Available online at www.sciencedirect.com
ScienceDirect
Computer Communications 30 (2007) 3063–3074
computer communications
www.elsevier.com/locate/comcom

Evaluation of the effect of SSL overhead in the performance of e-business servers operating in B2B scenarios

Daniel F. García [a,*], Rodrigo García [b], Joaquín Entrialgo [a], Javier García [a], Manuel García [a]

[a] Department of Computer Science and Engineering, University of Oviedo, Campus de Viesques, 33204 Gijon, Spain
[b] Center for the Development of Information and Communications Technologies, Scientific Park, 33203 Gijon, Spain

Available online 23 June 2007

Abstract

In the current business to business environments, transactions between e-business servers must be carried out with a high security level. To carry out secure transactions, the servers must do additional tasks, such us exchanging encryption keys and encrypting and decrypting the information interchanged during the transactions. The combination of several specific algorithms for these tasks constitutes a cipher suite. The additional tasks degrade the server performance and the challenge is to quantify the degradation as a function of the cipher suite selected.

Until now, several research works have evaluated the impact of security on the performance provided by web servers using static and very simple dynamic contents. However there is a lack of research into the impact of security on the performance of e-business servers which execute complex transactions, some of them involving additional transactions with other servers.

This work presents an evaluation of the impact of using SSL, with several representative configurations, on the performance of e-business servers. The business application used to carry out this execution is the TPC-App benchmark, which is a good representation of business-to-business environments. The benchmark runs on a cluster of two layers.

The results of this evaluation are unexpected, because the impact of SSL on performance is small compared to the results of previous works that evaluate web servers, for which the impact of SSL on performance is very high. Therefore, this work provides insight to solve the tradeoff between security and performance when an SSL cipher suite must be selected for a complex e-business system rather than for a simple web server.

Keywords: e-Business server performance; SSL overhead; B2B environments; Impact of security on performance; TPC-App benchmark

1. Introduction

The main goal of an application server in a business-to-business (B2B) environment is to provide its services to the maximum number of concurrent business clients. Generally, the interactions between e-business servers are always carried out within secure sessions commonly based on SSL (Secure Sockets Layer) connections [10,21]. The SSL protocol was originally designed at Netscape for its web browsers and servers, but was later standardized by IETF and is now called TLS (Transport Layer Security) [9]. The SSL/TSL protocol gives security to the HTTP transactions [16] using cryptographic techniques [19] that demand computational resources. Therefore the utilization of secure connections in business sessions between two or more machines would degrade the performance of an application server, that is, the throughput of the server would decrease and its response time would increase.

In this paper, we evaluate the influence (overhead) of security on application server performance, analyzing the server behavior as a function of the number of concurrent e-business clients supported in two scenarios: with and without security.

The experimental environment is based on our implementation of the TPC App benchmark [20], which provides

* Corresponding author. Present address: Department of Computer Science, office 1.2.14, Edf., Departmental Oeste, Campus de Viesques, 33204 Gijon, Spain. Tel.: +34 985 182 066; fax: +34 985 181 986.
E-mail address: dfgarcia@uniovi.es (D.F. García).

0140-3664/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2007.05.040

a realistic emulation of the workload supported by an application server in a B2B scenario.

2. Related work

The impact of security on web servers has been analyzed in the literature. These works, which evaluate the influence of security on client-to-business (C2B) environments, can be classified in two groups. In the first group, we consider the works devoted to evaluating the influence of the SSL protocol on the performance of the e-commerce servers. In the second group, we analyze the works devoted to improving the performance of the SSL protocol.

2.1. Evaluation of the influence of the SSL protocol

In a pioneer work, [14], Kinicki et al. compared the throughput and response times of an e-commerce site with and without SSL security. They carried out their performance comparison experiments on an e-commerce site made up of three computers: a web server, an application server and a database server. The authors conclude that SSL has a very high impact on the performance of C2B servers when the processing of a transaction only consists of serving one static web page. However, when the transaction involves a high level of processing in the application and database servers, the relative impact of SSL is negligible. The results are similar to the conclusions obtained in the research work presented in this paper for B2B environments.

Later in [13], Kant et al. analyzed the impact of SSL on the performance of internet servers for different configurations of the architecture of the servers. They used a static workload of a single page of 30 byte, or 36 Kbyte or 1 Mbyte, which is retrieved by all clients. The page of 30 byte is intended for analyzing the handshake performance and the page of 1 Mbyte is used for analyzing the bulk data encryption performance. The page of 36 Kbyte is used to analyze the two aspects of SSL in a combined manner. Their main conclusion was that the use of SSL increases the computational cost of the transactions by a factor of 5–7. However this result was obtained with an extremely simple workload, in which the main computational effort is due to the SSL protocol. This load scenario and the conclusion obtained from it are not applicable to the current B2B scenarios considered in the evaluation work presented in this article.

In [15], Lin et al. developed an analytical queuing model to analyze the impact of SSL on the performance of web servers when security configuration parameters are changed. The model considers https requests, with probability p, and http requests, with probability $1 - p$. Each type of request carries out a different sequence of activities in the queues of the model. The authors evaluated the increment of response time when the parameter p increases and also when the RSA key length is incremented. Finally, they evaluated the influence of three different symmetric encryption algorithms. This model is inappropriate for current web servers with a high proportion of dynamic content. Furthermore, it is not representative of current e-business servers considered in this research work, in which the web server interacts with back-end systems composed by an application and database servers.

In [7], extended in [8], Coarfa et al. analyzes the increment of the web server throughput when individual components of the TSL protocol are eliminated. Coarfa et al. carried out the experiments by executing two different traces on an Apache web server. One trace was obtained from the purchase of a book in Amazon, but discarding all the back-end processing. This trace is not representative of the global load supported by a typical web server operating in C2B environments, because it only considers an isolated operation. The other trace was obtained from the general web server of a computer science department of a university, which is not representative of real e-business environments either. The main result of this work is the characterization of the relative impact of the components of the TSL protocol on performance, showing that the initial key exchange is the operation with the highest impact. However, only a few of the results provided are useful for the evaluation of the global impact of SSL on server performance, because they are obtained emulating non-realistic operational conditions. For example, it is useless to interchange secret keys in the handshake, but then not use them to encrypt the data transferred or vice versa.

Beltran et al. evaluated in [3] the performance impact of SSL on web applications using the RUBiS benchmark, which realistically emulates an auction site, including browsing, selling and bidding operations. The experimental platform has two computers, an application server based on Tomcat and a database server based on MySQL. Additional computer injects the load using the Httperf tool. This experimental approach, based on a representative benchmark executed on a cluster of two servers, is similar to the evaluation approach presented in this article. However the results are very different. Beltran et al. found that the use of SSL greatly reduces the maximum throughput of a web server and they indicate that this result is probably due to the configuration of the load injector. When the server is heavy loaded and can not serve a client, this client tries to reconnect immediately. These continuous connection trials, each one requiring the execution of a full SSL handshake, consume more and more processor time, further reducing the throughput of the server. Under these experimental conditions, the evaluation of SSL overhead behaves like a denial of service attack.

In [22], Zhao et al. carried out an extensive study of the performance costs of the SSL processing without including external operations. For the standalone SSL analysis they developed a small Crypto-Benchmark. This is a program that creates a server context as well as a client context in a single computer, and sends messages between the two through memory buffers. This program was executed in a virtual emulation environment that allows the CPU cycles