Vol.2010-CSEC-50 No.12
2010/7/1

SSL/TLS renegotiation 機能の脆弱性に伴なう移行における問題点

須賀 祐治[†1]

2009 年 11 月に Marsh Ray，Steve Dispensa，Martin Rex によって SSL/TLS プロトコル[1),2)] の脆弱性が公表された[3)]．SSL/TLS は IP 層とアプリケーション層の間に位置し，アプリケーションデータの暗号化とデータ完全性を保証し，通信相手ノードを X.509 公開鍵証明書に拠り認証する機能を提供する．HTTP,SMTP,POP などのアプリケーション層の通信プロトコルと併用して用いられるため，本脆弱性は多くのアプリケーションやシステムに影響を及ぼすと考えられている．IETF では対策を講じた RFC 化を目指してインターネットドラフトが異例の速さで RFC5746[11)] として発行されたが，サーバサイドの移行は必ずしも進んでいない．本稿では，移行の障害となっている課題について整理していく．

Problems on the shifts to a new specification with countermeasures of the SSL/TLS renegotiation vulnerability

Yuji SUGA[†1]

In November 2009, Marsh Ray, Steve Dispensa and Martin Rex released details of a vulnerability in the SSL and TLS protocols[1),2)] that could allow Man-in-the-Middle attacks to be carried out[3)]. SSL and TLS operate between the IP and application layers and ensure application data encryption and data integrity, authenticating the target of communications using X.509 public key certificates. As they are used together with application layer communication protocols such as HTTP, SMTP, and POP, this vulnerability affects a large number of applications and systems. IETF published countermeasures with unprecedented speed as RFC5746[11)], however server-side implementations are not settled. In this report, we discuss about problems of the shift to new specifications.

1. はじめに

2009 年 11 月に Marsh Ray，Steve Dispensa，Martin Rex によって SSL/TLS プロトコル[1),2)] の脆弱性が公表された[3)]．本脆弱性は CVE-2009-3555[4)] および JVNVU#120541[5)] で管理されている．SSL/TLS は IP 層とアプリケーション層の間に位置し，アプリケーションデータの暗号化とデータ完全性を保証し，通信相手ノードを X.509 公開鍵証明書に拠り認証する機能を提供する．HTTP,SMTP,POP などのアプリケーション層の通信プロトコルと併用して用いられるため，本脆弱性は多くのアプリケーションやシステムに影響を及ぼすと考えられている．特に HTTPS(HTTP over SSL) プロトコル[6)] は多くのブラウザと Web サーバはが実装されており，Marsh Ray らの報告[3)] には HTTPS を用いた攻撃方法が紹介されている．さらにこれを Twitter API に適用し，攻撃者の Twitter アカウントにパスワード情報を投稿させる方法[8)] が公開されるなど実際に適用可能であることが示されている．HTTP 以外のプロトコルへの適用可能性については Thierry Zoller により検討されている[7)] が，FTPS, SMTPS は脆弱であり EAP-TLS は影響を受けないことが示されているが，POP や LDAP など未だに脆弱かどうか未知のプロトコルも残されている．

本脆弱性は実装の問題ではなく，SSL/TLS プロトコル仕様そのものの問題に起因する．OpenSSL[9)] や Apache[10)] などで対応パッチが公開されるなど一見すると対処することが可能かのように見えるが，これらはワークアラウンドな対策でしかなかった．当面の対策方法としては OpenSSL のパッチ[9)] で採用されているようにシンプルに renegotiation 機能を無効にする対策が考えられる（無効になっているかどうかの確認は[12)] で行うことができる）．

一方で，根本的な対処は問題のある現仕様をアップデートし，新仕様にあわせた実装に移行することである．TLS 仕様を策定した IETF においてもその認識があり，対策を講じた RFC 化を目指してインターネットドラフトが異例の速さで RFC5746[11)] として発行された．新 RFC の内容については後述するが，本脆弱性は TLS の全てのバージョンのプロトコルだけでなく SSL バージョン 3.0 にも影響を及ぼすため，SSL の仕様は IETF で策定されていないにも関わらず，新仕様を TLS と同様に適用可能と記されている．また OpenSSL 0.9.8m にて RFC5746 が実装されるとともに IE を除く主要ブラウザ Opera, Firefox 等で実装されるなど移行が進んでいる．このフットワークの速さは評価に値するが，サーバ側は

†1 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc.

RFC5746 への意向は進んでいない．本稿では，次節以降，この移行の障害となっている課題について整理していく．

2. renegotiation 機能を突いた中間者攻撃

本脆弱性の原因となっている renegotiation 機能は，SSL/TLS はアプリケーションデータをセキュアに送受信する前にハンドシェイクプロトコルを再送することであり，renegotiation 機能のための特別なメッセージが準備されているわけではない．ハンドシェイクプロトコルにて暗号アルゴリズムや鍵情報などを共有する機能を持つが，renegotiation 行うことでクライアント・サーバ間で合意されたアルゴリズム，鍵情報などをリフレッシュすることができる．

今回の脆弱性は中間者攻撃（Man in the middle attack）に分類される．これは通信に対する攻撃手法で，通信を行う 2 者の間に攻撃者が存在することで成立する攻撃である．この攻撃により，通信の傍受と改ざん（通信を行う 2 者それぞれに対する成りすましを含む）などが発生する．この攻撃手法が成立するかどうかを検討したり，対策を検討したりするうえで，あらかじめ中間に存在する攻撃者を仮定して検討する必要がある．実際に中間者攻撃を成立させるためには，その攻撃手法だけではなく，通信の間に割り込むための別の手法（例えばインターネットでは経路ハイジャック等）を併用しなければならない点に注意する．

具体的な攻撃シナリオとしては，1) セッション途中でクライアント認証（公開鍵証明書でクライアントを認証）に切り替える，2) HTTPS 通信から HTTP 通信に切り替えるケースで，攻撃者はサーバ・クライアント間のセッションをインターセプトすることが想定されている．HTTP レベルで攻撃者のデータと正当ユーザによるデータをマージしてサーバが解釈するために，サーバに対し正当ユーザに成りすましたアプリケーションデータを送信することを可能にする．ここで正当ユーザのアプリケーションデータはセキュアなままであり，攻撃者による改ざんやデータ搾取は行われていないことに注意する．攻撃者によるデータは HTTP リクエストとしては未完な状態にしておき，正当ユーザによるデータで完璧するよう細工する．場合によっては，攻撃者のデータと正当ユーザのデータは HTTP クッキーで結び付けられるために，サーバは 2 つのデータが同一ユーザによるリクエストであると解釈してリクエストを受領してしまう可能性がある．実際に中間者攻撃が成立する例については図 1 を参照のこと．

- (1) 通常の TLS ハンドシェイクを行う．
- (2) 攻撃者は正当なユーザの通信データを保持しておく．

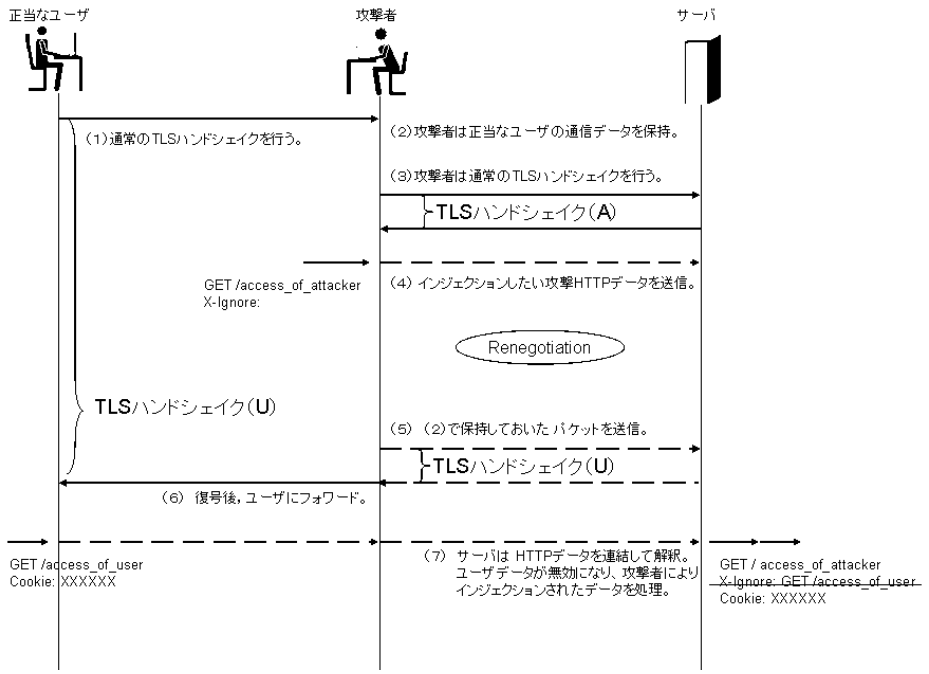

図 1 中間者攻撃の例

- (3) 攻撃者は通常の TLS ハンドシェイクを行う．このときサーバは普通の TLS ハンドシェイクとしてしか処理しない，つまり正当なユーザからのアクセスか攻撃者からのアクセスかを判別できない．
- (4) プロセス (3) で確立した鍵情報に基づき HTTP リクエストを送信する．ここで HTTP リクエストとしては未完な状態にしておく．
- (5) 攻撃者主導で Renegotiation を行う．実際には新たに TLS ハンドシェイクデータを送信する．プロセス (2) で保持しておいた正当なユーザからの情報を（3）で確立した通信路で送信する．サーバはプロセス (3) の通信を行った通信相手が Renegotiation を要求していると認識する．このとき正当なユーザからの要求であるか，攻撃者からの要求であるかを確認することはできない．
- (6) サーバからのメッセージを復号した後，改変せずそのまま正当なユーザにフォワー

ドする．このとき正当なユーザプロセス (1) のレスポンスであるとしか認識できない．

- (7) プロセス (6) で確立した暗号化済通信路を用いて HTTP リクエストを送信する．攻撃者はそのままフォワードする．このとき通信内容は暗号化されているため攻撃者は中身を見ることはできない．

この仕組みを用いて，Twitter API でのインジェクション攻撃（現在は対策済みで攻撃は成功しない）に限らずサーバが銀行の口座システムである場合など直接的に金銭に関わる被害を誘発する可能性も指摘されている．

3. 新仕様における改変点

対策が策定された RFC5746 での改変点を紹介する．この RFC では，TLS の拡張タイプの値としての `renegotiation_info` と，本来ならば暗号アルゴリズムを表現する Cipher Suite の状態として `TLS_EMPTY_RENEGOTIATION_INFO_SCSV` が導入されている．前者の `renegotiation_info` 拡張を用いて renegotiation を安全に行う実装であることを通信相手に宣言することができる．具体的には，クライアントとサーバがともにハンドシェイクプロトコルで安全に共有した情報を保存しておき，renegotiation を行う際に `renegotiation_info` 拡張を用いて，お互いしか知りえない情報を交換することで，それまで接続していた通信相手であることを確認するという手法である．後者としては，`renegotiation_info` 拡張を処理不能な TLS 拡張と認識し，通信を中断する実装が存在するため，`TLS_EMPTY_RENEGOTIATION_INFO_SCSV` を用いる方法も準備されている．

3.1 後方互換性の問題

RFC5746 に準拠することで対策済みの実装が普及し今回の問題が解消されることが望まれるが，移行には時間がかかると考えられる．後方互換性の観点から現バージョンとの互換性を確保すべきであるが，旧実装から renegotiation が行われた場合，正しい相手からのリクエストであるかどうかを安全に確認する手段はない．このため新実装では，旧実装からの renegotiation 要求を拒否することが推奨されている．これは，現在の一時的な対策に相当するもので，renegotiation 機能を利用することはできない．つまり，安全に renegotiation を行う必要がある利用形態では，新しい仕様が RFC 化された後，クライアントとサーバで，ともに新仕様に対応した新しい実装を導入する必要がある．

4. 移行に至らない要因

根本的な問題を RFC5746 が回避したにも関わらずサーバサイドでの移行は進んでいない．これは以下の 3 つの要因があると考えられる．

(1) 本脆弱性に関するリスクが不明瞭 攻撃が成功する前提条件として DNS 詐称などにより攻撃者がサーバクライアントの中間に位置してトランザクションをコントロールする必要がある．この成功確率が不明瞭，もしくは不可能性に近いと考えられているため，サーバ運営者は移行しないと考えられる．

(2) メッセージをインジェクションされた際の被害が不明瞭 攻撃が成功するのは 1 メッセージに対してのみ行えること，サーバサイドで HTTP レベルでのメッセージ結合を行わないことにより本攻撃を回避できることなどの情報が正確に把握できていないため，被害に対する損失が見積もれず，サーバ運営者は移行しないと考えられる．

(3) クライアントにおける新仕様の普及率が不明 新仕様と旧仕様には互換性がなく，移行した場合には旧仕様しか実装していないクライアント（Web ブラウザ）からでは SSL/TLS 通信ができない．これは機会損出の可能性を鑑み，サーバ運営者は移行しないと考えられる．

今後，定量的な尺度を導入することにより，これらの問題を解決する必要があると考えられる．

5. ま と め

SSL/TLS renegotiation 機能の脆弱性に関して RFC 化されたものの，特にサーバサイドの移行には課題があることを指摘した．今後，それらの課題に関して計測可能な手法と敷居値に関する検討を行い，早期に安全な新仕様への移行を進めていくための情報提供を行っていく予定である．

Vol.2010-CSEC-50 No.12
2010/7/1

参 考 文 献

1) Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008. http://www.ietf.org/rfc/rfc5246.txt
2) Alan O. Freier, Philip Karlton, Paul C. Kocher, "The SSL Protocol Version 3.0", Internet Draft, November 1996. http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00
3) Marsh Ray, Steve Dispensa, "Renegotiating TLS", November 2009. http://extendedsubset.com/Renegotiating_TLS.pdf
4) CVE-2009-3555, http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3555
5) JVNVU#120541, SSL および TLS プロトコルに脆弱性, http://jvn.jp/cert/JVNVU120541/index.html
6) E. Rescorla, "HTTP Over TLS", May 2000. http://www.ietf.org/rfc/rfc2818.txt
7) Thierry Zoller, TLS & SSLv3 renegotiation vulnerability, http://www.g-sec.lu/practicaltls.pdf
8) Anil Kurmus, TLS renegotiation vulnerability (CVE-2009-3555), http://www.securegoose.org/2009/11/tls-renegotiation-vulnerability-cve.html
9) OpenSSL Security Advisory [11-Nov-2009], http://www.openssl.org/news/secadv_20091111.txt
10) http://www.apache.org/dist/httpd/patches/apply_to_2.2.14/CVE-2009-3555-2.2.patch
11) E. Rescorla, M. Ray, S. Dispensa, N. Oskov, Transport Layer Security (TLS) Renegotiation Indication Extension, 2010. http://www.ietf.org/rfc/rfc5746.txt
12) TLS Renegotiation Test, http://netsekure.org/2009/11/tls-renegotiation-test/