

基于 SSL 提高网上安全交易性能的研究

张 雪¹, 马光思¹, 毛宏燕²

(1 西安建筑科技大学 信息与控制工程学院, 陕西 西安 710055; 2 华东师范大学 软件学院, 上海 200062)

摘 要: 结合网上安全交易支付模式的课题研究, 给出了建立个人 CA 中心, 订单安全交易及混合密钥应用的过程. 针对反复认证和密钥应用影响交互效率问题, 提出了利用 SSL 会话恢复及连接分类机制实现双向连接响应的性能优化策略. 综合双向握手、会话恢复的交互分析和实验结果表明, 所实现的研究成果能很好提高 Web 应用效率.

关键词: 网上交易; SSL 协议; 会话恢复; 连接分类

中图分类号: TP309.7

文献标识码: A

文章编号: 1000-7180(2011)02-0181-03

Research of Improving Safety E-Trade Performance Based on SSL

ZHANG Xue¹, MA Guang-si¹, MAO Hong-yan²

(1 School of Inform. & Con., Xi'an University of Architecture & Technology, Xi'an 710055, China;

2 Software Engineering Institute, East China Normal University, Shanghai 200062, China)

Abstract: In investigating the model of safety E-trade, the process of building personal CA, safety trade and mixing keys application are given. Aimed at the problems of low efficiency in repeated authentication and keys application, the policy using SSL session-resumed and classification mechanism to realize the bidirectional connection responses is proposed. By analyzing the bidirectional handshake and session-resumed interaction, the experiment results indicate that it highly improves the performance of web application.

Key words: E-trade; SSL; session resumed; connection classification

1 引言

电子商务中支付安全问题直接影响双方交易及金融安全, 现有支付研究多是以提高安全性为前提, 如: 改进协议、提高随机数质量、实施二次加密、加强 CA 管理、增设服务器端可信代理等^[1-3]. 但这些改进并未考虑服务器处理能力及连接响应数量对交易效率的影响. 文献[4]分析了 Web 环境下传输层安全 TLS 协议的性能问题, 给出了从改进协议和使用硬件设备两方面来提高 TLS 性能的解决方案. 文中基于安全套接层协议 SSL 建立的网上交易模式, 应用会话恢复和分类优化处理访问请求, 以加快响应时间, 提高交易效率.

2 网上安全支付模式

图 1 所示的网上安全支付模式. 其功能分为订单操作和支付操作两部分:

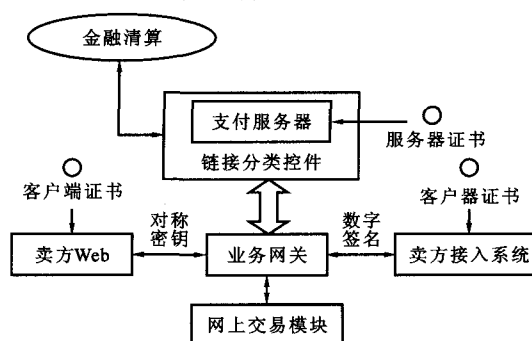


图 1 网上安全支付模式

(1) 订单操作为交易双方与支付服务器的交互,内容包括:身份认证、交易申请、订单分析、金融授权请求、发货通知等;支付操作为支付服务器与金融机构的交互,内容包括:支付要求、转账交易、响应返回等。支付服务器只需进行订单操作开发,预留支付接口,支付操作由金融机构完成。

(2) 网上安全支付模式中,身份认证、加密订单、签名及验证订单等过程,增加了通信次数及复杂性,极大影响了网上交易流程的响应速度。为解决这一问题,在服务器端引入连接分类机制,将请求分为新会话及恢复会话分别处理,能有效提高应用效率。

3 安全订单传输设计

Java 加密结构 JCA 包括数字签名和消息摘要 API,提供包括对称分组算法、对称加密及非对称加密等算法。本文安全订单传输使用 Jsp Servlet 实现动态加载,保证程序运行平台无关,且混合使用对称和非对称加密,加密密文时使用对称密钥,数字签名及对话密钥传输时使用非对称加密。

3.1 建立个人 CA 中心,签发证书

服务器及用户身份认证通过向专业认证中心申请 CA 实现,研究实例采用 OpenSSL^[5] 配合 JDK 中 keytool 工具建立个人 CA,实现证书签发、管理,交换交易双方密钥信息。生成 CA 主要步骤为:

```
Step1: genrsa -out ca-key.pem;
/生成 CA 私钥
Step2: req -new -out ca-req.csr -key;
/用私钥生成签名申请文件
Step3: openssl x509 -req -in ca-req.csr -
out ca-cert.pem -signkey ca-key.pem;
/用私钥对申请签名得出 CA 认证文件
Step4: keytool -certreq -file;
keytool -genkey -keystore;
/ JDK 生成密钥对及待签名证书;
Step5: openssl x509 -req;
keytool -import -file;
/使用 CA 私钥签名,并将信任证书导入 Java
密钥库 keystore;
```

Step6: 安装证书,完成 CA 认证管理。

3.2 订单安全交易

身份认证后进入安全交易过程,以订单提交为例,设计基于 SSL 协议的安全交易过程,订单提交由如下两个步骤组成:

(1) 买方加密订单及签名

Step1: 生成对话密钥;

Step2: 使用服务器方公开密钥加密对话密钥;

Step2: 使用私钥对订单签名;

Step3: 使用对话密钥对订单信息加密;

Step4: 向服务器传送已加密密文、签名文件及加密密钥。

(2) 服务器验证订单信息及签名

Step1: 解密数据包、验证签名;

Step2: 使用买方公钥验证签名;

Step3: 使用服务器自身私钥解密用户传送的已加密对话密钥;

Step4: 使用对话密钥解密订单。

订单加密过程如图 2 所示。

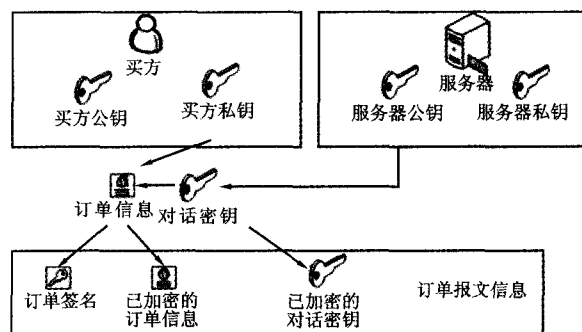


图2 订单加密过程

4 连接分类机制及性能研究

第3节的安全订单传输过程中,反映出服务器处理交互密钥,加解密交易订单,使得计算负荷明显增加,直接影响交易效率。如何解决这一问题,是当前研究工作的要点。

4.1 会话交互分析

SSL 握手协议^[6]在客户端和服务端之间连接时协商会话参数,并建立会话。会话包含的主要参数有会话 ID、对方的证书、加密套件以及主密钥。SSL 双向握手协议^[6]使服务器强制 SSL 客户端将其证书返回,客户端通过 Certificate 消息将自身证书发送给服务器,计算已交互的握手消息、主密钥的 Hash 值,利用自己的私钥对其加密,并通过 Certificate Verify 消息发送给服务器,详细交互过程见图 3。

会话恢复时客户端发送 Client Hello 消息,消息中的会话 ID 设置为计划恢复的会话 ID,服务器如果允许恢复该会话,则通过在 Server Hello 消息中设置相同的会话 ID 来应答,客户端计算已交互的握手消息的 Hash 值,利用原有会话的密钥和加密套件处理 Hash 值,并通过 Finished 消息发送给服

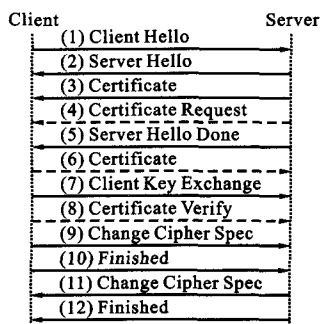


图3 C/S双向握手过程

务器,判断密钥和加密套件是否正确。详细交互过程见图4。比较图3与图4,增加会话恢复功能,恢复中断的交易,省去了双方交换密钥、加密套件及传输加密环节,能极大缩短通信时间。

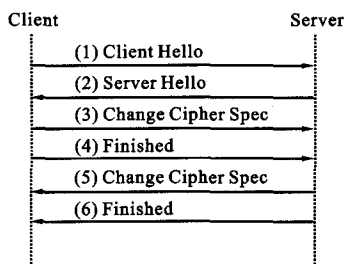


图4 会话恢复握手过程

一般会话恢复要在服务器端保留大量客户端缓存条目,服务器负担较重。当服务器超负荷时,一部分会话请求无法响应将会被拒绝,且若缓存失效时间内无法及时处理客户端请求,则超时的会话将会被丢弃,Session完成率降低。

4.2 分类机制及实验分析

实时SSL连接分类即决定服务器处理连接方式,保持最高连接数量在处理器负荷内,其原则为优先处理需时最短请求,减少队列等候时间,在队列中优先处理会话恢复请求,限制新连接响应,以提高单位时间内Session完成率。分析处理器处理能力与完成会话数量关系,引用公式(1)^[7]:

$$N(k) = \left\lfloor \frac{k \times A(k) - O(k) \times CTO}{CTN} \right\rfloor \quad (1)$$

其中, k 为样本采样时间, $A(k)$ 为服务器处理器数量, $O(k)$ 为 ks 内恢复会话数, $N(k)$ 为 ks 内新会话请求, CTO 为恢复会话处理器运行时间, CTN 为处理器运行新会话时间。处理器运行速度有限时,恢复会话数量越多,新会话请求数量越少,成功交易数量随完成Session递增。在Tomcat server中使用Httpperf测速SSL连接分类机制响应与客户请求关系,实验分析结果如图5所示。

使用传统SSL连接,当客户请求数量达到特定

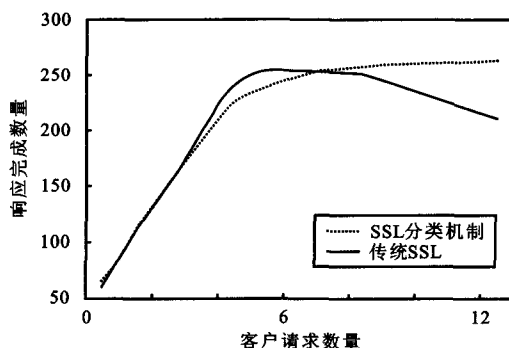


图5 响应与客户请求关系

峰值时,随着请求数量的增多响应完成数量逐步下降;使用连接分类机制后,响应完成数量随客户请求递增,并保持一定水平,提高了交易效率。

5 结束语

文中基于SSL连接分类机制实现了应用OpenSSL建立个人CA及Java Security API加密结构的安全订单交易过程。通过分配新会话与恢复会话连接,减轻了处理器负担,提高了Session完成率。理论分析和实验结果表明,在用户请求递增时,改进机制的效率显著提高。进一步的性能改善可考虑对其他协议^[8]、加密算法的优化或采用多核处理器并行,以保证数据安全及高效交互。

参考文献:

- [1] ZDNet 管理软件频道. CA 全新 ITIL 解决方案以最低成本创造最高价值[EB/OL]. (2009-06-11)[2009-12-19]. <http://www.zdnet.com.cn/managesoft/2009/0611/1377952.shtml>.
- [2] 翟东锴,徐孟春,赵欣,等. 一种加强SSL协议安全性的解决方案[J]. 计算机应用与软件, 2005(22): 108-109.
- [3] 赵榛,鲍飞,刘克钧. 用Java Applet实现SSL的128位强加密[J]. 华中科技大学学报:自然科学版, 2004, 32(4): 74-76.
- [4] 金仑,谢俊元. Web环境下提高TLS性能的研究[J]. 计算机工程与应用, 2005(21): 136-138.
- [5] Mark J Cox, Ralf S Engelschall, Dr Stephen Henson steve, et al. About the openssl project [EB/OL]. (1999-10-11)[2009-10-11]. <http://openssl.org/about/>.
- [6] 杭州华三通信技术有限公司. SSL技术白皮书[EB/OL]. (2008-12-20)[2009-11-24]. http://www.h3c.com.cn/Products_Technology/Technology/Security_Encrypt/Other_technology/Technology_book/200812/622834_30003_0.htm#_Toc212542729.

(下转第188页)

导致了三次非线性项系数的估计值低于对应的实际设置值,且校正后流水线 ADC 的性能与图 3(b)中所示的理想水平还存在一定的差距。

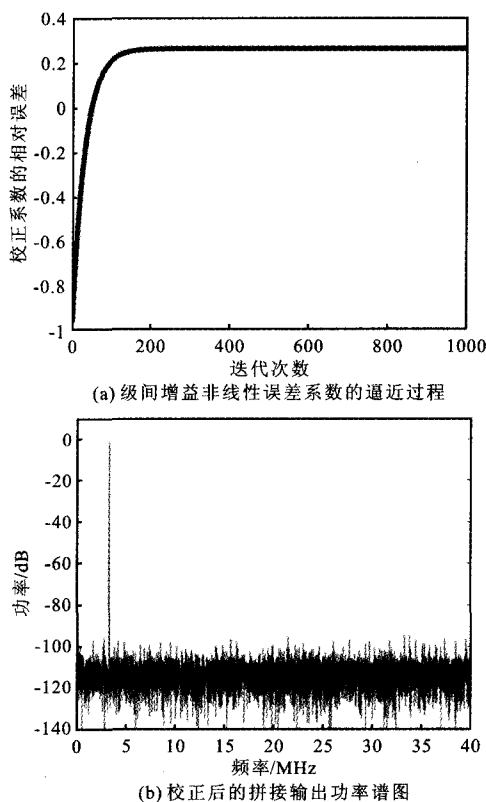


图 4 算法的收敛与校正

5 结束语

文中提出了一种针对流水线 ADC 级间增益非线性误差的后台补偿方法,给出了数字校正系统实现方案.该方法利用随机信号的二阶统计互相关特性,通过在第一级 DAC 输入端注入数字伪随机序列测量增益非线性系数,并使用此估计值在后台实现误差校正.此方法完全在数字域实现,可避免增加额外的比较器或信号发生电路,且不降低流水线 ADC 整体的量化精度.仿真实验表明,校正后的本底噪声功率和杂散性能均获得大幅改善,有效量化精度的提升超过 3 位,有助于高精度低功耗流水线 ADC 的设计与研制.

参考文献:

- [1] Scott Bardsley, Christopher Dillon, Ravi Kummaraguntla. A 100dB SFDR 80-MSPS 14Bit 0.35um BiCMOS pipeline ADC[J]. IEEE Journal of Solid-State Circuits, 2006, 41(9): 2144-2153.
- [2] Boris Murmann, Bernhard E. Boser. A 12bit 75MS/s pipelined ADC using open-loop residue amplification[J]. IEEE Journal of Solid-State Circuits, 2003, 38(12): 2040-2050.
- [3] Keane J P, Hurst P J, Lewis S H. Background inter-stage gain calibration technique for pipelined ADCs[J]. IEEE Transactions on Circuits and Systems I: Regular Papers, 2005, 52(1): 32-43.
- [4] 李天望,叶波,江金光. 1.8V 10 位 50Ms/s 低功耗流水线 ADC 的设计[J]. 微电子学与计算机, 2010, 27(4): 46-53.
- [5] 刘蒲霞,陆铁军,王宗民. 16 位流水线 ADC 系统级建模及仿真[J]. 微电子学与计算机, 2009, 26(12): 120-124.
- [6] Lewis S H, Gray P R. A pipelined 5-Msample/s 9bit analog-to-digital converter[J]. IEEE J. Solid-State Circuits, 1987, SSC-22(6): 954-961.
- [7] Galton I. Digital cancellation of D/A converter noise in pipelined A/D converters[J]. IEEE Trans. Circuits Syst. II, Analog Digit, 2000, 47(3): 185-196.
- [8] Albert O'Grady. Getting 14Bit performance from a 32-channel 14bit string DAC[R]. Analog Dialogue 37-02, 2003.
- [9] Ahmed M. Abdelatty Ali, Nagaraj K. Background calibration of operational amplifier gain error in pipelined A/D converters[J]. IEEE Transactions on Circuits and Systems-II: Analog and Digital Signal Processing, 2003, 50(8): 631-634.
- [10] Alma Delic-Ibukic. Continuous digital calibration of pipeline ADCs[J]. Electrical and Computer Engineering, 2000, 55(4): 1175-1185.

作者简介:

彭 隼 男, (1986-), 博士研究生. 研究方向为模数转换器(ADC)系统设计及其校正技术.

马 洪 男, (1966-), 教授, 博士生导师. 研究方向为非线性电路理论与技术.

(上接第 183 页)

- [7] Jordi Guitart, David Carrera, Vicenc Beltran, et al. Designing an overload control strategy for secure-commerce applications[J]. Computer Networks, 2007(51): 4492-4510.
- [8] 李娟, 毛宏燕, 马光思. SNMP v3 数据采集器 DCP 的研究与实现[J]. 微电子学与计算机, 2008, 25(12): 137-140.

作者简介:

张 雪 女, (1983-), 硕士研究生. 研究方向为软件理论.

马光思 男, (1949-), 教授. 研究方向为软件理论、信息安全.

毛宏燕 女, (1978-), 博士. 研究方向为软件理论、网络管理.