第18卷 第2期
1997年 6 月
郑州工业大学学报
Journal of Zhengzhou University of Technology
Vol. 18 No. 2.
Jun. 1997

外汇交易中心计算机异地同步下单信息安全系统简评

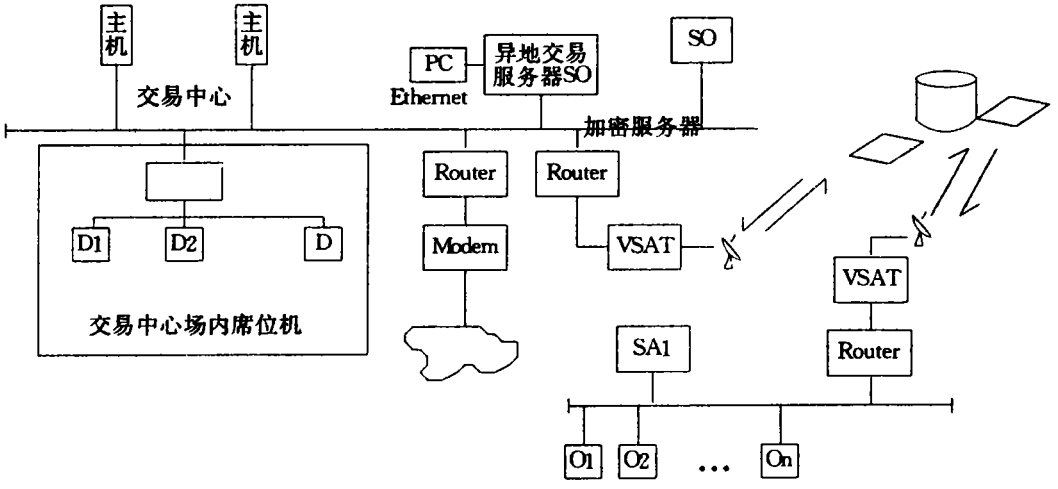
汤沛源 施鹏飞
（上海交通大学 上海 200030）

摘 要：本文针对外汇交易中心计算机异地同步下单系统的特点，分析了该系统中若干数据安全的问题，集中研究了为保证外汇交易业务数据信息的有效性、完整性和机密性，计算机外汇交易系统应提供的安全保密服务

关键词：外汇交易 信息安全 数据加密 密钥管理
中图分类号：TP315

1 引言

外汇交易中心计算机外汇交易业务包括本地交易和异地同步下单两个方面. 异地同步



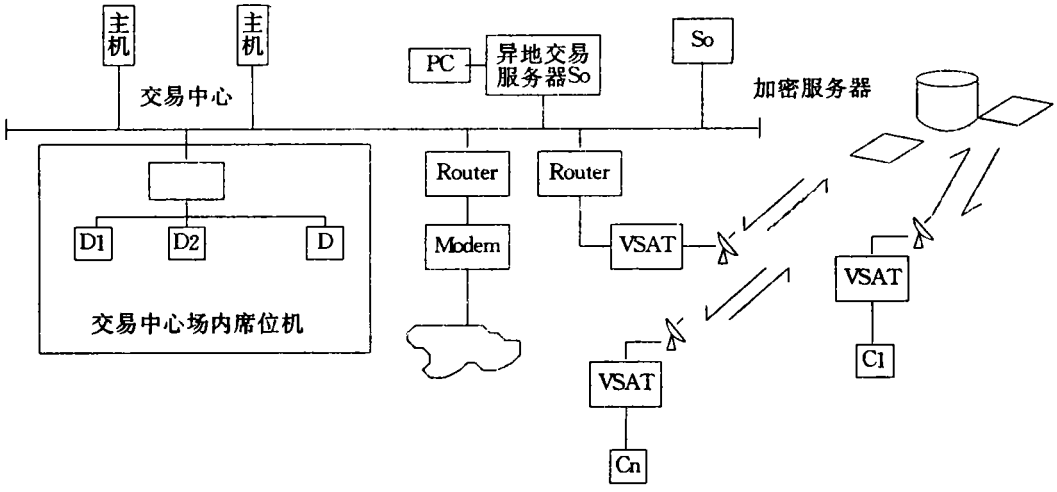
(1)主机；(2)交易中心异地交易服务器 *SO*，交易分中心服务器 *SA*1；
(3)交易中心内席位机 *Di*，交易分中心场内席位机 *Oi*

图1 异地同步下单系统结构

下单有两种形式：一种是由异地外汇交易分中心计算机局域网通过 *VSAT*、*DDN*、*PSTN*、*X*.25 等手段与外汇交易中心主场交易系统联成广域网组成，异地外汇交易分中心计算机局域网中的每一个终端是各家银行及其分支机构的交易员席位机，每个公司通过该席位进

收稿日期：1996－12－09

行外汇交易与主系统进行异地下单、撤单、查询等交易和事务性处理，计算机交易系统以双向竞价方式，根据价格优先、时间优先原则撮合成交，成交后的交易数据传送到结算中心进行结算，并通过卫星广播网实时反馈给各家银行及其分支机构，交易员可以通过计算机查询各种交易数据. 另一种方式是远程终端交易，就是把交易终端安装到各家银行及其分支机构的交易室里，让银行交易员可以坐在自己的办公室里进行交易，进行异地下单、撤单、查询等交易和事务性处理，计算机交易系统以双向竞价方式，根据价格优先、时间优先原则撮合成交，成交后的交易数据传送到结算中心进行结算，并通过卫星广播网实时反馈给各家银行及其分支机构，交易员可以通过计算机查询各种交易数据. 异地同步下单系统结构如图 1、2，异地外汇交易分中心如图 3. 由此可见，异地同步下单系统中处理的数据有许多机密的信息，它关系到商业秘密和不可估量的资金信息，已引起入侵者攻击的兴趣，有种种迹象表明有人正在试图侵入和窃取信息.



(1)主机 H;(2)交易中心异地交易服务器 SO;(3)远程交易终端 Cj

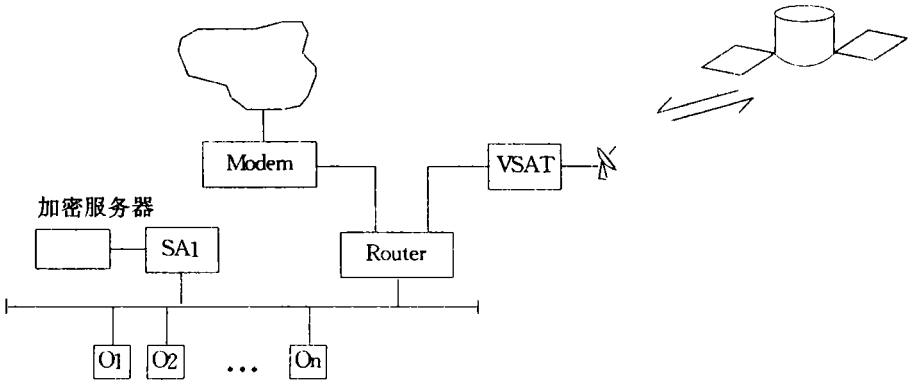
图 2　异地同步下单系统结构

2　异地同步下单系统中建立系统安全系统的必要性

2.1　计算机异地同步下单交易网络所面临的安全威胁

随着外汇交易业务发展的要求，各地相继或准备实现异地场外直接申报进行外汇交易. 在此之前，计算机外汇交易系统是一个封闭式网络. 封闭式网络只需考虑内部人员或授权用户的潜在泄露，而无需对付局外人. 异地交易开通之后，计算机外汇交易系统则是一个这样的网络，其敏感的部分是封闭的，但在控制下与外部网络连通保持一定的通信交换的网络，是一个部分封闭网或限制接入网(limited—access network). 异地同步下单通过 *VSAT*、*DDN*、*PSTN*、*X*.25 等手段的广域网利用远程服务器与外汇交易中心主场计算机交易系统连接起来，交易行情由行情发布服务器通过 *VSAT*、*X*.25、电话线、本地局域网等手段向外发布. 以明文形式传送的交易信息在途中所面临的安全威胁主要有以下几种：

1)线路窃听和信号分析:通过监视通信线路可以方便地分析各个异地交易厅的交易量、交易部位、资金流向等涉及商业机密的信息.



异地场内交易席位机·(1)异地交易分中心 $A1$ 的服务器 $SA1$;
(2)异地交易分中心 $A1$ 的场内席位机 $O1$、$O2$、On

图3 异地交易中心

2)网络非法连接:假冒用户进行非法交易或对交易信息进行非法篡改.

3)抵赖:合法连接用户抵赖曾发送过交易单.

2.2 计算机异地同步下单系统所需的安全业务

在系统网络中存储、交换、传递的金融业务信息,是涉及外汇交易中心、各家银行及其分支机构双方的经济利益的经济信息,任何不安全因素都会造成很大的经济损失.因此,针对以上系统所面临的安全威胁,要求提供以下安全服务:

1)连接鉴别:建立连接时鉴别合法连接.

2)交易信息内容的真实、有效、完整性:保证信息被完整地传递,即能验证收到的信息就是对方发出的信息.

3)交易信息内容的保密:对交换的信息进行加密,使第三方读不懂信息内容,防止将交易信息泄漏出去.有效防止窃听.

4)下单不可抵赖:接收的一方获得下单方下单的证据,以防止下单方以欺骗的手段否认下单或其内容的任何企图.

5)接收不可抵赖:下单的一方获得传送数据的证据,以防止收方以欺骗的手段否认收到下单或其内容的任何企图.

6)在交易不繁忙时采用发送无意义信息的方式有效防止信号分析.

7)存取控制:限制和控制对主机系统、应用和信息的访问.

2.3 计算机异地同步下单系统所需的安全服务的实现机制

连接鉴别和交易信息内容的真实、有效、完整性都可以由数字签名来实现.在数字签名中,一种密码运算产生一个密码效验和,该效验和可以验证信息内容的完整性.而连接鉴别则可以用合法用户给出其秘密密钥的信息来实现.

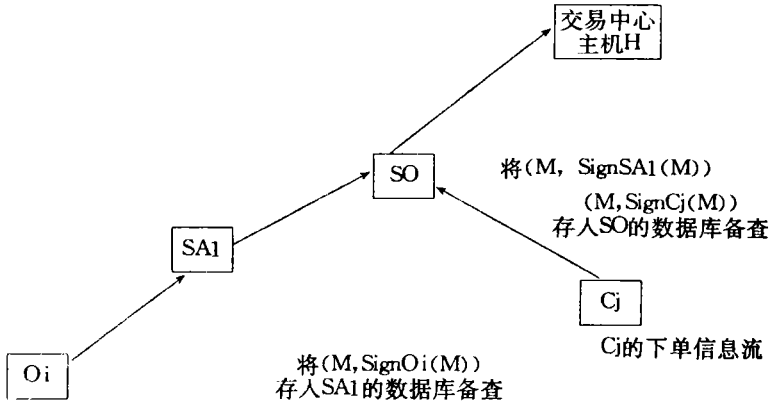
交易信息内容的保密可以通过对整个信息内容的加密来实现,加密采用传统密钥密码

体制.

下单不可抵赖要求发送方使用密码学的数字签名,并要求将信息及其密钥信息保存到再无争议为止. 接收不可抵赖由交易中心的数字签名而实现.

存取控制有别于上述各项安全服务,它并不是给信息本身提供安全保护,而是限制和控制对主机系统、应用和信息的访问.

异地同步下单交易下单信息流如图 4,设 $Oi(Cj)$ 的下单信息为 M,$Oi(Cj)$ 对 M 进行签名,并将 M 连同其签名 $SignOi(M)$ 一同加密送给 $A1$ 的服务器 $SA1$;$SA1$ 验证这一信息的合法性(先解密再验证数字签名),若合法则将其存入 $SA1$ 的数据库中,$A1$ 并在 M 上签名,连同 M 加密后送给外汇交易中心的异地交易服务器 SO,SO 将其解密再验证签名是否合法,若合法则将 M 连同 $A1$ 的签名一并存入 SO 的数据库中,并将 M 送交易中心的主机 H 进行撮合,Cj 对 M 进行签名,并将 M 连同其签名 $SignCj(M)$ 一同加密送给交易中心的异地交易服务器 SO,SO 将其解密再验证签名是否合法,如合法则将 M 连同 Cj 的签 名一并存入 SO 的数据库中,并将 M 送外汇交易中心的主机 H 进行撮合. 若 $Oi(Cj)$ 对撮合结果有异议,可逐步查出责任所在,以便各负其责.



其中:　M:　$Oi(Cj)$ 的(下单)交易信息;EA:　　表示 A 的加密处理;$SignA$:　表示 A 的签名处理

图 4　Oi 的下单信息流

2.4　计算机异地同步下单交易系统所需的密码体制

为达到系统的上述要求,必须使用密码技术并选择最佳的密码体制和加密算法. 密码学中,有传统密钥密码体制和公开密钥密码体制. 传统密钥密码体制中,加密密钥和解密密钥相同. 公开密钥密码体制中,只对解密密钥保密,而对加密密钥公开. 现有的传统密钥密码体制和公开密钥密码体制皆可用于对系统中的信息进行加密. 在商业领域,数据加密标准是应用广泛的传统密钥密码体制,RSA 是日益被接受的公开密钥密码体制. 公开密钥密码体制适于鉴别业务和密钥管理,传统密钥密码体制则在信息内容的保密及增加保密的复杂度和满足系统处理信息的能力上较为突出. 对系统进行加密保护,需要两种密码体制相互结合. 鉴别是用来验证远程实体身份的,传统的通行字方法无法满足分布式通信环境的要求,系统需要基于密码技术的鉴别.

3 计算机异地交易系统安全系统中的安全模块

3.1 密钥管理模块——异地交易服务器/异地交易分中心服务器端

异地交易服务器/异地交易分中心服务器的密钥则由公开密钥密码和传统密钥密码组成多层密钥结构. 公开密钥实现密钥的自动分发、身份识别、数字签名等安全功能,由二层*RSA*密钥组成. 传统密码的密钥将根据信息流的情况设置一至二层模式,最低层为会话密钥,不同报文使用不同密钥,会话密钥由安全卡自动生成并分发,对用户透明. *RSA*密钥由异地交易服务器/异地交易厅服务器内的安全卡在交易中心控制下生成,其生成和更新全部由多张智能卡控制,符合国际标准中密钥管理的多重控制及密钥分割的原则,安全卡内的密钥由其上的特殊物理安全措施加以保护,所有密码操作都在安全卡内完成. 密钥决不以明的行式出现在安全卡外. 这些措施使安全卡完全符合有关公钥密码和传统密码密钥管理的国际标准:*ISO*8732和*ISO*11666. 异地交易服务器/异地交易厅服务器采用高速加密器提供安全服务.

3.2 下单、撤单、查询安全模块——异地交易分中心服务器端/远程终端

该模块为下单提供数据加密、数字签名、数据完整性保护等功能,确保交易信息不被非法用户或合法用户所破译、伪造和修改,下单用户无法抵赖. 该模块还为撤单和查询过程提供身份识别、服务请求的加密和签名. 此模块是安全系统的最重要模块,参照加密签名和完整性验证的国际标准来开发. 该模块对用户是透明的,用户感觉不到他的存在.

3.3 下单、撤单、查询安全模块——异地交易服务器端

主场异地交易服务器为异地交易厅服务器端和远程终端交易的安全请求提供相应的安全服务,包括下单的加密、验证(有效性和完整性),对撤单和查询请求的身份识别及查询信息的加密.

3.4 访问控制模块

使内部及外部用户对系统的访问限制在已授权的活动和资源之内,并对每次访问都记录其签名. 其核心技术是安全高速的身份识别机制,采用*RSA*算法并基于*CCITTX*.509模式来做.

3.5 网络过滤器模块

由于操作系统和数据库本身的安全缺陷,仅仅靠加密有时难以防范对系统和数据库的高层渗透. 本交易系统的过滤器模块在服务器上和主机上皆可适用,但最后还应视整个网络结构而定. 外部进出信息都由加密服务器管理,包括对信息的加解密、身份识别等. 由于异地交易系统外部用户对系统的访问比较单纯,过滤器模块也相对简单,通过限定外部用户对系统的访问操作类型及外部用户只准访问自己的数据库等,可在加密服务器上过滤掉非法访问及操作.

3.6 审计和报告

对交易系统的任何攻击行为及企图都记录在案,并向系统监控人员报告,根据交易数据不完整的次数和连接不成功的次数或报警或记录.

4 结论

外汇交易日益依赖于计算机网络来实现交易、完成清算和交割，其面临的问题越来越多地集中在网络安全性上. 目前，实际的安全网络尚处在逐步建设之中.

参 考 文 献

1 W. Diffie and M. E. Hellman, New Directrions in Cryptography, IEEE Transactions on Information Theory, Vol. 22, No. 6, Nov 1977, pp. 644－654.

2 J. J. Tardo and K. Alagappan, SPX. Global authtication using pubic key certificates, in Proc. 1991 IEEE Comput. Soc. Symp. Res. Security Privacy, 1991, pp. 232－244.

3 Per Kaijser, Tom Parker and Denis Pinkas, SESAME. The solution to security for open Distributed systems, Comp. Comm, Vol. 17, No. 7, JULY, 1994.

4 ISO International Standard 7498－2: Open Systems Interconnection Reference Model －－ Part 2: Security Architecture, 1988.

5 J. E. Hershey, A. A. Hassan, and Rao Yarlagadala, Unconventional Cryptographic Keying Variable Management, IEEE Transaction or Communications, Vol. 43, No. 1, pp. 3－6, January 1995

6 C. Laferriere and R. Charland, Developing a System Security Architecture, Proceedings of the 5th Annual Canadian Computer Security Symposium, pp. 71－82, 1993.

Infomation Security of the Computer Foreign Trade system

Tang Peiyuan　　Shi Pengfei
(*Shanghai Jiaotong University　Shanghai* 200030)

Abstract This paper describes confidentiality intergrity and acailability of foreign trade information and analyzes problems about the confidentiality and security of data in the foreign trade system. The methods of ensuring the securities trade information security are given in this paper.

Keyword Foreign trade system　Information security　Date encryption　Key management