计算机工程与应用 2007 43 (19): 1-3 ISSN: 1002-8331 CN: 11-2127/TP

博士论坛

# SSL握手协议中客户端平衡密钥交换算法

齐 芳[1]，贾维嘉[1,2]，王国军[1]

1.中南大学 信息科学与工程学院，长沙 410083
2.香港城市大学 计算机科学系，香港

收稿日期 修回日期 网络版发布日期 2007-6-20 接受日期

摘要 SSL协议的基本设计目标是为两个通信实体之间提供数据的保密性和完整性。由于在SSL握手协议中最耗费计算资源和造成客户端与服务器端计算不平衡的步骤是服务器端解密运算，提出了客户端平衡的密钥交换算法，用来加速SSL会话的初始化和承担服务器端的解密的预运算。对算法中的同时对多个客户的请求进行解密的粒度的估计策略进行了阐述。模拟实验表明所提出的方案是有效的。

关键词 安全套接层协议 握手协议 密钥交换算法 解密运算

分类号

# Client balanced secret exchange algorithm in SSL handshake protocol

QI Fang[1]，JIA Wei-jia[1,2]，WANG Guo-jun[1]

1.School of Information Science and Engineering，Central South University，Changsha 410083，China
2.Department of Computer Science，City University of Hong Kong，Hong Kong，China

**Abstract**

The primary goal of the Secure Socket Layer（SSL） protocol is to provide confidentiality and data integrity between two communicating entities.Since the step that is most computationally expensive and causes computational imbalance between clients and server in the SSL handshake protocol is the decryption computation of the server，we show that a client balanced secret exchange algorithm can be used to speedup SSL session initialization and undertake the previous computation tasks of server’s decryption.It is also introduced that the estimation strategy of parameter which is the size of clients which will be decrypted at the same time.Finally，the proposed algorithm is evaluated to be efficient through simulation studies.

**Key words** Secure Socket Layer（SSL） handshake protocol secret exchange algorithm decryption computation

DOI:

通讯作者 齐 芳 E-mail：csqifang@mail.csu.edu.cn

扩展功能

本文信息

Supporting info

PDF(802KB)

[HTML全文](0KB)

参考文献

服务与反馈

把本文推荐给朋友

加入我的书架

加入引用管理器

复制索引

Email Alert

文章反馈

浏览反馈信息

相关信息

本刊中 包含“安全套接层协议”的相关文章

本文作者相关文章

· 齐 芳
· 贾维嘉
·
· 王国军