服务器知识手册（一）

狄登峰 主编

需要全本请访问 www.ertongbook.com

目　　录

电信解决方案 1
保障电信网络安全的五项措施 1
中间件 TUXEDO 在电信计费营帐系统中的应用 4
SunMicrosystems 公司电信行业解决方案 15
电信 CRM 建设难点与解决方案 23
北京市电信管理局应用方案 29
电信政务管理系统 31
信息产业部电信研究院的网络建设方案 36
企业 E 化方案 44
网上银行的交易流程及数据走向 44
构建安全的电子商务系统 53
电子商务安全技术分析 65
提高企业内网安全的十大策略 74
企业信息安全防护体系的构筑 78
搭建 B/S 模式的网络办公平台 81
轻松构建企业园区网 90
构建铜墙铁壁式的企业网络 100
电子商务平台技术：应用服务器 104
现代企业数据仓库系统建设 116
社区网络技术选型方案分析 122

电信解决方案

保障电信网络安全的五项措施

我们面临的威胁

在电信行业的网络业务系统中，经过多年建设安全防护已经初具规模。随着网络病毒和黑客的不断升级，现今的电信行业的安全体系已经不能满足以下的安全需求：

*网络业务系统大都采用 TCP/IP 作为主要的网络通讯协议，主要服务器为 UNIX 操作系统。TCP/IP 和 UNIX 都是以开放性著称的，系统之间易于互联和共享信息的设计思路贯穿于系统的方方面面，对访问控制、用户验证授权、实时和事后审计等只实现了基本安全控制功能，存在许多安全漏洞。

*电信的防火墙系统侧重在对通讯的源、目的地址和端口进行限制，鉴于当前 IT 系统安全性的严重状况，黑客还是可以从许多地方访问关键服务器，数据包中很可能包含入侵攻击代码，并没有形成一套完整的防护体系。

*黑客入侵过程一般包括利用各种资源踩点、对最弱系统的攻击、攻击深入、获取关键资源以及撤退等几个步骤。因此，针对每一个黑客攻击的步骤，都需要制定相应的防范措施；而且其中具有技术部分的内容，更加重要的是管理方面的，也就是安全策略的制定和实行。

*以前并没有对于项目范围内的重要信息数据(比

如，技术文档、源程序、企业运行数据、电子邮件、管理文档商业文档)的安全保护框架，以及承载这些数据的系统的安全保护框架进行全面的设计、评估。

显而易见，如果上述的安全需求得不到满足，由于信息安全威胁造成网络阻塞、应用中断(包括计费系统在内的关键应用)，数据失窃都会对电信运营商带来严重的经济和形象上的损失。

解决之道

针对特殊信息安全当前的形势，电信企业应从主动防护与被动监控、全面防护与重点防护相结合的角度出发，搭建具有主动防御能力的深层防御安全体系。

计策一：发散性的技术方案设计思路

在采用电信行业安全解决方案时，首先需要对关键资源进行定位，然后以关键资源为基点，按照发散性的思路进行安全分析和保护，并将方案的目的确定为电信网络系统建立一个统一规范的安全系统，使其具有统一的业务处理和管理流程、统一的接口、统一的协议以及统一的数据格式的规范。

计策二：网络层安全解决方案

网络层安全主要是基于以下几点考虑：控制不同的访问者对网络和设备的访问；划分并隔离不同安全域；防止内部访问者对无权访问区域的访问和误操作。

我们可以按照网络区域安全级别把网络划分成两大安全区域，即关键服务器区域和外部接入网络区域，在这两大区域之间需要进行安全隔离。在关键服务器区域内部，也同样需要按照安全级别的不同进行安全隔离。与此同时，还需要结合网络系统的安全防护与监控需要与实际应用环境，工作业务流程以及机构组织形式与机

构进行了密切结合，从而在系统中建立一个完善的安全体系，包括企业级的网络实时监控、入侵检测和防御、系统访问控制、网络入侵行为取证等，形成综合的和全面的端到端安全管理解决方案，从而大大加强系统的总体可控性。

计策三：网络层方案配置

在电信网络系统核心网段应该利用一台专用的安全工作站安装入侵检测(如，冠群金辰公司的干将/莫邪入侵检测系统)产品，将工作站直接联接到主干交换机的监控端口(SPANPort)，用以监控局域网内各网段间的数据包，并可在关键网段内配置含多个网卡并分别联接到多个子网的入侵检测工作站进行相应的监测。

计策四：主机、操作系统、数据库配置方案

由于电信行业的网络系统基于 Intranet 体系结构，兼呈局域网和广域网的特性，是一个充分利用了 Intranet 技术、范围覆盖广的分布式计算机网络，它面临的安全性威胁来自于方方面面。每一个需要保护的关键服务器上都应部署核心防护产品进行防范，并在中央安全管理平台上部署中央管理控制台，对全部的核心防护产品进行中央管理。

计策五：系统、数据库漏洞扫描

系统和数据库的漏洞扫描对电信行业这样的大型网络而言，具有重要的意义。充分利用已有的扫描工具完成这方面的工作，可免去专门购买其他的系统/数据库漏洞扫描工具。

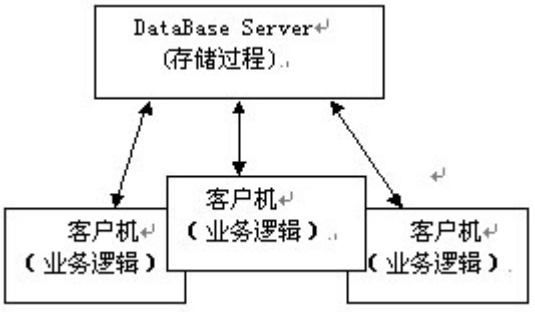
需要全本请访问 www.ertongbook.com

中间件 TUXEDO 在电信计费营帐系统中的应用

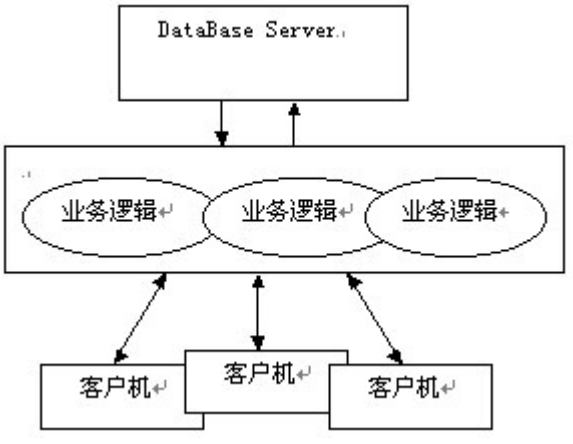
一、前言

传统的管理信息系统（MIS）开发采用客户/服务器（CLIENT/SERVER）模式，从体系结构上讲，一般采用两层结构，即应用（客户层）和数据服务层。客户端（应用层）提供用户操作界面，接受数据输入，向数据服务层发出数据请求并接受返回的数据结果，根据业务逻辑进行相关的运算，向客户显示相关信息；数据服务层接受客户端的数据请求，做相关数据处理，并将数据集或数据处理返回客户端。

在现在一些系统中，由于客户机较多，访问量和数据传输量都较大。为解决相应的瓶颈以及出于安全因素等方面的考虑，往往采用中间件组成三层（多层）结构应用体系（在两层结构应用开发中，常常会编写一些存储过程放在数据库端以供客户端调用，这已经有点类似三层结构）。三层结构应用体系将业务逻辑放在应用服务层，应用服务层接受客户机的业务请求，根据请求访问数据库，做相关处理，将处理结果返回客户机。应用服务层从物理上和逻辑上都可以独立出来，客户机（层）不直接访问数据库服务器（层），而是访问应用服务器（层）。客户层发出的不再是数据请求而是业务（事务）请求。两层与三层结构应用体系的比较如图 1 所示。



a、两层结构



b、三层结构

图 1 两层与三层结构应用体系比较

二、三层应用体系结构的优点

两层体系结构在实际应用中已暴露出一些问题。如：客户机直接（或通过存储过程）访问数据库，所有客户机均访问数据库，不利于安全控制，难以防止黑客的恶意攻击。同时，网络流量很大，易形成网络瓶颈。还会造成数据库访问瓶颈及数据库连接数过多，影响数据库

的响应速度，降低系统性能。另外，两层应用体系结构还有维护、扩展方面的问题。相比之下，三层应用体系结构显示以下优点。

进程管理：通过对服务进程的管理，使得在正常情况下，能用尽量少的服务进程处理尽量多的请求，减少进程的启动/终止次数。在峰值情况下，控制服务进程的总数，使得服务器在设定的负载下工作，不被压跨。总之，通过中间件对服务进程的有效管理，可以使系统在额定的功率下稳定工作，当请求服务的数量超过了服务器的处理速度时，中间件会把请求排队进行缓冲。

保持和复用数据库连接：服务进程访问数据库都要和数据库建立连接，如打开和关闭数据库等。中间件通过采用长驻服务进程的手段，使得与数据库的连接被保持和复用，从而大大减少与数据库连接的次数和时间。

支持交易优先级：通过对交易优先级的支持，保证优先级高的交易能尽快得到响应。

2.1 优化了系统结构

将系统分为三层（或多层），业务逻辑放在应用服务层，软件的维护集中在应用服务层，客户端的维护就相对简单多了，有利于软件维护及系统管理。

2.2 提高了应用系统的安全性

将客户端与数据库隔离起来，客户端无权限直接访问数据库，有利于安全管理，可有效防止恶意攻击。还可以利用中间件的安全管理特性进一步加强权限控制管理。

2.3 便于业务（事务）级权限管理

三层结构应用中可划分出业务（事务）级权限，一种业务一个服务程序（Service），利用中间件的安全管

理对其进行访问控制。数据库的权限只分为对表（或表中的列）的插入（Insert）、删除（Delete）、修改（Update）、查询（Select）权限，它属于数据库表级的权限，而实际应用中往往以业务（事务）为主线，也就要求对业务（事务）实现权限控制，三层结构应用可以方便地对客户端实现事务权限管理控制。业务（事务）级权限控制的引入丰富和方便了权限控制与管理，实际上两层应用体系结构中可通过存储过程类似地实现业务（事务）级权限控制，但采用三层应用体系结构实现业务（事务）级权限控制更加灵活、方便、实效。

2.4 卓越的扩展能力

若要提高系统性能、处理速度，可增加应用服务器，分担一部分应用服务工作即可，而原来的应用服务器几乎可以不动。

2.5 减少网络数据流量和提高数据库响应速度

两层应用体系结构中客户机直接（或通过存储过程）访问数据库，会造成数据库访问瓶颈及网络瓶颈，从而降低了整个系统的性能。

三层应用体系结构中，应用服务层的引入有效地解决了网络瓶颈和数据库连接数过多引起数据库性能下降的问题。应用服务层往往有多台服务器，可有效地解决客户机访问服务层瓶颈。应用服务器与数据库服务器（物理距离很近）可方便地采用宽带网连接，不会产生与数据库服务层网络瓶颈。

2.6 保护现有投资

原有性能较差的设备（微机、小型机）均可发挥作用。大量复杂计算的工作均可放在应用服务器上（可由多台小型机组成），对硬件要求不是很高，客户机只做用

户输入与显示，原有微机即可。采用三层应用体系结构后整个系统性能有很大地提高，也不会造成原有系统资源浪费。

2.7 提高系统性能

三层应用体系结构能更好地调整应用体系，还可利用中间件的特点来选择路由、平衡负载，提高整个系统的性能。

总的来说，三层应用体系结构使应用系统的性能、安全性、扩展性有了很大的提高，也方便了系统的维护和管理。

三、中间件 TUXEDO 的特点

要组成三层应用体系结构少不了要求采用中间件。中间件可以说是开发服务程序和管理这些服务程序运行的工具，是三层体系结构中一个非常重要的部分，它直接关系到整个应用系统的好坏，甚至成功与失败。

现在市场上的中间件很多，有 TUXEDO、CICS，有基于 CORBA 的 VisiBroker、M3，还有面向对象的 JavaBean，中间件的选用很大程度上要看其成熟度。电信计费营帐系统是直接面向用户的应用系统，只许成功，不许失败。浙江联通公司选用中间件 TUXEDO，也是基于成熟度及性能/价格比等方面的考虑。

TUXEDO 是 BEA 公司的非常成熟的产品，占有很大市场份额，它有以下特点：

（1）支持全局事务管理，支持 X/Open 规范，支持全局的两阶段提交。

（2）分布式应用管理，支持异构环境下的分布应用（如同一应用中有不同的数据库，多个数据源）。

（3）平衡负载。有多台机器做应用服务器时，系统

可自动根据每个机器的负载情况决定服务程序在负载小的那一台机器上执行。

（4）进程管理。系统根据需要（客户端请求量）自动增加或减少每个 Service 的进程数（1 个 Service 可启动 n 个相同的进程）。某个 Service 忙，则相应地增加（启动）其进程数；某个 Service 闲，则相应地减少（关闭）其进程数，从而减少该 Service 占用的系统资源（如：内存、数据库连接数等），使整个系统的 Service 最优化运行。

（5）优先级管理。可将 Service 根据优先级的不同赋权值，系统根据优先级权值将客户请求（Service）排队管理。

（6）路由管理。有多台机器做应用服务器时，用户可设定同一种事务（根据申请包中 FML 的某一个域）在不同的机器上执行。

（7）权限控制、安全管理。包括两个方面：·服务端控制，可限制用户对应用程序的启动、关闭，限制用户在应用中建立服务程序。·限制客户端对应用程序的访问。可由专门的 Service 做安全验证。

（8）丰富的通信方式。有同步调用、异步调用、管道通信、会话、广播、通知、队列、发布订阅等通信方式，能很好地满足应用开发的要求。

（9）可 MP 方式工作，多台应用服务器互相备份，实现其高可用性。

四、中间件在浙江联通计费营业帐务系统营业子系统中的实现

浙江联通计费营帐系统三层体系中客户端程序用 C++BUILDER，服务端（应用服务层）程序用 Pro*c 开

需要全本请访问 www.ertongbook.com

发，中间件采用 Bea 公司的 TUXEDO，数据库采用 ORACLE8。其体系结构如图 2 所示。

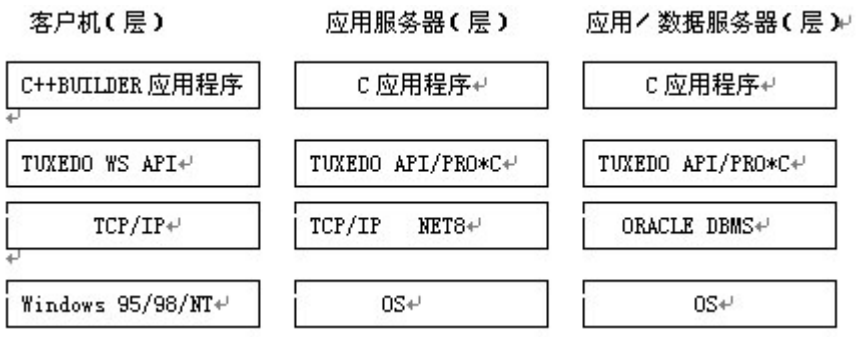


图 2 浙江联通计费营业帐务系统三层体系结构图

三层体系中客户端与服务端的通信是由 TUXEDO 的 API 函数实现，客户端由函数 Tpinit 与服务器建立连接，由函数 Tpcall 申请 Service 服务，再由相关的 TUXEDO 函数对数据解包。

数据传输采用 TUXEDO 提供的非常灵活的 FML 方式实现客户端与服务端的数据交换。

目前，浙江联通计费营帐系统中所有营业受理模块、除详细话单以外的查询模块均采用三层结构来实现。

营业模块包括开户、话费收缴、改号、换/补卡、套餐变更以及营业数据的查询等，营业模块是用得相当频繁得模块（有 300 台客户机要同时实现 25 种服务），在将来高峰时将达到 500 多台，所以在本系统中首先采用三层结构来实现前台各种业务受理工作。

4.1 营业受理系统服务端

在营业受理子系统中，根据前台业务的分类，我们将服务端的服务（SERVICE）分成三类：

1．公共服务函数：提供诸如操作员登录、操作员权限控制、两台清方式的第一次提交确认、欠费校验、黑名单校验等。

2．公共查询服务函数：应用 ORACLE 的动态 SQL 功能，完成客户端发出的各种查询请求。

3．各业务提交函数：完成客户端各个业务（开户、改号……）的提交确认。

根据这三类 SERVICE 的不同特点，需要三种不同的配置要求。

服务程序之所以采用一个公用模块（程序），是因为业务受理涉及面广，几乎涉及所有数据库表，若每一种业务都做一个服务程序，则要做很多个服务程序。程序开发和维护量很大，系统扩展、管理不方便。且运行性能也受到较大的影响，因为每个服务程序至少启动一个进程，而有些进程由于业务上的原因会很少利用（运用）却占用了系统资源（如：内存、数据库连接数等）。

4.2 营业受理系统客户端

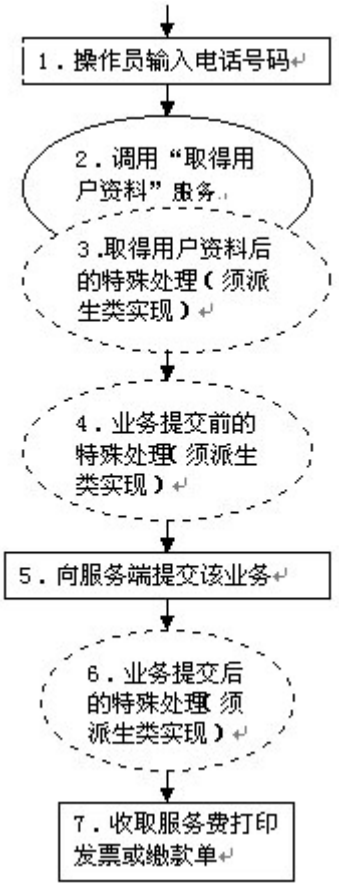
客户端的开发主要有两个问题需要解决：

1．如何实现营业前台庞杂多样的各种业务受理？

2．如何既简单又统一的实现界面中控件与 FML 缓冲、FML 缓冲与服务端的数据的一致和数据交换？

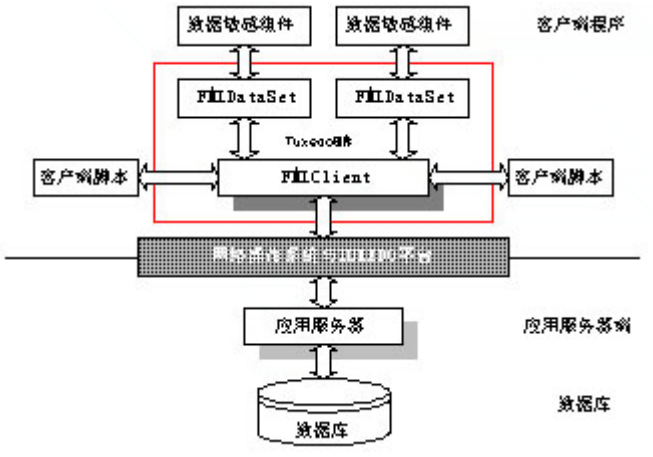
对于第一个问题，我们应用面向对象技术，定义了一个 C++Builder 虚类 SaleManBase，SaleManBase 类抽象出了一般业务的流程，同时给继承实现类又留有不同业务的实现接口。

SaleManBase 的简单流程如下图：



从上图可以看出，SaleManBase **类抽象出了一个典型业务的流程，同时它又给每个具体流程留有灵活的接口实现，如上图的第** 3、4、6 **步骤。**

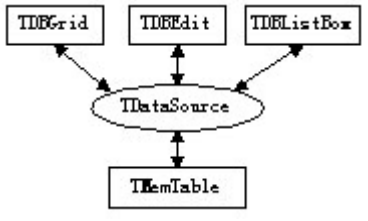
应用 SaleManBase **类，一般简单的业务（例如：改号、换卡等）只须在派生类中重载** 1 **至** 2 **个方法，添加** 10 **几行代码即可完成一个前台业务界面的编程。极大减轻了前台编程人员的负担，同时也简化了前台程序的管理和标准化。**



Tuxedo 组件在客户端与应用服务器间的关系

对于第二个问题，我们主要通过两个组件来解决；一个是 FMLClient 组件，用来实现前台界面与 TUXEDO 的 FML 缓冲之间的数据交换。一个是 MemTable 组件，用来实现界面上的数据敏感组件和 FMLClient 组件之间的接口。

如下图所示：



MemTable 组件与其他数据访问组件间的关系

这样，通过这两个组件，编程人员就可以很容易的实现前台界面控件与 TUXEDO 服务端的通讯了。

从上图可以看出 MemTable 组件在系统中与界面数据敏感控件之间的关系，在定义 MemTable 中的字段名字时，我们人为规定了其与 FML 缓存中字段名一致。同时，我们又在 FMLClient 中定义了一组从 MemTable 中根据字段名取数据，和向 MemTable 中设置数据的方法；通过 FMLClient 提供的这一组方法，编程人员可以非常方便的保持界面控件和服务端数据的一致。

4.3 营业受理系统得安全措施

4.3.1 应用级

客户端程序控制：从客户端进行业务受理必须输入密码（由用户设定）才能办理相关业务，如：用户资料更改、特服变更、改号、换卡等。

服务端程序控制：客户端传过来的 SQL 语句必须是合理有序的。服务程序（Service）

菜单访问控制：

每个操作员的菜单都是由管理员授予的，因此，操作员对于未授权的菜单是看不到和不能操作的。

4.3.2 系统级

数据库控制：用户帐号被授权对脚色（ROLE）进行存取，操作元的帐号不是数据库系统实际帐号而是应用程序帐号。

TUXEDO 控制：利用 TUXEDO 特性对客户端访问服务程序（Service）的权限进行控制，由专门的 Service 控制。

五、展望

大型数据库应用系统开发采用中间件已成为趋势，出于系统之间的良好接口和开放性考虑，中间件应选用基于面向对象的中间件，现在中间件面向对象的标准有：

CORBA、COM、JavaBean等，其中CORBA（CommonObjectRequestBrokerArchitecture）已为大多数厂商所接受。基于公用的面向对象标准的中间件，可简化异构环境下分布处理的复杂程度。对于多种分布式软件（如交易管理、负载平衡、Web主页、传统计算等），中间件减少了应用软件开发商的负担，使他们可以在跨越客户挑选的硬件、操作系统、网络、数据库管理系统和对象模型上建造分布式应用软件。

目前基于CORBA开发出来的中间件对大多数企业而言过于复杂，不易使用。但随着基于CORBA的中间件技术的进一步发展与成熟，三层体系结构的应用系统采用基于CORBA的中间件将成为一种趋势。

对于浙江联通计费营业帐务系统而言，将来要面向基于CORBA的应用也是较容易的，因为TUXEDO应用向基于CORBA的M3应用迁移是非常方便的。

SunMicrosystems公司电信行业解决方案

在1998年通讯装置市场价值达1100亿美元（NATA通讯市场评论）；预计将来个别部件的年增长率将达15－35％。但是这样的好消息却面临一个由于世界范围内通讯市场的违规操作和私有化所引起的竞争空前的环境。

这种竞争日渐剧烈的环境要求服务提供商必须以更快的速度来提供新的更加先进并且用户界面友好的服务，而同时不会使传统的通讯服务质量打折扣。这些需要促使许多通讯服务提供商选择基于互联网协议（IP）的网络来作为他们许多有附加值的服务的基础。这样的

需要全本请访问 www.ertongbook.com