学術交流委員会だより

平成13年度後期国際研究集会派遣会員報告書

派遣員 多田浩章 千葉労災病院

派遣国際研究集会：The 87th Scientific Assembly and Annual Meeting of the Radiological Society of North America

開催場所：McCormick Place, Chicago, Illinois, U.S.A

開催期間：Nov. 25-Nov. 30, 2001

Using SSL for Secure Web-Based Medical Image Viewing System

H. Tada

Department of Radiology, Chiba Rosai Hospital

Purpose:

The Secure Sockets Layer (SSL) is a security protocol that provides communications privacy over the Internet. We develop Web-based medical image viewing system, which enhanced security to use SSL. And examine the usability of using SSL.

Materials and Methods:

We prepare two servers, which runs the LINUX operating system. One is a DICOM image server constituted of the DICOM Central Test Node (CTN) software and a public domain database called PostgreSQL. Another one is a World Wide Web (WWW) image server constituted of a WWW server called Apache with a JAVA servlet engine called Tomcat, a SSL toolkit called OpenSSL, and a image serve application coded by ourselves. To confirm the action of SSL, Using a network protocol analyzer called Ethereal, we examine packet data from the system network. To check the performance, we measure the response time from doing query on client to all images displayed on client using Magnetic Resonance Angiography (MRA) source images converted file format to JPEG (125kB × 108 pieces) by this system.

Results:

We've confirmed that image data are disclosed when no use SSL, but then image data are not discriminative when use SSL. The response time is 53 sec each other.

Conclusion:

The conversion to communication over SSL is implemented without changing any server side applications. And we consider that even if we use a poorer client machine than we used, a decline in the response under using SSL will be acceptable range in comparison with disuse. Using SSL has provided the great usability for all Web-based medical system, which must be enhanced security.

はじめに

平成13年11月25日から30日までシカゴで開催された第87回北米放射線学会(RSNA2001)に参加してきました。幸運にも本学会の国際研究集会派遣会員として援助を受けることができ、本学会ならびに国際研究集会派遣制度に大変感謝しています。

以下は、演題申し込み時に送ったabstractと、実際にScientific Poster Sessionsにおいて発表した内容です。abstract中には、予備実験としてストップウォッチで計時した画像表示時間を示していますので、発表内容の測定データとは若干の相違がありますがご容赦ください。

セキュアWebベース医用画像表示システムにおけるSSLの利用

1. 目的

secure socket layer (SSL) はインターネット上の通信においてセキュリティを高めるために用いられるプロトコルである。われわれは、独自に開発したWebベース医用画像表示システム上でSSLを用いてセキュリティ強化を図っているが、このSSLを使うことの優位性について検証することを本研究の目的とした。

2. システム概要

WWW image server

CPU : Pentium III 550MHz

RAM : 256MB

OS : LINUX (RedHat6.2)

HTTP server : apache + mod_SSL

SSL : OpenSSL

Servlet container : Tomcat

JAVA : JAVA2 SDK

Image serve servlet : 自作

DICOM server

CPU : PentiumIII 700MHz

RAM : 512MB

OS : LINUX (RedHat6.2)

Image archive : image_server (CTN)

Data Base : PostgreSQL

クライアント

CPU : PentiumII 450MHz

RAM : 256MB

OS : WindowsNT 4.0 SP5

ブラウザ : Internet explorer5.5 SP2

3. 方法

3-1 SSL通信動態の確認

SSL通信動態を確認するために、ネットワークプロトコルアナライザ“Ethereal”を用いて、ネットワーク上を流れるパケットデータを監視する。

3-2 パフォーマンスの評価

パフォーマンスの評価のために、画像表示時間 (TTD : time to display) を測定する。

ここでTTDは、クライアント上で取得するシリーズを選択してから、そのシリーズのすべてのサムネイル画像がクライアント上に表示されるまでの時間と定義する。

測定に用いたシリーズは、シリーズA (512×512, 11枚)・シリーズB (512×512, 108枚)の2種類で、それぞれ5回ずつ測定した。計時にはEtherealのタイムスタンプを用いた。

4. 結果と考察

4-1 SSL通信動態

SSL非使用時にEtherealでパケットデータを監視すると、通信によってやり取りされるデータの内容が丸見えであった。

一方、SSL使用時には、通信データの先頭に挿入されているデータタイプを読み取ることによって、コミュニケーション確立用のデータが流れているのか、アプリケーションデータが流れているのかが判断できるので、どのような種類の通信が行われているのか判断できても、データの内容は暗号化されていて判別不可能であった。

4-2 パフォーマンスの評価

TTDの測定結果をTableに示す。

Table TTD

	SSL非使用	SSL使用	P値 (両側t検定)
シリーズA	4.494±0.014	4.408±0.003	0.207
シリーズB	49.18±0.21	49.27±0.23	0.632

Fig. 画像データを送信する際に観察されたフレーム構造

これより、SSLを使用してもパフォーマンスの低下を来さないことが確認された。

SSLは暗号化通信を行うため、送信側でのデータの暗号化処理と受信側でのデータ復号処理が必要になる。にもかかわらずSSL使用／非使用時にTTDに差が生じないということは、ネットワークを流れるデータが小さくなっていることが予想される。

そこで、Etherealによる監視内容から、実際のパケットデータの構造を図に示したのがFig.である。

これで分かるとおり、サーバクライアント間を流れるアプリケーションデータが、SSLによる暗号化により大幅に圧縮されていることが分かる。つまり、暗号—復号に伴う処理時間の延長は、データ自体が圧縮されることによる転送時間の短縮で相殺されていると判断できる。

5. 結語

WebベースのシステムでSSLを使用するには、HTTPサーバでSSLを使えるように調整するだけであり、SSLの使用は、サーバ上のアプリケーションを一切変更することなく「盗聴」・「改ざん」・「成りすまし」を防止できるという、簡便にセキュリティ強化を実現する手段であるといえる。

暗号化通信はセキュリティ強化だけではなく、ネットワーク負荷の軽減にも役立つものと考えられる。

SSLの使用は、セキュリティ強化の必要のあるすべてのWebベース医用システムに多大なメリットをもたらすものだと考えられる。