5N－7

SSLによる暗号化通信のための公開鍵の変更を考慮した時限付き証明書に関する研究

藤永卓人† 木村成伴‡ 海老原義彦‡
† 筑波大学電子情報学類 ‡ 筑波大学電子・情報工学系
e-mail: {fj,kimura,ebihara}@netlab.is.tsukuba.ac.jp

1 はじめに

近年の急速なインターネットの普及に伴い，その利用する者の個人情報の漏洩を防止することが重要な課題となっている．公開鍵暗号はそれを実現するために不可欠な技術であり，PGP[1] やS/MIME[2, 3], SSL[4] 等の暗号化通信などで利用されている．この暗号化通信では，公開鍵と秘密鍵の二種類の鍵が用いられるが，秘密鍵が何らかの問題により漏洩した場合，秘密鍵を盗まれた人物のなりすまし等が可能となる．しかし，現状ではこのことは殆ど考慮されていない．本稿ではSSL(Secure Socket Layer) 通信においてSSLサーバの秘密鍵が漏洩した場合の被害を最小にするために，鍵更新の期間を短縮した時限付き証明書方式の提案を行い，その評価を行う．

2 SSL通信

SSL通信では伝送されるデータを暗号化するために，共通鍵暗号が使われる．共通鍵暗号はサーバとクライアントが同一の共通鍵を持ち，この鍵によって暗号化と復号化を行う．SSL通信では複数の種類の秘密鍵暗号が用意され、通信開始時にサーバおよびクライアントで共通する暗号方式の内から1つが選択される。規格上は暗号方式としてDES，RC2，RC4，IDEA，3DES，Fortezzaが定められている．

共通鍵をサーバとクライアントで共用するためには公開鍵暗号が用いられる．公開鍵暗号では，公開鍵とそれとペアの秘密鍵が用いられる．公開鍵は第三者に公開された鍵であり，秘密鍵は持ち主だけが知っている公開されない鍵である．公開鍵で暗号化されたデータはそのペアとなる秘密鍵でしか復号化できないので，あらかじめ通信を行う相手に公開鍵を渡しておけば相手から伝送されるデータは第三者が盗聴することはできない．また，秘密鍵で暗号化されたデータはそのペアとなる公開鍵でしか復号化できないので，秘密鍵で伝送データを暗号化すれば相手認証も行うことができる．公開鍵暗号方式では，公開鍵の安全な受渡し方法が問題となるが，一般には，認証局による公開鍵の証明書を用いて，公開鍵の信頼性を高める手法がとられる．SSL通信では通信開始時に公開鍵が記入されている証明書をサーバがクライアントに通知することになっている．SSL通信で利用できる公開鍵暗号方式は規格上，RSA, Diffie&Hellman, Fortezzaなどが用意されている．

SSLのプロトコルの仕様は次のようになる

1. クライアントがサーバにSSLでの通信を要求する．
2. サーバは証明書をクライアントに送る．
3. クライアントはサーバの公開鍵を利用して暗号化された通信路でサーバに共通鍵作成に必要な情報を通知する．
4. サーバはクライアントに共通鍵作成に必要な情報を通知する．
5. サーバとクライアントはお互いに入手した情報から共通鍵を作成し，暗号化通信を行う．

3 公開鍵の変更を考慮した時限つき証明書

SSL通信においては秘密鍵が漏洩しない限り，安全な通信が確保される．しかし，秘密鍵が漏洩した場合はその限りではなく，暗号の解読や，改ざん，成りすましが可能になってしまう．証明書を発行している認証局はこの問題を解決するために，廃棄証明書リスト(CRL:Certificate Revocation List) を公開している．これには，秘密鍵を漏洩した恐れがあったり，証明書に記述された内容が事実ではなくなった場合，所有者によって認証局に廃棄届けが提出された証明書が記述されている．しかし，もし秘密鍵の正当な持ち主が秘密鍵の漏洩に気付かなければ，証明書の有効期限が切れるまで，解読，改ざん，成りすましが可能である．また，前節で示したようにSSL通信のプロトコルではクライアントは認証局に廃棄証明書リストを見に行くわけではないので，通信相手から得られた証明書が廃棄証明書リストに記入されていたとしても，そのことは認識されない．

Certification Limited Validation Period for Public Key Modification in Coded Communication by Secure Sockets Layer

Takuto Fujihaga, Shigetomo Kimura, Yoshihiko Ebihara
† College of Information Sciences, University of Tsukuba
‡ Institute of Electronics and Information Sciences, University of Tsukuba

以上の問題点を踏まえ，以下ではSSL通信のための改良方式を二つ提案する．

- クライアントがサーバから証明書を入手した直後に，常に認証局の廃棄証明書リストを参照する．
- サーバの証明書の有効期限をできるだけ短くする．

第一の方法では廃棄証明書リストをSSL通信を行う度に参照するため，証明書がリストに記入されてさえいれば被害を受けずに済む．この反面，クライアントから認証局への通信負荷が増加することが考えられる．

第二の方法ではサーバの証明書の有効期限が短いため，秘密鍵が漏洩したとしても，少なくとも証明書の有効期限までしか悪用はできない．この方式では，認証局での証明書変更手続きの負荷と鍵の安全性がトレードオフとなっている．

4 シミュレーションモデルと評価結果

本節では前節で提案した二方式についてシミュレーション実験を行い，両者の比較を行う．両方式のシミュレーションモデルをそれぞれ図1および2に示す．このときの，シミュレーション条件は以下の通りである．

- 認証局サーバは1台，SSLサーバは3台，SSLクライアントは15台とし，それぞれは直接ネットワーク接続されているとする．
- SSLクライアントの接続要求は平均λ回/秒のポアソン分布に従うものとする．
- SSLサーバはSSLクライアントからの要求を300m秒で処理するこの間，他のSSLクライアントからの要求は受け付けられず，FIFOの待ち行列に入れられる．
- SSLサーバが認証局に証明書を更新するのに要する時間を150m秒とする．この間，他の証明書更新要求は受け付けられず，FIFOの待ち行列に入れられる．
- SSLサーバが証明書を更新する間隔を6秒，60秒，600秒として実験を行う．

シミュレーション時間は1万秒とし，SSLサーバ・クライアント間の通信の確立回数と，認証局サーバでの証明書の負荷(単位時間当たりの処理時間)と証明書の平均待ち時間を求める．

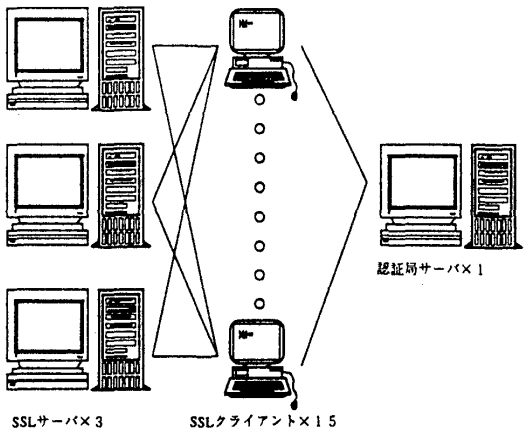

図1: クライアントが廃棄証明書リストを参照する場合のシミュレーションモデル

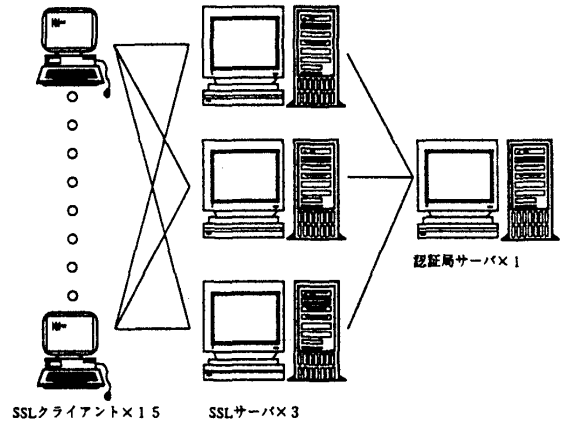

図2: サーバの証明書の有効期限を短くする場合のシミュレーションモデル

参考文献

[1] Simson Garfinkel, "PGP: Pretty Good Privacy," O'Reilly & Associates, Inc., 1994. (邦訳："PGP暗号メールと電子署名," オライリー・ジャパン, 1996)

[2] Steve Desse, Paul Hoffman, Blake Ramsdell, Laurence Lundbalade, Lisa Repka, "S/MIME Version 2 Message Specification", 1998.

[3] Steve Desse, Paul Hoffman, Blake Ramsdell, Jeff Weinstein "S/MIME Version 2 Certificate Handling,", 1998.

[4] Alan O Freier, Philip Karlton, Paul C. Kocher, "The SSL Protocol Version 3.0,", 1996.