SSL 安全性評価報告書

RSA 暗号を用いた鍵共有法、署名法について

2001 年 12 月 28 日

産業技術総合研究所

渡辺 創

SSL 安全性評価報告書
RSA 暗号を用いた鍵共有法, 署名法について

2001 年 12 月 28 日

1　まえがき

本報告書は, CRYPTREC2001 公開鍵暗号評価小委員会からの依頼に基づき, SSL および TLS で用いられている RSA 暗号を利用した鍵共有法, 署名法の安全性評価を報告したものである. 本評価では, 鍵共有法および署名法を抽象的に表現したものについての安全性評価を主に行なっている. その表現においてデータ表現法 (ヘッダのあるビットが何を表しているか等) は, プロトコル表現に含まれていない. 安全性評価としては, プロトコルを用いることにより, 暗号自体を解読せずに共有された秘密情報の漏洩や, 署名の偽造等の不正ができないかどうか, についての議論を中心に行なっている. そしてその評価の結果, 特に対象とする方式に問題は見られないという結論に至ったことを報告する.

2 章では, 現在広く用いられているプロトコルである SSL 3.0[1] および TLS 1.0[2] における, RSA 暗号を用いた鍵共有法, 署名法について概説する. 3 章ではこれら方式について, プロトコルでの使用における安全性について議論する. 最後に 4 章で本評価の結論をまとめる.

2　RSA 暗号を用いた鍵共有法, 署名法

本章では RSA を用いた鍵共有法, 署名法について簡単に述べる. それぞれ SSL 3.0 と TLS 1.0 について説明を行なう. プロトコルにおいて, 鍵共有法を用いて共有されるのは,

- 通信路暗号化に用いられる共通鍵暗号の秘密鍵 (SSL 3.0, TLS 1.0)
- データの完全性を保証するための MAC 生成, 検証用鍵 (TLS 1.0)

を生成するための「プレマスタシークレット」と呼ばれる秘密情報である.

2.1　RSA を用いた鍵共有法

RSA 暗号を用いた鍵共有法において, SSL 3.0, TLS 1.0 の間でプロトコルに違いは存在しない. そのプロトコルは以下の通りである.

1. サーバ→クライアント

   サーバは RSA 暗号の暗号化用公開鍵とその鍵の証明書をクライアントへ送る. 送る方法には以下のような 2 種類がある.

   (a) 署名用の鍵とその証明書を送り (Certificate メッセージ), 続けて RSA 暗号の暗号化用公開鍵と その鍵に関する情報への署名(署名で使用した鍵は証明されたもの) を送る (ServerKeyExchange メッセージ).

   (b) RSA 暗号の暗号化用公開鍵とその証明書を送る (Certificate メッセージ).

   ここで下線部は,

   - クライアントが生成した乱数
   - サーバが生成した乱数
   - RSA の公開鍵 (合成数 n と乗数 e)

   を並べた情報に対し, MD5 関数をかけたもの, SHA-1 関数をかけたものにさらに署名したものである. この際 RSA 署名が用いられることもある.

2. クライアント

   クライアントはどちらの場合も, 公開鍵の証明書 (やサーバの署名) を用いて, RSA 暗号化用公開鍵の正当性を検証する.

3. クライアント→サーバ

   クライアントは鍵の正当性検証に成功した場合, プロトコルバージョン (2 バイト, SSL 3.0 の場合は 30h, TLS 1.0 の場合は 31h) と自分で生成した乱数 (46 バイト) を結合し, 48 バイトのプレマスタシークレットを作成する. そしてそれを RSA 暗号を用いてサーバの公開鍵で暗号化し, サーバに送る (ClientKeyExchange メッセージ).

4. サーバ

   サーバは送られてきた暗号文を復号し, プレマスタシークレットを得る.

以上でサーバ, クライアントはプレマスタシークレットを共有する.

2.2 RSA を用いた署名法

SSL 3.0, TLS 1.0 において, RSA 署名法は様々な場面で用いられるが, それらの間でプロトコルに違いは存在しない. 以下それを列挙する.

1. 署名検証用公開鍵証明書 (CA によるサーバのための)

   - Certificate メッセージ (サーバ→クライアント)
   - サーバの署名検証用公開鍵を証明するために, CA が RSA 署名をしたもの
     - クライアントは, CA(複数の場合あり) の公開鍵を用いて CA の署名を検証

  - 検証成功でサーバの署名検証用公開鍵が認証

2. 暗号化用公開鍵証明書 (CA によるサーバのための)
   - Certificate メッセージ (サーバ→クライアント)
   - サーバの暗号化用公開鍵を証明するために, CA が RSA 署名をしたもの
     - クライアントは CA(複数の場合あり) の公開鍵を用いて CA の署名を検証
     - 検証成功でサーバの暗号化用公開鍵が認証
3. 暗号化用公開鍵証明書 (サーバによる)
   - ServerKeyExchange メッセージ (サーバ→クライアント)
   - サーバの暗号化用公開鍵を証明するために, サーバが RSA 署名をしたもの
     署名データは前節 1 の下線部で表したデータ
     - クライアントは (CA(複数の場合あり) によって前もって証明された) サーバの署名検証用公開鍵を用いて署名を検証
     - 検証成功でサーバの暗号化用公開鍵が認証
4. 署名検証用公開鍵証明書 (CA によるクライアントのための)
   - Certificate メッセージ (クライアント→サーバ, 送られるのは稀)
   - クライアントの署名検証用公開鍵を証明するために, CA が RSA 署名をしたもの
     - サーバは CA(複数の場合あり) の公開鍵を用いて CA の署名を検証
     - 検証成功でクライアントの署名検証用公開鍵が認証
5. クライアント認証用署名メッセージ (クライアントによる)
   - CertificateVerify メッセージ (クライアント→サーバ, 送られるのは稀)
   - クライアントを認証するために, クライアントが RSA 署名をしたもの
     署名対象データは, それまでの通信メッセージに対し, MD5, SHA-1 関数をかけたものを結合したデータ
     - サーバは (CA(複数の場合あり) によって前もって証明された) クライアントの署名検証用公開鍵を用いて署名を検証
     - 検証成功でクライアントを認証

3 RSA 暗号を用いた鍵共有法, 署名法の安全性

本章では SSL 3.0, TLS 1.0 で用いられている, RSA 暗号を用いた鍵共有法, 署名法の安全性について議論する.

3.1 RSA 暗号を用いた鍵共有法の安全性

前章で見たように, 鍵共有法自体は RSA 暗号の暗号化通信方式そのものである. したがって, その安全性は RSA 暗号自体の安全性に依拠している. この部分については依頼内容とは異なるため, 本報告では評価を行なわない.

適切に用いた場合 RSA 暗号による暗号化通信は安全であると仮定したとき, プロトコルにおいて安全性を脅かすと考えられる部分は,

1. 署名検証用公開鍵証明書の偽造可能性

   不正者が証明書で証明された公開鍵の持ち主になりすます可能性

2. 暗号化用公開鍵証明書の偽造可能性

   不正者が証明書で証明された公開鍵の持ち主になりすます可能性

3. 証明書によって証明される公開鍵 (暗号化用, 署名検証用) に対応する秘密鍵の推測可能性

   不正者が証明書で証明された公開鍵の持ち主になりすます可能性

4. 署名 (ServerKeyExchange, CertificateVerify メッセージ中) の偽造可能性

   不正者が署名生成用秘密鍵の持ち主になりすます可能性

5. プレマスタシークレットとして使用されるデータの偽造あるいは予測可能性

   不正者が以降行なわれる暗号化通信の内容を得る可能性

といった部分である. 以下それぞれの場合について詳しく述べる.

1. 署名検証用公開鍵証明書の偽造可能性

   単純な CA による (Root CA までの) 署名の連鎖により, 公開鍵証明書は成り立っている. 連鎖されている署名全て偽造不可能であれば, 証明書の偽造は不可能であると言える. これは作成時に使用される署名方式と, CA が署名の際に用いた鍵の安全性により決まる. 大多数の CA により使用されている署名方式は DSA(DSS), RSA である. 今回の評価では, これらの署名方式は安全であるとの仮定を置いているため, 鍵の露呈による偽造の可能性についてのみ考えれば良い. またこのとき, 公開鍵や署名から秘密鍵は得られないと仮定していることに注意 (以降でも同様に仮定).

   さて, このような仮定のもとで不正者が鍵の露呈による偽造を行なうには, CA の秘密鍵自体を得る必要がある. プロトコル (とそれが用いている PKI のシステム) において, 署名生成に用いられる CA の秘密鍵は, システムが適切に運営されていれば, その CA 以外知ることができない. またその秘密鍵が含まれた情報 (それが何らかの暗号で暗号化された情報等) は通信路上に流れることはない. したがって CA の秘密鍵を得ることはできない. よって, 署名検証用公開鍵証明書の偽造は不可能であると言える.

2. 暗号化用公開鍵証明書の偽造可能性

   この偽造可能性は, 署名検証用公開鍵証明書の場合と同様である. したがって安全性についても同様である.

3. 証明書によって証明される公開鍵に対応する秘密鍵の推測可能性

   本評価では, サーバあるいはクライアントによって, RSA 暗号の鍵対は適切に生成されていると仮定している. またプロトコルにおいて, サーバあるいはクライアントの秘密鍵は, システムが適切に運営されていれば, その保持者以外知ることができない. またその秘密鍵が含まれた情報 (それが何らかの暗号で暗号化された情報等) は通信路上に流れることはない. さらに仮定より, 公開鍵と署名, あるいは公開鍵と暗号文から秘密鍵を得ることはできない. よって, 証明される公開鍵に対応する秘密鍵を推測することはできないと言える.

4. 署名 (ServerKeyExchange, CertificateVerify メッセージ中) の偽造可能性

   たとえ署名を偽造できたとしても, プレマスタシークレットが得られなければ, 以降の通信で正しい返答ができなくなり, なりなりすましが露呈するようになっている. もちろん通信の撹乱を防ぐ意味でも, このような不正ができないことが望ましい. これまで述べてきたような仮定より, プレマスタシークレットと署名者の秘密鍵が得られなければ, 署名の偽造はできない. 他の項で行なったような議論と同様, やはり不正者は署名者の秘密鍵を得ることができないと言える. よって署名の偽造は不可能であると言える.

5. プレマスタシークレットとして使用されるデータの偽造あるいは予測可能性

   本評価では, 用いられている暗号技術の安全性, プレマスタシークレットとして使用されるデータの乱数性を仮定している. プロトコルにおいて, プレマスタシークレット (あるいは鍵共有法として DH 法を用いる場合, それを構成するための情報) を含む情報は暗号化されたもののみである. したがって予測はできないと言える. また暗号化されたデータからそれらの情報を得ることは, やはり仮定よりできないと言える. よって, プレマスタシークレットとして使用されるデータの偽造, あるいは予測はできないと言える.

3.2 RSA 暗号を用いた署名法の安全性

前章で見たように, 署名法自体は RSA 暗号の署名方式そのものである. したがって, その安全性は RSA 暗号自体の安全性に依拠している. この部分については依頼内容とは異なるため, 本報告では評価を行なわない.

本評価においては, 適切に用いていれば RSA 暗号による署名法は安全であると仮定している. 2.2 で述べたように, RSA 署名法が用いられる可能性があるのは以下の場面である.

1. 署名検証用公開鍵証明書 (CA によるサーバのための)
2. 暗号化用公開鍵証明書 (CA によるサーバのための)

3. 暗号化用公開鍵証明書 (サーバによる)

4. 署名検証用公開鍵証明書 (CA によるクライアントのための)

5. クライアント認証用署名メッセージ (クライアントによる)

考えるべき不正は署名の偽造である. 1-5 について, 前節の議論 (署名方式や秘密鍵の安全性) を用いることにより, 署名の偽造ができないことが示せる.

4 結論

SSL 3.0, TLS 1.0 での RSA 暗号を利用した鍵共有法, 署名法は, 単純な技術の組合せの上にもっとも基本的なスキームを採用しており, セキュリティホールが潜む余地はほとんどないと考えられる. もちろん, 実装時に用いられるデータの形式や, 乱数の発生方法, サーバのエラーメッセージの返し方等, セキュリティホールが潜む可能性のある部分は数多く残っている. 特にサーバ以外のエンティティ(CA 等) が関係しているため, その選定 (利用している技術等に基づき) にあたっては十分検討をすべきであろう.

参考文献

[1] SSL 3.0 SPECIFICATION, `http://home.netscape.com/eng/ssl3/`.

[2] The TLS Protocol Version 1.0, RFC2246, IETF, 1999.