証プログラムは鍵交換プロトコルにおいて使用されるすべての暗号プリミティブを列挙する．暗号プリミティブの種類は次から選択される．
- 共通鍵暗号（SKE）
- パスワードを用いた暗号化（EPW）
- 公開鍵暗号（PKE）
- Diffie-Hellman 族（DH）
- ディジタル署名スキーム（SIG）
- ハッシュ関数（HF）
- メッセージ認証コードスキーム（MAC）

(2) 検証プログラムは手順（1）にて列挙された暗号プリミティブについて以下を設定する．
- 鍵生成対象となる暗号プリミティブ（PKG）
- フローに現れる暗号プリミティブ（PAF）
- PKG や PAF の引数に含まれる暗号プリミティブ（PAO）

(3) 検証プログラムは鍵交換プロトコルにおけるすべてのフローを列挙する．検証プログラムは，これらのフローと手順（2）の引数について，次の要素を設定する．

† （株）KDDI 研究所, KDDI R&D Laboratories, Inc.

- フローと暗号プリミティブの引数の種類
  - ID データ（ID）
  - テンポラリデータ（TD）
  - 長期鍵（LLK）
  - パスワード（PW）
- フローと暗号プリミティブの引数の状況
  - 同じセッションにおいて一度だけ登場（OS）
  - 同じセッションにおいて何度も登場（AS）
  - 別のセッションにおいて繰り返し登場（RO）
- フローと暗号プリミティブの引数の状態
  - 公開状態（PS）
  - 秘密状態（SS）

(4) 検証プログラムは，2 節において示した，鍵交換プロトコルに対して要求されている安全性を選択する（複数選択可）．このとき，検証プログラムは鍵交換プロトコルにおいて要求されているセキュリティパラメータを設定し，各サイズがセキュリティパラメータを満足しているかどうかを確認する．満足していないサイズが 1 つでもある場合，検証プログラムはその鍵交換プロトコルを安全でないと判定する．

(5) 検証プログラムは手順 (4) の安全性に対し，手順 (3) の要素を用いて，4 節において示す検証ポイントをチェックする．このとき，検証プログラムは各攻撃に関係するデータを設定する．検証プログラムは設定したデータに対し，プロトコルフローの順に，手順 (3) の要素と手順 (4) の安全性を設定する．ここで，フローと暗号プリミティブの引数の状況と状態は更新されていくものとする．ただし，公開状態と秘密状態では，公開状態を優先するものとする．

4 検証ポイント

本節では，鍵交換プロトコルの 4 つ安全性に関して導出した検証ポイントを示す．

4.1 検出不可能なオンライン辞書攻撃安全

検証プログラムはこの攻撃に関係する情報として，すべてのフローを設定する．このとき，パーティが秘匿されたパスワードの正当性を確認する必要があるため，本検証ポイントは以下のとおりとなる．

(a_1) PW-RO-SS を含む PAF が SKE ∨ PKE ∨ MAC である．

4.2 未知鍵共有攻撃安全

検証プログラムはこの攻撃に関係する情報として，すべてのフローを設定する．このとき，暗号プリミティブの引数に含まれる ID が別の ID に入れ替えられないようにする必要があるため，本検証ポイントは以下のとおりとなる．

(b_1) PKG が SKE ∨ EPW ∨ SIG ∨ MAC であり，PKG の引数が ID-RO-PS ∧ (TD-OS-PS ∨ TD-AS-PS ∨ TD-OS-SS ∨ TD-AS-SS) を含んでいる．

(b_2) PKG が PKE ∨ HF であり，PKG の引数が ID-RO-PS ∧ (TD-OS-SS ∨ TD-AS-SS) を含んでいる．

(b_3) PAO が SKE ∨ EPW ∨ SIG ∨ MAC であり，PAO の引数が ID-RO-PS ∧ (TD-OS-PS ∨ TD-AS-PS ∨ TD-OS-SS ∨ TD-AS-SS) を含んでいる．

(b_4) PAO が PKE ∨ HF であり，PAO の引数が ID-RO-PS ∧ (TD-OS-SS ∨ TD-AS-SS) を含んでいる．

4.3 Strong Forward Secrecy

検証プログラムはこの攻撃に関係する情報として，すべての長期鍵と内部状態を設定する．このとき，セッション鍵の共有後に長期鍵と内部状態が知られているという条件のもと，鍵生成関数の引数に秘密状態のテンポラリデータが含まれている必要があるため，本検証ポイントは以下のとおりとなる．

(c_1) PKG が PKE ∨ DH ∨ HF ∨ MAC であり，PKG の引数が TD-OS-SS ∨ TD-AS-SS を含んでいる．

(c_2) PKG が HF ∨ MAC であり，PAO が DH であり，PAO の引数が TD-OS-SS ∨ TD-AS-SS を含んでいる．

4.4 Weak Backward Secrecy

検証プログラムはこの攻撃に関係する情報として，すべての内部状態を設定する．このとき，セッション鍵の共有前に内部状態が知られているという条件のもと，暗号プリミティブの引数に秘密状態のデータ及びテンポラリデータが含まれている必要があるため，本検証ポイントは以下のとおりとなる．

(d_1) PKG が SKE ∨ EPW ∨ PKE ∨ SIG ∨ HF ∨ MAC であり，PKG の引数が (LLK-RO-SS ∨ PW-RO-SS) ∧ (TD-OS-PS ∨ TD-OS-SS) を含んでいる．

(d_2) PKG が SKE ∨ EPW ∨ PKE であり，PKG の引数が (TD-OS-PS ∨ TD-AS-PS) ∧ TD-OS-SS を含んでいる．

(d_3) PAO が SKE ∨ EPW ∨ PKE ∨ HF ∨ MAC であり，PAO の引数が (LLK-RO-SS ∨ PW-RO-SS) ∧ (TD-OS-PS ∨ TD-OS-SS) を含んでいる．

(d_4) PAO が DH であり，PAO の引数が TD-OS-SS を含んでいる．

(d_5) PAO が SKE ∨ EPW ∨ PKE であり，PAO の引数が (TD-OS-PS ∨ TD-AS-PS) ∧ TD-OS-SS を含んでいる．

5 あとがき

本稿では，著者らが提案した鍵交換プロトコルに対する安全性検証手法に対し，以前示していなかった検出不可能なオンライン辞書攻撃安全，未知鍵共有攻撃安全，strong forward secrecy, weak backward secrecy の 4 つの安全性に関する検証ポイントを導出した．

参考文献

[1] Bellare, M., Pointcheval, D., and Rogaway, P.: Authenticated Key Exchange Secure Against Dictionary Attacks, EUROCRYPT 2000, LNCS 1807, pp.139–155 (2000).

[2] Dolev, D. and Yao, A.: On the Security of Public Key Protocols, SFCS 1981, pp.350–357 (1981).

[3] Ota, H., Kiyomoto S., and Tanaka T.: Security Verification for Authentication and Key Exchange Protocols, IJCSNS, Vol.9, No.3, pp.1–11 (2009).

[4] Ding, Y. and Horster, P.: Undetectable On-line Password Guessing Attacks, ACM SIGOPS Operating Systems Review, Vol.29, No.4, pp.77–86 (1995).

[5] Blake-Wilson, S. and Menezes, A.: Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol, PKC 1999, LNCS 1560, pp.154–170 (1999).

[6] Bresson, E., Manulis, M., and Schwenk J.: On Security Models and Compilers for Group Key Exchange Protocols, IWSEC 2007, LNCS 4752, pp.292–307 (2007).